

# **Pixel 3 and Pixel 3 XL (MDFPP31/WLANCEP10) Security Target**

Version 0.6  
2019/07/17

*Prepared for:*

**Google LLC**

1600 Amphitheatre Parkway  
Mountain View, CA 94043  
USA

*Prepared By:*



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

1.	Security Target Introduction.....	6
1.1	Security Target Reference .....	6
1.2	TOE Reference.....	6
1.3	TOE Overview.....	7
1.4	TOE Description.....	7
1.4.1	TOE Architecture.....	8
1.4.1.1	Physical Boundaries .....	8
1.4.1.2	Logical Boundaries .....	8
1.4.2	TOE Documentation.....	10
2.	Conformance Claims.....	11
2.1	Conformance Rationale.....	11
3.	Security Objectives .....	12
3.1	Security Objectives for the Operational Environment .....	12
4.	Extended Components Definition .....	13
5.	Security Requirements .....	16
5.1	TOE Security Functional Requirements.....	16
5.1.1	Security audit (FAU).....	19
5.1.1.1	Audit Data Generation (FAU_GEN.1) .....	19
5.1.1.2	Audit Storage Protection (FAU_STG.1) .....	19
5.1.1.3	Prevention of Audit Data Loss (FAU_STG.4).....	19
5.1.2	Cryptographic support (FCS).....	20
5.1.2.1	Cryptographic key generation (FCS_CKM.1) .....	20
5.1.2.2	Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) (FCS_CKM.1/WLAN)..	20
5.1.2.3	Cryptographic key establishment (FCS_CKM.2(1)) .....	20
5.1.2.4	Cryptographic key establishment (While device is locked) (FCS_CKM.2(2)).....	20
5.1.2.5	Cryptographic Key Distribution (GTK) (FCS_CKM.2/WLAN) .....	20
5.1.2.6	Extended: Cryptographic Key Support (FCS_CKM_EXT.1).....	20
5.1.2.7	Extended: Cryptographic Key Random Generation (FCS_CKM_EXT.2) .....	21
5.1.2.8	Extended: Cryptographic Key Generation (FCS_CKM_EXT.3) .....	21
5.1.2.9	Extended: Key Destruction (FCS_CKM_EXT.4) .....	21
5.1.2.10	Extended: TSF Wipe (FCS_CKM_EXT.5).....	22
5.1.2.11	Extended: Salt Generation (FCS_CKM_EXT.6).....	22
5.1.2.12	Cryptographic operation (FCS_COP.1(1)).....	22
5.1.2.13	Cryptographic operation (FCS_COP.1(2)).....	22
5.1.2.14	Cryptographic operation (FCS_COP.1(3)).....	22
5.1.2.15	Cryptographic operation (FCS_COP.1(4)).....	22

5.1.2.16	Cryptographic operation (FCS_COP.1(5)).....	23
5.1.2.17	Extended: HTTPS Protocol (FCS_HTTPS_EXT.1) .....	23
5.1.2.18	Extended: Initialization Vector Generation (FCS_IV_EXT.1).....	23
5.1.2.19	Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT.1) .....	23
5.1.2.20	Extended: Cryptographic Algorithm Services (FCS_SRV_EXT.1) .....	23
5.1.2.21	Extended: Cryptographic Algorithm Services (FCS_SRV_EXT.2) .....	23
5.1.2.22	Extended: Cryptographic Key Storage (FCS_STG_EXT.1) .....	24
5.1.2.23	Extended: Encrypted Cryptographic Key Storage (FCS_STG_EXT.2) .....	24
5.1.2.24	Extended: Integrity of encrypted key storage (FCS_STG_EXT.3) .....	25
5.1.2.25	Extended: TLS Protocol (FCS_TLSC_EXT.1).....	25
5.1.2.26	Extended: TLS Protocol (FCS_TLSC_EXT.2).....	25
5.1.2.27	Extensible Authentication Protocol-Transport Layer Security (FCS_TLSC_EXT.1/WLAN) .....	25
5.1.2.28	TLS Client Protocol (FCS_TLSC_EXT.2/WLAN) .....	26
5.1.3	User data protection (FDP) .....	26
5.1.3.1	Extended: Security access control (FDP_ACF_EXT.1).....	26
5.1.3.2	Extended: Security access control (FDP_ACF_EXT.2).....	26
5.1.3.3	Extended: Protected Data Encryption (FDP_DAR_EXT.1) .....	27
5.1.3.4	Extended: Sensitive Data Encryption (FDP_DAR_EXT.2).....	27
5.1.3.5	Extended: Subset information flow control (FDP_IFC_EXT.1).....	27
5.1.3.6	Extended: Storage of Critical Biometric Parameters.....	27
5.1.3.7	Extended: User Data Storage (FDP_STG_EXT.1) .....	27
5.1.3.8	Extended: Inter-TSF user data transfer protection (FDP_UPC_EXT.1) .....	27
5.1.4	Identification and authentication (FIA).....	28
5.1.4.1	Extended: Authentication failure handling (FIA_AFL_EXT.1).....	28
5.1.4.2	Extended: Bluetooth User Authorization (FIA_BLT_EXT.1).....	28
5.1.4.3	Extended: Bluetooth Mutual Authentication (FIA_BLT_EXT.2).....	28
5.1.4.4	Extended: Rejection of Duplicate Bluetooth Connections (FIA_BLT_EXT.3) .....	28
5.1.4.5	Extended: Secure Simple Pairing (FIA_BLT_EXT.4).....	28
5.1.4.6	Extended: Bluetooth User Authorization (FIA_BLT_EXT.6).....	29
5.1.4.7	Extended: Accuracy of Biometric Authentication (FIA_BMG_EXT.1).....	29
5.1.4.8	Port Access Entity Authentication (FIA_PAE_EXT.1) .....	29
5.1.4.9	Extended: Password Management (FIA_PMG_EXT.1) .....	29
5.1.4.10	Extended: Authentication Throttling (FIA_TRT_EXT.1) .....	29
5.1.4.11	Multiple Authentication Mechanisms (FIA_UAU.5) .....	29
5.1.4.12	Re-Authentication (FIA_UAU.6(1)).....	30
5.1.4.13	Re-Authentication (FIA_UAU.6(2)).....	30

5.1.4.14	Protected authentication feedback (FIA_UAU.7).....	30
5.1.4.15	Extended: Authentication for Cryptographic Operation (FIA_UAU_EXT.1) .....	30
5.1.4.16	Extended: Timing of Authentication (FIA_UAU_EXT.2).....	30
5.1.4.17	Extended: Validation of certificates (FIA_X509_EXT.1).....	31
5.1.4.18	Extended: X509 certificate authentication (FIA_X509_EXT.2) .....	31
5.1.4.19	X.509 Certificate Authentication (EAP-TLS) (FIA_X509_EXT.2/WLAN).....	31
5.1.4.20	Extended: Request Validation of certificates (FIA_X509_EXT.3).....	31
5.1.5	Security management (FMT) .....	31
5.1.5.1	Extended: Management of security functions behavior (FMT_MOF_EXT.1).....	31
5.1.5.2	Extended: Specification of Management Functions (FMT_SMF_EXT.1) .....	32
5.1.5.3	Specification of Management Functions (Wireless LAN) (FMT_SMF_EXT.1/WLAN) .....	36
5.1.5.4	Extended: Specification of Remediation Actions (FMT_SMF_EXT.2) .....	36
5.1.5.5	Extended: Current Administrator (FMT_SMF_EXT.3) .....	37
5.1.6	Protection of the TSF (FPT) .....	37
5.1.6.1	Extended: Anti-Exploitation Services (ASLR) (FPT_AEX_EXT.1).....	37
5.1.6.2	Extended: Anti-Exploitation Services (Memory Page Permissions) (FPT_AEX_EXT.2) .....	37
5.1.6.3	Extended: Anti-Exploitation Services (Overflow Protection) (FPT_AEX_EXT.3) .....	37
5.1.6.4	Extended: Domain Isolation (FPT_AEX_EXT.4).....	37
5.1.6.5	Extended: Anti-Exploitation Services (ASLR) (FPT_AEX_EXT.5).....	37
5.1.6.6	Extended: Application Processor Mediation (FPT_BBD_EXT.1) .....	37
5.1.6.7	Extended: JTAG Disablement (FPT_JTA_EXT.1).....	37
5.1.6.8	Extended: Key Storage (FPT_KST_EXT.1) .....	38
5.1.6.9	Extended: No Key Transmission (FPT_KST_EXT.2) .....	38
5.1.6.10	Extended: No Plaintext Key Export (FPT_KST_EXT.3).....	38
5.1.6.11	Extended: Self-Test Notification (FPT_NOT_EXT.1) .....	38
5.1.6.12	Reliable time stamps (FPT_STM.1).....	38
5.1.6.13	Extended: TSF Cryptographic Functionality Testing (FPT_TST_EXT.1) .....	38
5.1.6.14	TSF Cryptographic Functionality Testing (Wireless LAN) (FPT_TST_EXT.1/WLAN) .....	38
5.1.6.15	Extended: TSF Integrity Checking (FPT_TST_EXT.2(1)).....	38
5.1.6.16	Extended: Trusted Update: TSF version query (FPT_TUD_EXT.1).....	38
5.1.6.17	Extended: TSF Update Verification (FPT_TUD_EXT.2) .....	39
5.1.7	TOE access (FTA) .....	39
5.1.7.1	Extended: TSF- and User-initiated Locked State (FTA_SSL_EXT.1).....	39
5.1.7.2	Default TOE Access Banners (FTA_TAB.1).....	39
5.1.7.3	Wireless Network Access (FTA_WSE_EXT.1).....	39
5.1.8	Trusted path/channels (FTP).....	39

5.1.8.1	Extended: Trusted channel Communication (FTP_ITC_EXT.1)	39
5.1.8.2	Trusted Channel Communication (Wireless LAN) (FTP_ITC_EXT.1/WLAN)	40
5.2	TOE Security Assurance Requirements	40
5.2.1	Development (ADV)	40
5.2.1.1	Basic Functional Specification (ADV_FSP.1)	40
5.2.2	Guidance documents (AGD)	41
5.2.2.1	Operational User Guidance (AGD_OPE.1)	41
5.2.2.2	Preparative Procedures (AGD_PRE.1)	41
5.2.3	Life-cycle support (ALC)	42
5.2.3.1	Labelling of the TOE (ALC_CMC.1)	42
5.2.3.2	TOE CM Coverage (ALC_CMS.1)	42
5.2.3.3	Timely Security Updates (ALC_TSU_EXT.1)	42
5.2.4	Tests (ATE)	43
5.2.4.1	Independent Testing - Conformance (ATE_IND.1)	43
5.2.5	Vulnerability assessment (AVA)	43
5.2.5.1	Vulnerability Survey (AVA_VAN.1)	43
6.	TOE Summary Specification	44
6.1	Security audit	44
6.2	Cryptographic support	46
6.3	User data protection	51
6.4	Identification and authentication	55
6.5	Security Management	58
6.6	Protection of the TSF	58
6.7	TOE access	62
6.8	Trusted path/channels	63
7.	TSF Inventory	64

## LIST OF TABLES

<b>Table 1</b>	<b>TOE Security Functional Components</b>	19
<b>Table 2</b>	<b>Security Management Functions</b>	32
<b>Table 3</b>	<b>WLAN Security Management Functions</b>	36
<b>Table 4</b>	<b>EAL 1 augmented with ALC_TSU_EXT.1 Assurance Components</b>	40
<b>Table 5</b>	<b>Audit Events</b>	45
<b>Table 6</b>	<b>Asymmetric Key Generation</b>	46
<b>Table 7</b>	<b>BoringSSL Cryptographic Algorithms</b>	48
<b>Table 8</b>	<b>KDF Cryptographic Algorithms</b>	48
<b>Table 9</b>	<b>SDM845 Hardware Cryptographic Algorithms</b>	48
<b>Table 10</b>	<b>Functional Categories</b>	53
<b>Table 11</b>	<b>Power-up Cryptographic Algorithm Known Answer Tests</b>	61

## 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 is Pixel 3 and Pixel 3 XL provided by Google LLC. 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)

### 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 parenthetical number 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.
  - 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 ...”).
- 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** – Pixel 3 and Pixel 3 XL (MDFPP31/WLANCEP10) Security Target

**ST Version** – Version 0.6

**ST Date** – 2019/07/17

### 1.2 TOE Reference

**TOE Identification** – Google LLC Pixel 3 and Pixel 3 XL

**TOE Developer** – Google LLC

**Evaluation Sponsor** – Google LLC

### 1.3 TOE Overview

The Target of Evaluation (TOE) is Pixel 3 and Pixel 3 XL. The only variation between the two devices is the screen and battery size, shown below.

Feature	Pixel 3 Smartphone / Pixel 3 XL Smartphone
Display	OLED 5.5", 18:9 ratio (1920x1080) / OLED 6.3", 18.5:9 (2560x1440)
Camera	Rear 12.2 MP dual-pixel Standard-Angle Lens f/1.8 with LED Flash Front Dual Cameras with 8 MP Lens f/2.2 (wide-angle) and f/1.8 (Normal)
Communications	4G LTE Network / Mobile Hotspot / Bluetooth 5.0 / Wi-Fi Direct / USB and Bluetooth Tethering / Android Beam(NFC) / Media Server / Screen Sharing(Miracast) / HD Voice / MIDI Device / MirrorLink / S-GPS, A-GPS and Qualcomm Service for Enhanced Location Accuracy
Processor/ chipset	Processor: Qualcomm Snapdragon™ 845 up to 2.8 GHz x 4 + 1.7 GHz x 4 Octa-Core SDM845, GPU: Adreno 630
RAM	4 GB RAM
Storage	64/128 GB internal memory (non-expandable)
Battery	2915 mAh / 3430 mAh

The TOE allows basic telephony features (make and receive phone calls, send and receive SMS/MMS messages) as well as advanced network connectivity (allowing connections to both 802.11 Wi-Fi and 2G/3G/4G LTE mobile data networks). The TOE supports using client certificates to connect to access points offering WPA2 networks with 802.1x/EAP-TLS, or alternatively connecting to cellular base stations when utilizing mobile data.

The TOE offers mobile applications an Application Programming Interface (API) including that provided by the Android framework and supports API calls to the Android Management APIs.

### 1.4 TOE Description

The TOE is a mobile device to support enterprises and individual users alike. The Android 9.0 operating system includes a Linux 4.9 kernel. Additional libraries are provided to developers to help ensure secure application development and use for features such as Sensitive Data Protection.

The following models and versions are included in the evaluation:

Product	Carrier	OS version	Kernel	Build number	WFA Cert#
Google Pixel 3 (blueline)	Open	Android 9.0	4.9.14 8	PQ3A.190605.003.A3	WFA77734
Google Pixel 3 XL (crosshatch)	Open	Android 9.0	4.9.14 8	PQ3A.190605.003.A3	WFA78505

By default, some features and settings must be enabled for the TOE to be in evaluated configuration. The following features and settings must be enabled:

1. Enable the password on the lock screen
2. Disable SmartLock
3. Leave developer mode USB debugging in its default state of disabled
4. Disable Side Loading of Applications
5. VPN Full Tunnel Configuration
6. Enable Audit logging

Doing this ensures that the phone complies with the MDFPP requirements

Please refer to the Admin Guide on how to configure the required settings and features.

---

## 1.4.1 TOE Architecture

---

The TOE provides a rich API to mobile applications and provides users installing an application the option to either approve or reject an application based upon the API access that the application requires (or to grant applications access at runtime).

The TOE also provides users with the ability to protect Data-At-Rest with AES encryption, including all user and mobile application data stored in the user's data partition. The TOE uses a key hierarchy that combines a REK with the user's password to provide protection to all user and application cryptographic keys stored in the TOE.

Finally, the TOE can interact with a Mobile Device Management (MDM) system (not part of this evaluation) to allow enterprise control of the configuration and operation of the device so as to ensure adherence to enterprise-wide policies (for example, restricting use of a corporate provided device's camera, forced configuration of maximum login attempts, pulling of audit logs off the TOE, etc.) as well as policies governing enterprise applications and data (in a an employee-owned device [BYOD] scenario). An MDM is made up of two parts: the MDM agent and MDM server. The MDM Agent is installed on the phone as an administrator with elevated permissions (allowing it to change the relevant settings on the phone) while the MDM Server is used to issue the commands to the MDM Agent. Neither portion of the MDM process is considered part of the TOE, and therefore not being directly evaluated.

The TOE includes several different levels of execution including (from lowest to highest): hardware, a Trusted Execution Environment, Android's Linux kernel, and Android's user space, which provides APIs allowing applications to leverage the cryptographic functionality of the device.

---

### 1.4.1.1 Physical Boundaries

---

The TOE's physical boundary is the physical perimeter of its enclosure. The software of the device is Android 9 running on the Qualcomm Snapdragon 845. The TOE does not include the user applications that run on top of the operating system, but does include controls that limit application behavior. Further, the device provides support for downloadable MDM agents to be installed to limit or permit different functionality of the device. There is no built-in MDM agent pre-installed on the device.

The TOE communicates and interacts with 802.11-2012 Access Points and mobile data networks to establish network connectivity, and 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 Pixel 3 and Pixel 3 XL:

- 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 implements a security log, logcat, and intent logging that are each stored in a circular memory buffer of various sizes. An MDM agent can read/fetch the security log and intents and then handle appropriately (potentially storing the log to Flash or transmitting its contents to the MDM server). These log methods meet the logging

requirements outlined by FAU\_GEN.1 in MDFPPv3.1. Please see the Security audit section for further information and specifics.

---

#### 1.4.1.2.2 **Cryptographic support**

---

The TOE includes multiple cryptographic libraries with CAVP certified algorithms for a wide range of cryptographic functions including the following: 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, EAP-TLS, IPsec, and HTTPS and 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 allowing application developers to ensure their application meets the required criteria to remain compliant to MDFPP standards.

---

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

---

The TOE controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE protects user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected. The TOE's evaluated configuration supports Android Enterprise profiles to provide additional separation between application and application data belonging to the Enterprise profile. Please see the Admin Guide for additional details regarding how to set up and use Enterprise profiles.

---

#### 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 FCC mandated (making phone calls to an emergency number) or non-sensitive functions (e.g., choosing the keyboard input method or taking screen shots), a password (i.e., Password Authentication Factor) must be correctly entered to unlock the TOE. Also, even when unlocked, the TOE requires the user re-enter the password 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 up to 16 characters are supported.

The TOE can also serve as an 802.1X supplicant and can both use X.509v3 and validate certificates for EAP-TLS, TLS, and HTTPS 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 will remove Enterprise applications and remove MDM policies.

---

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

---

The TOE implements a number of features 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 through the use of the application processor's hardware. The TOE disallows all read access to the Root Encryption Key and retains all keys derived from the REK within its the Trusted Execution Environment (TEE). Application software can only use keys derived from the REK by reference and receive the result.

The TOE 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

also protects 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 as all applications must have signatures (even if self-signed).

---

#### 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 administrator specified (using the TOE's MDM API) advisory message (banner) when the user unlocks the TOE for the first use after reboot.

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 IEEE 802.11-2012, 802.1X, and EAP-TLS to secure communications channels between itself and other trusted network devices.

---

### 1.4.2 TOE Documentation

---

Google Android 9.0 (Pixel 3/3XL) Guidance Documentation, Version 2.1, 07/16/2019 [Admin Guide]

## 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 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
  - Part 3 Conformant
- Package Claims:
  - Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017 and General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016 (MDFPP31/WLANCEP10)
- Technical Decisions:

TD No.	Applied?	Rationale
TD0194 – WLANCEP10	Yes	Impacts required audit events
TD0236 – MDFPP31	No	Superseded by TD0244
TD0244 – MDFPP31/WLANCEP10	Yes	Allows additional TLSC curves
TD0301 – MDFPP31	Yes	Impacts Assurance Activities and allows for assignment for FIA_BMG_EXT.1.1
TD0304 – MDFPP31	Yes	Impacts Assurance Activities
TD0305 – MDFPP31	Yes	Impacts Assurance Activities
TD0346 – MDFPP31	Yes	Removes selection from FMT_SMF_EXT.2.1
TD0347 – MDFPP31	No	Use Case 2 not selected
TD0351 – MDFPP31	Yes	Adds DEK selections to FCS_CKM_EXT.2.1
TD0366 – MDFPP31	Yes	FCS_COP.1(5) updated to reflect crypt
TD0369 – MDFPP31	Yes	LTTCKM present.
TD0371 – MDFPP31	No	Use Case 2 not selected
TD0413 – MDFPP31	Yes	Any Allowed PP-Module
TD0426 – MDFPP31	Yes	Impacts Assurance Activities

### 2.1 Conformance Rationale

The ST conforms to the MDFPP31/WLANCEP10. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

### 3. Security Objectives

The Security Problem Definition may be found in the MDFPP31/WLANCCEP10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The MDFPP31/WLANCCEP10 offers additional information about the identified security objectives, but that has not been reproduced here and the MDFPP31/WLANCCEP10 should be consulted if there is interest in that material.

In general, the MDFPP31/WLANCCEP10 has defined Security Objectives appropriate for mobile device and as such are applicable to the Pixel 3 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.NO\_TOE\_BYPASS** Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

**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.

**OE.TRUSTED\_ADMIN** TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

## 4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the MDFPP31/WLANCEP10. The MDFPP31/WLANCEP10 defines the following extended requirements and since they are not redefined in this ST the MDFPP31/WLANCEP10 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\_SRV\_EXT.2: 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: TLS Protocol
- FCS\_TLSC\_EXT.2: Extended: TLS Protocol
- FCS\_TLSC\_EXT.1/WLAN: Extensible Authentication Protocol-Transport Layer Security
- FCS\_TLSC\_EXT.2/WLAN: TLS Client Protocol
- FDP\_ACF\_EXT.1: Extended: Security access control
- FDP\_ACF\_EXT.2: 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\_PBA\_EXT.1: Extended: Storage of Critical Biometric Parameters
- FDP\_STG\_EXT.1: Extended: User Data Storage
- FDP\_UPC\_EXT.1: Extended: Inter-TSF user data transfer protection
- FIA\_AFL\_EXT.1: Extended: Authentication failure handling
- FIA\_BLT\_EXT.1: Extended: Bluetooth User Authorization
- FIA\_BLT\_EXT.2: Extended: Bluetooth Mutual Authentication
- FIA\_BLT\_EXT.3: Extended: Rejection of Duplicate Bluetooth Connections

- FIA\_BLT\_EXT.4: Extended: Secure Simple Pairing
- FIA\_BLT\_EXT.6: Extended: Bluetooth User Authorization
- FIA\_BMG\_EXT.1: Extended: Accuracy of Biometric Authentication
- FIA\_PAE\_EXT.1: Port Access Entity 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\_X509\_EXT.1: Extended: Validation of certificates
- FIA\_X509\_EXT.2: Extended: X509 certificate authentication
- FIA\_X509\_EXT.2/WLAN: X.509 Certificate Authentication (EAP-TLS)
- 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.1/WLAN: Specification of Management Functions (Wireless LAN)
- FMT\_SMF\_EXT.2: Extended: Specification of Remediation Actions
- FMT\_SMF\_EXT.3: Extended: Current Administrator
- 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\_AEX\_EXT.5: Extended: Anti-Exploitation Services (ASLR)
- FPT\_BBD\_EXT.1: Extended: Application Processor Mediation
- FPT\_JTA\_EXT.1: Extended: JTAG Disablement
- 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.1/WLAN: TSF Cryptographic Functionality Testing (Wireless LAN)
- FPT\_TST\_EXT.2(1): Extended: TSF Integrity Checking
- FPT\_TUD\_EXT.1: Extended: Trusted Update: TSF version query
- FPT\_TUD\_EXT.2: Extended: TSF Update Verification
- FTA\_SSL\_EXT.1: Extended: TSF- and User-initiated Locked State
- FTA\_WSE\_EXT.1: Wireless Network Access

- FTP\_ITC\_EXT.1: Extended: Trusted channel Communication
- FTP\_ITC\_EXT.1/WLAN: Trusted Channel Communication (Wireless LAN)

**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 MDFPP31/WLANCEP10. The refinements and operations already performed in the MDFPP31/WLANCEP10 are not identified (e.g., highlighted) here, rather the requirements have been copied from the MDFPP31/WLANCEP10 and any residual operations have been completed herein. Of particular note, the MDFPP31/WLANCEP10 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 MDFPP31/WLANCEP10 which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the MDFPP31/WLANCEP10 that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. The MDFPP31/WLANCEP10 should be consulted for the assurance activity definitions.

### 5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Pixel 3 TOE.

Requirement Class	Requirement Component
<b>FAU: Security audit</b>	FAU_GEN.1: Audit Data Generation
	FAU_STG.1: Audit Storage Protection
	FAU_STG.4: Prevention of Audit Data Loss
<b>FCS: Cryptographic support</b>	FCS_CKM.1: Cryptographic key generation
	FCS_CKM.1/WLAN: Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)
	FCS_CKM.2(1): Cryptographic key establishment
	FCS_CKM.2(2): Cryptographic key establishment (While device is locked)
	FCS_CKM.2/WLAN: Cryptographic Key Distribution (GTK)
	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_SRV_EXT.2: 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: TLS Protocol
	FCS_TLSC_EXT.2: Extended: TLS Protocol
	FCS_TLSC_EXT.1/WLAN: Extensible Authentication Protocol-Transport Layer Security
	FCS_TLSC_EXT.2/WLAN: TLS Client Protocol
<b>FDP: User data protection</b>	FDP_ACF_EXT.1: Extended: Security access control
	FDP_ACF_EXT.2: 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_PBA_EXT.1: Extended: Storage of Critical Biometric Parameters
	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: Extended: Authentication failure handling
	FIA_BLT_EXT.1: Extended: Bluetooth User Authorization
	FIA_BLT_EXT.2: Extended: Bluetooth Mutual Authentication
	FIA_BLT_EXT.3: Extended: Rejection of Duplicate Bluetooth Connections
	FIA_BLT_EXT.4: Extended: Secure Simple Pairing
	FIA_BLT_EXT.6: Extended: Bluetooth User Authorization
	FIA_BMG_EXT.1: Extended: Accuracy of Biometric Authentication
	FIA_PAE_EXT.1: Port Access Entity Authentication
	FIA_PMG_EXT.1: Extended: Password

	Management
	FIA_TRT_EXT.1: Extended: Authentication Throttling
	FIA_UAU.5: Multiple Authentication Mechanisms
	FIA_UAU.6(1): Re-Authentication
	FIA_UAU.6(2): Re-Authentication
	FIA_UAU.7: Protected authentication feedback
	FIA_UAU_EXT.1: Extended: Authentication for Cryptographic Operation
	FIA_UAU_EXT.2: Extended: Timing of Authentication
	FIA_X509_EXT.1: Extended: Validation of certificates
	FIA_X509_EXT.2: Extended: X509 certificate authentication
	FIA_X509_EXT.2/WLAN: X.509 Certificate Authentication (EAP-TLS)
	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.1/WLAN: Specification of Management Functions (Wireless LAN)
	FMT_SMF_EXT.2: Extended: Specification of Remediation Actions
	FMT_SMF_EXT.3: Extended: Current Administrator
<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_AEX_EXT.5: Extended: Anti-Exploitation Services (ASLR)
	FPT_BBD_EXT.1: Extended: Application Processor Mediation
	FPT_JTA_EXT.1: Extended: JTAG Disablement
	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.1/WLAN: TSF Cryptographic Functionality Testing (Wireless LAN)

	FPT_TST_EXT.2(1): Extended: TSF Integrity Checking
	FPT_TUD_EXT.1: Extended: Trusted Update: TSF version query
	FPT_TUD_EXT.2: Extended: TSF 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: Wireless Network Access
<b>FTP: Trusted path/channels</b>	FTP_ITC_EXT.1: Extended: Trusted channel Communication
	FTP_ITC_EXT.1/WLAN: Trusted Channel Communication (Wireless LAN)

**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 auditable events for the not selected level of audit
3. All administrative actions
4. Start-up and shutdown of the Rich OS
5. Insertion or removal of removable media
6. Specifically defined auditable events in Table 1
7. [*No other auditable events*]
8. [*Specifically defined auditable events in Table 2*]

##### 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
5. additional information in Table 1
6. [*no additional information*]

#### 5.1.1.2 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.

#### 5.1.1.3 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)

#### FCS\_CKM.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 FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3,*  
*ECC schemes using ['NIST curves' P-384 and [P-256] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4].*

### 5.1.2.2 Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) (FCS\_CKM.1/WLAN)

#### FCS\_CKM.1.1/WLAN

Refinement: The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm PRF-384 and [*PRF-704*] and specified cryptographic key sizes 128 bits and [*256 bits*] using a Random Bit Generator as specified in FCS\_RBG\_EXT.1 that meet the following: IEEE 802.11-2012 and [*IEEE 802.11ac-2014*].

### 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']*.

### 5.1.2.4 Cryptographic key establishment (While device is locked) (FCS\_CKM.2(2))

#### FCS\_CKM.2(2).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",]*

for the purposes of encrypting sensitive data received while the device is locked.

### 5.1.2.5 Cryptographic Key Distribution (GTK) (FCS\_CKM.2/WLAN)

#### FCS\_CKM.2.1/WLAN

Refinement: The TSF shall decrypt Group Temporal Key in accordance with a specified cryptographic key distribution method AES Key Wrap in an EAPOL-Key frame that meets the following: RFC 3394 for AES Key Wrap, 802.11-2012 for the packet format and timing considerations and does not expose the cryptographic keys.

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

#### FCS\_CKM\_EXT.1.1

The TSF shall support [*immutable hardware*] REK(s) with a [*symmetric*] key of strength [*256 bits*].

**FCS\_CKM\_EXT.1.2**

Each REK shall be hardware-isolated from Rich OS on the TSF in runtime.

**FCS\_CKM\_EXT.1.3**

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

---

**5.1.2.7 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.

(TD0351 applied)

---

**5.1.2.8 Extended: Cryptographic Key Generation (FCS\_CKM\_EXT.3)**


---

**FCS\_CKM\_EXT.3.1**

The TSF shall use [

*asymmetric KEKs of [150-bit] security strength,  
symmetric KEKs of [256-bit] security strength corresponding to at least the security strength of the keys encrypted by the KEK*].

**FCS\_CKM\_EXT.3.2**

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

Derive the KEK from a Password Authentication Factor according to FCS\_COP.1.1(5)

and

*[Generate the KEK using an RBG that meets this profile (as specified in FCS\_RBG\_EXT.1),  
Generate the KEK using a key generation scheme that meets this profile (as specified in FCS\_CKM.1),  
Combine the KEK from other KEKs in a way that preserves the effective entropy of each factor by  
[encrypting one key with another]].* (TD0366 applied)

---

**5.1.2.9 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]*.
  - 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 by a read-verify.
  - For non-volatile flash memory, that is not wear-leveled, the destruction shall be executed *[by a block erase that erases the reference to memory that stores data as well as the data itself]*.
    - > Note: no non-volatile flash memory w/o wear leveling exists on this TOE.
  - For non-volatile flash memory, that is wear-leveled, the destruction shall be executed *[by a block erase]*.
  - For non-volatile memory other than EEPROM and flash, the destruction shall be executed by a single direct overwrite 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.

---

### 5.1.2.10 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 nonvolatile memory by following the requirements in FCS\_CKM\_EXT.4.1,*

*Overwriting all Protected Data according to the following rules:*

- For 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 by a read-verify).*
- For flash memory, that is not wear-leveled, the destruction shall be executed [by a block erase that erases the reference to memory that stores data as well as the data itself].*
- For flash memory, that is wear-leveled, the destruction shall be executed [by a block erase].*
- For non-volatile memory other than EEPROM and flash, the destruction shall be executed by a single direct overwrite with a random pattern that is changed before each write.].*

#### FCS\_CKM\_EXT.5.2

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

---

### 5.1.2.11 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.

---

### 5.1.2.12 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,*

*AES-CCMP-256 (as defined in NIST SP800-38C and IEEE 802.11ac-2013)]*

and cryptographic key sizes 128-bit key sizes and *[256-bit key sizes]*.

---

### 5.1.2.13 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.

---

### 5.1.2.14 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-384 and [P- 256] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5]*.

---

### 5.1.2.15 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 [*256, 384, 512-bits*] 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'.

---

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

---

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

The TSF shall perform conditioning in accordance with a specified cryptographic algorithm HMAC-*[SHA-256]* using a salt, and [*/script/*] and output cryptographic key sizes [*256*] that meet the following: NIST [*no standard*]. (TD0366 applied)

---

#### 5.1.2.17 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.1).

##### FCS\_HTTPS\_EXT.1.3

The TSF shall notify the application and [*not establish the connection*] if the peer certificate is deemed invalid.

---

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

---

##### FCS\_IV\_EXT.1.1

The TSF shall generate IVs in accordance with Table 11: References and IV Requirements for NIST-approved Cipher Modes.

---

#### 5.1.2.19 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 [*CTR\_DRBG (AES), a SHA-256 Hardware Hash\_DRBG*].

##### 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.

---

#### 5.1.2.20 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 [*selected algorithms*] in FCS\_CKM.2(2)

The following algorithms in FCS\_COP.1(1): AES-CBC, [*AES-GCM*]

All mandatory and selected algorithms in FCS\_COP.1(2)

All mandatory and selected algorithms in FCS\_COP.1(3)

All mandatory and selected algorithms in FCS\_COP.1(4)

[*All mandatory and [selected algorithms] in FCS\_CKM.1*].

---

#### 5.1.2.21 Extended: Cryptographic Algorithm Services (FCS\_SRV\_EXT.2)

---

##### FCS\_SRV\_EXT.2.1

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

- Algorithms in FCS\_COP.1(1)
- Algorithms in FCS\_COP.1(3)

by keys stored in the secure key storage.

---

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

---

##### FCS\_STG\_EXT.1.1

The TSF shall provide [*software-based*] secure key storage for asymmetric private keys and [*symmetric keys, persistent secrets*].

##### 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*]

---

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

---

##### FCS\_STG\_EXT.2.1

The TSF shall encrypt all DEKs, KEKs, [WPA2 WiFi PSK, Bluetooth Keys] and [*all software-based key storage*] by KEKs that are

[

*Protected by the REK with [*  
*encryption by a KEK chaining from a REK,*  
*encryption by a KEK that is derived from a REK*  
*],*

*Protected by the REK and the password with [*  
*encryption by a KEK chaining to a REK and the password-derived or biometric-unlocked KEK,*  
*encryption by a KEK that is derived from a REK and the password derived or biometric-unlocked KEK*  
*]*

].

##### FCS\_STG\_EXT.2.2

DEKs, KEKs, [WPA2 WiFi PSK, Bluetooth Keys] and [*all software-based key storage*] shall be encrypted using one of the following methods:

[

*using a SP800-56B key establishment scheme,*  
*using AES in the [*  
*GCM,*  
*CCM mode]*

].

---

#### 5.1.2.24 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 [*long-term trusted channel key material, all software-based key storage*] by [*JGCM, CCM*] 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.

---

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

---

##### FCS\_TLSC\_EXT.1.1

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

Mandatory Ciphersuites:

[*TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,*  
*TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246*]

Optional Ciphersuites:

[*TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 as defined in RFC 5289,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 as defined in RFC 5289,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289*]

##### FCS\_TLSC\_EXT.1.2

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

##### 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.

---

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

---

##### FCS\_TLSC\_EXT.2.1

The TSF shall present the Supported Elliptic Curves Extension in the Client Hello handshake message with the following NIST curves: [*secp256r1, secp384r1*]. (TD0244 applied, supersedes TD0236)

---

#### 5.1.2.27 Extensible Authentication Protocol-Transport Layer Security (FCS\_TLSC\_EXT.1/WLAN)

---

##### FCS\_TLSC\_EXT.1.1/WLAN

The TSF shall implement TLS 1.0 and [*TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] in support of the EAP-TLS protocol as specified in RFC 5216 supporting the following ciphersuites:

Mandatory Ciphersuites in accordance with RFC 5246:

[*TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA*

Optional Ciphersuites:

[*TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 5246,*  
*TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,*  
*TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289,*

*TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5430,  
 TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 as defined in RFC 5430,  
 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 4492,  
 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 4492,  
 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289,  
 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289].*

#### **FCS\_TLSC\_EXT.1.2/WLAN**

The TSF shall generate random values used in the EAP-TLS exchange using the RBG specified in FCS\_RBG\_EXT.1.

#### **FCS\_TLSC\_EXT.1.3/WLAN**

The TSF shall use X509 v3 certificates as specified in FIA\_X509\_EXT.1.

#### **FCS\_TLSC\_EXT.1.4/WLAN**

The TSF shall verify that the server certificate presented includes the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

#### **FCS\_TLSC\_EXT.1.5/WLAN**

The TSF shall allow an authorized administrator to configure the list of CAs that are allowed to sign authentication server certificates that are accepted by the TOE.

#### **FCS\_TLSC\_EXT.1.6/WLAN**

The TSF shall allow an authorized administrator to configure the list of algorithm suites that may be proposed and accepted during the EAP-TLS exchanges.

---

### **5.1.2.28 TLS Client Protocol (FCS\_TLSC\_EXT.2/WLAN)**

---

#### **FCS\_TLSC\_EXT.2.1/WLAN**

The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [secp256r1, secp384r1]. (TD0244 applied):

---

## **5.1.3 User data protection (FDP)**

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

---

#### **FDP\_ACF\_EXT.1.1**

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

#### **FDP\_ACF\_EXT.1.2**

The TSF shall provide an access control policy that prevents [*applications, groups of applications*] from accessing [*all*] data stored by other [*applications, groups of applications*]. Exceptions may only be explicitly authorized for such sharing by [*a common application developer, no one*].

ST Application Note: “common application developer” applies only to applications, “no one” can authorize exceptions for the personal and enterprise profiles to share data.

---

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

---

#### **FDP\_ACF\_EXT.2.1**

The TSF shall provide a separate [*address book, calendar, keychain*] for each application group and only allow applications within that process group to access the resource. Exceptions may only be explicitly authorized for such sharing by [*the administrator, no one*]

ST Application Note: “the administrator” applies only to the address book, the other selections cannot be shared between application groups.

---

### 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 [XTS] mode with key size [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 [*provide an interface which allows a VPN client to protect all IP traffic using IPsec*] with the exception of IP traffic required to establish the VPN connection.

---

### 5.1.3.6 Extended: Storage of Critical Biometric Parameters

---

#### FDP\_PBA\_EXT.1.1

The TSF shall protect the authentication template [*using a password as an additional factor*].

---

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

---

#### FDP\_STG\_EXT.1.1

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

---

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

---

#### FDP\_UPC\_EXT.1.1

The TSF shall 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 Extended: Authentication failure handling (FIA\_AFL\_EXT.1)

---

###### FIA\_AFL\_EXT.1.1

The TSF shall consider password and [*fingerp*rint] as critical authentication mechanisms.

###### FIA\_AFL\_EXT.1.2

The TSF shall detect when a configurable positive integer within [**0 and 2,147,483,647**] of [*non-unique*] unsuccessful authentication attempts occur related to last successful authentication for each authentication mechanism.

###### FIA\_AFL\_EXT.1.3

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

###### FIA\_AFL\_EXT.1.4

When the defined number of unsuccessful authentication attempts has exceeded the maximum allowed for a given authentication mechanism, all future authentication attempts will be limited to other available authentication mechanisms, unless the given mechanism is designated as a critical authentication mechanism.

###### FIA\_AFL\_EXT.1.5

When the defined number of unsuccessful authentication attempts for the last available authentication mechanism or single critical authentication mechanism has been surpassed, the TSF shall perform a wipe of all protected data.

###### FIA\_AFL\_EXT.1.6

The TSF shall increment the number of unsuccessful authentication attempts prior to notifying the user that the authentication was unsuccessful.

---

##### 5.1.4.2 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.

---

##### 5.1.4.3 Extended: Bluetooth Mutual 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.

---

##### 5.1.4.4 Extended: 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.

---

##### 5.1.4.5 Extended: Secure Simple Pairing (FIA\_BLT\_EXT.4)

---

###### FIA\_BLT\_EXT.4.1

The TOE shall support Bluetooth Secure Simple Pairing, both in the host and the controller. Furthermore, Secure Simple Pairing shall be used during the pairing process if the remote device also supports it.

---

#### 5.1.4.6 Extended: Bluetooth User Authorization (FIA\_BLT\_EXT.6)

---

##### FIA\_BLT\_EXT.6.1

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

---

#### 5.1.4.7 Extended: Accuracy of Biometric Authentication (FIA\_BMG\_EXT.1)

---

##### FIA\_BMG\_EXT.1.1

The one-attempt BAF False Accept Rate (FAR) for [*fingerprint*] shall not exceed [*1:100,000*] with a one-attempt BAF False Reject Rate (FRR) not to exceed 1 in [*1:20*]. (TD0301 applied)

##### FIA\_BMG\_EXT.1.2

The overall System Authentication False Accept Rate (SAFAR) shall be no greater than 1 in [*1:5,000*] within a 1% margin.

---

#### 5.1.4.8 Port Access Entity 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.

---

#### 5.1.4.9 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.

---

#### 5.1.4.10 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*] for all authentication mechanisms selected in FIA\_UAU.5.1. The minimum delay shall be such that no more than 10 attempts can be attempted per 500 milliseconds.

---

#### 5.1.4.11 Multiple Authentication Mechanisms (FIA\_UAU.5)

---

##### FIA\_UAU.5.1

The TSF shall provide password and [*fingerprint*] to support user authentication.

##### FIA\_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*following rules*]:

*To authenticate unlocking the device immediately after boot (first unlock after reboot):*

- *User passwords are required after reboot to unlock the user's Credential encrypted (CE files) and keystore keys. Fingerprint authentication is disabled immediately after boot.*

*To authenticate unlocking the device after device lock (not following a reboot):*

- *The TOE verifies user credentials (password or fingerprint) via the gatekeeper or fingerprint trusted application (running inside the Trusted Execution Environment, TEE), which compares the entered credential to a derived value or template.*

*To change protected settings or issue certain commands:*

- *The TOE requires password after a reboot, when changing settings (Screen lock, Fingerprint, and Smart Lock settings), and when factory resetting.”*

].

---

#### 5.1.4.12 Re-Authentication (FIA\_UAU.6(1))

---

##### FIA\_UAU.6(1).1

The TSF shall re-authenticate the user via the Password Authentication Factor under the conditions attempted change to any supported authentication mechanisms.

---

#### 5.1.4.13 Re-Authentication (FIA\_UAU.6(2))

---

##### FIA\_UAU.6(2).1

The TSF shall re-authenticate the user via an authentication factor defined in FIA\_UAU.5.1 under the conditions TSF-initiated lock, user-initiated lock, [*no other conditions*].

---

#### 5.1.4.14 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.

---

#### 5.1.4.15 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 [*all software-based key storage*] at startup.

---

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

---

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

The TSF shall allow [

- *Choosing of the keyboard input method,*
- *Make emergency phone calls,*
- *Take screen shots (stored internally),*
- *Receive calls,*
- *Turn TOE off,*
- *Restart TOE,*
- *Enable/disable airplane mode,*
- *Take photos (stored internally) - can view and delete photos taken since last screen lock,*
- *Toggle: WiFi, Bluetooth, Do not Disturb Mode, Flashlight, Auto-rotate, Batter Saver Mode, Mobile Data, Night Light Mode*
  - o *Note: WiFi/Bluetooth can be toggled to disconnect or connect to a remembered connection, but any new connection establishment requires a device unlock*
- *Adjust brightness level*
- *Adjust volume level or silence device*
- *View/clear notifications*
- *View Clock/Date*
- *View Lock Screen Banner*

] 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.

---

#### 5.1.4.17 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*]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - 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
  - 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
  - (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.

---

#### 5.1.4.18 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 [*TLS and HTTPS*], and [*no additional uses*].

##### FIA\_X509\_EXT.2.2

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

---

#### 5.1.4.19 X.509 Certificate Authentication (EAP-TLS) (FIA\_X509\_EXT.2/WLAN)

---

##### FIA\_X509\_EXT.2.1/WLAN

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for EAP-TLS exchanges.

##### FIA\_X509\_EXT.2.2/WLAN

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

---

#### 5.1.4.20 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 2 Security Management Functions**

to the user.

### FMT\_MOF\_EXT.1.2

The TSF shall restrict the ability to perform the 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.

## 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**.

**Table 2 Security Management Functions**

Management Function	FMT_SMF_EXT.1.1	FMT_MOF_EXT.1.1 Administrator	FMT_MOF_EXT.1.2
<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <b>Status Markers:</b>            M – Mandatory            I – Implemented optional function         </div> <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.</p> <p>Length: an integer value of characters            Complexity: Unspecified, Something, Numeric, Alphabetic, Alphanumeric, Complex.            Lifetime: an integer value of seconds (0 = no maximum).</p>	M		M M
<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.            Screen lock timeout: an integer number of minutes before the TOE locks (0 = no lock timeout)            Authentication failures: an integer number (-2,147,483,648 to 2,147,483,648 [negative integers and zero means no limit]).</p>	M		M M
<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>Both users (using the TOE's settings UI) and administrator (using the TOE's MDM APIs) can configure a third-party VPN client and then enable the VPN client to protect traffic. The User can set up VPN protection, but if an admin enables VPN protection, the user cannot disable it.</p>	M		I I
<p>4. enable/disable [GPS, Bluetooth BR/DR, Bluetooth LE, NFC, Wi-Fi, cellular]</p>	M M	I	I I

<p>The administrator can disable the radios using the TOE's MDM APIs. Once disabled, a user cannot enable the radio. The TOE's radios operate at frequencies of 2.4 GHz (NFC/Bluetooth), 2.4/5 GHz (Wi-Fi), and 850, 900, 1800, 1900 MHz (4G/LTE).</p>				
<p>5. enable/disable [<b>microphone, camera</b>]:</p> <p>a. across device (microphone),</p> <p>[ <b>b. on a per-app basis (microphone, camera)</b>]</p> <p>An administrator can enable/disable the device's microphone via an MDM API. Once the microphone has been disabled, the user cannot re-enable it until the administrator enables it.</p> <p>In the user's settings, a user can view a permission by type (i.e. camera, microphone). The user can access this by going to "Settings" -&gt; "App Permissions" -&gt; Selecting the permission and revoking any applications.</p>	M M		I I	
<p>6. transition to the locked state</p> <p>Both users (using the TOE's settings UI) and administrators (using the TOE's MDM APIs) can transition the TOE into a locked state.</p>	M		M	
<p>7. full wipe of protected data</p> <p>Both users (using the TOE's settings UI) and administrators (using the TOE's MDM APIs) can force the TOE to perform a full wipe (factory reset) of data.</p>	M		M	
<p>8. configure application installation policy by:</p> <p>a. <b>restricting the sources of applications, denying installation of applications]</b></p> <p>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.</p>	M		M	M
<p>9. import keys/secrets into the secure key storage</p> <p>Both users (using the TOE's settings UI) and administrators (using the TOE's MDM APIs) can import secret keys into the secure key storage.</p>	M		I	
<p>10. destroy imported keys/secrets and [<b>no other keys/secrets</b>] in the secure key storage</p> <p>Both users and administrators (using the TOE's MDM APIs) can destroy secret keys in the secure key storage.</p>	M		I	
<p>11. import X.509v3 certificates into the Trust Anchor Database</p> <p>Both users (using the TOE's settings UI) and administrators (using the TOE's MDM APIs) can import X.509v3 certificates into the Trust Anchor Database.</p>	M		M	
<p>12. remove imported X.509v3 certificates and [<b>no other certificates</b>] in the Trust Anchor Database</p> <p>Both users (using the TOE's settings UI) 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 untrusted).</p>	M		I	
<p>13. enroll the TOE in management</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</p>	M	M		

MDM agent application) on the TOE prior to enrollment.				
14. remove applications	M		M	
Both users (using the TOE's settings UI) and administrators (using the TOE's MDM APIs) can uninstall user and administrator installed applications on the TOE.				
15. update system software	M		M	
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.				
16. install applications	M		M	
Both users and administrators (using the TOE's MDM APIs) can install applications on the TOE.				
17. remove Enterprise applications	M		M	
An administrator (using the TOE's MDM APIs) can uninstall Enterprise installed applications on the TOE.				
18. configure the Bluetooth trusted channel: <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> </ul> <b>[k. no other Bluetooth configuration]</b>	M			
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 which utilizes NFC and Bluetooth, and can be enabled and disabled by the TOE user.				
19. enable/disable display notification in the locked state of: [ <b>all notifications]</b>	M		I	I
Notifications can be configured to display in the following formats: Users & administrators: show all notification content Users: hide sensitive content Users & administrators: hide notifications entirely				
If the administrator sets any of the above settings, the user cannot change it.				
20. enable data-at rest protection	M			
The TOE always encrypts its user data storage.				
21. enable removable media's data-at-rest protection				
The device's DAR protection cannot be disabled.				
22. enable/disable location services: <ul style="list-style-type: none"> <li>a. across device</li> </ul> <b>[d. no other method]</b>	M		I	I
The administrator (using the TOE's MDM APIs) can enable or disable location services.				
An additional MDM API can prohibit TOE users ability to enable and disable location services.				
23. Enable/disable the use of [ <b>selection: Biometric Authentication Factor</b> ]	I		I	I

24. enable/disable all data signaling over [USB]				
25. enable/disable [Wi-Fi hotspot, USB tethering, and Bluetooth tethering]				
The administrator (using the TOE's MDM APIs) can enable/disable all tethering methods (i.e. all or none disabled).				
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.				
26. enable/disable developer modes				
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.				
27. enable/disable bypass of local user authentication				
N/A – It is not possible to bypass local user auth for this TOE				
28. wipe Enterprise data				
An administrator can remove Enterprise applications and their data.				
29. approve [import, removal] by applications of X.509v3 certificates in the Trust Anchor Database				
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				
32. read audit logs kept by the TSF				
33. configure [selection: certificate, public-key] 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				
36. configure the unlock banner				
37. configure the auditable items				
38. retrieve TSF-software integrity verification values				
39. enable/disable [ <ul style="list-style-type: none"> <li>a. USB mass storage mode,</li> <li>b. USB data transfer without user authentication,</li> <li>c. USB data transfer without authentication of the connecting system</li> </ul> ]				
40. enable/disable backup to [all applications] to [remote system]				
41. enable/disable [ <ul style="list-style-type: none"> <li>a. Hotspot functionality authenticated by [pre-shared key],</li> <li>b. USB tethering authenticated by [no authentication]</li> </ul>				
The administrator (using the TOE's MDM APIs) can disable the Wi-Fi hotspot and USB tethering.				
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).				
42. approve exceptions for sharing data between [groups of application]				
43. place applications into application process groups based on [assignment: enterprise]				

<i>configuration settings]</i>				
44. Unenroll the TOE from management	I		I	I
45. Enable/disable the Always On VPN protection	I		I	I
46. Revoke Biometric template				
47. <i>[assignment: list of other management functions to be provided by the TSF]</i>				

### 5.1.5.3 Specification of Management Functions (Wireless LAN) (FMT\_SMF\_EXT.1/WLAN)

#### FMT\_SMF\_EXT.1.1/WLAN

The TSF shall be capable of performing the following management functions:

**Table 3 WLAN Security Management Functions**

Management Function	Function	Available to User role	Available to Admin	Restricted to Admin
48. configure security policy for each wireless network: a. <i>[specify the CA(s) from which the TSF will accept WLAN authentication server certificate(s)]</i> b. security type c. authentication protocol d. client credentials to be used for authentication	M		I	
49. specify wireless networks (SSIDs) to which the TSF may connect;  An administrator can specify a list of wireless networks to which the TOE may connect and can restrict the TOE to only allow a connection to the specified networks.	I		I	
50. enable/disable certificate revocation list checking;				
51. disable ad hoc wireless client-to-client connection capability,				
52. disable wireless network bridging capability (for example, bridging a connection between the WLAN and cellular radios on a smartphone so it can function as a hotspot);				
53. disable roaming capability;				
54. enable/disable IEEE 802.1X pre-authentication;				
55. enable/disable and configure PMK caching: a. set the amount of time (in minutes) PMK entries are cached; b. set the maximum number of PMK entries that can be cached.				

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

#### FMT\_SMF\_EXT.2.1

The TSF shall offer [*wipe of protected data, wipe of sensitive data, remove Enterprise applications, remove all device stored Enterprise resource data, remove Enterprise secondary authentication data*] upon un-enrollment and [*no other triggers*].

---

**5.1.5.5 Extended: Current Administrator (FMT\_SMF\_EXT.3)**

---

**FMT\_SMF\_EXT.3.1**

The TSF shall provide a mechanism that allows users to view a list of currently authorized administrators and the management functions that each administrator is authorized to perform.

---

**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.

---

**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.

---

**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 Extended: Anti-Exploitation Services (ASLR) (FPT\_AEX\_EXT.5)**

---

**FPT\_AEX\_EXT.5.1**

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

**FPT\_AEX\_EXT.5.2**

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

---

**5.1.6.6 Extended: 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.

---

**5.1.6.7 Extended: JTAG Disablement (FPT\_JTA\_EXT.1)**

---

**FPT\_JTA\_EXT.1.1**

The TSF shall [*control access by a signing key*] to JTAG.

---

**5.1.6.8 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.

---

**5.1.6.9 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.

---

**5.1.6.10 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.

---

**5.1.6.11 Extended: Self-Test Notification (FPT\_NOT\_EXT.1)**

---

**FPT\_NOT\_EXT.1.1**

The TSF shall transition to non-operational mode and [*no other actions*] when the following types of failures occur: failures of the self-test(s)

TSF software integrity verification failures

[*no other failures*]

---

**5.1.6.12 Reliable time stamps (FPT\_STM.1)**

---

**FPT\_STM.1.1**

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

---

**5.1.6.13 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.

---

**5.1.6.14 TSF Cryptographic Functionality Testing (Wireless LAN) (FPT\_TST\_EXT.1/WLAN)**

---

**FPT\_TST\_EXT.1.1/WLAN**

The [*TOE*] shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

**FPT\_TST\_EXT.1.2/WLAN**

The [*TOE*] shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic services.

---

**5.1.6.15 Extended: TSF Integrity Checking (FPT\_TST\_EXT.2(1))**

---

**FPT\_TST\_EXT.2(1).1**

The TSF shall verify the integrity of the bootchain up through the Application Processor OS kernel stored in mutable media prior to its execution through the use of [*an immutable hardware hash of an asymmetric key*].

---

**5.1.6.16 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.

---

### **5.1.6.17 Extended: TSF Update Verification (FPT\_TUD\_EXT.2)**

---

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

The TSF shall verify software updates to the Application Processor system software and [*baseband processor software*] using a digital signature verified by the manufacturer trusted key prior to installing those updates.

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

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

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

The TSF shall verify that the digital signature verification key used for TSF updates [*matches an immutable hardware public key*].

#### **FPT\_TUD\_EXT.2.4**

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

---

### **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. [*lock sound is played*].

---

#### **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 Wireless Network Access (FTA\_WSE\_EXT.1)**

---

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

The TSF shall be able to attempt connections only to wireless networks specified as acceptable networks as configured by the administrator in FMT\_SMF\_EXT.1.1/WLAN.

---

### **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 [*TLS, HTTPS*] protocol 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*].

### **5.1.8.2 Trusted Channel Communication (Wireless LAN) (FTP\_ITC\_EXT.1/WLAN)**

#### **FTP\_ITC\_EXT.1.1/WLAN**

The TSF shall use 802.11-2012, 802.1X, and EAP-TLS to provide a trusted communication channel between itself and a wireless access point 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/WLAN**

The TSF shall initiate communication via the trusted channel for wireless access point connections.

## **5.2 TOE Security Assurance Requirements**

The SARs for the TOE are the 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.

<b>Requirement Class</b>	<b>Requirement Component</b>
<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 4 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 fulfill 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.1.1d**

The developer shall provide a configuration list for the TOE.

**ALC\_CMS.1.1c**

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

**ALC\_CMS.1.2c**

The configuration list shall uniquely identify the configuration items.

**ALC\_CMS.1.1e**

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.

**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.1.4c**

The description shall include where users can seek information about the availability of new updates including details (e.g. CVE identifiers) of the specific public vulnerabilities corrected by each update.

**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:

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

### 6.1 Security audit

**FAU\_GEN.1:** The TOE uses three different forms of logs to meet all the required management logging events specified in Table 1 and Table 2 of the MDfPP:

1. Security Logs
2. Logcat Logs
3. Intents

Each of the above logging methods are described below.

- *Security Logs:* A table that depicts the list of all auditable events (for MDFPP31/WLANCEP10) can be found here: <https://developer.android.com/reference/android/app/admin/SecurityLog>. Additionally, the following link provides the additional information that can be grabbed when an MDM requests a copy of the logs: <https://developer.android.com/reference/android/app/admin/SecurityLog.SecurityEvent>. Each log contains a keyword or phrase describing the event, the date and time of the event, and further event-specific values that provide success, failure, and other information relevant to the event. While these logs can be read by an administrator via an MDM agent, no audit is generated during the event, therefore FAU\_SAR.1 is not claimed.
- *Logcat Logs:* Similar to Security Logs, Logcat Logs contain date, time, and further even-specific values within the logs. In addition, Logcat Logs provide a value that maps to a user ID to identify which user caused the event that generated the log. Finally, Logcat Logs tend to be more human-readable and descriptive, not requiring the user to know the template of the log to understand its values. Logcat Logs cannot be exported but can be viewed via an ADB shell to the device.
- *Intents:* Intents are events that are generated by applications and can be viewed by anyone in the system. They contain all the same information as the logs above along with much more information identifying the package/application and user that created and logged the intent. Application specific and system wide Intents can be viewed via an ADB shell connected to the device. An MDM agent can subscribe, monitor, and create a copy of the intents to transmit them back to the management server.

The following table enumerates the events that the TOE audits. Requirements marked with "(O)" are from the Table 2: Additional Auditable Events of the MDFPP31. Requirements appended with "/WLAN" are audit events required by the WLANEP10. Any requirements that are not marked with "(O)" or "/WLAN" are from Table 1 in MDfPP31.

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 Rich OS	
<b>FCS_CKM.1</b>	[None]	
<b>FCS_CKM.6</b>	[None]	
<b>FCS_CKM_EXT.1</b>	[None]	
<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/WLAN</b>	Failure to establish an EAP-TLS session.	Reason for failure.
<b>FCS_TLSC_EXT.1/WLAN</b>	Establishment/termination of an EAP-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_X509_EXT.1</b>	Failure to validate X.509v3 certificate.	Reason for failure of validation.
<b>FPT_TST_EXT.1</b>	Initiation of self-test.	
<b>FPT_TST_EXT.1</b>	Failure of self-test.	
<b>FPT_TST_EXT.1/WLAN</b>	Execution of this set of TSF self-tests: [none]	(Done as part of FPT_TST_EXT.1)
<b>FPT_TST_EXT.2(1)</b>	Start-up of TOE.	
<b>FTA_WSE_EXT.1</b>	All attempts to connect to access points.	Identity of access point being connected to as well as success and failures (including reason for failure).
<b>FTP_ITC_EXT.1/WLAN</b>	All attempts to establish a trusted channel. (TD0194 applied)	Identification of the non-TOE endpoint of the channel.

**Table 5 Audit Events**

**FAU\_STG.1:** For security logs, the TOE stores all audit records in memory, making it only accessible to the logd daemon, and only device owner applications can call the MDM API to retrieve a copy of the logs. Additionally, only new logs can be added. There is no designated method allowing for the deletion or modification of logs already present in memory, but reading the security logs clears the buffer at the time of the read.

For Logcat Logs, these are stored in memory and can only be accessed via an ADB Shell. These logs can be deleted, but only by the phone's administrator after enabling USB Debugging accesses from the phone's settings.

Intents follow the same flow as the Logcat Logs described in the paragraph above in all respects, except that they cannot be deleted by an administrator. There is no method to allow designated deletion of intents by any administrator or user.

**FAU\_STG.4:** The security log, logcat and intents are stored in memory in a circular log buffer of 10KB/64KB/NA, respectively. Once the log is full, it begins overwriting the oldest message and continues overwriting the oldest message with each new auditable event. For intents, since there is no defined size of the buffer (the limit is the free storage size of the device), there is no overwriting of the oldest log. The buffer size for intents increases and decreases as intents are created or destroyed. The number of intents drives the size of the buffer, as opposed to the buffer size limiting the number of intents present. The lifetime of intents depends on how applications and processes leveraging them define their use.

## 6.2 Cryptographic support

**FCS\_CKM.1:** The TOE provides generation of asymmetric keys including

Algorithm	Key/Curve Sizes	Usage
RSA, FIPS 186-4	2048/3072/4096	API/Application & Sensitive Data Protection (DAR.2)
ECDSA, FIPS 186-4	P-256/384	API/Application
ECDHE keys (not domain parameters)	P-256/384	TLS KeyEx (WPA2 w/ EAP-TLS & HTTPS)

**Table 6 Asymmetric Key Generation**

The TOE's cryptographic algorithm implementations have received NIST algorithm certificates (please see **Table 7**, **Table 8**, and **Table 9** in FCS\_COP.1 for all of the TOE'S algorithm certificates). The TOE itself does not generate any RSA/ECDSA authentication key pairs for TOE functionality (the user or administrator must load certificates for use with WPA2 with EAP-TLS authentication); however, the TOE provides key generation APIs to mobile applications to allow them to generate RSA/ECDSA key pairs. The TOE generates only ECDH key pairs (as BoringSSL does not support DH/DHE cipher suites) and does not generate domain parameters (curves) for use in TLS Key Exchange.

The TOE will provide a library for application developers to use for Sensitive Data Protection (SDP). This library (class) generates asymmetric 4096 bit RSA keys for use to encrypt and decrypt data that comes to the device while in a locked state. Any data received for a specified application (that opts into SDP via this library), is encrypted using the public key and stored until the device is unlocked. The public key stays in memory no matter the state of the device (locked or unlocked). However, when the device is locked, the private key is evicted from memory and unavailable for use until the device is unlocked. Upon unlock, the private key is re-derived and used to decrypt data received and encrypted while locked.

**FCS\_CKM.1/WLAN:** The TOE adheres to IEEE 802.11-2012 and IEEE 802.11ac-2014 for key generation. The TOE's wpa\_supplicant provides the PRF384 and PRF704 for WPA2 derivation of 128-bit and 256-bit AES Temporal Key (using the HMAC implementation provided by BoringSSL) and employs its BoringSSL AES-256 DRBG when generating random values used in the EAP-TLS and 802.11 4-way handshake. The TOE supports the AES-128 CCMP and AES-256 CCMP encryption mode. The TOE has successfully completed certification (including WPA2 Enterprise) and received Wi-Fi CERTIFIED Interoperability Certificates from the Wi-Fi Alliance. The Wi-Fi Alliance maintains a website providing further information about the testing program: <http://www.wi-fi.org/certification>.

Device Name	Model Number	Wi-Fi Alliance Certificate Numbers
Pixel 3	G103A/B	WFA77734
Pixel 3 XL	G103C/D	WFA78505

**FCS\_CKM.2(1):** The TOE performs key establishment as part of EAP-TLS and TLS session establishment. **Table 6 Asymmetric Key Generation** enumerates the TOE'S supported key establishment implementations (RSA/ECDH for TLS/EAP-TLS).

**FCS\_CKM.2(2):** The TOE provides an SDP library for applications that uses a hybrid crypto scheme based on 4096-bit RSA based key establishment. Applications can utilize this library to implement SDP that encrypts incoming data received while the phone is locked in a manner compliant with this requirement.

**FCS\_CKM.2.1/WLAN:** The TOE adheres to RFC 3394 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 includes a Root Encryption Key (REK) stored in a 256-bit fuse bank within the application processor. The TOE generates the REK/fuse value during manufacturing using its hardware DRBG. The application

processor protects the REK by preventing any direct observation of the value and prohibiting any ability to modify or update the value. The application processor loads the fuse value into an internal hardware crypto register and the Trusted Execution Environment (TEE) provides trusted applications the ability to derive KEKs from the REK (using an SP 800-108 KDF to combine the REK with a salt). Additionally, when the REK is loaded, the fuses for the REK become locked, preventing any further changing or loading of the REK value. The TEE does not allow trusted applications to use the REK for encryption or decryption, only the ability to derive a KEK from the REK. The TOE includes a TEE application that calls into the TEE in order to derive a KEK from the 256-bit REK/fuse value and then only permits use of the derived KEK for encryption and decryption as part of the TOE key hierarchy. More information regarding Trusted Execution Environments may be found here: <http://www.globalplatform.org/mediaguidetee.asp>.

**FCS\_CKM\_EXT.2:** The TOE utilizes its approved RBGs to generate DEKs. When generating AES keys for itself (for example, the TOE's sensitive data encryption keys or for the Secure Key Storage), the TOE utilizes the RAND\_bytes() API call from its BoringSSL AES-256 CTR\_DRBG to generate a 256-bit AES key. The TOE also utilizes that same DRBG when servicing API requests from mobile applications wishing to generate AES keys (either 128 or 256-bit).

In all cases, the TOE generates DEKs using a compliant RBG seeded with sufficient entropy so as to ensure that the generated key cannot be recovered with less work than a full exhaustive search of the key space.

**FCS\_CKM.2(2):** The TOE uses ECDH with a P-256 curve key establishment for protection of application sensitive data received while the device is locked.

**FCS\_CKM\_EXT.3:** The TOE derives all password-based KEKs by combining the user's password with a BoringSSL RBG generated salt value using scrypt. Scrypt uses HMAC-SHA-256 (an iteration of PBKDFv2), followed by ROMix operations that increase the required memory manipulation (slowing the ability of brute-force attacks), finally sandwiched with another iteration of PBKDFv2. See FCS\_COP.1 for a more thorough explanation of scrypt.

The TOE generates all non-derived KEKs using the RAND\_bytes() API call from its BoringSSL AES-256 CTR\_DRBG to ensure a full 150/256-bits of strength for asymmetric/symmetric keys, respectively. And the TOE combines KEKs by encrypting one KEK with the other so as to preserve entropy.

**FCS\_CKM\_EXT.4:** The TOE clears sensitive cryptographic material (plaintext keys, authentication data, other security parameters) from memory when no longer needed or when transitioning to the device's locked state (in the case of the Sensitive Data Protection keys). Public keys (such as the one used for Sensitive Data Protection) can remain in memory when the phone is locked, but all crypto-related private keys are evicted from memory upon device lock. No plaintext cryptographic material resides in the TOE's Flash as the TOE encrypts all keys stored in Flash. When performing a full wipe of protected data, the TOE cryptographically erases the protected data by clearing the Data-At-Rest DEK. Because the TOE's keystore resides within the user data partition, the TOE effectively cryptographically erases those keys when clearing the Data-At-Rest DEK. In turn, the TOE clears the Data-At-Rest DEK and Secure Key Storage SEK through a secure direct overwrite (BLKSECDISCARD ioctl) of the wear-leveled Flash memory containing the key followed by a read-verify.

**FCS\_CKM\_EXT.5:** The TOE stores all protected data in encrypted form within the user data partition (either protected data or sensitive data). Upon request, the TOE cryptographically erases the Data-At-Rest DEK protecting the user data partition and the SDP Master KEK protecting sensitive data files in the user data partition, clears those keys from memory, reformats the partition, and then reboots. The TOE's clearing of the keys follows the requirements of FCS\_CKM\_EXT.4.

**FCS\_CKM\_EXT.6:** The TOE generates salt nonces (which are just salt values used in WPA2) using its /dev/urandom.

Salt value and size	RBG origin	Salt storage location
User password salt (128-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 ECDHE private value (256, 384)	BoringSSL's AES-256 CTR_DRBG	N/A (ephemeral)
WPA2 4-way handshake supplicant nonce (SNonce)	BoringSSL's AES-256 CTR_DRBG	N/A (ephemeral)

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

The TOE's BoringSSL Library provides the following algorithms (BoringSSL code can be found here: [https://android.googlesource.com/platform/external/boringssl/+android-cts-9.0\\_r1](https://android.googlesource.com/platform/external/boringssl/+android-cts-9.0_r1)):

SFR	Algorithm	NIST Standard	Cert#
FCS_CKM.1 (Key Gen)	RSA IFC Key Generation	FIPS 186-4, RSA	C782
	ECDSA ECC Key Generation	FIPS 186-4, ECDSA	C782
FCS_CKM.2 (Key Establishment)	RSA-based Key Exchange	Vendor affirm 800-56B	N/A
	ECC-based Key Exchange	SP 800-56A, CVL KAS ECC	C782
FCS_COP.1(1) (AES)	AES 128/256 CBC, GCM, KW	FIPS 197, SP 800-38A/D/F	C782
FCS_COP.1(2) (Hash)	SHA Hashing	FIPS 180-4	C782
FCS_COP.1(3) (Sign/Verify)	RSA Sign/Verify	FIPS 186-4, RSA	C782
	ECDSA Sign/Verify	FIPS 186-4, ECDSA	C782
FCS_COP.1(4) (Keyed Hash)	HMAC-SHA 1/256/384/512	FIPS 198-1 & 180-4	C782
FCS_RBG_EXT.1 (Random) FCS_CKM_EXT.2	DRBG Bit Generation	SP 800-90A (Counter)	C782

**Table 7 BoringSSL Cryptographic Algorithms**

The TOE's Trusted Execution Environment's Kernel software (in this case QTEE 5.0) and Android's LockSettings service provides the TOE'S key based key derivation function.

SFR	Algorithm	NIST Standard	Cert#
FCS_CKM_EXT.3	KBKDF	SP 800-108	KDF171
FCS_CKM_EXT.3	LockSettings service KBKDF	SP 800-108	C831

**Table 8 KDF Cryptographic Algorithms**

The TOE's Wi-Fi chipset provides an AES-CCMP implementation, and the TOE's application processor (Snapdragon 845 [SDM845]) provide additional cryptographic algorithms.

SFR	Algorithm	NIST Standard	Cert#
FCS_COP.1(1) (AES) (Wi-Fi)	AES 128/256 CCM	FIPS 197, SP 800-38C	4748
FCS_COP.1(1) (AES) (QTI CEC*)	AES 128/256 CBC	FIPS 197, SP 800-38A	4959
FCS_COP.1(1) (AES) (QTI UFS**)	AES 128/256 XTS	FIPS 197, SP 800-38E	4958/4957
FCS_COP.1(2) (Hash) (QTI CEC)	SHA 1/256 Hashing	FIPS 180-4	4049
FCS_COP.1(2) (Hash) (DRBG)	SHA 256 Hashing	FIPS 180-4	4047, 4048
FCS_COP.1(4) (Keyed Hash) (QTI CEC)	HMAC-SHA-1/256	FIPS 198-1 & 180-4	3305
FCS_RBG_EXT.1 (Random) (DRBG) FCS_CKM_EXT.2	DRBG Bit Generation	SP 800-90A (Hash-256)	1788

**Table 9 SDM845 Hardware Cryptographic Algorithms**

\*QTI CEC – Qualcomm Technologies, Inc. Crypto Engine Core v5.4.1

\*\*QTI UFS - Qualcomm Technologies, Inc. Inline Crypto Engine (UFS) v3.1.0

The TOE's application processor includes a source of hardware entropy that the TOE distributes throughout, and the TOE's RBGs make use of that entropy when seeding/instantiating themselves.

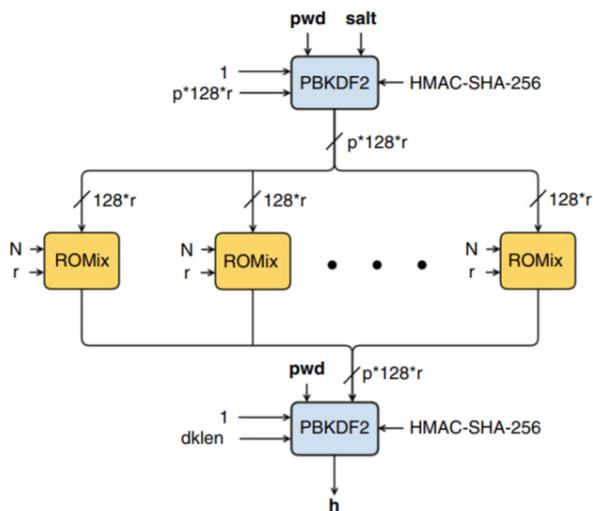
The TOE's BoringSSL library supports the TOE's cryptographic Android Runtime (ART) methods (through Android's conscrypt JNI provider) afforded to mobile applications and also supports Android user-space processes and

daemons (e.g., wpa\_supplicant). The TOE's Application Processor provides hardware accelerated cryptography utilized in Data-At-Rest (DAR) encryption of the user data partition.

The TOE stretches the user's password to create a password derived key. The TOE stretching function uses a series of steps to increase the memory required for key derivation (thus thwarting GPU-acceleration, off-line brute force, and precomputed dictionary attacks) and ensure proper conditioning and stretching of the user's password.

The TOE conditions the user's password using two iterations of PBKDFv2 w HMAC-SHA-256 in addition to some ROMix operations in an algorithm named script. Script consists of one iteration of PBKDFv2, followed by a series of ROMix operations, and finished with a final iteration of PBKDFv2. The ROMix operations increase the memory required for key derivation, thus thwarting GPU-acceleration (which can greatly decrease the time needed to brute force PBKDFv2 alone).

The following script diagram shows how the password and salt are used with PBKDFv2 and ROMix to fulfil the requirements for password conditioning.



The resulting derived key from this operation is used to decrypt the FBE DEK (see the key hierarchy above for further explanation on how this key is used in FBE) and to derive the User Keystore Daemon Value.

The TOE uses HMAC as part of the TLS ciphersuites and makes HMAC functionality available to mobile applications. For TLS, the TOE uses HMAC using SHA-1 (with a 160-bit key) to generate a 160-bit MAC, SHA-256 (with a 256-bit key) to generate a 256-bit MAC, SHA-384 (with a 384-bit key) to generate a 384-bit MAC. For mobile applications, the TOE provides all of the previous HMACs as well as SHA-512 (with a 512-bit key) to generate a 512-bit MAC. FIPS 198-1 & 180-4 dictate the block size used, and they specify block sizes/output MAC lengths of 512/160, 512/160, 1024/384, and 1024/512-bits for HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 respectively.

**FCS\_HTTPS\_EXT.1:** The TOE supports the HTTPS protocol (compliant with RFC 2818) so that (mobile and system) applications executing on the TOE can act as HTTPS clients and 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 by reading from /dev/urandom for use with all keys. In all cases, the TOE uses /dev/urandom and generates the IVs in compliance with the requirements of table 11 of MDFPP31/WLANCEP10.

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

1. A SHA-256 Hash\_DRBG provided in the hardware of the Application Processor.
2. An AES-256 CTR\_DRBG provided by BoringSSL. This is the only accredited and supported DRBG present in the system and available to independently developed applications. As such, the TOE provides mobile applications access (through an Android Java API) to random data drawn from its AES-256 CTR\_DRBG.

The TOE initializes its AP Hash\_DRBG with enough data from its hardware noise source to ensure at least 256-bits of entropy. The TOE then uses its AP Hash\_DRBG to continuously fill the Linux Kernel Random Number Generator input pool.

The TOE seeds its BoringSSL AES-256 CTR\_DRBG using 384-bits of data from /dev/urandom, thus ensuring at least 256-bits of entropy. The TOE uses its BoringSSL DRBG for all random generation uses outside of salts.

**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), keyed message digests (HMAC-SHA-256), generation of asymmetric keys for key establishment (RSA and ECDH), and generation of 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 application processor module (user and kernel) APIs.

**FCS\_SRV\_EXT.2:** The TOE provides applications with APIs to perform the functions referenced in FCS\_COP.1(1) and FCS\_COP.1(3).

**FCS\_STG\_EXT.1:** The TOE provides the user, administrator, and mobile applications the ability to import and use asymmetric public and private keys into the TOE'S software-based Secure Key Storage. Additionally, the user and administrator can request the TOE to destroy the keys stored in the Secure Key Storage. While normally mobile applications cannot use or destroy the keys of another application, applications that share a common application developer (and are thus signed by the same developer key) may do so. In other words, applications with a common developer (and which explicitly declare a shared UUID in their application manifest) may use and destroy each other's keys located within the Secure Key Storage.

**FCS\_STG\_EXT.2:** The TOE employs a key hierarchy that protects all DEKs and KEKs by encryption with either the REK or by the REK and password derived KEK.

Long-term Trusted channel Key Material (Bluetooth and WiFi keys) are encrypted using AES encryption. Additionally, all LTTCKM is subject to an SHA-256 checksum verification to verify the integrity of the two files containing LTTCKM (Wi-Fi PSKs and BT keys).

All keys are 256-bits in size. All keys are generated using the TOE'S BoringSSL AES-256 CTR\_DRBG or application processor SHA-256 Hash\_DRBG. By utilizing only 256-bit KEKs, the TOE ensures that all keys are encrypted by an equal or larger sized key.

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

**FCS\_STG\_EXT.3:** The TOE protects the integrity of all DEKs and KEKs (other than LTTCKM keys) stored in Flash by using authenticated encryption/decryption methods (CCM, GCM). The TOE protects the two files containing Wi-Fi and BT LTTCKM keys through a SHA-256 checksum used for integrity verification and encrypts that checksum using an AES-GCM-256 key protected by the TOE's secure key storage (KeyStore).

**FCS\_TLSC\_EXT.1/2:** The TOE provides mobile applications (through its Android API) the use of TLS version 1.2 including support for the selections in chosen in section 5 for FCS\_TLSC\_EXT.1.

When an application uses the APIs provided in the Admin Guide to attempt to establish a trusted channel connection based on EAP-TLS, TLS or HTTPS, the TOE supports only Subject Alternative Name (SAN) (DNS and IP address) as reference identifiers (the TOE does not accept reference identifiers in the Common Name[CN]). The

TOE supports client (mutual) authentication. The TOE in its evaluated configuration and by design, supports only evaluated elliptic curves for TLS (P-256 & P-384 and no others) and has a fixed set of supported curves (thus the admin cannot and need not configure any curves). While the TOE supports the use of wildcards in X.509 reference identifiers (SAN only), the TOE does not support certificate pinning. If the TOE cannot determine the revocation status of a peer certificate, the TOE provides the ability for application developers to select what happens for their application: give the user the option to connect/disconnect, deny the connection, or connect anyways.

**FCS\_TLSC\_EXT.1/2/WLAN:** The TSF supports TLS versions 1.0, 1.1, and 1.2 and also supports the selected ciphersuites utilizing SHA-1, SHA-256, and SHA-384 (see the selections in section 5 for FCS\_TLSC\_EXT.1/WLAN) for use with EAP-TLS as part of WPA2. The TOE in its evaluated configuration and by design, supports only evaluated elliptic curves (P-256 & P-384 and no others) and has a fixed set of supported curves (thus the admin cannot and need not configure any curves).

The TOE, allows the user to load and utilize authentication certificates for EAP-TLS used with WPA. The Android UI (Settings->Security->Credential storage: Install from device storage) allows the user to import an RSA or ECDSA certificate and designate its use as WiFi.

### 6.3 User data protection

**FDP\_ACF\_EXT.1.1:** 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 cannot automatically grant it to the requesting application. For example, any dangerous permissions requested by an application will be displayed to the user and require confirmation before proceeding or some other approach can 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 request (or 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 running 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 application is allowed to continue running. If the user disapproves, the devices continues to run, but cannot use the services protected by the denied permissions. 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 (2<sup>nd</sup> installed app) that requests this permission and that has been signed with the same developer key used to sign the application (1<sup>st</sup> installed app) declaring the permission (in the case of the example, the Android Framework itself).

An example of a `signatureOrSystem` 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 to 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 9.0 (Level 28) API found here <https://developer.android.com/about/versions/pie/android-9.0> provides a description of the services available to mobile applications.

While Android provides a large number of individual permissions, they are generally grouped into categories or features that provide similar functionality. **Table 10** shows a series of functional categories centered on common functionality.

Service Features	Description
------------------	-------------

Service Features	Description
Sensitive I/O Devices & Sensors	Location services, Audio & Video capture, Body sensors
User Personal Information & Credentials	Contacts, Calendar, Call logs, SMS
Metadata & Device ID Information	IMEI, Phone Number
Data Storage Protection	App data, App cache
System Settings & Application Management	Date time, Reboot/Shutdown, Sleep, Force-close application, Administrator Enrollment
Wi-Fi, Bluetooth, USB Access	Wi-Fi, Bluetooth, USB tethering, debugging and file transfer
Mobile Device Management & Administration	MDM APIs
Peripheral Hardware	NFC, Camera, Headphones
Security & Encryption	Certificate/Key Management, Password, Revocation rules

**Table 10 – Functional Categories**

**FDP\_ACF\_EXT.1.2:** Applications with a common developer have the ability to allow sharing of data between their applications. A common application developer can sign their generated APK with a common certificate or key and set the permissions of their application to allow data sharing. When the different applications' signatures match and the proper permissions are enabled, information can then be shared as needed.

The TOE supports Enterprise profiles to provide additional separation between application and application data belonging to the Enterprise profile. Applications installed into the Enterprise versus Personal profiles cannot access each other's secure data, applications, and can have separate device administrators/managers. This functionality is built into the device by default and does not require an application download. The Enterprise administrative app (an MDM agent application installed into the Enterprise Profile) may enable cross-profile contacts search, in which case, the device owner can search the address book of the enterprise profile. Please see the Admin Guide for additional details regarding how to set up and use Enterprise profiles. Ultimately, the enterprise profile is under control of the personal profile. The personal profile can decide to remove the enterprise profile, thus deleting all information and applications stored within the enterprise profile. However, despite the "control" of the personal profile, the personal profile cannot dictate the enterprise profile to share applications or data with the personal profile; the enterprise profile MDM must allow for sharing of contacts before any information can be shared.

**FDP\_ACF\_EXT.2:** The TOE allows an administrator to allow sharing of the enterprise profile address book with the normal profile.

**FDP\_DAR\_EXT.1:** The TOE provides Data-At-Rest AES-256 XTS hardware encryption for all data stored on the TOE in the user data partition (which includes both user data and TSF data). The TOE also has TSF data relating to key storage for TSF keys not stored in the system's Secure Key Store. The TOE separately encrypts those TSF keys and data. Additionally, the TOE includes a read-only filesystem in which the TOE'S system executables, libraries, and their configuration data reside. For its Data-At-Rest encryption of the data partition on the internal Flash (where the TOE stores all user data and all application data), the TOE uses an AES-256 bit DEK with XTS feedback mode to encrypt each file in the data partition using dedicated application processor hardware.

**FDP\_DAR\_EXT.2:** The TOE provides a Java library for Sensitive Data Protection (SDP) that application developers can use to opt-in for sensitive data protection. When developers opt-in for SDP, all data that is received on the device destined for that application is treated as sensitive. This library generates a 4096 bit RSA key that acts as a master KEK for the SDP encryption process. When an application that has opted-in for SDP receives incoming data while the device is locked, a 256 bit AES symmetric DEK is generated to encrypt that data. The public key from the master RSA KEK above is then used to encrypt the AES DEK. Once the device is unlocked, the RSA KEK private key is re-derived and can be used to decrypt the AES DEK for each piece of information that was stored while the device was locked. The TOE then takes that decrypted data and re-encrypts it following FDP\_DAR\_EXT.1.

**FDP\_IFC\_EXT.1:** The TOE will route all traffic other than traffic necessary to establish the VPN connection to the

VPN gateway (when the gateway's configuration specifies so). The TOE includes an interceptor kernel module that controls inbound and output packets. When a VPN is active, the interceptor will route all incoming packets to the VPN and conversely route all outbound packets to the VPN before they are output.

The only exception to all traffic being routed to the VPN is in the instance of ICMP echo requests. The TOE uses ICMP echo responses on the local subnet to facilitate network troubleshooting and categorizes it as a part of ARP. As such, if an ICMP echo request is issued on the subnet the TOE is part of, it will respond with an ICMP echo response, but no other instances of traffic will be routed outside of the VPN.

**FDP\_PBA\_EXT.1:** The TOE requires the user to enter their password to enroll, re-enroll or un-enroll any biometric templates. When the user attempts biometric authentication to the TOE, the biometric sensor takes an image of the presented biometric for comparison to the enrolled templates. The captured image is compared to all the stored templates on the device to determine if there is a match. The complete biometric authentication process is handled inside the TEE (including image capture, all processing and match determination). The image is provided to the biometric service to check the enrolled templates for a match to the captured image.

**FDP\_STG\_EXT.1:** The TOE'S Trusted Anchor Database consists of the built-in certs and any additional user or admin/MDM loaded certificates. The built-in certs are individually stored in the device's read-only system image in the /system/etc/security/cacerts directory, and the user can individually disable certs through Android's user interface [Settings->Security-> Trusted Credentials]. Because the built-in CA certificates reside on the read-only system partition, the TOE places a copy of any disabled built-in certificate into the /data/misc/user/X/cacerts-removed/ directory, where 'X' represents the user's number (which starts at 0). The TOE stores added CA certificates in the corresponding /data/misc/user/X/cacerts-added/ directory and also stores a copy of the CA certificate in the user's Secure Key Storage (residing in the /data/misc/keystore/user\_X/ directory). The TOE uses Linux file permissions that prevent any mobile application or entity other than the TSF from modifying these files. Only applications registered as an administrator (such as an MDM Agent Application) have the ability to access these files, staying in accordance to the permissions established in FMT\_SMF\_EXT.1 and FMT\_MOF\_EXT.1.

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

SSL:

javax.net.ssl.SSLContext:

<https://developer.android.com/reference/javax/net/ssl/SSLContext>

Developers then need to swap SocketFactory for SecureSocketFactory, part of a private library provided by Google.

Developers can request this library by emailing: [niapsec@google.com](mailto:niapsec@google.com)

HTTPS:

javax.net.ssl.HttpsURLConnection:

<https://developer.android.com/reference/javax/net/ssl/HttpsURLConnection>

Developers then need to swap HttpsURLConnections for SecureUrl part of a private library provided by Google.

Developers can request this library by emailing: [niapsec@google.com](mailto:niapsec@google.com)

Bluetooth:

android.bluetooth:

<http://developer.android.com/reference/android/bluetooth/package-summary.html>

## 6.4 Identification and authentication

**FIA\_AFL\_EXT.1:** The TOE maintains in persistent storage, for each user, the number of failed password logins since the last successful login (the phone, in its evaluated configuration, only supports password authentication), and upon reaching the maximum number of incorrect logins, the TOE performs a full wipe of all protected data (and in fact, wipes all user data). An administrator can adjust the number of failed logins for the cryptlock screen from the default of ten failed logins to a value between 0 (deactivate wiping) and 2,147,483,647 through an MDM. The TOE validates passwords by providing them to Android's Gatekeeper (which runs in the Trusted Execution Environment). If the presented password fails to validate, the TOE increments the incorrect password counter before displaying a visual error to the user. Android's Gatekeeper keeps this password counter in secure storage and is incremented before the password is validated. Upon successful validation of the password, this counter is reset back to zero.

Additionally, the phone allows the user to unlock the device using a fingerprint sensor. The user has up to 5 attempts to unlock the device before the fingerprint sensor is temporarily disabled for 30 seconds. While the sensor is disabled, the user can input their password to unlock the phone. After a total of 4 failed rounds of attempted fingerprint unlock (20 total unlock attempts), the fingerprint sensor is disabled entirely until the user enters their password to unlock the device. Note that restarting the phone at any point disables the fingerprint sensor automatically until the user enters a correct password and unlocks the phone, and therefore TOE restart disruptions are not applicable for this authentication mechanism.

**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). The TOE requires this authorization (via manual input) for mobile application use of the Bluetooth trusted channel and in situations where temporary (non-bonded) connections are formed.

**FIA\_BLT\_EXT.2:** The TOE prevents data transfer of any type until Bluetooth pairing has completed. Additionally, the TOE supports OBEX (Object Exchange) through L2CAP (Logical Link Control and Adaptation Protocol).

**FIA\_BLT\_EXT.3:** The TOE rejects duplicate Bluetooth connections by only allowing a single connection per paired device.

**FIA\_BLT\_EXT.4:** The TOE'S Bluetooth host and controller supports Bluetooth Secure Simple Pairing and the TOE utilizes this pairing method when the remote host also supports it.

**FIA\_BLT\_EXT.6:** The TOE requires explicit user authorization before granting trusted remote devices access to services associated with the OPP and MAP Bluetooth profiles. Additionally, the TOE requires explicit user authorization before granting untrusted remote devices access to services associated with all following Bluetooth profiles.

**FIA\_BMG\_EXT.1:** The TOE's fingerprint sensor provides a FAR of 1:100,000 with an FRR of 3.1%, which is rounded and mapped to a 1:25 rate. Prior to the rounding, the 3.1% FRR meets the requirements for FIA\_BMG\_EXT.

Users have up to 5 attempts to unlock the phone using fingerprint before the fingerprint unlock method is disabled for 30 seconds. After the 4th unsuccessful round of unlock attempts (a total of 20 fingerprint attempts), the fingerprint sensor is disabled entirely and the user is prompted for their password. The fingerprint unlock remains disabled until the user enters their password.

Since the user can attempt to unlock the phone a total of 20 times before the fingerprint is disabled, the SAFAR of the phone is 1:5,000.

**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 the selections in section 5 for FIA\_PMG\_EXT.1)). The TOE defaults to requiring passwords to have a minimum of four characters but no more than sixteen, contain at least one letter; however, an MDM application can change these defaults. The Smart Lock feature is not allowed in the evaluated config as this feature circumvents the requirements for FIA\_PMG\_EXT.1 and many others.

**FIA\_TRT\_EXT.1:** Android's GateKeeper throttling is used to prevent brute-force attacks. After a user enters an incorrect password, GateKeeper APIs return a value in milliseconds (500ms default) in which the caller must wait before attempting to validate another password. Any attempts before the defined amount of time has passed will be ignored by GateKeeper. Gatekeeper also keeps a count of the number of failed validation attempts since the last successful attempt. These two values together are used to prevent brute-force attacks of the TOE's password.

**FIA\_UAU.5:** The TOE, in its evaluated configuration, allows the user to authenticate using either a password or fingerprint. Upon boot, the first unlock screen presented requires the user to enter their password to unlock the device. The fingerprint sensor is disabled until the user enters their password for the first time.

Upon device lock during normal use of the device, the user has the ability to unlock the phone either by entering their password or using fingerprint authentication. Throttling of these inputs can be read about in the FIA\_AFL\_EXT.1 section. The entered password is compared to a value derived as described in Section 6.1. FIA\_BMG\_EXT.1 describes the password authentication process and its security measures.

Some security related user settings (e.g. changing the password, modifying, deleting, or adding stored fingerprint templates, SmartLock settings, etc.) and actions (e.g. factory reset) require the user to enter their password before modifying these settings or executing these actions. In these instances, fingerprint authentication is not accepted to permit the referenced functions.

The TOE's evaluated configuration disallows other authentication mechanisms, such as pattern, PIN, or Smart Lock mechanisms (on-body detection, trusted places, trusted devices, trusted face, trusted voice).

**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.

**FIA\_UAU\_EXT.1:** As described before, the TOE's key hierarchy requires the user's password in order to derive the KEK\_\* keys in order to decrypt other KEKs and DEKs. Thus, until it has the user's password, the TOE cannot decrypt the DEK utilized for Data-At-Rest encryption, and thus cannot decrypt the user's protected data.

**FIA\_UAU\_EXT.2:** The TOE, when configured to require a user password, allows a user to perform the actions assigned in FIA\_UAU\_EXT.2.1 (see selections in section 5 for FIA\_UAU\_EXT.2) without first successfully authenticating. Choosing the input method allows the user to select between different keyboard devices (say, for example, if the user has installed additional keyboards). Note that the TOE automatically names and saves (to the internal Flash) any screen shots or photos taken from the lock screen, and the TOE provides the user no opportunity to name them or change where they are stored.

When configured, the user can also launch Google Assistant to initiate some features of the phone. However, if the command requires access to the user's data (e.g. contacts for calls or messages), the phone requires the user to manually unlock the phone before the action can be completed.

Beyond those actions, a user cannot perform any other actions other than observing notifications displayed on the lock screen until after successfully authenticating. Additionally, the TOE provides the user the ability to hide the contents of notifications once a password (or any other locking authentication method) is enabled.

**FIA\_UAU.6(1)/FIA\_UAU.6(2):** The TOE requires the user to enter their password or supply their biometric in order to unlock the TOE. Additionally, the TOE requires the user to confirm their current password when accessing the “Settings->Display->LockScreen->Screen Security->Select screen lock” menu in the TOE’s user interface. The TOE can disable Smart Lock through management controls. 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. Additionally, the TOE verifies the extendedKeyUsage Server Authentication purpose during WPA2/EAP-TLS negotiation. 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 if 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/FIA\_X509\_EXT.2/WLAN:** The TOE uses X.509v3 certificates during EAP-TLS, TLS, and HTTPS. The TOE comes with a built-in set of default 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 and an administrator/MDM can import a new trusted CA certificate into the Trust Anchor Database (the TOE stores the new CA certificate in the Security Key Store).

The TOE does not establish TLS connections itself (beyond EAP-TLS used for WPA2 Wi-Fi 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 be assured that the TOE will not establish the trusted connection if the peer certificate cannot be verified (including validity, certification path, and revocation [through OCSP]). If, during the process of certificate verification, the TOE cannot establish a connection with the server acting as the OCSP Responder, the TOE will not deem the server’s certificate as valid and will not establish a TLS connection with the server.

The user or administrator explicitly specifies the trusted CA that the TOE will use for EAP-TLS authentication of the server’s certificate. For mobile applications, the application developer will specify whether the TOE should use the Android system Trusted CAs, use application-specified trusted CAs, or a combination of the two. In this way, the TOE always knows which trusted CAs to use.

The TOE, when acting as a WPA2 supplicant uses X.509 certificates for EAP-TLS authentication. Because the TOE may not have network connectivity to a revocation server prior to being admitted to the WPA2 network and because the TOE cannot determine the IP address or hostname of the authentication server (the Wi-Fi access point proxies the supplicant’s authentication request to the server), the TOE will accept the certificate of the server.

**FIA\_X509\_EXT.3:** The NIAPSEC library created by the vendor provides the following functions to allow for certificate path validation and revocation checking:

- public boolean isValid(List<Certificate> certs)
- public Boolean isValid(Certificate cert)

The first function allows for validation and revocation checking against a list of certificates, while the second checks a singular certificate. Revocation checking is completed using OCSP. Please see the FIA\_X509\_EXT.2/WLAN section for a further explanation on how the TOE handles revocation checking.

## 6.5 Security Management

**FMT\_MOF\_EXT.1/FMT\_SMF\_EXT.1:** The TOE provides the management functions described in **Table 2 Security Management Functions** in section 5. 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. It is worth noting that the TOE'S ability to specify authorized application repositories takes the form of allowing enterprise applications (i.e., restricting applications to only those applications installed by an MDM Agent).

**FMT\_SMF\_EXT.1/WLAN:** The TOE provides the management functions described in **Table 3 WLAN Security Management Functions** in section 5. As with **Table 2 Security Management Functions**, 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. It is worth noting that the TOE'S ability to specify authorized application repositories takes the form of allowing enterprise applications (i.e., restricting applications to only those applications installed by an MDM Agent).

**FMT\_SMF\_EXT.2:** The TOE offers MDM agents the ability to wipe protected data, wipe sensitive data, remove Enterprise applications, remove all device stored Enterprise resource data, and remove Enterprise secondary authentication data upon un-enrollment. The TOE offers MDM agents the ability to wipe protected data (effectively wiping the device) at any time. Similarly, the TOE also offers the ability to remove Enterprise applications and a full wipe of managed profile data of the TOE'S Enterprise data/applications at any time.

**FMT\_SMF\_EXT.3:** The TOE offers MDM agents and the user (through the "Settings->Security->Device administrators" menu) the ability to view each application that has been granted admin rights, and further to see what operations each admin app has been granted.

## 6.6 Protection of the TSF

**FPT\_AEX\_EXT.1:** The Linux kernel of the TOE'S Android operating system provides address space layout randomization utilizing the `get_random_int(void)` kernel random function to provide eight 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.

**FPT\_AEX\_EXT.2:** The TOE's Android 9.0 operating system utilizes 4.9.148 Linux kernels (<https://source.android.com/devices/architecture/kernel/modular-kernels#core-kernel-requirements>), 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. The Android operating system (as of Android 2.3) sets the ARM No eExecute (XN) bit on memory pages and the TOE'S ARMv8 Application Processor's Memory Management Unit (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 eExecute (NX) to prevent code execution on the stack and heap'. Section D.5 of the ARMv8 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 in addition to taking advantage of hardware-based No eExecute to prevent code execution on the stack and heap. Specifically, the vendor builds the TOE (Android and support libraries) using `gcc-fstack-protector` compile option to enable stack overflow protection and Android takes advantage of hardware-based eExecute-Never to make the stack and heap non-executable. The vendor 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 protects its REK by limiting access to only trusted applications within the TEE (Trusted Execution Environment). The TOE key manager includes a TEE module which utilizes the REK 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.

Additionally, the TOE'S Android operating system provides 'sandboxing' that ensures that each third-party 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 or files and cannot access the memory space or files of other applications (notwithstanding access between applications with a common application developer).

The TOE, in its evaluated configuration has its bootloader in the locked state. This prevents a user from installing a new software image via another method than Google's proscribed OTA methods. The TOE allows an operator to download and install an OTA update through the system settings (Settings->System->Advanced->System update->Check for update) while the phone is running, or by separately downloading an OTA image, and then "sideloading" the OTA update from Android's recovery mode. In both cases, the TOE will verify the digital signature of the new OTA before applying the new firmware.

For the first install of the Common Criteria compliant build, the administrator must unlock the device's bootloader via the fastboot interface, "sideload" the correct build, reboot the phone back to the fastboot interface, re-lock the bootloader, and finally start the phone normally. For both the locking and unlocking of the bootloader, the device is factory reset as part of the process. This prevents an attacker from modifying or switching the image running on the device to allow access to sensitive data. After this first install of the official build, further updates can be done via normal OTA updates.

**FPT\_AEX\_EXT.5:** The TOE models provide Kernel Address Space Layout Randomization (KASLR) as a hardening feature to randomize the location of kernel data structures at each boot, including the core kernel as a random physical address, mapping the core kernel at a random virtual address in the vmalloc area, loading kernel modules at a random virtual address in the vmalloc area, and mapping system memory at a random virtual address in the linear area. The entropy used to dictate the randomization is based on the hardware present within the phone. For ARM devices, such as the TOE, 13–25 bits of entropy are generated on boot, from which the starting memory address is generated.

**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) through internal controls of the TOE'S SoC, which contains both the AP and the CP. The AP restricts hardware access control through a protection unit that restricts software access from the baseband processor through a dedicated 'modem interface'. The protection unit combines the functionality of the Memory Protection Unit (MPU), the Register Protection Unit (RPU), and the Address Protection Unit (APU) into a single function that conditionally grants access by a master to a software defined area of memory, to registers, or to a pre-decoded address region, respectively. The modem interface provides a set of APIs (grouped into five categories) to enable a high-level OS to send messages to a service defined on the modem/baseband processor. The combination of hardware and software restrictions ensures that the TOE'S AP prevents software executing on the modem or baseband processor from accessing the resources of the application processor (outside of the defined methods, mediated by the application processor).

**FPT\_JTA\_EXT.1:** The TOE'S prevents access to its processor's JTAG interface by requiring use of a signing key to authenticate prior to gaining JTAG access. Only a JTAG image with the accompanying device serial number (which is different for each mobile device) that has been signed by Google's private key can be used to access a device's JTAG interface. The Google private key corresponds to the Google RSA 2048-bit public key (a SHA-256 hash of which is fused into the TOE'S application processor).

**FPT\_KST\_EXT.1:** The TOE does not store any plaintext key material in its internal Flash; 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 depletes or is removed), all keys stored in the internal Flash are

wrapped with a KEK. Please refer to section 6.2 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 any keys in order to utilize them.

**FPT\_KST\_EXT.2:** The TOE itself (i.e., the mobile device) comprises a cryptographic module that utilizes cryptographic libraries including BoringSSL, application processor cryptography (which leverages AP hardware), and the following system-level executables that utilize KEKs: dm-crypt, wpa\_supplicant, and the Secure Key Store.

1. QCT's dm-crypt and application processor hardware provides Data-At-Rest encryption of the user data partition in Flash
2. wpa\_supplicant provides 802.11-2014/WPA2 services
3. the Secure Key Store application provides key generation, storage, deletion services to mobile applications and to user through the UI

The TOE ensures that plaintext key material is not exported by not allowing the REK to be exported 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\_EXT.4). Note that the TOE does not use the user's biometric fingerprint to encrypt/protect key material (and instead only relies upon the user's password).

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

Furthermore, the components of the device are designed to prevent transmission of key material outside the device. Each internal system component requiring access to a plaintext key (for example the Wi-Fi driver) must have the necessary precursor(s), whether that be a password from the user or file access to key in Flash (for example the encrypted AES key used for encryption of the Flash data partition). With those appropriate precursors, the internal system-level component may call directly to the system-level library to obtain the plaintext key value. The system library in turn requests decryption from a component executing inside the trusted execution environment and then directly returns the plaintext key value (assuming that it can successfully decrypt the requested key, as confirmed by the CCM/GCM verification) to the calling system component. That system component will then utilize that key (in the example, the dm-crypt daemon that holds the key in order to encrypt and decrypt reads and writes to the encrypted user data partition in Flash). In this way, only the internal system components responsible for a given activity have access to the plaintext key needed for the activity, and that component receives the plaintext key value directly from the system library.

For a user's mobile applications, those applications do not have any access to any system-level components and only have access to keys that the application has imported into the Secure Key Store. Upon requesting access to a key, the mobile application receives the plaintext key value back from the system library through the Android API. Mobile applications do not have access to the memory space of any other mobile application so it is not possible for a malicious application to intercept the plaintext key value to then log or transmit the value off the device.

**FPT\_NOT\_EXT.1:** When the TOE encounters a critical failure (either a self-test failure or TOE software integrity verification failure), a failure message is displayed to the screen, and the TOE attempts to reboot. If the failure persists between boots, 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 (which installs and verifies APK signatures and certificates), image verifier, wpa\_supplicant, and Secure Key Store applications. These TOE components obtain time from the TOE using system API calls [e.g., time() or gettimeofday()]. An application (unless a system application is residing in /system/priv-app or signed by the vendor) 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. Further, this stored time is used both for the time/date tags in audit logs and is used to track inactivity timeouts that force the TOE into a locked state.

**FPT\_TST\_EXT.1:** The TOE automatically performs known answer power on self-tests (POST) on its cryptographic algorithms to ensure that they are functioning correctly. Each component providing cryptography (application processor, and BoringSSL) performs known answer tests on their cryptographic algorithms to ensure they are working correctly. Should any of the tests fail, the TOE displays an error message stating "Boot Failure" and halts the boot process, displays an error to the screen, and forces a reboot of the device.

Algorithm	Implemented in	Description
AES encryption/decryption	BoringSSL	Comparison of known answer to calculated value
ECDH key agreement	BoringSSL	Comparison of known answer to calculated value
DRBG random bit generation	BoringSSL	Comparison of known answer to calculated value
ECDSA sign/verify	BoringSSL	Comparison of known answer to calculated value
HMAC-SHA	BoringSSL	Comparison of known answer to calculated value
RSA sign/verify	BoringSSL	Comparison of known answer to calculated value
SHA hashing	BoringSSL	Comparison of known answer to calculated value
AES encryption/decryption	Application Processor	Comparison of known answer to calculated value
HMAC-SHA	Application Processor	Comparison of known answer to calculated value
DRBG random bit generation	Application Processor	Comparison of known answer to calculated value
SHA hashing	Application Processor	Comparison of known answer to calculated value
AES-XTS encrypt/decrypt	Application Processor	Comparison of known answer to calculated value

**Table 11 Power-up Cryptographic Algorithm Known Answer Tests**

**FPT\_TST\_EXT.2(1):** 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 it loads. Additionally, the TOE performs checking of the entire /system partition through use of Android's dm\_verity mechanism (and while the TOE will still operate, it will log any blocks/executables that have been modified).

**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 software version) and hardware (model and version). Additionally, the TOE provides users the ability to review the currently installed apps (including 3rd party 'built-in' applications) and their version.

**FPT\_TUD\_EXT.2:** The TOE verifies all OTA (Over The Air) updates to the TOE software (which includes baseband processor updates) using a public key chaining ultimately to the Root Public Key, a hardware protected key whose SHA-256 hash resides inside the application processor. Should this verification fail, the software update will fail and the update will not be installed.

The application processor 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 Root Public Key, 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.

The TOE also provides roll-back protection for OTA updates to prevent a user from installing a prior/previous version of software. Using the bootloader update method, administrators can circumvent this roll-back protection. However, to be able to access the bootloader, an attacker would need unlock access to the phone. Additionally, should an attacker gain the ability to unlock the boot loader, the process of unlocking the bootloader triggers a full

wipe of the phone, preventing any sensitive information from remaining on the phone after a roll-back attack.

**ALC\_TSU\_EXT.1:** Google supports a bug filing system for the Android OS outlined here: <https://source.android.com/setup/contribute/report-bugs>. This allows developers or users to search for, file, and vote on bugs that need to be fixed. This helps to ensure that all bugs that affect large numbers of people get pushed up in priority to be fixed. The method outlined above requires the user to submit their bug to Android's website. As such, the user of the device needs to establish a trusted channel web connection to securely file the bug by following the set-up steps to establish a secure HTTPS/TLS/EAP-TLS connection from the TOE, then visiting the above web portal to submit the report.

Google also commits to pushing out monthly security updates for the Android operating system (including the Java layer and kernel, not including applications). Monthly security updates have historically been supported on Google products for 3 years after release. These systematic updates are designed to address the highest issue problems as quickly as possible and allows Google to ensure their Pixel products remain as safe as possible and any issues are addressed promptly.

Google's creates 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. Google maintains a security blog (<https://android-developers.googleblog.com/>) to disseminate information directly to the public.

## 6.7 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 (if configured) or after a (also configurable) period of inactivity, and as part of that transition, the TOE will display a lock screen to obscure the previous contents and play a "lock sound" to indicate the phone's transition; however, the TOE'S lock screen still displays email notifications, calendar appointments, user configured widgets, text message notifications, the time, date, call notifications, battery life, signal strength, and carrier network. But without authenticating first, a user cannot perform any related actions based upon these notifications (they cannot respond to emails, calendar appointments, or text messages) other than the actions assigned in FIA\_UAU\_EXT.2.1 (see selections in section 5).

Note that during power up, the TOE presents the user with an unlock screen. While at this screen, users can access some basic device functionality (e.g. making an emergency call) and basic system data is decrypted. Once the user enters their password, the user data partition is then decrypted and the full functionality of the phone is unlocked. After this initial screen, upon (re)locking the phone, the user is presented with an "unlock for all features and data" unlock screen. This screen puts the phone in the same state as the aforementioned lock screen, encrypting user data and locking any functionality that requires data that is decrypted by the user's password. While locked, the actions described in FIA\_UAU\_EXT.2.1 are available for the user to utilize.

**FTA\_TAB.1:** The TOE can be configured to display a user-specified message 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, the security type, authentication protocol, and the client credentials to be used for authentication. 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.

---

## 6.8 Trusted path/channels

---

**FTP\_ITC\_EXT.1/FTP\_ITC\_EXT.1/WLAN:** The TOE provides secured (encrypted and mutually authenticated) communication channels between itself and other trusted IT products through the use of IEEE 802.11-2012, 802.1X, and EAP-TLS and TLS. The TOE permits itself and applications to initiate communicate via the trusted channel, and the TOE initiates communications via the WPA2 (IEEE 802.11-2012, 802.1X with EAP-TLS) trusted channel for connection to a wireless access point. The TOE provides mobile applications and MDM agents access to HTTPS and TLS via published APIs, thus facilitating administrative communication and configured enterprise connections. These APIs are accessible to any application that needs an encrypted end-to-end trusted channel.

## 7. TSF Inventory

Below is a list of user-mode TSF binaries and libraries that are used to provide the security functionality of the device. Each of the below are built with the `-fstack-protector-strong` option set. For each binary/library, the name, path, and security function are provided.

Name	Path	Security Function
keystore	/system/bin	Key Store
gatekeeperd	/system/bin	Key MGMT
qseecomd	/system/bin	DAR
time_daemon	/system/bin	Time
vold	/system/bin	DAR
wpa_supplicant	/system/bin	WPA2
adbd	/system/bin	Security System Settings/Recovery
libcrypto.so	/system/lib	Crypto
libcrypto.so	/system/lib64	Crypto
libkeystore_binder.so	/system/lib	KeyStore
libkeystore_binder.so	/system/lib64	KeyStore
libkeyutils.so	/system/lib64	DAR
libssl.so	/system/lib	SSL/TLS
libssl.so	/system/lib64	SSL/TLS
update_engine_sideload	/recovery/root/sbin	Recovery/Initial Image Load
recovery	/recovery/root/sbin	Recovery
mke2fs_static	/recovery/root/sbin	Recovery
charger	/recovery/root/sbin	Recovery
init	/recovery/root	Recovery