

---

# **Samsung Electronics Co., Ltd. Samsung Galaxy Note 7 on Android 6 (MDFPP20) Security Target**

Version 0.3  
2016/10/03

---

*Prepared for:*

**Samsung Electronics Co., Ltd.**

416 Maetan-3dong, Yeongtong-gu, Suwon-si, Gyeonggi-do, 443-742 Korea

*Prepared By:*



[www.gossamersec.com](http://www.gossamersec.com)

<b>1. SECURITY TARGET INTRODUCTION</b>	<b>4</b>
1.1 SECURITY TARGET REFERENCE	5
1.2 TOE REFERENCE	5
1.3 TOE OVERVIEW	5
1.4 TOE DESCRIPTION	5
1.4.1 TOE Architecture	6
1.4.2 TOE Documentation	9
<b>2. CONFORMANCE CLAIMS</b>	<b>10</b>
2.1 CONFORMANCE RATIONALE	10
<b>3. SECURITY OBJECTIVES</b>	<b>11</b>
3.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	11
<b>4. EXTENDED COMPONENTS DEFINITION</b>	<b>12</b>
<b>5. SECURITY REQUIREMENTS</b>	<b>14</b>
5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS	14
5.1.1 Security audit (FAU)	15
5.1.2 Cryptographic support (FCS)	16
5.1.3 User data protection (FDP)	22
5.1.4 Identification and authentication (FIA)	23
5.1.5 Security management (FMT)	26
5.1.6 Protection of the TSF (FPT)	34
5.1.7 TOE access (FTA)	37
5.1.8 Trusted path/channels (FTP)	37
5.2 TOE SECURITY ASSURANCE REQUIREMENTS	37
5.2.1 Development (ADV)	38
5.2.2 Guidance documents (AGD)	38
5.2.3 Life-cycle support (ALC)	39
5.2.4 Tests (ATE)	40
5.2.5 Vulnerability assessment (AVA)	40
<b>6. TOE SUMMARY SPECIFICATION</b>	<b>42</b>
6.1 CRYPTOGRAPHIC SUPPORT	42
6.2 USER DATA PROTECTION	47
6.3 IDENTIFICATION AND AUTHENTICATION	56
6.4 SECURITY MANAGEMENT	58
6.5 PROTECTION OF THE TSF	58
6.6 TOE ACCESS	61
6.7 TRUSTED PATH/CHANNELS	62
6.8 KNOX WORKSPACE CONTAINER FUNCTIONALITY	62
6.9 SECURITY AUDIT	63
<b>7. TSF INVENTORY</b>	<b>65</b>

## LIST OF TABLES

Table 1 TOE Security Functional Components	15
Table 2 Security Management Functions	27
Table 3 EAL 1 augmented with ALC_TSU_EXT.1 Assurance Components	38
Table 4 BoringSSL Cryptographic Algorithms	44
Table 5 Samsung Kernel Cryptographic Algorithms	44
Table 6 SCrypto TEE Cryptographic Algorithms	44

---

<b>Table 7 Chipset Hardware Cryptographic Algorithms</b> .....	45
<b>Table 8 Permissions</b> .....	55
<b>Table 9 Power-up Cryptographic Algorithm Self-Tests</b> .....	60
<b>Table 10 Audited Events</b> .....	64

## 1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE consists of the Samsung Galaxy Note 7 on Android 6 provided by Samsung Electronics Co., Ltd.. The TOE is being evaluated as a Mobile Device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

### Acronyms and Terminology

<b>AA</b>	Assurance Activity
<b>CC</b>	Common Criteria
<b>CCEVS</b>	Common Criteria Evaluation and Validation Scheme
<b>EAR</b>	Entropy Analysis Report
<b>GUI</b>	Graphical User Interface
<b>NFC</b>	Near Field Communication
<b>PCL</b>	Product Compliant List
<b>PP</b>	Protection Profile
<b>SAR</b>	Security Assurance Requirement
<b>SE</b>	Secure Element
<b>SFR</b>	Security Functional Requirement
<b>SOF</b>	Strength of Function
<b>ST</b>	Security Target
<b>TEE</b>	Trusted Execution Environment (TrustZone)
<b>TOE</b>	Target of Evaluation
<b>U.S.</b>	United States
<b>VR</b>	Validation Report

### Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP\_ACC.1(1) and FDP\_ACC.1(2) indicate that the ST includes two iterations of the FDP\_ACC.1 requirement, (1) and (2).
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [*selected-assignment*]).

- Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
- Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "... **all** objects ..." or "... ~~some~~ **big** things ...").
- The MDFPP uses an additional convention – the ‘case’ – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

## 1.1 Security Target Reference

**ST Title** – Samsung Electronics Co., Ltd. Samsung Galaxy Note 7 on Android 6 (MDFPP20) Security Target

**ST Version** – Version 0.3

**ST Date** – 2016/10/03

## 1.2 TOE Reference

**TOE Identification** – Samsung Electronics Co., Ltd. Samsung Galaxy Note 7 on Android 6.

**TOE Developer** – Samsung Electronics Co., Ltd.

**Evaluation Sponsor** – Samsung Electronics Co., Ltd.

## 1.3 TOE Overview

The Target of Evaluation (TOE) is the Samsung Galaxy Note 7 on Android 6.

## 1.4 TOE Description

The TOE is a mobile device based on Android 6.0.1 with modifications made to increase the level of security provided to end users and enterprises. The TOE is intended to be used as part of an enterprise messaging solution providing mobile staff with enterprise connectivity.

The TOE includes a Common Criteria mode (or “CC mode”) that an administrator can invoke through the use of an MDM or through a dedicated administrative application (see the Guidance for instructions to obtain the application). The TOE must meet the following prerequisites in order for an administrator to transition the TOE to CC mode.

- Require a screen lock password (swipe, PIN, pattern, or facial recognition screen locks are not allowed).
- The maximum password failure retry policy should be less than or equal to ten.
- Device encryption must be enabled or a screen lock password required to decrypt data on boot.
- Revocation checking must be enabled.
- External storage must be encrypted.
- Password recovery policy must not be enabled.
- Password history length must not be set.

When CC mode has been enabled, the TOE behaves as follows.

- The TOE sets the system wide Android CC mode property to “Enabled” if all the prerequisites have been met.
- The TOE performs power-on self-tests.

- The TOE performs secure boot integrity checking of the kernel and key system executables.
- The TOE prevents loading of custom firmware/kernels and requires all updates occur through FOTA (Samsung’s Firmware Over The Air firmware update method)
- The TOE uses CAVP approved cryptographic ciphers when joining and communicating with wireless networks.
- The TOE utilizes CAVP approved cryptographic ciphers for TLS.
- The TOE ensures FOTA updates utilize 2048-bit PKCS #1 RSA-PSS formatted signatures (with SHA-512 hashing).

The TOE includes a containerization capability, KNOX Workspace, which is part of the KNOX platform. This container provides a way to segment applications and data into two separate areas on the device, such as a personal area and a work area, each with its own separate apps, data and security policies. For this effort the TOE was evaluated both without and with a KNOX Workspace container created (and to create a KNOX Workspace container, one must purchase an additional license). Thus, the evaluation includes several KNOX-specific claims that apply to a KNOX Workspace container when created.

There are different models of the TOE, the Samsung Galaxy Note 7 on Android 6, and these models differ in their internal components (as described in the table below).

The model numbers of the mobile device used during evaluation testing are as follows:

Device Name	Model Number	Chipset/CPU	Build Arch/ISA	Android Version	Kernel Version	Build Number
Galaxy Note 7	SM-N930F	Exynos 8890	A64	6.0.1	3.18.14	MMB29K
Galaxy Note 7	SM-N930V	Qualcomm MSM8996	A64	6.0.1	3.18.20	MMB29M

The devices include a final letter or number at the end of the name that denotes that the device is for a specific carrier (for example, V = Verizon Wireless and A = AT&T, which were used during the evaluation). The following list of letters/numbers denotes the specific models which may be validated:

- V – Verizon Wireless,
- P - Sprint,
- R4 – US Cellular,
- S – SK Telecom,
- L – LG Uplus,
- K - KT, Korea Telecom
- A – AT&T,
- T – T-Mobile,
- C/F/I - International

For each device there are specific models which are validated. This table lists the specific carrier models which have the validated configuration.

Device Name	Base Model Number	Carrier Models
Galaxy Note 7 (Qualcomm)	SM-N930	T, P, R4, V, A
Galaxy Note 7 (System LSI)	SM-N930	F, S, K, L

Where “None” is listed that means a device without a carrier model designation suffix can also be placed into the validated configuration.

### 1.4.1 TOE Architecture

The TOE combines with a Mobile Device Management solution that enables the enterprise to watch, control and administer all deployed mobile devices, across multiple mobile service providers as well as facilitate secure

communications through a VPN. This partnership provides a secure mobile environment that can be managed and controlled by the environment and reduce the risks that can be introduced through a Bring-Your-Own-Device (BYOD) model.

Data on the TOE is protected through the implementation of Samsung On-Device Encryption (ODE) which utilizes a CAVP certified cryptographic algorithms to encrypt device storage. This functionality is combined with a number of on-device policies including local wipe, remote wipe, password complexity, automatic lock and privileged access to security configurations to prevent unauthorized access to the device and stored data.

The Samsung Enterprise Software Development Kit (SDK) builds on top of the existing Android security model by expanding the current set of security configuration of options to more than 600 configurable policies and including additional security functionality such as application whitelisting and blacklisting.

KNOX provides the ability to enhance the BYOD model by creating a separate container for the Enterprise. Within this container, the Enterprise can provision separate applications and ensure they are kept separate from anything the user may do outside the KNOX Workspace container. The Enterprise can use policy controls to manage the device as a whole or the KNOX Workspace container specifically, as needed by the organization.

---

#### **1.4.1.1 Physical Boundaries**

The TOE is a multi-user mobile device based on Android (6.0.1) that incorporates the Samsung Enterprise SDK. The TOE does not include the user applications that run on top of the operating system, but does include controls that limit application behavior. When the TOE is used within an enterprise environment, the enterprise can manage the configuration of the mobile device through a compliant device management solution.

The TOE communicates and interacts with 802.11-2012 Access Points and mobile data networks to establish network connectivity, and the through that connectivity interacts with MDM servers that allow administrative control of the TOE.

---

#### **1.4.1.2 Logical Boundaries**

This section summarizes the security functions provided by the Samsung Galaxy Note 7 on Android 6:

- Security Audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

---

##### **1.4.1.2.1 Security Audit**

The TOE is designed to be able to generate logs for a range of security relevant events. The TOE stores the logs locally so they can be accessed by an administrator or they can be exported to an MDM.

---

##### **1.4.1.2.2 Cryptographic support**

The TOE includes a cryptographic library with CAVP certified algorithms for a wide range of cryptographic functions including: asymmetric key generation and establishment, symmetric key generation,

encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key and protected data destruction. These primitive cryptographic functions are used to implement security protocols such as TLS, IPsec, and HTTPS and also to encrypt the media (including the generation and protection of data and key encryption keys) used by the TOE. Many of these cryptographic functions are also accessible as services to applications running on the TOE.

---

#### **1.4.1.2.3 User data protection**

---

The TOE is designed to control access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE is designed to protect user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected. The functionality provided by a KNOX Workspace container enhances the security of user data by providing an additional layer of separation between apps and data while the device is in use.

---

#### **1.4.1.2.4 Identification and authentication**

---

The TOE supports a number of features related to identification and authentication. From a user perspective, except for making phone calls to an emergency number, a password (i.e., Password Authentication Factor) must be correctly entered to unlock the TOE. Also, even when the TOE is unlocked the password must be re-entered to change the password. Passwords are obscured when entered so they cannot be read from the TOE's display and the frequency of entering passwords is limited and when a configured number of failures occurs, the TOE will be wiped to protect its contents. Passwords can be constructed using upper and lower cases characters, numbers, and special characters and passwords between 4 and 16 characters are supported.

The TOE can also serve as an 802.1X supplicant and can use X509v3 and validate certificates for EAP-TLS, TLS and IPsec exchanges.

---

#### **1.4.1.2.5 Security management**

---

The TOE provides all the interfaces necessary to manage the security functions identified throughout this Security Target as well as other functions commonly found in mobile devices. Many of the available functions are available to users of the TOE while many are restricted to administrators operating through a Mobile Device Management solution once the TOE has been enrolled. Once the TOE has been enrolled and then un-enrolled, it removes all MDM policies and disables CC mode.

---

#### **1.4.1.2.6 Protection of the TSF**

---

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as cryptographic keys so that they are not accessible or exportable. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). It enforces read, write, and execute memory page protections, uses address space layout randomization, and stack-based buffer overflow protections to minimize the potential to exploit application flaws. It is also designed to protect itself from modification by applications as well as to isolate the address spaces of applications from one another to protect those applications.

The TOE includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any of the self-tests fail, the TOE will not go into an operational mode. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation.

---

#### **1.4.1.2.7 TOE access**

---

The TOE can be locked, obscuring its display, by the user or after a configured interval of inactivity. The TOE also has the capability to display an advisory message (banner) when users unlock the TOE for use.



---

The TOE is also able to attempt to connect to wireless networks as configured.

---

#### **1.4.1.2.8 Trusted path/channels**

---

The TOE supports the use of 802.11-2012, 802.1X, EAP-TLS, TLS and IPsec to secure communications channels between itself and other trusted network devices.

---

#### **1.4.2 TOE Documentation**

---

- Samsung Android 6 on Galaxy Devices Guidance Documentation, version 2.5, October 4, 2016
- Samsung Android 6 on Galaxy Devices User Guidance Documentation, version 2.5, October 4, 2016

---

## 2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
  - Part 3 Extended
- Protection Profile For Mobile Device Fundamentals, Version 2, 17 September 2014 (MDFPP20)
- Package Claims:
  - Assurance Level: EAL 1 augmented with ALC\_TSU\_EXT.1

---

### 2.1 Conformance Rationale

The ST conforms to the MDFPP20. As explained previously, the security problem definition, security objectives, and security requirements are defined the PP.

---

### 3. Security Objectives

The Security Problem Definition may be found in the MDFPP20 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The MDFPP20 offers additional information about the identified security objectives, but that has not been reproduced here and the MDFPP20 should be consulted if there is interest in that material.

In general, the MDFPP20 has defined Security Objectives appropriate for Mobile Device and as such are applicable to the Samsung Galaxy Note 7 on Android 6 TOE.

---

#### 3.1 Security Objectives for the Operational Environment

- **OE.CONFIG** TOE administrators will configure the Mobile Device security functions correctly to create the intended security policy.
- **OE.NOTIFY** The Mobile User will immediately notify the administrator if the Mobile Device is lost or stolen.
- **OE.PRECAUTION** The Mobile User exercises precautions to reduce the risk of loss or theft of the Mobile Device.

## 4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the MDFPP20. The MDFPP20 defines the following extended SFRs and SARs and since they are not redefined in this ST the MDFPP20 should be consulted for more information in regard to those CC extensions.

### Extended SFRs:

- FCS\_CKM\_EXT.1: Extended: Cryptographic Key Support
- FCS\_CKM\_EXT.2: Extended: Cryptographic Key Random Generation
- FCS\_CKM\_EXT.3: Extended: Cryptographic Key Generation
- FCS\_CKM\_EXT.4: Extended: Key Destruction
- FCS\_CKM\_EXT.5: Extended: TSF Wipe
- FCS\_CKM\_EXT.6: Extended: Salt Generation
- FCS\_HTTPS\_EXT.1: Extended: HTTPS Protocol
- FCS\_IV\_EXT.1: Extended: Initialization Vector Generation
- FCS\_RBG\_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
- FCS\_SRV\_EXT.1: Extended: Cryptographic Algorithm Services
- FCS\_STG\_EXT.1: Extended: Cryptographic Key Storage
- FCS\_STG\_EXT.2: Extended: Encrypted Cryptographic Key Storage
- FCS\_STG\_EXT.3: Extended: Integrity of encrypted key storage
- FCS\_TLSC\_EXT.1: Extended: EAP TLS Protocol
- FCS\_TLSC\_EXT.2: Extended: TLS Protocol
- FDP\_ACF\_EXT.1: Extended: Security access control
- FDP\_DAR\_EXT.1: Extended: Protected Data Encryption
- FDP\_DAR\_EXT.2: Extended: Sensitive Data Encryption
- FDP\_IFC\_EXT.1: Extended: Subset information flow control
- FDP\_STG\_EXT.1: Extended: User Data Storage
- FDP\_UPC\_EXT.1: Extended: Inter-TSF user data transfer protection
- FIA\_AFL\_EXT.1: Authentication failure handling
- FIA\_BLT\_EXT.1: Extended: Bluetooth User Authorization
- FIA\_BLT\_EXT.2: Extended: Bluetooth Authentication
- FIA\_PAE\_EXT.1: Extended: PAE Authentication
- FIA\_PMG\_EXT.1: Extended: Password Management
- FIA\_TRT\_EXT.1: Extended: Authentication Throttling
- FIA\_UAU\_EXT.1: Extended: Authentication for Cryptographic Operation
- FIA\_UAU\_EXT.2: Extended: Timing of Authentication

- FIA\_UAU\_EXT.3: Extended: Re-Authentication
- FIA\_X509\_EXT.1: Extended: Validation of certificates
- FIA\_X509\_EXT.2: Extended: X509 certificate authentication
- FIA\_X509\_EXT.3: Extended: Request Validation of certificates
- FMT\_MOF\_EXT.1: Extended: Management of security functions behavior
- FMT\_SMF\_EXT.1: Extended: Specification of Management Functions
- FMT\_SMF\_EXT.2: Extended: Specification of Remediation Actions
- FPT\_AEX\_EXT.1: Extended: Anti-Exploitation Services (ASLR)
- FPT\_AEX\_EXT.2: Extended: Anti-Exploitation Services (Memory Page Permissions)
- FPT\_AEX\_EXT.3: Extended: Anti-Exploitation Services (Overflow Protection)
- FPT\_AEX\_EXT.4: Extended: Domain Isolation
- FPT\_BBD\_EXT.1: Application Processor Mediation
- FPT\_KST\_EXT.1: Extended: Key Storage
- FPT\_KST\_EXT.2: Extended: No Key Transmission
- FPT\_KST\_EXT.3: Extended: No Plaintext Key Export
- FPT\_NOT\_EXT.1: Extended: Self-Test Notification
- FPT\_TST\_EXT.1: Extended: TSF Cryptographic Functionality Testing
- FPT\_TST\_EXT.2: Extended: TSF Integrity Testing
- FPT\_TUD\_EXT.1: Extended: Trusted Update: TSF version query
- FPT\_TUD\_EXT.2: Extended: Trusted Update Verification
- FTA\_SSL\_EXT.1: Extended: TSF- and User-initiated locked state
- FTA\_WSE\_EXT.1: Extended: Wireless Network Access
- FTP\_ITC\_EXT.1: Extended: Trusted channel Communication

**Extended SARs:**

- ALC\_TSU\_EXT.1: Timely Security Updates

## 5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the MDFPP20. The refinements and operations already performed in the MDFPP20 are not identified (e.g., highlighted) here, rather the requirements have been copied from the MDFPP20 and any residual operations have been completed herein. Of particular note, the MDFPP20 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the MDFPP20 which includes all the SARs for EAL 1 augmented with ALC\_TSU\_EXT.1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the MDFPP20 that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the assurance requirements alone. The MDFPP20 should be consulted for the assurance activity definitions.

### 5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the Samsung Galaxy Note 7 on Android 6 TOE.

Requirement Class	Requirement Component
<b>FAU: Security audit</b>	FAU_GEN.1: Audit Data Generation
	FAU_SAR.1: Audit Review
	FAU_STG.1: Audit Storage Protection
	FAU_STG.4: Prevention of Audit Data Loss
<b>FCS: Cryptographic support</b>	FCS_CKM.1(1): Cryptographic key generation
	FCS_CKM.1(2): Cryptographic key generation
	FCS_CKM.2(1): Cryptographic key establishment
	FCS_CKM.2(2): Cryptographic key distribution
	FCS_CKM_EXT.1: Extended: Cryptographic Key Support
	FCS_CKM_EXT.2: Extended: Cryptographic Key Random Generation
	FCS_CKM_EXT.3: Extended: Cryptographic Key Generation
	FCS_CKM_EXT.4: Extended: Key Destruction
	FCS_CKM_EXT.5: Extended: TSF Wipe
	FCS_CKM_EXT.6: Extended: Salt Generation
	FCS_COP.1(1): Cryptographic operation
	FCS_COP.1(2): Cryptographic operation
	FCS_COP.1(3): Cryptographic operation
	FCS_COP.1(4): Cryptographic operation
	FCS_COP.1(5): Cryptographic operation
	FCS_HTTPS_EXT.1: Extended: HTTPS Protocol
	FCS_IV_EXT.1: Extended: Initialization Vector Generation
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_SRV_EXT.1: Extended: Cryptographic Algorithm Services
	FCS_STG_EXT.1: Extended: Cryptographic Key Storage
	FCS_STG_EXT.2: Extended: Encrypted Cryptographic Key Storage
	FCS_STG_EXT.3: Extended: Integrity of encrypted key storage
	FCS_TLSC_EXT.1: Extended: EAP TLS Protocol
	FCS_TLSC_EXT.2: Extended: TLS Protocol
<b>FDP: User data</b>	FDP_ACF_EXT.1(*): Extended: Security access control

<b>protection</b>	FDP_DAR_EXT.1: Extended: Protected Data Encryption
	FDP_DAR_EXT.2: Extended: Sensitive Data Encryption
	FDP_IFC_EXT.1: Extended: Subset information flow control
	FDP_STG_EXT.1: Extended: User Data Storage
	FDP_UPC_EXT.1: Extended: Inter-TSF user data transfer protection
<b>FIA: Identification and authentication</b>	FIA_AFL_EXT.1(*): Authentication failure handling
	FIA_BLT_EXT.1: Extended: Bluetooth User Authorization
	FIA_BLT_EXT.2: Extended: Bluetooth Authentication
	FIA_PAE_EXT.1: Extended: PAE Authentication
	FIA_PMG_EXT.1: Extended: Password Management
	FIA_TRT_EXT.1: Extended: Authentication Throttling
	FIA_UAU.7: Protected authentication feedback
	FIA_UAU_EXT.1: Extended: Authentication for Cryptographic Operation
	FIA_UAU_EXT.2: Extended: Timing of Authentication
	FIA_UAU_EXT.3: Extended: Re-Authentication
	FIA_X509_EXT.1: Extended: Validation of certificates
	FIA_X509_EXT.2: Extended: X509 certificate authentication
	FIA_X509_EXT.3: Extended: Request Validation of certificates
<b>FMT: Security management</b>	FMT_MOF_EXT.1: Extended: Management of security functions behavior
	FMT_SMF_EXT.1: Extended: Specification of Management Functions
	FMT_SMF_EXT.2(*): Extended: Specification of Remediation Actions
<b>FPT: Protection of the TSF</b>	FPT_AEX_EXT.1: Extended: Anti-Exploitation Services (ASLR)
	FPT_AEX_EXT.2: Extended: Anti-Exploitation Services (Memory Page Permissions)
	FPT_AEX_EXT.3: Extended: Anti-Exploitation Services (Overflow Protection)
	FPT_AEX_EXT.4: Extended: Domain Isolation
	FPT_BBD_EXT.1: Application Processor Mediation
	FPT_KST_EXT.1: Extended: Key Storage
	FPT_KST_EXT.2: Extended: No Key Transmission
	FPT_KST_EXT.3: Extended: No Plaintext Key Export
	FPT_NOT_EXT.1: Extended: Self-Test Notification
	FPT_STM.1: Reliable time stamps
	FPT_TST_EXT.1: Extended: TSF Cryptographic Functionality Testing
	FPT_TST_EXT.2: Extended: TSF Integrity Testing
	FPT_TUD_EXT.1: Extended: Trusted Update: TSF version query
	FPT_TUD_EXT.2: Extended: Trusted Update Verification
<b>FTA: TOE access</b>	FTA_SSL_EXT.1: Extended: TSF- and User-initiated locked state
	FTA_TAB.1: Default TOE Access Banners
	FTA_WSE_EXT.1: Extended: Wireless Network Access
<b>FTP: Trusted path/channels</b>	FTP_ITC_EXT.1: Extended: Trusted channel Communication

**Table 1 TOE Security Functional Components**

### 5.1.1 Security audit (FAU)

#### 5.1.1.1 Audit Data Generation (FAU\_GEN.1)

##### FAU\_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:  
1. Start-up and shutdown of the audit functions;

2. All administrative actions;
3. Start-up and shutdown of the OS and kernel;
4. Insertion or removal of removable media;
5. Establishment of a synchronizing connection;
6. Specifically defined auditable events in Table 10 of the MDFPP20;
7. [*Audit records reaching [95] percentage of audit capacity,*].

#### FAU\_GEN.1.2

The TSF shall record within each audit record at least the following information:

1. Date and time of the event;
2. type of event;
3. subject identity;
4. the outcome (success or failure) of the event; and
5. additional information in Table 10 Audited Events of the TSS.

---

#### 5.1.1.2 Audit Review (FAU\_SAR.1)

---

##### FAU\_SAR.1.1

The TSF shall provide [the administrator] with the capability to read [all audited events and record contents] from the audit records.

##### FAU\_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

---

#### 5.1.1.3 Audit Storage Protection (FAU\_STG.1)

---

##### FAU\_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

##### FAU\_STG.1.2

The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

---

#### 5.1.1.4 Prevention of Audit Data Loss (FAU\_STG.4)

---

##### FAU\_STG.4.1

The TSF shall overwrite the oldest stored audit records if the audit trail is full.

---

### 5.1.2 Cryptographic support (FCS)

---

#### 5.1.2.1 Cryptographic key generation (FCS\_CKM.1(1))

---

##### FCS\_CKM.1(1).1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [- *[RSA schemes] using cryptographic key sizes of [2048-bit or greater] that meet the following: [Appendix B.3, ANSI X9.31-1998, Section 4.1];*, - *[ECC schemes] using ['NIST curves' P-256, P-384 and [P-521]] that meet the following: [FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4];* - *[FFC schemes] using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.1].*

---

#### 5.1.2.2 Cryptographic key generation (FCS\_CKM.1(2))

---

##### FCS\_CKM.1(2).1

The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [PRF-384] and specified cryptographic key sizes [128



bits] using a Random Bit Generator as specified in FCS\_RBG\_EXT.1 that meet the following:  
[IEEE 802.11-2012].

---

### 5.1.2.3 Cryptographic key establishment (FCS\_CKM.2(1))

---

#### FCS\_CKM.2(1).1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

- [RSA-based key establishment schemes] that meets the following: [NIST Special Publication 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography'];
- and [- *Elliptic curve-based key establishment schemes*] that meets the following: [NIST Special Publication 800-56A, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography'];
- [Finite field-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography'];] for the purposes of encrypting sensitive data received while the device is locked. (TD0048 applied).

---

### 5.1.2.4 Cryptographic key distribution (FCS\_CKM.2(2))

---

#### FCS\_CKM.2(2).1

The TSF shall decrypt Group Temporal Key (GTK) in accordance with a specified cryptographic key distribution method [AES Key Wrap in an EAPOL-Key frame] that meets the following: [NIST SP 800-38F, IEEE 802.11-2012 for the packet format and timing considerations] and does not expose the cryptographic keys.

---

### 5.1.2.5 Extended: Cryptographic Key Support (FCS\_CKM\_EXT.1)

---

#### FCS\_CKM\_EXT.1.1

The TSF shall support a [*hardware-protected*] REK with a [*symmetric*] key of strength [*256 bits*]. (TD0038 applied)

#### FCS\_CKM\_EXT.1.2

System software on the TSF shall be able only to request [*encryption/decryption, NIST SP 800-108 key derivation*] by the key and shall not be able to read, import, or export a REK.

#### FCS\_CKM\_EXT.1.3

A REK shall be generated by a RBG in accordance with FCS\_RBG\_EXT.1.

#### FCS\_CKM\_EXT.1.4

A REK shall not be able to be read from or exported from the hardware..

---

### 5.1.2.6 Extended: Cryptographic Key Random Generation (FCS\_CKM\_EXT.2)

---

#### FCS\_CKM\_EXT.2.1

All DEKs shall be randomly generated with entropy corresponding to the security strength of AES key sizes of [*256*] bits.

---

### 5.1.2.7 Extended: Cryptographic Key Generation (FCS\_CKM\_EXT.3)

---

#### FCS\_CKM\_EXT.3.1

The TSF shall use[/*256-bit/ symmetric KEKs*] corresponding to at least the security strength of the keys encrypted by the KEK. (TD0038 applied)

#### FCS\_CKM\_EXT.3.2

The TSF shall generate all KEKs using one or more of the following methods:

- a) derive the KEK from a Password Authentication Factor using PBKDF and
- [b) generate the KEK using an RBG that meets this profile (as specified in FCS\_RBG\_EXT.1),**
- d) Combine the KEK from other KEKs in a way that preserves the effective entropy of each factor by [encrypting one key with another] (Per TD0038)].**

---

#### 5.1.2.8 Extended: Key Destruction (FCS\_CKM\_EXT.4)

---

##### FCS\_CKM\_EXT.4.1

The TSF shall destroy cryptographic keys in accordance with the specified cryptographic key destruction methods:

- by clearing the KEK encrypting the target key,
- in accordance with the following rules:
  - For volatile memory, the destruction shall be executed by a single direct overwrite [**consisting of zeroes**]. (TD0028 applied)
  - For non-volatile EEPROM, the destruction shall be executed by a single direct overwrite consisting of a pseudo random pattern using the TSF's RBG (as specified in FCS\_RBG\_EXT.1), followed a read-verify.
  - For non-volatile flash memory that is not wear-leveled, the destruction shall be executed [**by a single direct overwrite consisting of zeros followed by a read-verify**]. (TD0057 applied)
  - For non-volatile flash memory that is wear-leveled, the destruction shall be executed [**by a single direct overwrite consisting of zeros**]
  - For non-volatile memory other than EEPROM and flash, the destruction shall be executed by overwriting three or more times with a random pattern that is changed before each write.

##### FCS\_CKM\_EXT.4.2

The TSF shall destroy all plaintext keying material and critical security parameters when no longer needed.

---

#### 5.1.2.9 Extended: TSF Wipe (FCS\_CKM\_EXT.5)

---

##### FCS\_CKM\_EXT.5.1

The TSF shall wipe all protected data by [**Cryptographically erasing the encrypted DEKs and/or the KEKs in non-volatile memory by following the requirements in FCS\_CKM\_EXT.4.1;**]

##### FCS\_CKM\_EXT.5.2

The TSF shall perform a power cycle on conclusion of the wipe procedure.

---

#### 5.1.2.10 Extended: Salt Generation (FCS\_CKM\_EXT.6)

---

##### FCS\_CKM\_EXT.6.1

The TSF shall generate all salts using a RBG that meets FCS\_RBG\_EXT.1.

---

#### 5.1.2.11 Cryptographic operation (FCS\_COP.1(1))

---

##### FCS\_COP.1(1).1

The TSF shall perform [encryption/decryption] in accordance with a specified cryptographic algorithm

- AES-CBC (as defined in FIPS PUB 197, and NIST SP 800-38A) mode,
  - AES-CCMP (as defined in FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2012), and
  - [- **AES Key Wrap (KW) (as defined in NIST SP 800-38F),**
  - **AES-GCM (as defined in NIST SP 800-38D)**
  - **AES-XTS (as defined in NIST SP 800-38E) mode,**]
- and cryptographic key sizes 128-bit key sizes and [**256-bit key sizes**].

---

### 5.1.2.12 Cryptographic operation (FCS\_COP.1(2))

---

#### FCS\_COP.1(2).1

The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm SHA-1 and [*SHA-256, SHA-384, SHA-512*] and message digest sizes 160 and [*256, 384, 512*] that meet the following: [FIPS Pub 180-4].

---

### 5.1.2.13 Cryptographic operation (FCS\_COP.1(3))

---

#### FCS\_COP.1(3).1

The TSF shall perform [cryptographic signature services (generation and verification)] in accordance with a specified cryptographic algorithm  
- [RSA schemes] using cryptographic key sizes [of 2048-bit or greater] that meet the following: [FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 4]  
and [- [*ECDSA schemes*] using [*'NIST curves' P-256, P-384 and [P-521]]*] that meet the following: [*FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5*];].

---

### 5.1.2.14 Cryptographic operation (FCS\_COP.1(4))

---

#### FCS\_COP.1(4).1

The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm HMAC-SHA-1 and [*HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512*] and cryptographic key sizes [*160, 256, 384, 512*] and message digest sizes 160 and [*256, 384, 512*] bits that meet the following: [FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-4, 'Secure Hash Standard'].

---

### 5.1.2.15 Cryptographic operation (FCS\_COP.1(5))

---

#### FCS\_COP.1(5).1

The TSF shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm [HMAC-*[SHA-256, SHA-512]*], with [*8192 for Keystore, 16384 for SKMM and 32768 for Secure Storage*] iterations, and output cryptographic key sizes [*256*] that meet the following: [NIST SP 800-132].

---

### 5.1.2.16 Extended: HTTPS Protocol (FCS\_HTTPS\_EXT.1)

---

#### FCS\_HTTPS\_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

#### FCS\_HTTPS\_EXT.1.2

The TSF shall implement HTTPS using TLS (FCS\_TLSC\_EXT.2).

#### FCS\_HTTPS\_EXT.1.3

The TSF shall notify the application and [*no other action*] if the peer certificate is deemed invalid.

---

### 5.1.2.17 Extended: Initialization Vector Generation (FCS\_IV\_EXT.1)

---

#### FCS\_IV\_EXT.1.1

The TSF shall generate IVs in accordance with Table 14: References and IV Requirements for NIST-approved Cipher Modes.

---

### 5.1.2.18 Extended: Cryptographic Operation (Random Bit Generation) (FCS\_RBG\_EXT.1)

---

#### FCS\_RBG\_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with [*NIST Special Publication 800-90A using [Hash\_DRBG (any), HMAC\_DRBG (any), CTR\_DRBG (AES)]*].

#### FCS\_RBG\_EXT.1.2

The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [***TSF-hardware-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

#### FCS\_RBG\_EXT.1.3

The TSF shall be capable of providing output of the RBG to applications running on the TSF that request random bits.

---

### 5.1.2.19 Extended: Cryptographic Algorithm Services (FCS\_SRV\_EXT.1)

---

#### FCS\_SRV\_EXT.1.1

The TSF shall provide a mechanism for applications to request the TSF to perform the following cryptographic operations:

- All mandatory and [***(per TD0059) selected algorithms***] in FCS\_CKM.2(1)
- The following algorithms in FCS\_COP.1(1): AES-CBC, [***AES Key Wrap, AES-GCM, AES-XTS***]
- All mandatory and selected algorithms in FCS\_COP.1(3)
- All mandatory and selected algorithms in FCS\_COP.1(2)
- All mandatory and selected algorithms in FCS\_COP.1(4)
- [- ***All mandatory and (per TD0059) selected algorithms***] in FCS\_CKM.1(1),
- ***The selected algorithms in FCS\_COP.1(5)***].

---

### 5.1.2.20 Extended: Cryptographic Key Storage (FCS\_STG\_EXT.1)

---

#### FCS\_STG\_EXT.1.1

The TSF shall provide [***hardware-isolated***] secure key storage for asymmetric private keys and [symmetric keys].

#### FCS\_STG\_EXT.1.2

The TSF shall be capable of importing keys/secrets into the secure key storage upon request of [***the user, the administrator***] and [***applications running on the TSF***].

#### FCS\_STG\_EXT.1.3

The TSF shall be capable of destroying keys/secrets in the secure key storage upon request of [***the user***].

#### FCS\_STG\_EXT.1.4

The TSF shall have the capability to allow only the application that imported the key/secret the use of the key/secret. Exceptions may only be explicitly authorized by [***a common application developer***].

#### FCS\_STG\_EXT.1.5

The TSF shall allow only the application that imported the key/secret to request that the key/secret be destroyed. Exceptions may only be explicitly authorized by [***a common application developer***].

---

### 5.1.2.21 Extended: Encrypted Cryptographic Key Storage (FCS\_STG\_EXT.2)

---

#### FCS\_STG\_EXT.2.1

The TSF shall encrypt all DEKs and KEKs and [***no other keys***] by KEKs that are [***1) Protected by the REK with [a. encryption by a REK, b. encryption by a KEK chaining to a REK],***  
***2) Protected by the REK and the password with [a. encryption by a REK and the password-derived KEK,***  
***b. encryption by a KEK chaining to a REK and the password-derived KEK]***].

#### FCS\_STG\_EXT.2.2

DEKs and KEKs and [***no other keys***] shall be encrypted using one of the following methods: [***using AES in the [GCM, CBC mode]***]. (TD0038 applied)

---

### 5.1.2.22 Extended: Integrity of encrypted key storage (FCS\_STG\_EXT.3)

---

#### FCS\_STG\_EXT.3.1

The TSF shall protect the integrity of any encrypted DEKs and KEKs and [*no other keys*] by [*- [GCM] cipher mode for encryption according to FCS\_STG\_EXT.2;*].

#### FCS\_STG\_EXT.3.2

The TSF shall verify the integrity of the [MAC] of the stored key prior to use of the key.

---

### 5.1.2.23 Extended: EAP TLS Protocol (FCS\_TLSC\_EXT.1)

---

#### FCS\_TLSC\_EXT.1.1

The TSF shall implement TLS 1.0 and [*TLS 1.1, TLS 1.2*] supporting the following ciphersuites:  
[Mandatory Ciphersuites:

- o TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 5246

Optional Ciphersuites: [

- o *TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 5246,*
- o *TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 5246,*
- o *TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 5246,*
- o *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 4492,*
- o *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 4492,*
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 4492,*
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 4492,*
- o *TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,*
- o *TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,*
- o *TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,*
- o *TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,*
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289,*
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 as defined in RFC 5289,*
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289,*
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289*]].

#### FCS\_TLSC\_EXT.1.2

The TSF shall verify that the server certificate presented for EAP-TLS [*chains to one of the specified CAs*].

#### FCS\_TLSC\_EXT.1.3

The TSF shall not establish a trusted channel if the peer certificate is invalid.

#### FCS\_TLSC\_EXT.1.4

The TSF shall support mutual authentication using X.509v3 certificates.

#### FCS\_TLSC\_EXT.1.5

The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [*secp256r1, secp384r1, secp521r1*] and no other curves.

---

### 5.1.2.24 Extended: TLS Protocol (FCS\_TLSC\_EXT.2)

---

#### FCS\_TLSC\_EXT.2.1

The TSF shall implement TLS 1.2 (RFC 5246) supporting the following ciphersuites: [Mandatory Ciphersuites:

- o TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 5246

Optional Ciphersuites: [

- o *TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 5246,*
- o *TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 5246,*
- o *TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 5246,*
- o *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 4492,*
- o *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 4492,*
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 4492,*

- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA* as defined in RFC 4492,
- o *TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256* as defined in RFC 5246,
- o *TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256* as defined in RFC 5246,
- o *TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256* as defined in RFC 5246,
- o *TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256* as defined in RFC 5246,
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256* as defined in RFC 5289,
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384* as defined in RFC 5289 ,
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256* as defined in RFC 5289,
- o *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384* as defined in RFC 5289]].

#### FCS\_TLSC\_EXT.2.2

The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

#### FCS\_TLSC\_EXT.2.3

The TSF shall not establish a trusted channel if the peer certificate is invalid.

#### FCS\_TLSC\_EXT.2.4

The TSF shall support mutual authentication using X.509v3 certificates.

#### FCS\_TLSC\_EXT.2.5

The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [*secp256r1, secp384r1, secp521r1*] and no other curves.

### 5.1.3 User data protection (FDP)

#### 5.1.3.1 Extended: Security access control (FDP\_ACF\_EXT.1(1))

##### FDP\_ACF\_EXT.1(1).1

The TSF shall provide a mechanism to restrict the system services that are accessible to an application.

##### FDP\_ACF\_EXT.1(1).2

The TSF shall provide an access control policy that prevents [*application processes*] from accessing [*all*] data stored by other [*application processes*]. Exceptions may only be explicitly authorized for such sharing by [*a common application developer*].

##### FDP\_ACF\_EXT.1(1).3

The TSF shall enforce an access control policy that prohibits an application from granting both write and execute permission to a file on the device except for [*application's private data folder*]. (TD0103 applied)

#### 5.1.3.2 Extended: Security access control (FDP\_ACF\_EXT.1(2))

##### FDP\_ACF\_EXT.1(2).1

The TSF shall provide a mechanism to restrict the system services that are accessible to an application.

##### FDP\_ACF\_EXT.1(2).2

The TSF shall provide an access control policy that prevents [*groups of application processes*] from accessing [*all*] data stored by other [*groups of application processes*]. Exceptions may only be explicitly authorized for such sharing by [*the administrator*].

#### 5.1.3.3 Extended: Protected Data Encryption (FDP\_DAR\_EXT.1)

##### FDP\_DAR\_EXT.1.1

Encryption shall cover all protected data.

##### FDP\_DAR\_EXT.1.2

Encryption shall be performed using DEKs with AES in the [*CBC, GCM, XTS*] mode with key size [*128,256*] bits.



---

#### 5.1.3.4 Extended: Sensitive Data Encryption (FDP\_DAR\_EXT.2)

---

##### FDP\_DAR\_EXT.2.1

The TSF shall provide a mechanism for applications to mark data and keys as sensitive.

##### FDP\_DAR\_EXT.2.2

The TSF shall use an asymmetric key scheme to encrypt and store sensitive data received while the product is locked.

##### FDP\_DAR\_EXT.2.3

The TSF shall encrypt any stored symmetric key and any stored private key of the asymmetric key(s) used for the protection of sensitive data according to FCS\_STG\_EXT.2.1 selection 2.

##### FDP\_DAR\_EXT.2.4

The TSF shall decrypt the sensitive data that was received while in the locked state upon transitioning to the unlocked state using the asymmetric key scheme and shall re-encrypt that sensitive data using the symmetric key scheme.

---

#### 5.1.3.5 Extended: Subset information flow control (FDP\_IFC\_EXT.1)

---

##### FDP\_IFC\_EXT.1.1

The TSF shall [*enable all IP traffic (other than IP traffic required to establish the VPN connection) to flow through the IPsec VPN client*].

---

#### 5.1.3.6 Extended: User Data Storage (FDP\_STG\_EXT.1)

---

##### FDP\_STG\_EXT.1.1

The TSF shall provide protected storage for the Trust Anchor Database.

---

#### 5.1.3.7 Extended: Inter-TSF user data transfer protection (FDP\_UPC\_EXT.1)

---

##### FDP\_UPC\_EXT.1.1

The TSF provide a means for non-TSF applications executing on the TOE to use TLS, HTTPS, Bluetooth BR/EDR, and [*Bluetooth LE*] to provide a protected communication channel between the non-TSF application and another IT product that is logically distinct from other communication channels, provides assured identification of its end points, protects channel data from disclosure, and detects modification of the channel data.

##### FDP\_UPC\_EXT.1.2

The TSF shall permit the non-TSF applications to initiate communication via the trusted channel.

---

### 5.1.4 Identification and authentication (FIA)

---

#### 5.1.4.1 Authentication failure handling (FIA\_AFL\_EXT.1(1))

---

##### FIA\_AFL\_EXT.1(1).1

The TSF shall detect when a configurable positive integer within [**1-100**] of unsuccessful authentication attempts occur related to last successful **non container** authentication by that user.

##### FIA\_AFL\_EXT.1(1).2

When the defined number of unsuccessful **non container** authentication attempts has been surpassed, the TSF shall perform wipe of all protected data.

##### FIA\_AFL\_EXT.1(1).3

The TSF shall maintain the number of unsuccessful **non container** authentication attempts that have occurred upon power off.

---

#### 5.1.4.2 Authentication failure handling (FIA\_AFL\_EXT.1(2))

---

##### FIA\_AFL\_EXT.1(2).1

The TSF shall detect when a configurable positive integer within [1-99] of unsuccessful authentication attempts occur related to last successful **container** authentication by that user.

##### FIA\_AFL\_EXT.1(2).2

When the defined number of unsuccessful **container** authentication attempts has been surpassed, the TSF shall perform wipe of all protected data.

##### FIA\_AFL\_EXT.1(2).3

The TSF shall maintain the number of unsuccessful **container** authentication attempts that have occurred upon power off.

---

#### 5.1.4.3 Extended: Bluetooth User Authorization (FIA\_BLT\_EXT.1)

---

##### FIA\_BLT\_EXT.1.1

The TSF shall require explicit user authorization before pairing with a remote Bluetooth device.

##### FIA\_BLT\_EXT.1.2

The TSF shall require explicit user authorization before granting trusted remote devices access to services associated with the following Bluetooth profiles: [OPP, MAP], and shall require explicit user authorization before granting untrusted remote devices access to services associated with the following Bluetooth profiles: [all Bluetooth profiles].

---

#### 5.1.4.4 Extended: Bluetooth Authentication (FIA\_BLT\_EXT.2)

---

##### FIA\_BLT\_EXT.2.1

The TSF shall require Bluetooth mutual authentication between devices prior to any data transfer over the Bluetooth link.

##### FIA\_BLT\_EXT.2.2

Removed to FIA\_BLT\_EXT.3 per TD0030.

---

#### 5.1.4.5 Rejection of Duplicate Bluetooth Connections (FIA\_BLT\_EXT.3)

---

##### FIA\_BLT\_EXT.3.1

The TSF shall discard connection attempts from a Bluetooth device address (BD\_ADDR) to which a current connection already exists. (Formerly FIA\_BLT\_EXT.2.2 per TD0030)

---

#### 5.1.4.6 Extended: PAE Authentication (FIA\_PAE\_EXT.1)

---

##### FIA\_PAE\_EXT.1.1

The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the 'Supplicant' role.

---

#### 5.1.4.7 Extended: Password Management (FIA\_PMG\_EXT.1)

---

##### FIA\_PMG\_EXT.1.1

The TSF shall support the following for the Password Authentication Factor:

1. Passwords shall be able to be composed of any combination of [*upper and lower case letters*], numbers, and special characters: [ ! @ # \$ % ^ & \* ( ) + = \_ / - ' " : ; , ? ` ~ | < > { } [ ] ];
2. Password length up to [16] characters shall be supported.

---

#### 5.1.4.8 Extended: Authentication Throttling (FIA\_TRT\_EXT.1)

---

##### FIA\_TRT\_EXT.1.1

The TSF shall limit automated user authentication attempts by [*enforcing a delay between*



*incorrect authentication attempts*]. The minimum delay shall be such that no more than 10 attempts can be attempted per 500 milliseconds.

---

#### 5.1.4.9 Protected authentication feedback (FIA\_UAU.7)

---

##### FIA\_UAU.7.1

The TSF shall provide only [obscured feedback to the device's display] to the user while the authentication is in progress.

---

#### 5.1.4.10 Extended: Authentication for Cryptographic Operation (FIA\_UAU\_EXT.1)

---

##### FIA\_UAU\_EXT.1.1

The TSF shall require the user to present the Password Authentication Factor prior to decryption of protected data and encrypted DEKs, KEKs and [*no other keys*] at startup.

---

#### 5.1.4.11 Extended: Timing of Authentication (FIA\_UAU\_EXT.2)

---

##### FIA\_UAU\_EXT.2.1

The TSF shall allow [*enter password to unlock, make emergency calls, receive calls, take pictures and screen shots (automatically named and stored internally by the TOE), turn the TOE off, restart the TOE, enable emergency mode, enable and disable airplane mode, see notifications, configure sound/vibrate/mute, set the volume (up and down) for various sound categories, see the configured banner, access Notification Panel functions (including toggles Always on Display, Flashlight, Do not disturb toggle, Airplane mode, Power saving, Auto rotate, and Sound (on, mute, vibrate) and access user configured Edge applications*)] on behalf of the user to be performed before the user is authenticated.

##### FIA\_UAU\_EXT.2.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

---

#### 5.1.4.12 Extended: Re-Authentication (FIA\_UAU\_EXT.3)

---

##### FIA\_UAU\_EXT.3.1

The TSF shall require the user to enter the correct Password Authentication Factor when the user changes the Password Authentication Factor, and following TSF- and user-initiated locking in order to transition to the unlocked state, and [*when changing the lock screen, when changing one's password, and when initializing the keystore*].

---

#### 5.1.4.13 Extended: Validation of certificates (FIA\_X509\_EXT.1)

---

##### FIA\_X509\_EXT.1.1

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a certificate in the Trust Anchor Database.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [*the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

o (Conditional) Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.

#### FIA\_X509\_EXT.1.2

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

### 5.1.4.14 Extended: X509 certificate authentication (FIA\_X509\_EXT.2)

#### FIA\_X509\_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for EAP-TLS exchanges, and [*IPsec, TLS, HTTPS*], and [*no additional uses*].

#### FIA\_X509\_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [*not accept the certificate*].

### 5.1.4.15 Extended: Request Validation of certificates (FIA\_X509\_EXT.3)

#### FIA\_X509\_EXT.3.1

The TSF shall provide a certificate validation service to applications.

#### FIA\_X509\_EXT.3.2

The TSF shall respond to the requesting application with the success or failure of the validation.

## 5.1.5 Security management (FMT)

### 5.1.5.1 Extended: Management of security functions behavior (FMT\_MOF\_EXT.1)

#### FMT\_MOF\_EXT.1.1

The TSF shall restrict the ability to perform the functions in column 3 of ~~Table 1~~ **Table 2 Security Management Functions** to the user.

#### FMT\_MOF\_EXT.1.2(1)

The TSF shall restrict the ability to perform the **non container** functions in column 5 of **Table 2 Security Management Functions** to the administrator when the device is enrolled and according to the administrator-configured policy.

#### FMT\_MOF\_EXT.1.2(2)

**The TSF shall restrict the ability to perform the container functions in column 7 of Table 2 Security Management Functions to the administrator when the device is enrolled and according to the administrator-configured policy.**

### 5.1.5.2 Extended: Specification of Management Functions (FMT\_SMF\_EXT.1)

#### FMT\_SMF\_EXT.1.1

The TSF shall be capable of performing the functions: **in column 2 of Table 2 Security Management Functions**.

#### FMT\_SMF\_EXT.1.2(1)

**The TSF shall be capable of allowing the administrator to perform the non-container functions in column 4 of Table 2 Security Management Functions.**

#### FMT\_SMF\_EXT.1.2(2)

**The TSF shall be capable of allowing the administrator to perform the container functions in column 6 of Table 2 Security Management Functions.**

**Table 2 Security Management Functions**

<p style="text-align: center;"><b>Management Function</b></p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <p><b>Status Markers:</b>                      M – Mandatory                      I – Implemented</p> </div>	FMT_SMF_EXT.1.1	FMT_MOF_EXT.1.1	FMT_SMF_EXT.1.2(1)	FMT_MOF_EXT.1.2(1)	FMT_SMF_EXT.1.2(2)	FMT_MOF_EXT.1.2(2)
<p>1. configure password policy:</p> <ul style="list-style-type: none"> <li>a. minimum password length</li> <li>b. minimum password complexity</li> <li>c. maximum password lifetime</li> </ul> <p>The administrator can configure the required password characteristics (minimum length, complexity, and lifetime) using the Android MDM APIs. There are distinct settings for the passwords used to unlock the base device and KNOX Workspace container.</p> <p>Length: an integer value of characters (0 = no minimum)                      Complexity: Unspecified, Something, Numeric, Alphabetic, Alphanumeric, Complex.                      Lifetime: an integer value of days (0 = no maximum)</p>	M		M	M	I	I
<p>2. configure session locking policy:</p> <ul style="list-style-type: none"> <li>a. screen-lock enabled/disabled</li> <li>b. screen lock timeout</li> <li>c. number of authentication failures</li> </ul> <p>The administrator can configure the session locking policy using the Android MDM APIs. There are distinct settings for base device and KNOX Workspace container inactivity.</p> <p>The user can also adjust each of the session locking policies for the base device and KNOX Workspace container; however, if set by the administrator, the user can only set a more strict policy (e.g., setting the device to allow fewer authentication failures than configured by the administrator).</p> <p>Screen lock timeout: an integer number of minutes before the TOE locks (0 = no lock timeout)                      Authentication failures: an integer number (0 = no limit)</p>	M		M	M	I	I
<p>3. enable/disable the VPN protection:</p> <ul style="list-style-type: none"> <li>a. across device</li> <li>[ c. <b>no other method</b>]</li> </ul> <p>The user can configure and then enable the TOE's VPN to protect traffic.</p>	M		I	I		

Management Function		FMT_SME_EXT.1.1	FMT_MOF_EXT.1.1	FMT_SME_EXT.1.2(1)	FMT_MOF_EXT.1.2(1)	FMT_SME_EXT.1.2(2)	FMT_MOF_EXT.1.2(2)
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: auto;"> <b>Status Markers:</b>                      M – Mandatory                      I – Implemented                 </div>							
The administrator (through an MDM Agent that utilizes the TOE’s MDM APIs) can restrict the TOE’s ability to connect to a VPN.							
4.	enable/disable [ <b>nfc, Bluetooth, Wi-Fi, and cellular radios</b> ]  The administrator can disable the radios using the TOE’s MDM APIs. Once disabled, a user cannot enable the radio. The TOE’s radio’s operate at frequencies of 2.4 GHz (NFC/Bluetooth), 2.4/5 GHz (Wi-Fi), and 850 MHz (4G/LTE). The administrator cannot fully disable/restrict cellular voice capabilities	M		I	I		
5.	enable/disable [ <b>camera, microphone</b> ]: (TD0044 applied) a. across device [ <b>c. no other method</b> ]  An administrator may configure the TOE (through an MDM agent utilizing the TOE’s MDM APIs) to turn off the camera and or microphones. If the administrator has disabled either the camera or the microphones, then the user cannot use those capture devices.  The administrator can also disable the use of the camera or microphone inside a KNOX Workspace container without affecting access to those devices when outside the container.	M		I	I	I	I
6.	specify wireless networks (SSIDs) to which the TSF may connect (TD0064 applied)  An administrator can specify a list of wireless network SSIDs to which the TOE may connect and can restrict the TOE to only allow a connection to the specified SSIDs.	I		I	I		
7.	configure security policy for each wireless network: a. [ <b>specify the CA(s) from which the TSF will accept WLAN authentication server certificate(s)</b> ] b. security type c. authentication protocol d. client credentials to be used for authentication  Both users and administrators (using the TOE’s MDM APIs) can define wireless connection policies for specific SSIDs.	M		M			

Management Function		FMT_SME_EXT.1.1	FMT_MOF_EXT.1.1	FMT_SME_EXT.1.2(1)	FMT_MOF_EXT.1.2(1)	FMT_SME_EXT.1.2(2)	FMT_MOF_EXT.1.2(2)
<p><b>Status Markers:</b> M – Mandatory I – Implemented</p>							
8. transition to the locked state		M		M	-	I	
Both users and administrators (using the TOE’s MDM APIs) can transition the TOE or KNOX Workspace container into a locked state.							
9. full wipe of protected data		M		M		I	
Both users and administrators (using the TOE’s MDM APIs) can force the TOE to perform a full wipe (factory reset) of data. Administrators can also cause the contents of a KNOX Workspace container to be wiped by deleting the container.							
10. configure application installation policy by: <b>c. denying installation of applications]</b>		M		M	M	I	I
The administrator using the TOE’s MDM APIs can configure the TOE so that applications cannot be installed and can also block the use of the Google Market Place. There are distinct settings for disabling the installation of applications for the base device and KNOX Workspace container.							
11. import keys/secrets into the secure key storage		M		I			
Both users and administrators (using the TOE’s MDM APIs) can import secret keys into the secure key storage.							
12. destroy imported keys/secrets and [ <b>no other keys/secrets</b> ] in the secure key storage		M		I			
Both users and administrators (using the TOE’s MDM APIs) can destroy secret keys in the secure key storage.							
13. import X.509v3 certificates into the Trust Anchor Database		M		M			
Both users and administrators (using the TOE’s MDM APIs) can import X.509v3 certificates into the Trust Anchor Database.							
14. remove imported X.509v3 certificates and [ <b>default X.509v3 certificates</b> ] in the Trust Anchor Database		M		I			
Both users and administrators (using the TOE’s MDM APIs) can remove imported X.509v3 certificates from the Trust Anchor Database as well as disable any of the TOE’s default Root CA certificates (in the latter case, the CA certificate still resides in the TOE’s read-only system partition; however, the TOE will treat that Root CA certificate and any certificate chaining to it as							

<p style="text-align: center;"><b>Management Function</b></p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p><b>Status Markers:</b>                      M – Mandatory                      I – Implemented</p> </div>	FMT_SME_EXT.1.1	FMT_MOF_EXT.1.1	FMT_SME_EXT.1.2(1)	FMT_MOF_EXT.1.2(1)	FMT_SME_EXT.1.2(2)	FMT_MOF_EXT.1.2(2)
<p>untrusted).</p>						
<p>15. enroll the TOE in management (TD0058 applied)</p> <p>TOE users can enroll the TOE in management according to the instructions specific to a given MDM. Presumably any enrollment would involve at least some user functions (e.g., install an MDM agent application) on the TOE prior to enrollment.</p>	M	M				
<p>16. remove applications</p> <p>Both users and administrators (using the TOE’s MDM APIs) can uninstall user and administrator installed applications on the TOE (non-container) and applications inside a KNOX Workspace container.</p>	M		M		I	
<p>17. update system software</p> <p>Users can check for updates and cause the device to update if an update is available. An administrator can use MDM APIs to query the version of the TOE and query the installed applications and an MDM agent on the TOE could issue pop-ups, initiate updates, block communication, etc. until any necessary updates are completed.</p>	M		M			
<p>18. install applications</p> <p>Both users and administrators (using the TOE’s MDM APIs) can install applications on the TOE (non-container) and applications inside a KNOX Workspace container.</p>	M		M		I	
<p>19. remove Enterprise applications</p> <p>Both users and administrators (using the TOE’s MDM APIs) can uninstall user and administrator installed applications on the TOE (non-container) and applications inside a KNOX Workspace container. Note that there is no distinction between Enterprise and other applications.</p>	M		M		I	
<p>20. configure the Bluetooth trusted channel:</p> <ul style="list-style-type: none"> <li>a. disable/enable the Discoverable mode (for BR/EDR)</li> <li>b. change the Bluetooth device name</li> <li>[ c. <i>allow/disallow Android Beam and S-Beam to be used with Bluetooth</i></li> <li>f. <i>disable/enable the Bluetooth services and or profiles available on the device</i>]</li> </ul>	M		I			

Management Function		FMT_SME_EXT.1.1	FMT_MOF_EXT.1.1	FMT_SME_EXT.1.2(1)	FMT_MOF_EXT.1.2(1)	FMT_SME_EXT.1.2(2)	FMT_MOF_EXT.1.2(2)
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: auto;"> <b>Status Markers:</b>                      M – Mandatory                      I – Implemented                 </div>							
TOE users can enable Bluetooth discoverable mode for a short period of time and can also change the device name which is used for the Bluetooth name. Additional wireless technologies include Android Beam and S-Beam which are related to NFC and can be enabled and disabled by the TOE user.							
21. enable/disable display notification in the locked state of: [ <b>f. all notifications</b> ]	M						
TOE users can configure the TOE to allow or disallow notifications while in a locked state.							
22. enable/disable all data signaling over [ <b>USB</b> ]	I		I	I			
The administrator (using the TOE’s MDM APIs) can disable USB communication features (tethering, debugging, mass storage access, etc.) to prevent data signaling via USB.							
23. enable/disable [ <b>Wi-Fi tethering, USB tethering, and Bluetooth tethering</b> ]	I		I	I			
The administrator (using the TOE’s MDM APIs) can individually disable each tethering method.							
Unless disabled by the administrator, TOE users can individually enable and disable tethering via a Wi-Fi hotspot, USB connection, and Bluetooth pairing.							
The TOE acts as a server (acting as an access point, a USB Ethernet adapter, and as a Bluetooth Ethernet adapter respectively) in order to share its network connection with another device.							
24. enable/disable developer modes	I		I	I			
The administrator (using the TOE’s MDM APIs) can disable Developer Mode.							
Unless disabled by the administrator, TOE users can enable and disable Developer Mode.							
25. enable data-at rest protection	I		I	I			
The administrator (using the TOE’s MDM APIs) can configure a device encryption policy. Once enabled the TOE internal flash will be encrypted.							

Management Function		FMT_SME_EXT.1.1	FMT_MOF_EXT.1.1	FMT_SME_EXT.1.2(1)	FMT_MOF_EXT.1.2(1)	FMT_SME_EXT.1.2(2)	FMT_MOF_EXT.1.2(2)
<p><b>Status Markers:</b> M – Mandatory I – Implemented</p>							
Users can also encrypt the TOE internal flash even if not enforced by administrator policy. However, if the policy is set the user cannot decrypt the TOE.							
<p>26. enable removable media’s data-at-rest protection</p> <p>The administrator (using the TOE’s MDM APIs) can configure a device removable media encryption policy. Once enabled, files on external SD cards will be encrypted. Users can also encrypt the TOE internal flash even if not enforced by administrator policy. However, if the policy is set the user cannot decrypt the TOE.</p>		I		I	I		
27. enable/disable bypass of local user authentication							
28. wipe Enterprise data						I	
<p>29. approve [<i>import</i>] by applications of X.509v3 certificates in the Trust Anchor Database</p> <p>The TOE will prompt the User to approve requests by an application to import an X.509v3 CA Certificate into the TOE’s Trust Anchor Database. The User, when prompted, can allow or deny the import.</p>							
30. configure whether to establish a trusted channel or disallow establishment if the TSF cannot establish a connection to determine the validity of a certificate							
31. enable/disable the cellular protocols used to connect to cellular network base stations							
<p>32. read audit logs kept by the TSF</p> <p>The administrator (using MDM APIs) can view the TOE’s audit records.</p>		I		I			
33. configure [selection: <i>certificate, public-key</i> ] used to validate digital signature on applications							
34. approve exceptions for shared use of keys/secrets by multiple applications							
35. approve exceptions for destruction of keys/secrets by applications that did not import the key/secret							
<p>36. configure the unlock banner</p> <p>The administrator (using the TOE’s MDM APIs) can defined a banner of a maximum of 256 characters to be displayed while the TOE is locked. There is no method for the user to change the banner.</p>		I		I	I		



Management Function		FMT_SME_EXT.1.1	FMT_MOF_EXT.1.1	FMT_SME_EXT.1.2(1)	FMT_MOF_EXT.1.2(1)	FMT_SME_EXT.1.2(2)	FMT_MOF_EXT.1.2(2)
<p><b>Status Markers:</b> M – Mandatory I – Implemented</p>							
37. configure the auditable items							
38. retrieve TSF-software integrity verification values							
39. enable/disable [ <ul style="list-style-type: none"> <li>a. <b>USB mass storage mode</b></li> </ul> <p>The administrator (using the TOE’s MDM APIs) can disable USB mass storage mode.</p>	I		I	I			
40. enable/disable backup to [ <i>local system, remote system</i> ]		I		I	I		
41. enable/disable [ <ul style="list-style-type: none"> <li>a. <b>Hotspot functionality authenticated by [pre-shared key],</b></li> <li>b. <b>USB tethering authenticated by [no authentication]</b></li> </ul> <p>The administrator (using the TOE’s MDM APIs) can disable the Wi-Fi hotspot and USB tethering.</p> <p>Unless disabled by the administrator, TOE users can configure the Wi-Fi hotspot with a pre-shared key and can configure USB tethering (with no authentication).</p>	I		I	I			
42. approve exceptions for sharing data between [ <i>groups of application processes</i> ]							I
43. place applications into application process groups based on [ <i>assignment: application characteristics</i> ]							
44. enable/disable location services: <ul style="list-style-type: none"> <li>a. across device</li> <li>[ c. <b>no other method</b>]</li> </ul> <p>The administrator (using the TOE’s MDM APIs) can disable location services.</p> <p>Unless disabled by the administrator, TOE users can enable and disable location services.</p>	M		I	I			
45. [enable/disable USB host storage disable CC Mode]				I	I	I	I

---

### 5.1.5.3 Extended: Specification of Remediation Actions (FMT\_SMF\_EXT.2(1))

---

#### FMT\_SMF\_EXT.2(1).1

The TSF shall offer [*wipe of protected data, wipe of sensitive data, [remove MDM policies and disable CC mode]*] upon **non container** unenrollment and [*no other triggers*].

---

### 5.1.5.4 Extended: Specification of Remediation Actions (FMT\_SMF\_EXT.2(2))

---

#### FMT\_SMF\_EXT.2(2).1

The TSF shall offer [*remove Enterprise applications, full wipe of container data*] upon **container** unenrollment and [*no other triggers*].

---

## 5.1.6 Protection of the TSF (FPT)

---

### 5.1.6.1 Extended: Anti-Exploitation Services (ASLR) (FPT\_AEX\_EXT.1)

---

#### FPT\_AEX\_EXT.1.1

The TSF shall provide address space layout randomization (ASLR) to applications.

#### FPT\_AEX\_EXT.1.2

The base address of any user-space memory mapping will consist of at least 8 unpredictable bits.

#### FPT\_AEX\_EXT.1.3

The TSF shall provide address space layout randomization (ASLR) to the kernel.

#### FPT\_AEX\_EXT.1.4

The base address of any kernel-space memory mapping will consist of at least 4 unpredictable bits.

---

### 5.1.6.2 Extended: Anti-Exploitation Services (Memory Page Permissions) (FPT\_AEX\_EXT.2)

---

#### FPT\_AEX\_EXT.2.1

The TSF shall be able to enforce read, write, and execute permissions on every page of physical memory.

#### FPT\_AEX\_EXT.2.2

The TSF shall prevent write and execute permissions from being simultaneously granted to any page of physical memory [*excluding memory used for JIT (just-in-time) compilation and memory allocated with mmap*].

---

### 5.1.6.3 Extended: Anti-Exploitation Services (Overflow Protection) (FPT\_AEX\_EXT.3)

---

#### FPT\_AEX\_EXT.3.1

TSF processes that execute in a non-privileged execution domain on the application processor shall implement stack-based buffer overflow protection.

---

### 5.1.6.4 Extended: Domain Isolation (FPT\_AEX\_EXT.4)

---

#### FPT\_AEX\_EXT.4.1

The TSF shall protect itself from modification by untrusted subjects.

#### FPT\_AEX\_EXT.4.2

The TSF shall enforce isolation of address space between applications.

### 5.1.6.5 Application Processor Mediation (FPT\_BBD\_EXT.1)

#### FPT\_BBD\_EXT.1.1

The TSF shall prevent code executing on any baseband processor (BP) from accessing application processor (AP) resources except when mediated by the AP.

### 5.1.6.6 Extended: Key Storage (FPT\_KST\_EXT.1)

#### FPT\_KST\_EXT.1.1

The TSF shall not store any plaintext key material in readable non-volatile memory.

### 5.1.6.7 Extended: No Key Transmission (FPT\_KST\_EXT.2)

#### FPT\_KST\_EXT.2.1

The TSF shall not transmit any plaintext key material outside the security boundary of the TOE.

### 5.1.6.8 Extended: No Plaintext Key Export (FPT\_KST\_EXT.3)

#### FPT\_KST\_EXT.3.1

The TSF shall ensure it is not possible for the TOE user(s) to export plaintext keys.

### 5.1.6.9 Extended: Self-Test Notification (FPT\_NOT\_EXT.1)

#### FPT\_NOT\_EXT.1.1

The TSF shall transition to non-operational mode and [*force User authentication failure*] when the following types of failures occur:

- failures of the self-test(s)
- TSF software integrity verification failures
- [*no other failures*].

### 5.1.6.10 Reliable time stamps (FPT\_STM.1)

#### FPT\_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

### 5.1.6.11 Extended: TSF Cryptographic Functionality Testing (FPT\_TST\_EXT.1)

#### FPT\_TST\_EXT.1.1

The TSF shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of all cryptographic functionality.

### 5.1.6.12 Extended: TSF Integrity Testing (FPT\_TST\_EXT.2)

#### FPT\_TST\_EXT.2.1

The TSF shall verify the integrity of the bootchain up through the Application Processor OS kernel, and [

System executable	File System locaion	Security Function
app_process	/system/bin	APP
charon	/system/bin	VPN
dalvikvm	/system/bin	VM
dhcpcd	/system/bin	Integrity
gatekeeperd	/system/bin	Key store / Key Mgnt
icd	/system/bin	Integrity
keystore	/system/bin	Key store
mcDriverDaemon	/system/bin	Trustzone Daemon
qseecomd	/system/bin	Trustzone Daemon

System executable	File System locaion	Security Function
sdp_cryptod	/system/bin	DAR
time_daemon	/system/bin	TIME
vold	/system/bin	DAR
wpa_supplicant	/system/bin	WLAN
libSecurityManagerNative.so	/system/lib , /system/lib64	CCMode
libcharon.so	/system/lib , /system/lib64	VPN
libcrypto.so	/system/lib , /system/lib64	Crypto
libdirencryption.so	/system/lib , /system/lib64	DAR
libjavacrypto.so	/system/lib , /system/lib64	Crypto
libkeystore_binder.so	/system/lib , /system/lib64	Key store
libkeyutils.so	/system/lib , /system/lib64	Key store
libknox_km.so	/system/lib , /system/lib64	DAR
libsdp_crypto.so	/system/lib , /system/lib64	DAR
libsdp_kekm.so	/system/lib , /system/lib64	DAR
libsdp_sdk.so	/system/lib , /system/lib64	DAR
libsec_devenc.so	/system/lib , /system/lib64	DAR
libsec_ecryptfs.so	/system/lib , /system/lib64	DAR
libsec_ode_keymanager.so	/system/lib , /system/lib64	DAR
libskmm.so	/system/lib , /system/lib64	Key Mgnt
libskmm_helper.so	/system/lib , /system/lib64	Key Mgnt
libsoftwarekeymaster.so	/system/lib , /system/lib64	Key Mgnt
libssl.so	/system/lib , /system/lib64	Crypto
libstrongswan.so	/system/lib , /system/lib64	VPN
libQSEECOMAPI.so	/system/vendor/lib, /system/vendor/lib64	Trustzone Library

], stored in mutable media prior to its execution through the use of [*a digital signature using a hardware-protected asymmetric key, a hardware-protected hash*].

#### 5.1.6.13 Extended: Trusted Update: TSF version query (FPT\_TUD\_EXT.1)

##### FPT\_TUD\_EXT.1.1

The TSF shall provide authorized users the ability to query the current version of the TOE firmware/software.

##### FPT\_TUD\_EXT.1.2

The TSF shall provide authorized users the ability to query the current version of the hardware model of the device.

##### FPT\_TUD\_EXT.1.3

The TSF shall provide authorized users the ability to query the current version of installed mobile applications.

#### 5.1.6.14 Extended: Trusted Update Verification (FPT\_TUD\_EXT.2)

##### FPT\_TUD\_EXT.2.1

The TSF shall verify software updates to the Application Processor system software and [*communications processor software, bootloader software, carrier specific configuration*] using a digital signature by the manufacturer prior to installing those updates.

##### FPT\_TUD\_EXT.2.2

The TSF shall [*update only by verified software*] the TSF boot integrity [*key, hash*].

##### FPT\_TUD\_EXT.2.3

The TSF shall verify that the digital signature verification key used for TSF updates [*is validated to a public key in the Trust Anchor Database*].

#### FPT\_TUD\_EXT.2.4

The TSF shall verify mobile application software using a digital signature mechanism prior to installation.

#### FPT\_TUD\_EXT.2.7

The TSF shall verify that software updates to the TSF are a current or later version than the current version of the TSF.

---

### 5.1.7 TOE access (FTA)

#### 5.1.7.1 Extended: TSF- and User-initiated locked state (FTA\_SSL\_EXT.1)

##### FTA\_SSL\_EXT.1.1

The TSF shall transition to a locked state after a time interval of inactivity.

##### FTA\_SSL\_EXT.1.2

The TSF shall transition to a locked state after initiation by either the user or the administrator.

##### FTA\_SSL\_EXT.1.3

The TSF shall, upon transitioning to the locked state, perform the following operations:

- a) clearing or overwriting display devices, obscuring the previous contents;
- b) [no other actions].

---

#### 5.1.7.2 Default TOE Access Banners (FTA\_TAB.1)

##### FTA\_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

---

#### 5.1.7.3 Extended: Wireless Network Access (FTA\_WSE\_EXT.1)

##### FTA\_WSE\_EXT.1.1

The TSF shall be able to attempt connections to wireless networks specified as acceptable networks as configured by the administrator in FMT\_SMF\_EXT.1.

---

### 5.1.8 Trusted path/channels (FTP)

#### 5.1.8.1 Extended: Trusted channel Communication (FTP\_ITC\_EXT.1)

##### FTP\_ITC\_EXT.1.1

The TSF shall use 802.11-2012, 802.1X, and EAP-TLS and [IPsec and TLS] to provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels, provides assured identification of its end points, protects channel data from disclosure, and detects modification of the channel data.

##### FTP\_ITC\_EXT.1.2

The TSF shall permit the TSF to initiate communication via the trusted channel.

##### FTP\_ITC\_EXT.1.3

The TSF shall initiate communication via the trusted channel for wireless access point connections, administrative communication, configured enterprise connections, and [no other connections].

---

## 5.2 TOE Security Assurance Requirements

The SARs for the TOE are the EAL 1 augmented with ALC\_TSU\_EXT.1 components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
<b>ADV: Development</b>	ADV_FSP.1: Basic functional specification
<b>AGD: Guidance documents</b>	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
<b>ALC: Life-cycle support</b>	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM coverage
	ALC_TSU_EXT.1: Timely Security Updates
<b>ATE: Tests</b>	ATE_IND.1: Independent testing - conformance
<b>AVA: Vulnerability assessment</b>	AVA_VAN.1: Vulnerability survey

**Table 3 EAL 1 augmented with ALC\_TSU\_EXT.1 Assurance Components**

## 5.2.1 Development (ADV)

### 5.2.1.1 Basic functional specification (ADV\_FSP.1)

#### ADV\_FSP.1.1d

The developer shall provide a functional specification.

#### ADV\_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

#### ADV\_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

#### ADV\_FSP.1.2c

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

#### ADV\_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

#### ADV\_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

#### ADV\_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### ADV\_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

## 5.2.2 Guidance documents (AGD)

### 5.2.2.1 Operational user guidance (AGD\_OPE.1)

#### AGD\_OPE.1.1d

The developer shall provide operational user guidance.

#### AGD\_OPE.1.1c

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

**AGD\_OPE.1.2c**

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

**AGD\_OPE.1.3c**

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

**AGD\_OPE.1.4c**

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

**AGD\_OPE.1.5c**

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

**AGD\_OPE.1.6c**

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

**AGD\_OPE.1.7c**

The operational user guidance shall be clear and reasonable.

**AGD\_OPE.1.1e**

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

---

**5.2.2.2 Preparative procedures (AGD\_PRE.1)**

---

**AGD\_PRE.1.1d**

The developer shall provide the TOE including its preparative procedures.

**AGD\_PRE.1.1c**

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

**AGD\_PRE.1.2c**

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

**AGD\_PRE.1.1e**

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AGD\_PRE.1.2e**

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

---

**5.2.3 Life-cycle support (ALC)**

---

**5.2.3.1 Labelling of the TOE (ALC\_CMC.1)**

---

**ALC\_CMC.1.1d**

The developer shall provide the TOE and a reference for the TOE.

**ALC\_CMC.1.1c**

The TOE shall be labelled with its unique reference.

**ALC\_CMC.1.1e**

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

---

### 5.2.3.2 TOE CM coverage (ALC\_CMS.1)

---

#### ALC\_CMS.2.1d

The developer shall provide a configuration list for the TOE.

#### ALC\_CMS.2.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

#### ALC\_CMS.2.2c

The configuration list shall uniquely identify the configuration items.

#### ALC\_CMS.2.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

---

### 5.2.3.3 Timely Security Updates (ALC\_TSU\_EXT.1)

---

#### ALC\_TSU\_EXT.1.1d

The developer shall provide a description in the TSS of how timely security updates are made to the TOE.

#### ALC\_TSU\_EXT.1.1c

The description shall include the process for creating and deploying security updates for the TOE software/firmware.

#### ALC\_TSU\_EXT.1.2c

The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.

#### ALC\_TSU\_EXT.1.3c

The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.

#### ALC\_TSU\_EXT.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

---

### 5.2.4 Tests (ATE)

#### 5.2.4.1 Independent testing - conformance (ATE\_IND.1)

---

##### ATE\_IND.1.1d

The developer shall provide the TOE for testing.

##### ATE\_IND.1.1c

The TOE shall be suitable for testing.

##### ATE\_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

##### ATE\_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

---

### 5.2.5 Vulnerability assessment (AVA)

#### 5.2.5.1 Vulnerability survey (AVA\_VAN.1)

---

##### AVA\_VAN.1.1d

The developer shall provide the TOE for testing.

##### AVA\_VAN.1.1c

The TOE shall be suitable for testing.



**AVA\_VAN.1.1e**

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AVA\_VAN.1.2e**

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

**AVA\_VAN.1.3e**

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

## 6. TOE Summary Specification

This chapter describes the security functions:

- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels
- Security Audit

### 6.1 Cryptographic support

**FCS\_CKM.1(1):** The TOE supports asymmetric key generation for all types in accordance with FIPS 186-4. The TOE generates RSA in its SCrypto library generated and DH/ECDH/ECDSA (including P-521) keys in both its SCrypto and BoringSSL libraries. The TOE supports generating keys with a security strength of 112-bits and larger, thus supports 2048-bit RSA and DH keys, and 256-bit ECDH/ECDSA keys. The TOE's RSA and ECDSA implementation have the CAVP certificates described in the FCS\_COP.1 section below.

**FCS\_CKM.1(2):** The TOE adheres to 802.11-2012 for key generation. The TOE's wpa\_supplicant provides the PRF384 for WPA2 derivation of 128-bit AES Temporal Key and also employs its BoringSSL AES-256 DRBG when generating random values use in the EAP-TLS and 802.11 4-way handshake. The TOE has been designed for compliance, and the Device has successfully completed certification (including WPA2 Enterprise) and received WiFi CERTIFIED Interoperability Certificates from the WiFi Alliance. The WiFi Alliance maintains a website providing further information about the testing program: <http://www.wi-fi.org/certification>

Device Name	Model Number	WFA Certificate #'s
Galaxy Note 7	SM-N930x	65738, 65739, 66000, 66146, 66150, 66151, 66152, 66153, 66154, 66155, 66156, 66157, 66158, 66159, 66161, 66347, 66348, 66349, 66350, 66368, 66389, 66390, 66391, 66393, 66394, 66395, 66682

**FCS\_CKM.2(1):** The TOE supports RSA (800-56B), DHE (FFC 800-56A), and ECDHE (ECC 800-56A) methods in TLS key establishment/exchange. The TOE has CVL KAS and ECDSA CAVP algorithm certificates for Elliptic Curve key establishment and key generation respectively as described in the FCS\_COP.1 section below. The TOE has an RSA CAVP algorithm certificate for RSA key generation and for RSA key establishment as described in the FCS\_COP.1 section below (in addition Samsung vendor-affirms the TOE's RSA key establishment follows 800-56B). The user and administrator need take no special configuration of the TOE as the TOE automatically generates the keys needed for negotiated TLS ciphersuite. Because the TOE only acts as a TLS client, the TOE only performs 800-56B encryption (specifically the encryption of the Pre-Master Secret using the Server's RSA public key) when participating in TLS\_RSA\_\* based TLS handshakes. Thus, the TOE does not perform 800-56B decryption. However, the TOE's TLS client correctly handles other cryptographic errors (for example, invalid checksums, incorrect certificate types, corrupted certificates) by sending a TLS fatal alert.

**FCS\_CKM.2(2):** The TOE adheres to RFC 3394, SP 800-38F, and 802.11-2012 standards and unwraps the GTK (sent encrypted with the WPA2 KEK using AES Key Wrap in an EAPOL-Key frame). The TOE, upon receiving an

EAPOL frame, will subject the frame to a number of checks (frame length, EAPOL version, frame payload size, EAPOL-Key type, key data length, EAPOL-Key CCMP descriptor version, and replay counter) to ensure a proper EAPOL message and then decrypt the GTK using the KEK, thus ensuring that it does not expose the Group Temporal Key (GTK).

**FCS\_CKM\_EXT.1:** The TOE supports a Root Encryption Key (REK) within the main (application) processor. Requests for encryption or decryption chaining to the REK are only accessible through the Trusted Execution Environment, or TEE (TrustZone). The REK lies in a series of 256-bit fuses, which the TOE programs during manufacturing. The TEE does not allow direct access to the REK but provides access to use a Trusted Application (Trustlet) specific derived HEK (Hardware Encryption Key, which is derived from the REK through a KDF function) for encryption and decryption.

The REK value is generated during manufacturing either by the TOE (if it detects that the REK fuses have not been set) using its hardware DRBG or is generated during fabrication using an external RBG that meets the requirements of this PP in that the process utilizes a SHA-256 Hash\_DRBG seeded by a hardware entropy source identical in architecture to that within the TOE. This fabrication process includes strict controls (including physical and logical access control to the manufacturing room where programming takes place as well as video surveillance and access only to specific, authorized, trusted individuals) to ensure that fabricator cannot access any REK values between generation and programming.

**FCS\_CKM\_EXT.2:** The TOE supports Data Encryption Key (DEK) generation using its approved RBGs. The TOE generates AES 256-bit DEKs using its BoringSSL CTR\_DRBG in response to an application through either the Android Java API (for Android applications) or through the native C API (used internally by the TSF). For example, the ODE (Onboard Device Encryption, responsible for encryption/decryption of the user data partition) obtains random data using the native C API.

**FCS\_CKM\_EXT.3:** The TOE generates KEKs (which are always AES 256-bit keys generated by either the BoringSSL CTR\_DRBG or Kernel Crypto's HMAC\_DRBG) through a combination of methods. First, the TOE generates a KEK (denoted as a Domain KEK, or DKEK) for each user of the TOE, for each Domain (where a Domain provides separation of application data, e.g., "Corporate" or "Home"). Note that the current TOE only supports a single Domain for each user.

The TOE generates a number of different KEKs. In addition to the DKEK, applications may request key generation (either through the Android/Java APIs), and the TOE utilizes its BoringSSL CTR\_DRBG to satisfy those requests. The requesting application ultimately chooses whether to use that key as a DEK or a KEK (and can choose whether it wishes that key to be 128 or 256-bits), but it is worth mentioning here, as an application can utilize such a key as a KEK, should it choose.

**FCS\_CKM\_EXT.4:** The TOE destroys cryptographic keys when they are no longer in use by the system. The exceptions to this are public keys (that protect the boot chain and software updates) and the REK, which are never cleared. Keys stored in RAM during use are destroyed by a zero overwrite. Keys stored in Flash (i.e. eMMC) are destroyed by cryptographic erasure through a BLKSECDISCARD command (as defined in the JEDEC eMMC 5.0 specification, JESD84-B50) to the flash controller for the location where the ODE and SD Card keys are stored. Once these are erased, all keys (and data) stored within the encrypted data partition of the TOE are considered cryptographically erased.

**FCS\_CKM\_EXT.5:** The TOE provides a TOE Wipe function that first erases the encrypted ODE DEK used to encrypt the entire data partition using a Secure Trim command to ensure that TOE writes zeros to the eMMC blocks containing the encrypted ODE DEK (the crypto footer contains the encrypted ODE DKEK and encrypted ODE DEK as well as the encrypted SDCard DKEK and encrypted SDCard MKs). After overwriting that, the TOE will reformat the partition. Upon completion of reformatting the Flash partition holding user data, the TOE will perform a power-cycle.

**FCS\_CKM\_EXT.6:** The TOE creates salt and nonces (which are just salt values used in WPA2) using its AES-256 CTR\_DRBG.

Salt value and size	RBG origin	Salt storage location
User password salt (256-bit)	BoringSSL's AES-256 CTR_DRBG	Flash filesystem

TLS client_random (256-bit)	BoringSSL's AES-256 CTR_DRBG	N/A (ephemeral)
TLS pre_master_secret (384-bit)	BoringSSL's AES-256 CTR_DRBG	N/A (ephemeral)
TLS DHE/ECDHE private value (256, 384, 512)	BoringSSL's AES-256 CTR_DRBG	N/A (ephemeral)
WPA2 4-way handshake supplicant nonce (SNonce)	BoringSSL's AES-256 CTR_DRBG through wpa_supplicant	N/A (ephemeral)

**FCS\_COP.1:** The TOE performs cryptographic algorithms in accordance with the following NIST standards and has received the following CAVP algorithm certificates.

The BoringSSL library provides the following algorithms

Algorithm	NIST Standard	SFR Reference	Cert#
AES 128/256 CBC, CCM, GCM, KW	FIPS 197, SP 800-38A/C/D/F	FCS_COP.1(1)	3917
CVL ECC/FFC	SP 800-56A	FCS_CKM.1(1)	802
CVL ECC CDH P-224/256/384/521	SP 800-56A	FCS_CKM.1(1)	777
DSA FFC Key Gen	FIPS 186-4	FCS_CKM.1(1)	1071
DRBG CTR	SP 800-90A	FCS_RBG_EXT.1(1)	1132
ECDSA PKG/PKV/SigGen/SigVer	FIPS 186-4	FCS_CKM.1(1) FCS_CKM.2(1) FCS_COP.1(3)	857
HMAC SHA-1/256/384/512	FIPS 198-1 & 180-4	FCS_COP.1(4)	2545
RSA SIG(gen)/SIG(ver)	FIPS 186-4	FCS_COP.1(3)	2000
SHS SHA-1/256/384/512	FIPS 180-4	FCS_COP.1(2)	3227

**Table 4 BoringSSL Cryptographic Algorithms**

The Samsung Kernel Cryptographic (“Kernel Crypto”) Module provides the following algorithms

Algorithm	NIST Standard	SFR Reference	Cert#
AES 128/256 CBC	FIPS 197, SP 800-38A	FCS_COP.1(1)	3837
HMAC SHA-1/256/384/512	FIPS 198-1 & 180-4	FCS_COP.1(4)	2488
DRBG SHA-256 HMAC_DRBG	SP 800-90A	FCS_RBG_EXT.1(2)	1083
SHS SHA-1/256/384/512	FIPS 180-4	FCS_COP.1(2)	3161

**Table 5 Samsung Kernel Cryptographic Algorithms**

The Samsung SCrypto TEE library provides the following algorithms

Algorithm	NIST Standard	SFR Reference	Cert#’s
AES	FIPS 197, SP 800-38	FCS_COP.1(1)	3887, 3888
CVL ECC CDH	SP 800-56A	FCS_CKM.1(1)	752, 753
DRBG	SP 800-90A	FCS_RBG_EXT.1(1)	1111, 1112
ECDSA	FIPS 186-4	FCS_CKM.1(1) FCS_CKM.2(1) FCS_COP.1(3)	842, 843
HMAC SHA	FIPS 198-1 & 180-4	FCS_COP.1(4)	2525, 2526
RSA	FIPS 186-2	FCS_CKM.1(1) FCS_CKM.2(1) FCS_COP.1(3)	1981, 1982
SHS	FIPS 180-4	FCS_COP.1(2)	3207, 3208

**Table 6 SCrypto TEE Cryptographic Algorithms**

The Chipset hardware provides the following algorithms

Algorithm	NIST Standard	SFR Reference	Cert#’s
AES 128/256 CBC, XTS	FIPS 197, SP 800-38A	FCS_COP.1(1)	3839/3556, 3558

**Table 7 Chipset Hardware Cryptographic Algorithms**

The TOE’s application processors include hardware entropy implementations that supply random data within the TEE and to the Linux kernel RNG (/dev/random).

Note that kernel-space system applications utilize the cryptographic algorithm implementations in the Samsung Kernel Cryptographic Module (Kernel Crypto) or in the Chipset hardware, while user-space system applications and mobile applications utilize the BoringSSL library (either through a Java API or through the native C API). In the case of each cryptographic library, the library itself includes any algorithms required (for example, BoringSSL provides hash functions for use by HMAC and digital signature algorithms).

Trusted Applications executing with the Trusted Execution Environment (TEE) utilize the SCrypto library. For example, the trusted application implementing the Android KeyMaster that supports the Android Key Store utilizes the SCrypto library for all of its cryptographic functionality.

For its HMAC implementations, the TOE accepts all key sizes of 160, 256, 384, & 512; supports all SHA sizes save 224 (e.g., SHA-1, 256, 384, & 512), utilizes the specified block size (512 for SHA-1 and 256, and 1024 for SHA-384 & 512), and output MAC lengths of 160, 256, 384, and 512.

The TOE conditions the user’s password exactly as per SP 800-132 (and thus as per SP 800-197-1) with no deviations by using PBKDF2 with 16,384 HMAC-SHA-512 iterations to combine a 128-bit salt with the user’s password. The time needed to derive keying material does not impact or lessen the difficulty faced by an attacker’s exhaustive guessing as the combination of the password derived KEK with REK value entirely prevents offline attacks and the TOE’s maximum incorrect login attempts (between 1 and 10 incorrect attempts with 6 character, minimum, passwords) prevents exhaustive online attacks.

The TOE’s algorithm certificates represent the BoringSSL library, Kernel Cryptographic module, SCrypto library, and Chipset hardware implementations. These implementations have been tested upon Android 6.0.1 (Marshmallow) running atop both Exynos and Qualcomm ARMv8 chipsets. The TOE’s Exynos 8890 processor includes the Samsung Flash Memory Protector (FMP V3.0) described in AES certificates 3839, while the TOE’s Qualcomm MSM8996 (known as the “Snapdragon 820”) includes hardware AES XTS (Inline Crypto Engine, ICE) implementations for encryption and decryption.

**FCS\_HTTPS\_EXT.1:** The TOE includes the ability to support the HTTPS protocol (compliant with RFC 2818) so that (mobile and system client) applications executing on the TOE can securely connect to external servers using HTTPS. Administrators have no credentials and cannot use HTTPS or TLS to establish administrative sessions with the TOE as the TOE does not provide any such capabilities.

**FCS\_IV\_EXT.1:** The TOE generates IVs for data storage encryption and for key storage encryption. The TOE uses AES-XTS and AES-CBC mode for data encryption and AES-GCM for key storage.

**FCS\_RBG\_EXT.1:** The TOE provides a number of different RBGs including

1. An AES-256 CTR\_DRBG provided by BoringSSL. The TOE provides mobile applications access (through an Android Java API) to random data drawn from its AES-256 CTR\_DRBG.
2. An AES-256 CTR\_DRBG provided by SCrypto
3. A SHA-256 HMAC\_DRBG provided by Kernel Crypto
4. A hardware SHA-256 Hash\_DRBG provided by the Qualcomm AP

The TOE ensures that it initializes each RBG with sufficient entropy ultimately accumulated from a TOE-hardware-based noise source. The TOE uses its hardware-based noise source to continuously fill /dev/random with random data with full entropy, and in turn, the TOE draws from /dev/random to seed both of its AES-256 CTR\_DRBG and

its SHA-256 HMAC\_DRBG. The TOE seeds each of its AES-256 CTR\_DRBGs using 384-bits of data from /dev/random, thus ensuring at least 256-bits of entropy. Finally the TOE seeds its SHA-256 HMAC\_DRBG with 440-bits of data from /dev/random, also ensuring that it contains at least 256-bits of entropy.

**FCS\_SRV\_EXT.1:** The TOE provides applications access to the cryptographic operations including encryption (AES), hashing (SHA), signing and verification (RSA & ECDSA), key hashing (HMAC), password-based key-derivation functions (PKBDFv2 HMAC-SHA-512), generate asymmetric keys for key establishment (RSA, DH, and ECDH), and generate asymmetric keys for signature generation and verification (RSA, ECDSA). The TOE provides access through the Android operating system’s Java API, through the native BoringSSL API, and through the kernel. The vendor also developed testing applications to enable execution of the NIST algorithm testing suite in order to verify the correctness of the algorithm implementations.

**FCS\_STG\_EXT.1:** The TOE provides users and applications running on the TOE the ability to generate, import, and securely store symmetric and asymmetric keys through the TOE’s Android Key Store. The TOE allows a user to import a certificate (in PKCS#12 [PFX] format) and provides applications running on the TOE an API to import a certificate or secret key. In either case, the TOE will place the key into the user’s key store (and the TOE will remove the PKCS#12 password-based protection if the imported key is a certificate) and doubly encrypt the imported key with DEKs, which in turn are encrypted by a KEK derived from the user’s DKEK and a KEK derived from the REK. All user and application keys placed into the user’s keystore are secured in this fashion. Note that while operating in CC mode, the TOE also encrypts (using ODE) the Flash filesystem in which all keystore blobs reside (as encrypted files), providing yet another layer of encryption protection to keystore objects.

The user of the TOE can elect to delete keys from the keystore, as well as to securely wipe the entire device.

The TOE affords applications control (control over use and destruction) of keys that they create or import, and only the user or a common application developer can explicitly authorize access, use, or destruction of one application’s key by any other application.

Entity	Can import?	Can destroy?	Allow other app to use?	Allow other app to destroy
User	Yes	Yes	Yes	
Administrator	Yes	Yes		
Mobile application	Yes	Yes		
Common application developer			Yes	Yes

**FCS\_STG\_EXT.2:** The TOE provides protection for all stored keys (i.e. those written to storage media for persistent storage) chained to both the user’s password and the REK. All keys are encrypted with AES-GCM or AES-CBC (in the case of SD card File Encryption Keys). All KEKs are 256-bit, ensuring that that the TOE encrypts every key with another key of equal or greater strength/size.

In the case of WiFi, the TOE utilizes the 802.11-2012 KCK and KEK keys to unwrap (decrypt) the WPA2 Group Temporal Key received from the access point. Additionally, the TOE protects persistent WiFi keys (user certificates) by storing them in the Android Key Store.

**FCS\_STG\_EXT.3:** The key hierarchy shows AES-256 GCM is used to encrypt all KEKs and the GCM encryption mode itself ensures integrity as authenticated decryption operations fail if the encrypted KEK becomes corrupted.

**FCS\_TLSC\_EXT.1:** The TSF supports TLS versions 1.0, 1.1, and 1.2 with client (mutual) authentication and supports all sixteen ciphersuites (see the selections in section 5.1.2.23) for use with EAP-TLS as part of WPA2. The TOE, by design, supports only evaluated elliptic curves (P-256, P-384, & P-521 and no others) and requires/allows no configuration of the supported curves.

**FCS\_TLS\_EXT.2:** The TOE provides mobile applications (through its Android API) the use of TLS versions 1.0, 1.1, and 1.2 including support for all sixteen selectable ciphersuites (see the selections in section 5.1.2.24). The TOE supports Common Name (CN) and Subject Alternative Name (SAN) (DNS and IP address) as reference identifiers. The TOE supports client (mutual) authentication. The TOE, by design, supports only evaluated elliptic curves (P-256, P-384, & P-521 and no others) and requires/allows no configuration of the supported curves. While



the TOE supports the use of wildcards in X.509 reference identifiers (CN and SAN), the TOE does not support certificate pinning.

## 6.2 User data protection

### FDP\_ACF\_EXT.1:

The TOE provides the following categories of system services to applications.

1. normal – A lower-risk permission that gives an application access to isolated application-level features, with minimal risk to other applications, the system, or the user. The system automatically grants this type of permission to a requesting application at installation, without asking for the user's explicit approval (though the user always has the option to review these permissions before installing).
2. dangerous – A higher-risk permission that would give a requesting application access to private user data or control over the device that can negatively impact the user. Because this type of permission introduces potential risk, the system may not automatically grant it to the requesting application. For example, any dangerous permissions requested by an application may be displayed to the user and require confirmation before proceeding, or some other approach may be taken to avoid the user automatically allowing the use of such facilities.
3. signature – A permission that the system is to grant only if the requesting application is signed with the same certificate as the application that declared the permission. If the certificates match, the system automatically grants the permission without notifying the user or asking for the user's explicit approval.
4. signatureOrSystem – A permission that the system is to grant only to packages in the Android system image *or* that are signed with the same certificates. Please avoid using this option, as the signature protection level should be sufficient for most needs and works regardless of exactly where applications are installed. This permission is used for certain special situations where multiple vendors have applications built in to a system image which need to share specific features explicitly because they are being built together.

An example of a normal permission is the ability to vibrate the device: `android.permission.VIBRATE`. This permission allows an application to make the device vibrate, and an application that does not declare this permission would have its vibration requests ignored.

An example of a dangerous privilege would be access to location services to determine the location of the mobile device: `android.permission.ACCESS_FINE_LOCATION`. The TOE controls access to Dangerous permissions during the installation of the application. The TOE prompts the user to review the application's requested permissions (by displaying a description of each permission group, into which individual permissions map, that an application requested access to). If the user approves, then the mobile device continues with the installation of the application. Thereafter, the mobile device grants that application during execution access to the set of permissions declared in its Manifest file.

An example of a signature permission is the `android.permission.BIND_VPN_SERVICE`, that an application must declare in order to utilize the VpnService APIs of the device. Because the permission is a Signature permission, the mobile device only grants this permission to an application that requests this permission *and* that has been signed with the same developer key used to sign the application declaring the permission (in the case of the example, the Android Framework itself).

An example of a systemOrSignature permission is the `android.permission.LOCATION_HARDWARE`, which allows an application to use location features in hardware (such as the geofencing API). The device grants this permission to requesting applications that either have been signed with the same developer key used to sign the android application declaring the permissions or that reside in the "system" directory within Android, which for Android 4.4 and above, are applications residing in the `/system/priv-app/` directory on the read-only system partition). Put another way, the device grants systemOrSignature permissions by Signature or by virtue of the requesting application being part of the "system image."

Additionally, Android includes the following flags that layer atop the base categories.

1. privileged – this permission can also be granted to any applications installed as privileged apps on the system image. Please avoid using this option, as the signature protection level should be sufficient for most needs and works regardless of exactly where applications are installed. This permission flag is used for certain special situations where multiple vendors have applications built in to a system image which need to share specific features explicitly because they are being built together.
2. system – Old synonym for "privileged".
3. development – this permission can also (optionally) be granted to development applications (e.g., to allow additional location reporting during beta testing).
4. appop – this permission is closely associated with an app op for controlling access.
5. pre23 - this permission can be automatically granted to apps that target API levels below API level 23 (Marshmallow/6.0).
6. installer - this permission can be automatically granted to system apps that install packages.
7. verifier- this permission can be automatically granted to system apps that verify packages.
8. preinstalled – this permission can be automatically granted any application pre-installed on the system image (not just privileged apps) (the TOE does not prompt the user to approve the permission).

For older applications (those targeting Android’s pre-23 API level, i.e., API level 22 [lollipop] and below), the TOE will prompt a user at the time of application installation whether they agree to grant the application access to the requested services. Thereafter (each time the application is run), the TOE will grant the application access to the services specified during install.

For newer applications (those targeting API level 23 or later), the TOE grants individual permissions at application run-time by prompting the user for confirmation of each permissions category requested by the application (and only granting the permission if the user chooses to grant it).

The Android 6.0 (Level 23) API, found here <https://developer.android.com/about/versions/marshmallow/android-6.0.html> provides a description of the services available to mobile applications, and the below table lists those services requiring an application to request privileges in order to utilize those permissions:

Permission	ProtectionLevel Description
android.permission.ACCESS_CACHE_FILESYSTEM	signature
android.permission.ACCESS_CHECKIN_PROPERTIES	signature
android.permission.ACCESS_COARSE_LOCATION	dangerous
android.permission.ACCESS_CONTENT_PROVIDERS_EXTERNALLY	signature
android.permission.ACCESS_IMS_CALL_SERVICE	signature system
android.permission.ACCESS_INPUT_FLINGER	signature
android.permission.ACCESS_KEYGUARD_SECURE_STORAGE	signature
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	normal
android.permission.ACCESS_MOCK_LOCATION	signature
android.permission.ACCESS_MTP	signature
android.permission.ACCESS_NETWORK_CONDITIONS	signature
android.permission.ACCESS_NETWORK_STATE	normal
android.permission.ACCESS_NOTIFICATION_POLICY	normal
android.permission.ACCESS_NOTIFICATIONS	signature
android.permission.ACCESS_SURFACE_FLINGER	signature
android.permission.ACCESS_VOICE_INTERACTION_SERVICE	signature
android.permission.ACCESS_WIFI_STATE	normal
android.permission.ACCESS_WIMAX_STATE	normal
android.permission.ACCOUNT_MANAGER	signature
android.permission.ALLOW_ANY_CODEC_FOR_PLAYBACK	signature
android.permission.ASEC_ACCESS	signature
android.permission.ASEC_CREATE	signature
android.permission.ASEC_DESTROY	signature



Permission	ProtectionLevel Description
android.permission.ASEC_MOUNT_UNMOUNT	signature
android.permission.ASEC_RENAME	signature
android.permission.BACKUP	signature
android.permission.BATTERY_STATS	signature
android.permission.BIND_ACCESSIBILITY_SERVICE	signature
android.permission.BIND_APPWIDGET	signature
android.permission.BIND_CARRIER_SERVICES	signature
android.permission.BIND_CHOOSER_TARGET_SERVICE	signature
android.permission.BIND_DEVICE_ADMIN	signature
android.permission.BIND_DIRECTORY_SEARCH	signature system
android.permission.BIND_INCALL_SERVICE	system signature
android.permission.BIND_INPUT_METHOD	signature
android.permission.BIND_INTENT_FILTER_VERIFIER	signature
android.permission.BIND_KEYGUARD_APPWIDGET	signature
android.permission.BIND_MIDI_DEVICE_SERVICE	signature
android.permission.BIND_NFC_SERVICE	signature
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	signature
android.permission.BIND_PACKAGE_VERIFIER	signature
android.permission.BIND_PRINT_SERVICE	signature
android.permission.BIND_PRINT_SPOOLER_SERVICE	signature
android.permission.BIND_REMOTE_DISPLAY	signature
android.permission.BIND_REMOTEVIEWS	signature
android.permission.BIND_ROUTE_PROVIDER	signature
android.permission.BIND_TELECOM_CONNECTION_SERVICE	system signature
android.permission.BIND_TEXT_SERVICE	signature
android.permission.BIND_VOICE_INTERACTION	signature
android.permission.BIND_VPN_SERVICE	signature
android.permission.BIND_WALLPAPER	signature
android.permission.BLUETOOTH	normal
android.permission.BLUETOOTH_ADMIN	normal
android.permission.BLUETOOTH_MAP	signature
android.permission.BLUETOOTH_PRIVILEGED	system signature
android.permission.BLUETOOTH_STACK	signature
android.permission.BODY_SENSORS	dangerous
android.permission.BROADCAST_PACKAGE_REMOVED	signature
android.permission.BROADCAST_SMS	signature
android.permission.BROADCAST_STICKY	normal
android.permission.BROADCAST_WAP_PUSH	signature
android.permission.CALL_PHONE	dangerous
android.permission.CALL_PRIVILEGED	signature
android.permission.CAMERA	dangerous
android.permission.CAMERA_DISABLE_TRANSMIT_LED	signature
android.permission.CAMERA_SEND_SYSTEM_EVENTS	signature
android.permission.CAPTURE_AUDIO_HOTWORD	signature
android.permission.CAPTURE_AUDIO_OUTPUT	signature
android.permission.CAPTURE_SECURE_VIDEO_OUTPUT	signature
android.permission.CAPTURE_VIDEO_OUTPUT	signature
android.permission.CHANGE_APP_IDLE_STATE	signature
android.permission.CHANGE_BACKGROUND_DATA_SETTING	signature
android.permission.CHANGE_COMPONENT_ENABLED_STATE	signature
android.permission.CHANGE_CONFIGURATION_checkPermission	signature
android.permission.CHANGE_DEVICE_IDLE_TEMP_WHITELIST	system signature

Permission	ProtectionLevel Description
android.permission.CHANGE_NETWORK_STATE	normal
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal
android.permission.CHANGE_WIFI_STATE	normal
android.permission.CHANGE_WIMAX_STATE	normal
android.permission.CLEAR_APP_CACHE	signature
android.permission.CLEAR_APP_USER_DATA	signature
android.permission.CONFIGURE_WIFI_DISPLAY	signature
android.permission.CONFIRM_FULL_BACKUP	signature
android.permission.CONNECTIVITY_INTERNAL	signature
android.permission.CONTROL_KEYGUARD_checkPermission	signature
android.permission.CONTROL_LOCATION_UPDATES	signature
android.permission.CONTROL_WIFI_DISPLAY	signature
android.permission.COPY_PROTECTED_DATA	signature
android.permission.CRYPT_KEEPER	signature
android.permission.DELETE_CACHE_FILES	signature
android.permission.DELETE_PACKAGES	signature
android.permission.DEVICE_POWER	signature
android.permission.DIAGNOSTIC	signature
android.permission.DISABLE_KEYGUARD	normal
android.permission.DISPATCH_NFC_MESSAGE	signature
android.permission.DUMP	signature
android.permission.DVB_DEVICE	signature
android.permission.EXPAND_STATUS_BAR	normal
android.permission.FACTORY_TEST	signature
android.permission.FILTER_EVENTS	signature
android.permission.FLASHLIGHT	normal
android.permission.FORCE_BACK	signature
android.permission.FORCE_STOP_PACKAGES	signature
android.permission.FREEZE_SCREEN	signature
android.permission.GET_ACCOUNTS_checkPermission	dangerous
android.permission.GET_ACCOUNTS_PRIVILEGED	signature
android.permission.GET_APP_OPS_STATS	signature
android.permission.GET_DETAILED_TASKS	signature
android.permission.GET_PACKAGE_IMPORTANCE	signature
android.permission.GET_PACKAGE_SIZE	normal
android.permission.GET_TOP_ACTIVITY_INFO	signature
android.permission.GLOBAL_SEARCH	signature
android.permission.GLOBAL_SEARCH_CONTROL	signature
android.permission.GRANT_REVOKE_PERMISSIONS	signature
android.permission.GRANT_RUNTIME_PERMISSIONS_checkPermission	signature
android.permission.HARDWARE_TEST	signature
android.permission.HDMI_CEC	signature
android.permission.INJECT_EVENTS	signature
android.permission.INSTALL_LOCATION_PROVIDER	signature system
android.permission.INSTALL_PACKAGES	signature
android.permission.INTENT_FILTER_VERIFICATION_AGENT	signature
android.permission.INTERACT_ACROSS_USERS	signature
android.permission.INTERACT_ACROSS_USERS_FULL	signature
android.permission.INTERNAL_SYSTEM_WINDOW	signature
android.permission.INTERNET	normal
android.permission.INVOKE_CARRIER_SETUP	signature
android.permission.KILL_BACKGROUND_PROCESSES	normal

Permission	ProtectionLevel Description
android.permission.KILL_UID	signature
android.permission.LOCAL_MAC_ADDRESS	signature
android.permission.LOCATION_HARDWARE	signature
android.permission.LOOP_RADIO	signature
android.permission.MANAGE_ACTIVITY_STACKS	signature
android.permission.MANAGE_APP_TOKENS	signature
android.permission.MANAGE_CA_CERTIFICATES	signature
android.permission.MANAGE_DEVICE_ADMINS	signature
android.permission.MANAGE_DOCUMENTS	signature
android.permission.MANAGE_FINGERPRINT	system   signature
android.permission.MANAGE_NETWORK_POLICY	signature
android.permission.MANAGE_PROFILE_AND_DEVICE_OWNERS	signature
android.permission.MANAGE_USB	signature
android.permission.MANAGE_USERS	signature
android.permission.MANAGE_VOICE_KEYPHRASES	signature
android.permission.MEDIA_CONTENT_CONTROL	signature
android.permission.MODIFY_APPWIDGET_BIND_PERMISSIONS	signature
android.permission.MODIFY_AUDIO_SETTINGS	normal
android.permission.MODIFY_NETWORK_ACCOUNTING	signature
android.permission.MODIFY_PHONE_STATE	signature
android.permission.MOUNT_FORMAT_FILESYSTEMS	system   signature
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	system   signature
android.permission.MOVE_PACKAGE	signature
android.permission.NET_ADMIN	signature
android.permission.NET_TUNNELING	signature
android.permission.NFC	normal
android.permission.NFC_TRANSACTION	dangerous
android.permission.NOTIFY_PENDING_SYSTEM_UPDATE	signature
android.permission.OBSERVE_GRANT_REVOKE_PERMISSIONS	signature
android.permission.OEM_UNLOCK_STATE	signature
android.permission.OVERRIDE_WIFI_CONFIG	signature
android.permission.PACKAGE_USAGE_STATS	signature   appop
android.permission.PACKAGE_VERIFICATION_AGENT	signature
android.permission.PEERS_MAC_ADDRESS	signature
android.permission.PERFORM_CDMA_PROVISIONING	signature
android.permission.PERFORM_SIM_ACTIVATION	signature
android.permission.PERSISTENT_ACTIVITY	normal
android.permission.PROCESS_OUTGOING_CALLS	dangerous
android.permission.QUERY_DO_NOT_ASK_CREDENTIALS_ON_BOOT	signature
android.permission.READ_CALENDAR	dangerous
android.permission.READ_CALL_LOG	dangerous
android.permission.READ_CELL_BROADCASTS	dangerous
android.permission.READ_CONTACTS	dangerous
android.permission.READ_DREAM_STATE	signature
android.permission.READ_EXTERNAL_STORAGE	dangerous
android.permission.READ_FRAME_BUFFER	signature
android.permission.READ_INPUT_STATE	signature
android.permission.READ_LOGS	signature
android.permission.READ_NETWORK_USAGE_HISTORY	signature
android.permission.READ_PHONE_STATE	dangerous
android.permission.READ_PRECISE_PHONE_STATE	signature
android.permission.READ_PRIVILEGED_PHONE_STATE	signature

Permission	ProtectionLevel Description
android.permission.READ_SEARCH_INDEXABLES	signature
android.permission.READ_SMS	dangerous
android.permission.READ_SYNC_SETTINGS	normal
android.permission.READ_SYNC_STATS	normal
android.permission.READ_WIFI_CREDENTIAL	signature
android.permission.REAL_GET_TASKS	signature
android.permission.REBOOT	signature
android.permission.RECEIVE_BLUETOOTH_MAP	signature
android.permission.RECEIVE_BOOT_COMPLETED	normal
android.permission.RECEIVE_DATA_ACTIVITY_CHANGE	signature
android.permission.RECEIVE_DIRECTED_SMS	signature   system
android.permission.RECEIVE_EMERGENCY_BROADCAST	signature
android.permission.RECEIVE_MMS	dangerous
android.permission.RECEIVE_SMS	dangerous
android.permission.RECEIVE_STK_COMMANDS	system   signature
android.permission.RECEIVE_WAP_PUSH	dangerous
android.permission.RECEIVE_WIFI_CREDENTIAL_CHANGE	signature
android.permission.RECORD_AUDIO	dangerous
android.permission.RECOVERY	signature
android.permission.REMOTE_AUDIO_PLAYBACK	signature
android.permission.REMOVE_TASKS	signature
android.permission.REORDER_TASKS	normal
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal
android.permission.REQUEST_INSTALL_PACKAGES	normal
android.permission.RESTART_PACKAGES	normal
android.permission.RETRIEVE_WINDOW_CONTENT	signature   privileged
android.permission.SCORE_NETWORKS	signature   system
android.permission.sec.BLUETOOTH_SECUREMODE_INTERNAL	signature   system
android.permission.sec.DLP_SERVICE_AGENT	signature
android.permission.sec.ENTERPRISE_CONTAINER	signature
android.permission.sec.ENTERPRISE_DEVICE_ADMIN	signature
android.permission.sec.MDM_ANALYTICS	signature
android.permission.sec.MDM_APN	signature
android.permission.sec.MDM_APP_BACKUP	signature
android.permission.sec.MDM_APP_MGMT	signature
android.permission.sec.MDM_APP_PERMISSION_MGMT	signature
android.permission.sec.MDM_AUDIT_LOG	signature
android.permission.sec.MDM_BLUETOOTH	signature
android.permission.sec.MDM_BLUETOOTH_SECUREMODE	signature
android.permission.sec.MDM_BROWSER_SETTINGS	signature
android.permission.sec.MDM_CALLING	signature
android.permission.sec.MDM_CERTIFICATE	signature
android.permission.sec.MDM_CONSTRAINED_INTERNAL	signature
android.permission.sec.MDM_DATE_TIME	signature
android.permission.sec.MDM_DUAL_SIM	signature
android.permission.sec.MDM_EMAIL	signature
android.permission.sec.MDM_ENTERPRISE_CONTAINER	signature
android.permission.sec.MDM_ENTERPRISE_SSO	signature
android.permission.sec.MDM_EXCHANGE	signature
android.permission.sec.MDM_FIREWALL	signature
android.permission.sec.MDM_GEOFENCING	signature
android.permission.sec.MDM_HW_CONTROL	signature

Permission	ProtectionLevel Description
android.permission.sec.MDM_INVENTORY	signature
android.permission.sec.MDM_KIOSK_MODE	signature
android.permission.sec.MDM_KIOSK_MODE_INTERNAL	signature
android.permission.sec.MDM_LDAP	signature
android.permission.sec.MDM_LDAP_INTERNAL	signature
android.permission.sec.MDM_LICENSE_INTERNAL	signature
android.permission.sec.MDM_LICENSE_LOG	signature
android.permission.sec.MDM_LOCATION	signature
android.permission.sec.MDM_LOCKSCREEN	signature
android.permission.sec.MDM_MULTI_USER_MGMT	signature
android.permission.sec.MDM_NOTIFY_ICCID_AVAILABLE	signature
android.permission.sec.MDM_PHONE_RESTRICTION	signature
android.permission.sec.MDM_REMOTE_CONTROL	signature
android.permission.sec.MDM_RESTRICTION	signature
android.permission.sec.MDM_ROAMING	signature
android.permission.sec.MDM_SECURITY	signatureOrSystem
android.permission.sec.MDM_SMARTCARD	signature
android.permission.sec.MDM_UMC_INTERNAL	signature
android.permission.sec.MDM_VPN	signature
android.permission.sec.MDM_WIFI	signature
android.permission.sec.OTP_PROVISION	signature
android.permission.sec.RECEIVE_BLOCKED_SMS_MMS	signature
android.permission.sec.SMIME_CERTIFICATE	signature
android.permission.SEND_RESPOND_VIA_MESSAGE	signature
android.permission.SEND_SMS	dangerous
android.permission.SERIAL_PORT	signature
android.permission.SET_ACTIVITY_WATCHER	signature
android.permission.SET_ALWAYS_FINISH	signature
android.permission.SET_ANIMATION_SCALE	signature
android.permission.SET_DEBUG_APP	signature
android.permission.SET_INPUT_CALIBRATION	signature
android.permission.SET_KEYBOARD_LAYOUT	signature
android.permission.SET_ORIENTATION	signature
android.permission.SET_POINTER_SPEED	signature
android.permission.SET_PREFERRED_APPLICATIONS	signature
android.permission.SET_PROCESS_LIMIT	signature
android.permission.SET_SCREEN_COMPATIBILITY	signature
android.permission.SET_TIME	signature
android.permission.SET_TIME_ZONE	normal
android.permission.SET_WALLPAPER	normal
android.permission.SET_WALLPAPER_COMPONENT	signature system
android.permission.SET_WALLPAPER_HINTS	normal
android.permission.SHUTDOWN	signature
android.permission.SIGNAL_PERSISTENT_PROCESSES	signature
android.permission.START_ANY_ACTIVITY	signature
android.permission.START_TASKS_FROM_RECENTS	signature
android.permission.STATUS_BAR	signature system
android.permission.STATUS_BAR_SERVICE	signature
android.permission.STOP_APP_SWITCHES	signature
android.permission.SYSTEM_ALERT_WINDOW	signature preinstalled
android.permission.TALKBACK_NOTIFICATION	signature system
android.permission.TEMPORARY_ENABLE_ACCESSIBILITY	signature

Permission	ProtectionLevel Description
android.permission.TRANSMIT_IR	normal
android.permission.UPDATE_APP_OPS_STATS	signature
android.permission.UPDATE_CONFIG	signature
android.permission.UPDATE_DEVICE_STATS	signature
android.permission.UPDATE_LOCK	signature
android.permission.USE_FINGERPRINT	normal
android.permission.USE_SIP	dangerous
android.permission.VIBRATE	normal
android.permission.WAKE_LOCK	normal
android.permission.WRITE_APN_SETTINGS	signature
android.permission.WRITE_CALENDAR	dangerous
android.permission.WRITE_CALL_LOG	dangerous
android.permission.WRITE_CONTACTS	dangerous
android.permission.WRITE_DREAM_STATE	signature
android.permission.WRITE_EXTERNAL_STORAGE	dangerous
android.permission.WRITE_GSERVICES	signature
android.permission.WRITE_MEDIA_STORAGE	signature
android.permission.WRITE_SECURE_SETTINGS	signature
android.permission.WRITE_SETTINGS	signature   preinstalled
android.permission.WRITE_SYNC_SETTINGS	normal
com.android.alarm.permission.SET_ALARM	normal
com.android.launcher.permission.INSTALL_SHORTCUT	normal
com.android.launcher.permission.UNINSTALL_SHORTCUT	normal
com.android.voicemail.permission.ADD_VOICEMAIL	dangerous
com.android.voicemail.permission.READ_VOICEMAIL	system   signature
com.android.voicemail.permission.WRITE_VOICEMAIL	system   signature
com.google.android.gms.permission.READ_VALUABLES_IMAGES	signature
com.google.android.gms.permission.SHOW_TRANSACTION_RECEIPT	signature
com.google.android.gms.permission.SHOW_WARM_WELCOME_TAPANDPAY_APP	signature
com.kddi.android.permission.MANAGE_CPA	dangerous
com.samsung.accessory.manager.permission.AUTHENTICATION_CONTROL	signature   system
com.samsung.accessory.permission.TRANSPORTING_NOTIFICATION_ITEM	signature
com.samsung.android.memo.READ_memo	signatureOrSystem
com.samsung.android.memo.WRITE_memo	signatureOrSystem
com.samsung.android.permission.ACCESS_SAFE_MODE	signature
com.samsung.android.permission.CHANGE_DISPLAY_COLOR	signature   system
com.samsung.android.permission.LOCK_TASK_MODE	normal
com.samsung.android.permission.MANAGE_CUSTOM_STARTING_WINDOW	signature   system
com.samsung.android.permission.MODIFY_THEME	signature   system
com.samsung.android.permission.RECEIVE_BT_GEAR	signature   system
com.samsung.android.permission.SAMSUNG_OVERLAY_COMPONENT	dangerous
com.samsung.android.permission.SSRM_NOTIFICATION_PERMISSION	signatureOrSystem
com.samsung.android.permisson.START_DOCK_OR_HOME	signature
com.samsung.android.virtualscreen.permission.MANAGE_VIRTUAL_SCREEN	signature   system
com.samsung.container.LAUNCH_INFO	signature   system
com.samsung.container.OBSERVER	signature   system
com.samsung.permission.BARCODE_READ	signature   system
com.samsung.permission.HOME_TRIPLE_CLICK	signature
com.samsung.permission.HRM_EXT	signatureOrSystem
com.samsung.permission.PALM_MOTION	signatureOrSystem
com.samsung.permission.SSENSOR	signatureOrSystem
com.sec.android.permission.IN_APP_SOUND	signature



Permission	ProtectionLevel Description
com.sec.android.permission.SMART_UNLOCK	signature
com.sec.android.permission.USE_GSCALER	signatureOrSystem
com.sec.android.permission.VOIP_INTERFACE	signature system
com.sec.enterprise.knox.KNOX_CONTAINER_VPN	signature
com.sec.enterprise.knox.KNOX_GENERIC_VPN	signature
com.sec.enterprise.knox.MDM_CONTENT_PROVIDER	normal
com.sec.enterprise.knox.permission.KNOX_ACTIVATE_DEVICE_PERMISSIONS	signature
com.sec.enterprise.knox.permission.KNOX_ATTESTATION	signature
com.sec.enterprise.knox.permission.KNOX_DEACTIVATE_LICENSE	signature
com.sec.enterprise.knox.permission.MDM_ENTERPRISE_TIMA_NOTIFICATION	signature
com.sec.enterprise.mdm.permission.BROWSER_PROXY	signature
com.sec.enterprise.mdm.permission.MDM_SILENT_ACTIVATION	signature
com.sec.enterprise.permission.KNOX_DLP	signature
com.sec.enterprise.permission.MDM_PROXY_ADMIN_INTERNAL	signature
com.sec.enterprise.permission.MDM_SPDCONTROL	signature
com.sec.knox.container.keyguard.ACCESS	system signature
com.sec.knox.container.peripheral.POLICY_UPDATE	system signature
com.sec.mms.permission.RECEIVE_MESSAGES_INFORMATION	signatureOrSystem
com.sec.permission.BLUETOOTH_DEBUG	signature
com.threelm.permission.DEVICE_INIT	signature
diagandroid.app.receiveDetailedApplicationState	signatureOrSystem
diagandroid.data.receivePDPCContextState	signatureOrSystem
diagandroid.phone.receiveDetailedCallState	signatureOrSystem
nof.permission.RECEIVE_USER_MODE	signature
org.simalliance.openmobileapi.BIND_TERMINAL	system signature
org.simalliance.openmobileapi.SYSTEM_TERMINAL	system signature
skplanet.permission.USE_PLAYREADY	normal

**Table 8 Permissions**

**FDP\_DAR\_EXT.1:** The TOE provides AES-128 XTS (on TOE models using a Qualcomm MSM8996, “Snapdragon 820” processor) or AES-256 CBC (on TOE models using an Exynos 8890 processor) encryption of all data (which includes both user data and TSF data) stored on the TOE through On Device Encryption (ODE) of the data partition. The TOE also has TSF data for its ODE keys, which the TOE stores outside the ODE encrypted data partition, and the TOE also includes a read-only filesystem in which the TOE’s system executables, libraries, and their configuration data reside. For its ODE encryption of the data partition (where the TOE stores all user data and all application data), the TOE uses an AES-256 bit DEK with either XTS or CBC feedback mode to encrypt the entire partition. The TOE also provides AES-256 CBC encryption of protected data stored on the external SDCard using FEKs. The TOE encrypts each individual file stored on the SDCard, generating a unique FEK for each file.

**FDP\_IFC\_EXT.1:** The TOE includes an IPsec VPN Client that ensures that all traffic other than traffic necessary to establish the VPN connection (802.11-2012 traffic and IKEv2) flows through the VPN. The TOE routes all packets through the kernel’s IPsec interface (ipsec0) when the VPN is active. The kernel compares packets routed through this interface to the SPDs configured for the VPN to determine whether or PROTECT, BYPASS, or DISCARD each packet. The vendor designed the TOE’s VPN, when operating in CC Mode, to allow no configuration and to always force all traffic through the VPN. The TOE ignores any IKEv2 traffic selector negotiations with the VPN GW and will always create an SPD PROTECT rule that matches all traffic. Thus, the kernel will match all packets, subsequently encrypt those packets, and finally forward them to the VPN Gateway.

**FDP\_STG\_EXT.1:** The TOE’s Trusted Anchor Database consists of the built-in certs (individually stored in /system/etc/security/cacerts) which the user can disable using the TOE’s Android user interface [Settings->Security-> Trusted Credentials]) and consists of any additional user or admin/MDM loaded certificates. Disabled default certificates and user added certificates reside in the /data/misc/user/0/cacerts-

removed and /data/misc/user/0/cacerts-added directories respectively. The built-in ones are protected as they are part of the TSF's read only system partition, while the TOE protects user-loaded certificates by storing them with appropriate permissions to prevent modification by mobile applications. The TOE also stores the user-loaded certificates in the user's keystore.

**FDP\_UPC\_EXT.1:** The TOE provides APIs allowing non-TSF applications (mobile applications) the ability to establish a secure channel using TLS, HTTPS, Bluetooth BR/EDR and Bluetooth LE. Mobile applications can use the following Android APIs for TLS, HTTPS, and Bluetooth respectively:

- javax.net.ssl.SSLContext:
  - <http://developer.android.com/reference/javax/net/ssl/SSLContext.html>
- javax.net.ssl.HttpURLConnection:
  - <http://developer.android.com/reference/javax/net/ssl/HttpsURLConnection.html>
- android.bluetooth:
  - <http://developer.android.com/reference/android/bluetooth/package-summary.html>

### 6.3 Identification and authentication

**FIA\_AFL\_EXT.1(1):** The TOE maintains, for each user, the number of failed logins since the last successful login, and upon reaching the maximum number of incorrect logins, the TOE performs a full wipe of all protected data (and in fact, wipes all users' data). An administrator can adjust the number of failed logins from the (CC Mode) limit of ten failed logins to a value between one and ten through an MDM. The TOE maintains the number of failed logins across power-cycles (so for example, assuming a configured maximum retry of ten incorrect attempts, if one were to enter five incorrect passwords and power cycle the phone, the phone would only allow five more incorrect login attempts before wiping) by storing the number of logins remaining within its Flash filesystem. The TOE also separately stores (in a different Flash location) the number of master user (user\_0) logins attempts remaining for the crypt-lock screen (before the TOE will wipe itself). This value defaults to a vendor specified number (typically set to 10), and prior to the first unlock after power-up, the user data partition is encrypted and the TOE does not have access to data stored within it.

**FIA\_BLT\_EXT.1:** The TOE requires explicit user authorization before it will pair with a remote Bluetooth device. When pairing with another device, the TOE requires that the user either confirm that a displayed numeric passcode matches between the two devices or that the user enter (or choose) a numeric passcode that the peer device generates (or must enter).

**FIA\_BLT\_EXT.2:** The TOE requires explicit user authorization or user authorization before data transfer over the link. When transferring data with another device, the TOE requires that the user must confirm authorization pop up displayed allowing data transfer (Obex Object Push) or confirm user passkey displayed numeric passcode matches between the two devices (RFCOMM).

**FIA\_BLT\_EXT.3:** The TOE tracks active connections and actively ignores connection attempts from Bluetooth device addresses for which the TOE already has an active connection.

**FIA\_PAE\_EXT.1:** The TOE can join WPA2-802.1X (802.11i) wireless networks requiring EAP-TLS authentication, acting as a client/supplicant (and in that role connect to the 802.11 access point and communicate with the 802.1X authentication server).

**FIA\_PMG\_EXT.1:** The TOE authenticates the user through a password consisting of basic Latin characters (upper and lower case, numbers, and the special characters noted in the selection (see section 5.1.4.7)). The TOE can support a minimum password length of as few as four characters and a maximum of no more than sixteen characters. The TOE defaults to requiring passwords to have a minimum of four characters that contain at least one letter and one number. An MDM application can change these defaults and impose password restrictions (like quality, specify another minimum length, the minimum number of letters, numeric characters, lower case letters, upper case letters, symbols, and non-letters).

**FIA\_TRT\_EXT.1:** The TOE allows users to authenticate through external ports (either a USB keyboard or a Bluetooth keyboard paired in advance of the login attempt). If not using an external keyboard, a user must



authenticate through the standard User Interface (using the TOE touchscreen). The TOE limits the number of authentication attempts through the UI to no more than five attempts within 30 seconds (irrespective of what keyboard the operator uses). Thus if the current [the  $n^{\text{th}}$ ] and prior four authentication attempts have failed, and the  $n-4^{\text{th}}$  attempt was less than 30 second ago, the TOE will prevent any further authentication attempts until 30 seconds has elapsed. Note as well that the TOE will wipe itself when it reaches the maximum number of unsuccessful authentication attempts (as described in FIA\_AFL\_EXT.1 above).

**FIA\_UAU.7:** The TOE allows the user to enter the user's password from the lock screen. The TOE will, by default, display the most recently entered character of the password briefly or until the user enters the next character in the password, at which point the TOE obscures the character by replacing the character with a dot symbol. The user can configure the TOE's behavior for the normal lockscreen so that it does not briefly display the last typed character; however, the TOE always briefly displays the last entered character for the crypt-lock screen.

**FIA\_UAU\_EXT.1:** As described before, the TOE's Key Hierarchy requires the user's password in order to derive the PKEK1 & PKEK2 keys in order to decrypt other KEKs and DEKs. Thus, until it has the user's password, the TOE cannot decrypt the DEK utilized by ODE to decrypt protected data.

**FIA\_UAU\_EXT.2:** The TOE, when configured to require a user password (as is the case in CC mode), allows only those actions described in section 5.1.4.11. Beyond those actions, a user cannot perform any other actions other than observing notifications displayed on the lock screen until after successfully authenticating.

**FIA\_UAU\_EXT.3:** The TOE requires the user to enter their password in order to unlock the TOE. Additionally the TOE requires the user to confirm their current password when accessing the "Settings->LockScreen and Security" menu in the TOE's user interface. Only after entering their current user password can the user then elect to change their password.

**FIA\_X509\_EXT.1:** The TOE checks the validity of all imported CA certificates by checking for the presence of the basicConstraints extension and that the CA flag is set to TRUE as the TOE imports the certificate into the TOE's Trust Anchor Database. If the TOE detects the absence of either the extension or flag, the TOE will import the certificate as a user public key and add it to the keystore (not the Trust Anchor Database). The TOE also checks for the presence of the basicConstraints extension and CA flag in each CA certificate in a server's certificate chain. Similarly, the TOE verifies the extendedKeyUsage Server Authentication purpose during certificate validation. The TOE's certificate validation algorithm examines each certificate in the path (starting with the peer's certificate) and first checks for validity of that certificate (e.g., has the certificate expired? or is it not yet valid? whether the certificate contains the appropriate X.509 extensions [e.g., the CA flag in the basic constraints extension for a CA certificate, or that a server certificate contains the Server Authentication purpose in the ExtendedKeyUsagefield], then verifies each certificate in the chain (applying the same rules as above, but also ensuring that the Issuer of each certificate matches the Subject in the next rung "up" in the chain and that the chain ends in a self-signed certificate present in either the TOE's trusted anchor database or matches a specified Root CA), and finally the TOE performs revocation checking for all certificates in the chain..

**FIA\_X509\_EXT.2:** The TOE uses X.509v3 certificates as part of EAP-TLS, TLS and IPsec authentication. The TOE comes with a built-in set of default of Trusted Credentials (Android's set of trusted CA certificates). And while the user cannot remove any of the built-in default CA certificates, the user can disable any of those certificates through the user interface so that certificates issued by disabled CA's cannot validate successfully. In addition, a user can import a new trusted CA certificate into the Key Store or an administrator can install a new certificate through an MDM.

The TOE does not establish TLS connections itself (beyond EAP-TLS used for WPA2 Wifi connections), but provides a series of APIs that mobile applications can use to check the validity of a peer certificate. The mobile application, after correctly using the specified APIs can be assured as to the validity of the peer certificate and will not establish the trusted connection if the peer certificate cannot be verified (including validity, certification path, and revocation [through CRL and OCSP]). During revocation checking, the TOE first attempts to determine a certificate's revocation status through OCSP (if the Authority Information Access, AIA, extension is present). If the certificate lacks AIA or if the OCSP server does not respond, or if the OCSP responder returns an unknown status; the TOE attempts to determine revocation status using CRLs, if the certificate includes a CRL Distribution Point

(CDP). If the TOE cannot establish a connection with the server acting as the CDP, the TOE will deem the server's certificate as invalid and not establish a TLS connection with the server.

**FIA\_X509\_EXT.3:** The TOE's Android operating system provides applications the `java.security.cert.CertPathValidator` Java API Class of methods validating certificates and certification paths (certificate chains establishing a trust chain from a certificate to a trust anchor). This class is also recommended to be used by third-party Android developers for certificate validation. However, `TrustedCertificateStore` must be used to chain certificates to the Android System Trust Anchor Database (anchors should be retrieved and provided to `PKIXParameters` used by `CertPathValidator`). The available APIs may be found here:

- <http://developer.android.com/reference/java/security/cert/package-summary.html>

## 6.4 Security management

**FMT\_MOF.1/FMT\_SMF\_EXT.1:** The TOE provides the management functions described in the table in section 5.1.5.2. The table includes annotations describing the roles that have access to each service and how to access the service. The TOE enforces administrative configured restrictions by rejecting user configuration (through the UI) when attempted.

**FMT\_SMF\_EXT.2(1):** The TOE disables CC mode, when unenrolled. The TOE also provides the capability to the MDM Agent to wipe all protected data and to remove any installed Enterprise applications.

## 6.5 Protection of the TSF

**FPT\_AEX\_EXT.1:** The Linux kernel of the TOE's Android operating system provides address space layout randomization utilizing a non-cryptographic kernel random function to provide 8 unpredictable bits to the base address of any user-space memory mapping. The random function, though not cryptographic, ensures that one cannot predict the value of the bits. Similarly, the TOE also provide Kernel Address Space Layout Randomization, to ensure that the base address of kernel-space memory mappings consist of 4 unpredictable bits.

**FPT\_AEX\_EXT.2:** The TOE's Android 6.0.1 operating system utilizes a 3.10/3.18 Linux kernel, whose memory management unit (MMU) enforces read, write, and execute permissions on all pages of virtual memory and ensures that write and execute permissions are not simultaneously granted on all memory (exceptions are only made for Dalvik JIT compilation). The Android operating system (as of Android 2.3) sets the ARM eXecute Never (XN) bit on memory pages and the TOE's ARMv8 Application Processor's MMU circuitry enforces the XN bits. From Android's documentation (<https://source.android.com/devices/tech/security/index.html>), Android 2.3 forward supports "Hardware-based No eXecute (NX) to prevent code execution on the stack and heap". Section D.5 of the ARM v8 Architecture Reference Manual contains additional details about the MMU of ARM-based processors: <http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.ddi0487a.f/index.html>

**FPT\_AEX\_EXT.3:** The TOE's Android operating system provides explicit mechanisms to prevent stack buffer overruns (enabling `-fstack-protector`) in addition to taking advantage of hardware-based No eXecute to prevent code execution on the stack and heap. Samsung requires and applies these protections to all TSF executable binaries and libraries.

**FPT\_AEX\_EXT.4:** The TOE protects itself from modification by untrusted subjects using a variety of methods. The first protection employed by the TOE is a Secure Boot process that uses cryptographic signatures to ensure the authenticity and integrity of the bootloader and kernels using data fused into the device processor.

The TOE's Secure Boot process employs a series of public keys to form a chain of trust that operates as follows. The Application Processor (AP) contains the SHA-256 hash of the Secure Boot Public Key (an RSA 2048-bit key embedded in end of the signed bootloader image), and upon verifying the SBPK attached to the bootloader produces the expected hash, the AP uses this public key to verify the PKCS 1.5 RSA 2048 w/ SHA-256 signature of the bootloader image, to ensure its integrity and authenticity before transitioning execution to the bootloader. The bootloader, in turn, contains the Image Signing Public Key (ISPK), which the bootloader will use to verify the

PKCS 1.5 RSA 2048 w/ SHA-1 signature on either kernel image (primary kernel image or recovery kernel image). Note that when configured for Common Criteria mode, the TOE only accepts updates to the TOE firmware Over The Air; however, when not configured for CC mode, the TOE allows updates through the bootloader's ODIN mode. The primary kernel includes an embedded FOTA Public Key, which the TOE uses to verify the authenticity and integrity of Firmware Over-The-Air update signatures (which contain a PKCS 2.1 PSS RSA 2048 w/ SHA-512 signature).

The TOE protects access to the REK and derived HEK to only trusted applications<sup>1</sup> within the TEE (TrustZone). The TOE key manager includes a TEE module which utilizes the HEK to protect all other keys in the key hierarchy. All TEE applications are cryptographically signed, and when invoked at runtime (at the behest of an untrusted application), the TEE will only load the trusted application after successfully verifying its cryptographic signature. Furthermore, SKMM\_TA or device encryption library checks the integrity of the system by checking the result from both Secure Boot/SecurityManager and from the Integrity Check Daemon before servicing any requests. Without this TEE application, no keys within the TOE (including keys for ScreenLock, the key store, and user data) can be successfully decrypted, and thus are useless.

The third protection is the TOE's internal SecurityManager watchdog service. The SecurityManager manages the CC mode of the TOE by looking for unsigned kernels or failures from other, non-cryptographic checks on system integrity, and upon detecting of a failure in either, disables the CC mode and notifies the TEE application. The TEE application then locks itself, again rendering all TOE keys useless.

Finally, the TOE's Android OS provides "sandboxing" that ensures that each non-system mobile application executes with the file permissions of a unique Linux user ID, in a different virtual memory space. This ensures that applications cannot access each other's memory space (it is possible for two processes to utilize shared memory, but not directly access the memory of another application) or files and cannot access the memory space or files of system-level applications.

**FPT\_BBD\_EXT.1:** The TOE's hardware and software architecture ensures separation of the application processor (AP) from the baseband or communications processor (CP). From a software perspective, the AP and CP communicate logically through the Android Radio Interface Layer (RIL) daemon. This daemon, which executes on the AP, coordinates all communication between the AP and CP. It makes requests of the CP and accepts the response from the CP; however, the RIL daemon does not provide any reciprocal mechanism for the CP to make requests of the AP. Because the mobile architecture provides only the RIL daemon interface, the CP has no method to access the resources of the software executing on the AP.

**FPT\_KST\_EXT.1:** The TOE does not store any plaintext key material in its internal Flash; instead, the TOE encrypts all keys before storing them. This ensures that irrespective of how the TOE powers down (e.g., a user commands the TOE to power down, the TOE reboots itself, or battery is removed), all keys in internal Flash are wrapped with a KEK. Please refer to section 6.1 of the TSS for further information (including the KEK used) regarding the encryption of keys stored in the internal Flash. As the TOE encrypts all keys stored in Flash, upon boot-up, the TOE must first decrypt and utilize keys.

**FPT\_KST\_EXT.2:** The TOE utilizes a cryptographic library consisting of an implementation of BoringSSL, the kernel crypto module, the key management module, and the following system-level executables that utilize KEKs: dm-crypt, eCryptfs, wpa\_supplicant, and the keystore.

The TOE ensures that plaintext key material does not leave by not allowing the REK to leave and by ensuring that only authenticated entities can request utilization of the REK. Furthermore, the TOE only allows the system-level executables access to plaintext DEK values needed for their operation. The TSF software (the system-level executables) protects those plaintext DEK values in memory both by not providing any access to these values and by clearing them when no longer needed (in compliance with FCS\_CKM.4).

**FPT\_KST\_EXT.3:** The TOE does not provide any way to export plaintext DEKs or KEKs (including all keys stored in the keystore) as the TOE chains all KEKs to the HEK/REK.

---

<sup>1</sup> A TrustZone application is a trusted application that executes in a hardware-isolated domain.

**FPT\_NOT\_EXT.1:** When the TOE encounters a self-test failure or when the TOE software integrity verification fails, the TOE transitions to a non-operational mode. The user may attempt to power-cycle the TOE to see if the failure condition persists, and if it does persist, the user may attempt to boot to the recovery mode/kernel to wipe data and perform a factory reset in order to recover the device.

**FPT\_STM.1:** The TOE requires time for the Package Manager, FOTA image verifier, TLS certificate validation, wpa\_supplicant, and key store applications. These TOE components obtain time from the TOE using system API calls [e.g., time() or gettimeofday()]. An application cannot modify the system time as mobile applications need the android “SET\_TIME” permission to do so. Likewise, only a process with root privileges can directly modify the system time using system-level APIs. The TOE uses the Cellular Carrier time (obtained through the Carrier’s network time server) as a trusted source; however, the user can also manually set the time through the TOE’s user interface.

**FPT\_TST\_EXT.1:** The TOE performs known answer power on self-tests (POST) on its cryptographic algorithms to ensure that they are functioning correctly. The kernel itself performs known answer tests on its cryptographic algorithms to ensure they are working correctly and the SecurityManager service invokes the self-tests of BoringSSL at start-up to ensure that those cryptographic algorithms are working correctly. The Chipset hardware performs a power-up self-test to ensure that its AES implementation is working as does the TEE SCrypto cryptographic library. Should any of the tests fail, the TOE will reboot to see if that will clear the error.

Algorithm	Implemented in	Description
AES encryption/decryption	BoringSSL, SCrypto, Kernel Crypto, Chipset hardware	Comparison of known answer to calculated valued
ECDH key agreement	BoringSSL	Comparison of known answer to calculated valued
DRBG random bit generation	BoringSSL, SCrypto, Kernel Crypto	Comparison of known answer to calculated valued
ECDSA sign/verify	BoringSSL, SCrypto,	Sign operation followed by verify
HMAC-SHA	BoringSSL, SCrypto, Kernel Crypto	Comparison of known answer to calculated valued
RSA sign/verify	BoringSSL, SCrypto,	Comparison of known answer to calculated valued
SHA hashing	BoringSSL, SCrypto, Kernel Crypto	Comparison of known answer to calculated valued

**Table 9 Power-up Cryptographic Algorithm Self-Tests**

**FPT\_TST\_EXT.2:** The TOE ensures a secure boot process in which the TOE verifies the digital signature of the bootloader software for the Application Processor (using a public key whose hash resides in the processor’s internal fuses) before transferring control. The bootloader, in turn, verifies the signature of the Linux kernel (either the primary or the recovery kernel) it loads.

The TOE also includes an Integrity Check Daemon (ICD) that provides an integrity verification result into TrustZone. The ICD compares the SHA-256 hashes contained in an RSA PKCS#1 signed security profile with the hashes it calculates using the specified path. The security profile includes hashes of the kernel, the ICD itself, and specified modules and libraries. If any calculated hash does not match, then the ICD reports this to the TrustZone..

**FPT\_TUD\_EXT.1:** The TOE’s user interface provides a method to query the current version of the TOE software/firmware (Android version, baseband version, kernel version, build number, and security software version) and hardware (model and version). Additionally, the TOE provides users the ability to review the currently installed apps (including 3<sup>rd</sup> party “built-in” applications) and their version.

**FPT\_TUD\_EXT.2:** When in CC mode, the TOE verifies all updates to the TOE software using a public key (FOTA public key) chaining ultimately to the Secure Boot Public Key (SBPK), a hardware protected key whose SHA-256 hash resides inside the application processor (note that when not in CC mode, the TOE allows updates to the TOE software through ODIN mode of the bootloader). After verifying an update’s FOTA signature, the TOE will then

install those updates to the TOE. The TOE will check a new image to ensure that the image is not older than the current image, and if so, the TOE will reject the new image and not update the TOE software.

The application processing verifies the bootloader's authenticity and integrity (thus tying the bootloader and subsequent stages to a hardware root of trust: the SHA-256 hash of the SBPK, which cannot be reprogrammed after the "write-enable" fuse has been blown).

The Android OS on the TOE requires that all applications bear a valid signature before Android will install the application.

**ALC\_TSU\_EXT:** Samsung utilizes industry best practices to ensure their devices are patched to mitigate security flaws. Samsung provides customers with a developer web portal (<http://developer.samsung.com/notice/How-to-Use-the-Forum>) in which one can ask questions as well as inform Samsung of potential issues with their software (as Samsung moderators monitor the forums), and as an Android OEM, also works with Google on reported Android issues (<http://source.android.com/source/report-bugs.html>) to ensure customer devices are secure.

Samsung will create updates and patches to resolve reported issues as quickly as possible, at which point the update is provided to the wireless carriers. The delivery time for resolving an issue depends on the severity, and can be as rapid as a few days before the carrier handoff for high priority cases. The wireless carriers perform additional tests to ensure the updates will not adversely impact their networks and then plan device rollouts once that testing is complete. Carrier updates usually take at least two weeks to as much as two months (depending on the type and severity of the update) to be rolled out to customers. However, the Carriers also release monthly Maintenance Releases in order to address security-critical issues, and Samsung itself maintains a security blog (<http://security.samsungmobile.com>) in order to disseminate information directly to the public.

Samsung communicates with the reporting party to inform them of the status of the reported issue. Further information about updates is handled through the carrier release notes. Issues reported to Google directly are handled through Google's notification processes.

## 6.6 TOE access

**FTA\_SSL\_EXT.1:** The TOE transitions to its locked state either immediately after a User initiates a lock by pressing the power button or after a configurable period of inactivity, and as part of that transition, the TOE will display a lock screen to obscure the previous contents; however, the TOE's lock screen still allows a user to perform the functions listed in section 5.1.4.11 before authenticating. But without authenticating first, a user cannot perform any related actions based upon these notifications (for example, they cannot respond to emails, calendar appointment requests, or text messages) other than answering an incoming phone call.

Note that during power up, the TOE presents the user with an initial power-up ODE screen, where the user can only make an emergency call or enter the ODE password in order to allow the TOE to decrypt the OBE key so as to be able to access the data partition. After successfully authenticating at the power-up login screen, the TOE (when subsequently locked) presents the user with the lock screen.

**FTA\_TAB.1:** The TOE can be configured to display a user-specified message (maximum of 23 characters) on the Lock screen, and additionally an administrator can also set a Lock screen message using an MDM.

**FTA\_WSE\_EXT.1:** The TOE allows an administrator to specify (through the use of an MDM) a list of wireless networks (SSIDs) to which the user may direct the TOE to connect to. When not enrolled with an MDM, the TOE allows the user to control to which wireless networks the TOE should connect, but does not provide an explicit list of such networks, rather the user may scan for available wireless network (or directly enter a specific wireless network), and then connect. Once a user has connected to a wireless network, the TOE will automatically reconnect to that network when in range and the user has enabled the TOE's WiFi radio.



---

## 6.7 Trusted path/channels

---

**FTP\_ITC\_EXT.1:** The TOE provides secured (encrypted and mutually authenticated) communication channels between itself and other trusted IT products through the use of 802.11-2012, 802.1X, and EAP-TLS, TLS and IPsec. The TOE permits itself and applications to initiate communications via the trusted channel, and the TOE initiates communicate via the trusted channel for connection to a wireless access point. The TOE provides access to TLS via published APIs which are accessible to any application that needs an encrypted end-to-end trusted channel. The TOE also meets the Protection Profile for IPsec Virtual Private Network (VPN) Clients.

---

## 6.8 KNOX Workspace Container Functionality

---

To differentiate the functionality provided by a KNOX Workspace container, this section enumerates the functionality provided by the container.

**FDP\_DAR\_EXT.2:** The TOE provides mobile applications residing with a KNOX Workspace container the ability to store sensitive data and have the TOE encrypt it accordingly. The TOE protects such sensitive data in a segregated database not directly accessible by any mobile application, and furthermore, the TOE encrypts the data contents within the database with keys that the TOE clears from memory when the container transitions to the lock state. A container (and thus the applications within) can have a lock-state independent from that of the overall mobile device (with an administrator or user defined timeout) and the user and administrator can set the container's lock-state to also lock when the user locks the mobile device.

**FDP\_ACF\_EXT.1.2:** The TOE, through a combination of Android's multi-user capabilities and Security Enhancements (SE) for Android, provides the ability to create isolated containers within the device. Within a container a group of applications can be installed, and access to those applications is then restricted to usage solely within the container. The container boundary restricts the ability of sharing data such that applications outside the container cannot see, share or even copy data to those inside the container and vice versa. Exceptions to the boundary (such as allowing a copy operation) must be authorized by the administrator via policy. Furthermore, the container boundary policy can control access to hardware features, such as the camera or microphone, and restrict the ability of applications within the container to access those services.

**FIA\_AFL\_EXT.1(2):** The KNOX Workspace container maintains, in Flash, the number of failed logins since the last successful login, and upon reaching the maximum number of incorrect logins, the KNOX Workspace container performs a full wipe of data protected by KNOX (i.e. data inside the container). An administrator can adjust the number of failed logins from the default of ten failed logins to a value between one and one hundred through an MDM.

**FIA\_UAU.7:** The KNOX Workspace container allows the user to enter the user's password from the KNOX lock screen. The KNOX Workspace container will, by default, display the most recently entered character of the password briefly or until the user enters the next character in the password, at which point the KNOX Workspace container obscures the character by replacing the character with a dot symbol.

**FIA\_UAU\_EXT.3:** The KNOX Workspace container requires the user to enter their password in order to unlock the KNOX Workspace container. Additionally the KNOX Workspace container requires the user to confirm their current password when accessing the "KNOX Settings -> KNOX unlock method" menu in the KNOX Workspace container's user interface. Only after entering their current user password can the user then elect to change their password.

**FMT\_MOF.1/FMT\_SMF\_EXT.1:** The KNOX Workspace container grants the user the exclusive functions specified in the SFR (see section 5.1.5).

The control over the camera and microphone within the KNOX Workspace container only affects access to those resources inside the container, not outside the container. If either of these is disabled outside the container then they will not be available within the container, even if they are enabled.

**FMT\_SMF\_EXT.2(2):** The KNOX Workspace container, when a container is unenrolled (or removed), wipes all data inside the KNOX Workspace container.

**FTA\_SSL\_EXT.1:** The KNOX Workspace container transitions to its locked state either immediately after a User initiates a lock by pressing the container lock button from the notification bar or after a configurable period of inactivity, and as part of that transition, the KNOX Workspace container will display a lock screen to obscure the previous contents. When the KNOX Workspace container is locked, it can still display calendar appointments and other notifications allowed by the administrator to be shown on outside the container (in the notification area). But without authenticating first to the KNOX Workspace container, a user cannot perform any related actions based upon these container notifications (they cannot respond to emails, calendar appointments, or text messages).

The KNOX Workspace container timeout is independent from the TOE timeout and as such can be set to different values.

## 6.9 Security Audit

**FAU\_GEN.1:** The following table enumerates the events that the TOE audits.

Requirement	Audit Event	Content
<b>FAU_GEN.1</b>	Start-up and shutdown of the audit functions	
<b>FAU_GEN.1</b>	All administrative actions	
<b>FAU_GEN.1</b>	Start-up and shutdown of the OS and kernel	
<b>FAU_GEN.1</b>	Insertion or removal of removable media	
<b>FAU_GEN.1</b>	Establishment of a synchronizing connection	
<b>FAU_GEN.1</b>	Reaching the configured audit log critical size limit	
<b>FCS_CKM_EXT.5</b>	Success or failure of the wipe.	
<b>FCS_CKM.1(1)</b>	Failure of key generation activity for authentication keys.	
<b>FCS_HTTPS_EXT.1</b>	Failure of the certificate validity check.	Issuer Name and Subject Name of certificate.
<b>FCS_STG_EXT.1</b>	Import or destruction of key.	Identity of key. Role and identity of requestor.
<b>FCS_STG_EXT.3</b>	Failure to verify integrity of stored key.	Identity of key being verified.
<b>FCS_TLSC_EXT.1</b>	Failure to establish a EAP-TLS session.	Reason for failure.
<b>FCS_TLSC_EXT.1</b>	Establishment/termination of an EAP-TLS session	Non-TOE endpoint of connection
<b>FCS_TLSC_EXT.2</b>	Failure to establish a TLS session.	Reason for failure.
<b>FCS_TLSC_EXT.2</b>	Failure to verify presented identifier.	Presented identifier and reference identifier.
<b>FCS_TLSC_EXT.2</b>	Establishment/termination of a TLS session.	Non-TOE endpoint of connection.
<b>FDP_DAR_EXT.2</b>	Failure to encrypt/decrypt data.	
<b>FDP_STG_EXT.1</b>	Addition or removal of certificate from Trust Anchor Database.	Subject name of certificate.
<b>FIA_UAU_EXT.3</b>	User changes Password Authentication Factor.	
<b>FIA_X509_EXT.1</b>	Failure to validate X.509v3 certificate.	Reason for failure of validation.
<b>FIA_X509_EXT.2</b>	Failure to establish connection to determine revocation status.	
<b>FMT_SMF_EXT.1</b>	Change of settings.	Role of user that changed setting. Value of new setting.
<b>FMT_SMF_EXT.1</b>	Success or failure of function.	Role of user that performed function.

Requirement	Audit Event	Content
		Function performed. Reason for failure.
FMT_SMF_EXT.1	Initiation of software update.	Version of update.
FMT_SMF_EXT.1	Initiation of application installation or update.	Name and version of application.
FPT_TST_EXT.2	Start-up of TOE.	Boot Mode.
FPT_TUD_EXT.2	Success or failure of signature verification for software updates.	
FPT_TUD_EXT.2	Success or failure of signature verification for applications.	
FTA_TAB.1	Change in banner setting.	
FTA_WSE_EXT.1	All attempts to connect to access points.	Identity of access point.

**Table 10 Audited Events**

**FAU\_STG.1:** The TOE stored audit records in a file within the filesystem accessible only to Linux processes with system permissions (effectively the TSF itself and MDM agents possessing a valid KNOX license using the defined APIs). These restrictions prevent the unauthorized modification or deletion of the audit records stored in the audit files.

**FAU\_STG.4:** The TOE pre-allocates a file system area (between 10MB and 50MB in size, depending upon available storage on the device) by creating a /data/system/[admin\_uid]\_bubble/bubbleFile and directory (/data/system/[admin\_uid]) in which to archive compressed audit logs. If the TOE lacks sufficient space (at least 10MB), then the TOE returns a failure code in response to the administrator's attempt to enable the AuditLog. Once enabled, the TOE writes audit events into nodes until they reach a given size, and then compresses and archives the records. The TOE utilizes a circular buffer approach to handle when the accumulated, compressed audit events exceed the allocated file system size. When the limit is reached, the TOE removes the oldest audit logs, freeing space for new records.



## 7. TSF Inventory

Below is a list of user-mode TSF binaries and libraries. All are built with the `-fstack-protector` option set. For each binary/library, the name, path and security function is provided.

Name	Path	Security Function
app_process	/system/bin	APP
charon	/system/bin	VPN
dalvikvm	/system/bin	VM
gatekeeperd	/system/bin	Key store/Key Mgmt
keystore	/system/bin	Key store
mcDriverDaemon	/system/bin	Trustzone Daemon
qseecomd	/system/bin	Trustzone Daemon
secure_storage_daemon	/system/bin	DAR
sfothelper	/system/bin	FOTA
time_daemon	/system/bin	Time
vold	/system/bin	DAR
wpa_supplicant	/system/bin	WLAN
icd_test	/system/etc	Integrity
libSecurityManagerNative.so	/system/lib , /system/lib64	CCMode
libcharon.so	/system/lib , /system/lib64	VPN
libcrypto.so	/system/lib , /system/lib64	Crypto
libdirencryption.so	/system/lib , /system/lib64	DAR
libhydra.so	/system/lib , /system/lib64	VPN
libjavacrypto.so	/system/lib , /system/lib64	Crypto JNI
libkeystore_binder.so	/system/lib , /system/lib64	Key store
libkeyutils.so	/system/lib , /system/lib64	Key store
libsec_devenc.so	/system/lib , /system/lib64	DAR
libsec_ecryptfs.so	/system/lib , /system/lib64	DAR
libsec_ode_keymanager.so	/system/lib , /system/lib64	DAR
libsecure_storage.so	/system/lib , /system/lib64	DAR
libsecure_storage_jni.so	/system/lib , /system/lib64	DAR
libskmm.so	/system/lib , /system/lib64	Key Mgmt
libskmm_helper.so	/system/lib , /system/lib64	Key Mgmt