Smart-Ex 03 Security Target

Common Criteria: EAL2

Document Version : 1.1

Document Date : 2 Feb 2025

Document management

Document identification

Document title	Smart-Ex 03 Security Target
Document version	1.1
Document date	2 Feb 2025
Author	Securelytics.my
Release Authority	ECOMS

Document history

Version	Date	Description
0.1	27 JULY 2023	Initial draft.
0.2	13 SEPT 2023	Update on the TOE Scope of Evaluation and SFRs.
0.3	18 OCT 2023	Updated based on comments by TOE Developer.
0.4	2 JAN 2024	Updated based on comments by TOE Developer.
0.5	14 MAR 2024	Updated based on comments by TOE Developer.
0.6	28 JUL 2024	Updated based on comments by TOE Developer.
0.7	1 NOV 2024	Updated based on updates from TOE Developer.
0.8	21 NOV 2024	Updated based on updates from TOE Developer.
0.9	8 DEC 2024	Updated based on EOR from SEF.

Version	Date	Description
0.10	12 DEC 2024	Updated based on new info shared by TOE Developer and ATE findings.
0.11	18 DEC 2024	Update info requested by TOE Developer.
0.12	23 DEC 2024	Updated based on CR from CB.
0.13	24 DEC 2024	Updated based on CR from CB.
1.0	19 JAN 2025	Final Released.
1.1	2 Feb 2025	Final Released. Minor updates.

Table of Contents

1 SECURITY TARGET INTRODUCTION

1.1 ST Reference

Doc Title	Smart-Ex 03 Security Target
Doc Version	1.1
Doc Date	2 Feb 2025

1.2 TOE Reference

TOE Title	Smart-Ex
TOE Version	03

1.3 Defined terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term	Description
Authentication data	It is information used to verify the claimed identity of a user.
ACL	Access control lists
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TSC	TOE Scope of Control, the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
TSF	TOE Security Function, set consisting of all hardware, software, and firmware of the product.
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.
SFP	Security Functional Policy, set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.
Unauthorised user	An unauthorised user is an individual that does not have authorisation to use the functionality of the TOE.
User/TOE User	TOE authorised user to operate the TOE.
User data	Data created by and for the TOE user, which may or does not affect the operation of the TSF.
TOE Mobile Apps	Consist of eDIAGNOSTICS, eIS, eLOGKIT, ecomManagerService and eXTEND, which are pre-installed by TOE Developer in the TOE device.
TOE Developer	Defined as the product developer of the TOE. The TOE Developer produced the TOE in form and provides the updates and upgrade of the TOE via the Developer Management System. Developer Management System is a system deployed by the TOE Developer to push updates on the underlying Android OS and push updates on the TOE Mobile Apps.

1.4 TOE Overview

1.4.1 TOE Usage and major security functions

Smart-Ex 03 smartphone is a mobile phone designed and developed by Pepperl+Fuchs SE. The product is designed to be used in explosion hazardous locations and for heavy duty use in industrial environments.

Smart-Ex 03 smartphone (herein after referred to as “Target of Evaluation” (TOE)) runs an Android OS . The TOE features a complex design of safety capabilities. Besides its intrinsically safe electronic design, embedded sensors inside the smartphone monitor thermal incidents that may impact the smartphone integrity.

In addition, to the mentioned thermal monitoring, the TOE is equipped with an intelligent thermal management system that prevents overheating and maintains optimal performance even in hot environments as well as with a Smart-Battery to ensure optimal battery life.

The rugged design of the TOE includes special housing materials, strengthened glass and shock-absorbing materials, making the TOE highly resistant to physical shocks, falls, or rough handling. The TOE had undergo rigorous testing procedures, including drop tests, impact resistance evaluations, and temperature stress tests, to ensure their ability to withstand various adverse conditions and protects the user in hazardous environments.

The following table highlights the range of security functions implemented by the TOE.

Table 1: TOE Security Functions

Security Function	Description
Security Audit	Smart-Ex 03 smartphone as the TOE has the capability to collect, stored and maintained the security events audit log trails of the device components such as sensors, hardware and processor. inclusive of event logs generated by the configuration made on the Android OS, as well as hardware components within the TOE as a smartphone. In which, these components are important to ensure the TOE operates in a good condition, safely from any hazardous conditions and maintain its integrity from any internal or external damages.
Cryptographic Function	Smart-Ex 03 smartphone has the capability of performing security functions related to cryptographic processes through the functionality of the Android OS as well as supported by the chip processes that enable several features such as secure boot and secure data protection storage.

Security Function	Description
User Data Protection	Smart-Ex 03 smartphone as the TOE has the capability and capacity to protect the data stored inside the smartphone (as part of TOE secure operations) consist of audit log trails, collected data from sensors, data performance of hardware, configuration files of Android OS and configuration files of the hardware components. This function to ensure the data consist of files and configuration managed, stored and protected inside the TOE are protected due to unfortunate event inflicted to the TOE such as battery failure, uncontrolled temperature level climb (temperature acceptance (Ta) range accepted: -20 °C ≤ Ta ≤ +60 °C) and physical damages.
Identification and Authentication	Smart-Ex 03 smartphone has the capability to enforce access control based on identification and authentication by enabling security function such as: PIN code, Pattern, Password Based and Biometric fingerprint on the login screen, that enforce security capabilities in protecting the device lock screen security enabled by the TOE User.
Security Management	Smart-Ex 03 smartphone as the TOE is being constructed with management functions that maintain the device conditions to ensure continues capability and capacity from the aspects of device integrity and data securely being protected in the mobile device through device monitoring that is accessible by both TOE User and TOE Developer (If being shared or allow access by TOE user). The security management functions are performed and enforced by the TOE and TOE Mobile Apps (which are: eIS, eLOGKIT, eDIAGNOSTICS, eXTEND and ecomManagerService).
Physical Tampering and Fault Tolerance	Smart-Ex 03 smartphone as the TOE equipped with smart battery sensors and intelligent thermal management systems, the TOE can effectively dissipate heat, prevent overheating and maintains optimal performance even in hot environments. Likewise, the TOE alerts the user on the high and low temperature (temperature acceptance (Ta) range accepted: -20 °C ≤ Ta ≤ +60 °C) through sensors located in the battery compartment as well as around the selected hardware chips in the smartphone. In which, this function mainly to ensure safe operation of Smart-Ex 03 in harsh environments it has been designed for.

Security Function	Description
	With such rugged design of the TOE, it includes reinforced frames, strengthened glass, and shock-absorbing materials, making the smartphone highly resistant to physical shocks, falls, or rough handling.
TOE Access	Smart-Ex 03 smartphone protects the data from unauthorised access as well as prevent any means of accessing sensitive data inside the device without proper credentials. Protection has been applied through the secure configuration enforced by the Android OS supported by the chip processing.

1.4.2 TOE Type

Smart-Ex 03 smartphone is a device that features a protection mechanism in the form of smartphone from the aspects of externally and internally. With high performance hardware such as thermal sensors located in specific area inside the smartphone as well as physical protections that prevent high impact damages that may compromise the smartphone integrity.

The scope of evaluation covers the smart battery sensors, physical protection of the device (smartphone casing and its sensor), TOE mobile applications, evaluated configuration of Android OS and evaluated configuration of the hardware components operated within the device.

In addition, the TOE consist of the following models, its country specific variants which are based on the same system architecture and software baseline.

Table 2: TOE Model

Model	Platform	Kernel	Android Version
Smart-Ex 03 DZ1*	QCM6490	5.4.233	13
Smart-Ex 03 DZ2*	QCM6490	5.4.233	13
Smart-Ex 03*	QCM6490	5.4.233	13

Note that, the notation "*" are meant as the TOE model is based on country specific variants that may vary in the aspect such as Android GMS services must not be installed in certain countries as per Google Licensing requirement and others that shall be advised by the TOE Developer.

The model that will be using for the evaluation will be Smart-Ex 03*. Note that, the other two models in the table above having the same software, hardware, firmware and configuration that uses by the Smart-Ex 03*. Thus, due to the similar build up, both models are included in the scope of evaluation. The different labelling on the models are basically the different name used for marketing in different country and region.

The excluded scope of evaluation are being stated below.

i. User interface components which consist of capacitive touch display and hardware buttons

ii. Mobile applications installed by TOE user and that are not pre-installed by TOE Developer.

iii. Smartphone accessories including the protective case (Ex-protection) and peripherals.

1.4.3 Supporting Hardware, Software and/or Firmware.

The following are the list of supporting hardware, software and/or firmware required by the TOE to operate, in which are not part of TOE scope of evaluation.

Minimum System Requirements	
Operating Systems	Android™ 13 basic architecture as provided by the Android Open Source Project (AOSP) and associated Google Mobile Services (GMS) and GMS API.
Platform	QCM6490, except cryptographic functions provided by the platform and as required to evaluate the security functions provided by the device.
Memory and Storage	Dual channel, non-PoP LPDDR5/LPDDR4X SDRAM, UFS 2.x/3.1, two-lane HS gear 4, SD v3.0, eMMC 5.1, PCIe two-lane NVMe
Display Touch Screen	15.24 cm / 6 inch; 1080 x 2160 pixels; capacitive multitouch; operational while wearing gloves.
Hardware Buttons	On/Off button, right Multi-Function Button, left PTT button, SOS button and Volume Up/Down buttons.
Battery	Li-Ion battery , (exchangeable)
Wireless Technology Requirements	i. WiFi: 6E ready, 802.11 a/b/g/n/ac/ax/e/k/r/v, support for Enterprise deployments. ii. Bluetooth: 5.2 Low Energy support.
Interfaces	USB-C (USB 3.1), 3.5mm analogue audio port, GPIO interface
SIM Configurations	Dual SIM (eSIM + nano SIM).

1.5 TOE Description

The following are the TOE description that shall elaborate further on the details related to the TOE architecture overview and scope of evaluation in the aspects of TOE physical scope and TOE logical scope.

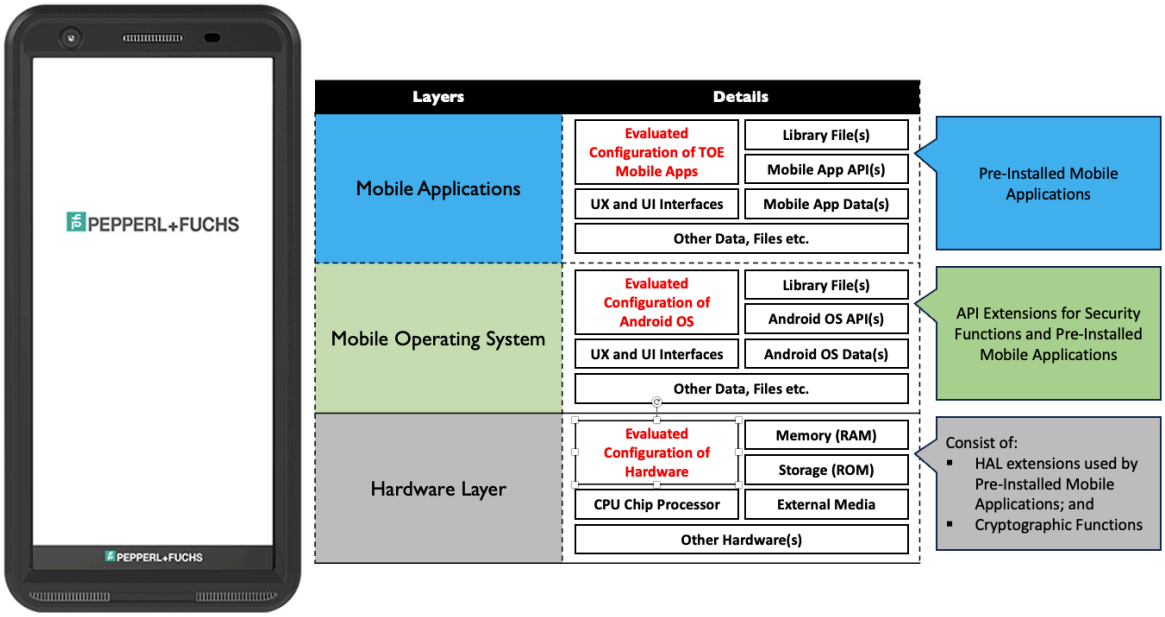

Figure 1: TOE Evaluation Scope

Above in the Figure 1 has highlighted in **RED FONT** is the scope of the TOE.

The TOE (Smart-Ex 03 smartphone) consists of two (2) main parts of operations, which are physical operations and logical operations. The TOE operates as a smartphone designed to be used, handled and designed to operate in hazardous and harsh environments.

1.5.1 Physical Scope of the TOE

In this section, the elaboration covers the physical scope of the TOE and the physical boundaries of the TOE operations. Note that, the TOE physical boundary is the physical perimeter of the device.

With respect to physical operations, the TOE are providing physical security of the smartphone by protecting it through complex design of safety capabilities. It also features embedded hardware sensors inside the smartphone and its battery. These sensors are able to detect high temperatures (beyond temperature acceptance (Ta) range accepted: -20 °C ≤ Ta ≤ +60 °C) that may have an impact on the smartphone integrity from physical and safety perspectives.

With respect to logical operations, the TOE are being operated using Android OS with all pre-installed (default) mobile applications known as TOE Mobile Apps (which are: eIS, eLOGKIT, eDIAGNOSTICS, eXTEND and ecomManagerService) as well mobile applications as provided by the Android Open Source Project (AOSP) and/or as part of GMS.

Mobile applications that are provided by the Android Open Source Project (AOSP) and/or as part of GMS are not in scope of the TOE. In which, that are being installed by TOE Developer to communicate with the smartphone hardware sensors for the purpose of monitoring, collecting device health data, to take defined actions such as generating audit trails and/or generates user-advice messages if determined thresholds are met.

The TOE also has a set of additional APIs provided to configure the devices. These are part of ecomManagerService. Some of these APIs impact the security of the device and are included as part of TOE Mobile Apps.

The TOE is also able to interact with and Enterprise Mobility Management (EMM) system (sometimes also referred to as Mobile Device Management (MDM) system) through Android Management API and Developer extensions following the Android OEM Configuration mechanism. Android OEM Configuration refers to app framework that allows device manufacturers (OEMs) to configure, customize, and manage specific settings, features, or apps on their Android devices without requiring significant software modifications or updates. It enables OEMs to adapt Android to meet the specific needs of product developer.

All operations of the TOE are based on evaluated configuration of TOE Mobile Apps, evaluated configuration of Android OS and evaluated configuration of Hardware that are defined as scope of evaluation related to the operations of hardware, Android OS and pre-installed TOE mobile apps.

Data generated by these pre-installed TOE mobile apps will only be shared upon authorization of TOE User or TOE Developer Services such as Support, Diagnostics or Analytics. The TOE can operate within the environment that is based on hardware configuration of the TOE defined in section 1.5.3.

Note that, all the components stated in section 1.5.2 (excluded in TOE scope of evaluation) and section 1.5.3 in this document shall be treated as not part of the TOE scope.

1.5.2 Logical Scope of the TOE

The following is the list of TOE logical scope that defined in this document, covers by the Security Functional Requirements (SFRs).

A. **Security Audit.** Smart-Ex 03 smartphone as the TOE has the capability to collect, stored and managed all the security events audit log trails of the device components such as sensors, hardware and processor. inclusive of event logs generated by the configuration made on the Android OS as well as within the TOE Mobile Apps. These audit logs are securely stored and maintained within the TOE device so that they can be accessed by TOE Developer and/or exported to an EMM system.

B. **Cryptographic Function.** The TOE has several cryptographic functions that enable security capabilities of performing encryption, decryption, signing and hashing on relevant data, files and configuration enables within the TOE. This security features are triggered by the Android OS and/or TOE User with the support of chip processor of the TOE.

C. **User Data Protection.** The TOE uses file based encryption as default method to protect user data stored on the device. The TOE has the capability of protect data, files and configurations by securely stored in the TOE and preventing from any attempts to reallocate or modify these data, files and configurations without proper identification and authentication.

   The TOE support device configurations enforced by user EMM to separate data between professional and personal use. TOE supports multiple users by using Android OS standard multi-user set-up. In this aspect, a user is considered a natural person. Each user is associated with an account and can have multiple profiles which are linked to a parent profile. Profiles assure separation of user data, even though the users share system resources and system wide settings for e.g. wireless configurations. The TOE mobile applications along with other system applications rely on the Android standard concept of “Application Sandboxing” to further ensure data safety and protection. TOE supports display time-out functions which have to be enabled by the TOE User.

   The TOE includes pre-installed applications or services, developed by the TOE Developer known as TOE Mobile Apps, which are: eDIAGNOSTICS, eIS, ecomManagerService, eXTEND and eLOGKIT. These pre-installed mobile applications are being use on the implemented of sensors and related system data generated by the platform to provide additional services to TOE User, TOE Device Administrator and TOE Service Department.

   For all of these pre-installed mobile applications (consist of: eDIAGNOSTICS, eIS, eLOGKIT, ecomManagerService and eXTEND), the TOE User or TOE Developer is in control of the data. No data are being sent in the background to TOE developer without user consent.

D. **Identification and Authentication.** As to support the processes of any security functions, these functions enable TOE User to properly identify and authenticate device user and preventing any attempts of accessing the TOE device without proper credentials. The security functions are being enforced by enabling security function such as: PIN code, Pattern, Password Based and Biometric fingerprint on the login screen.

E. **Security Management.** TOE has the management functions to ensure the smartphone operates securely and its integrity being maintained within the physical and logical boundaries as defined herein. The management functions are presented to the TOE User/TOE Developer via Android inherent management functions. In the event of any issues found in the TOE, the data can be shared with TOE Developer via email, file sharing and manual data transfer using cable with authorisation of TOE User. Access to the management function require TOE User to properly identify and authenticated. The security management functions are performed and enforced by the TOE and TOE Mobile Apps (which are: eIS, eLOGKIT, eDIAGNOSTICS, eXTEND and ecomManagerService).

F. **Physical Tampering and Fault Tolerance.** TOE has the monitoring, alerts and prevention capability in providing protection to the smartphone (as in the TOE) through triggered security events that are recorded by security audit function and managed by security management function. From the physical protection aspects, the TOE is able to ensure the components inside the smartphone are being protected by the rugged design of TOE casing supported with reinforced frames, strengthened glass, and shock-absorbing materials, making the smartphone highly resistant to physical shocks, falls, or rough handling.

   The TOE has the capability of providing a means to protect the TSF data by providing reliable forms of encapsulation materials protection, which is injected into the metal shielding chambers, protecting the hardware components of the TOE device. Aside of that, self-test during boot up and initial start-up of the device ensuring the TOE integrity from logical and physical are being checked.

   Furthermore, the thermal protection of the device consists of two layers of protection. Temperature thresholds (temperature acceptance (Ta) range accepted: -20 °C ≤ Ta ≤ +60 °C) are monitored by device hardware (hardware coded, thus can't be influenced by software) and will make sure the device is not functional anymore if these thresholds are exceeded. The software base protection (eIS) also monitors the temperature behaviour, alerts the user and/or generates audit trails if temperature thresholds are crossed and/or if tampering is suspected.

G. **TOE Access.** The TOE has the capabilities to allow specific access to the security functions with respects of proper identification and authentication has been successful performed, whilst enabling the TOE User and TOE Developer to have access to security functionalities within the TOE from the aspects of TOE Mobile Apps, Android OS functions and hardware functions.

Note that, All operations of the TOE are based on evaluated configuration of TOE Mobile Apps, evaluated configuration of Android OS and evaluated configuration of Hardware that are defined as scope of evaluation related to the operations of hardware, Android OS and pre-installed TOE mobile apps.

2 CONFORMANCE CLAIM

The ST and TOE are conformant to version 3.1 (REV 5) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 5), April 2017.
- **Part 3 conformant, EAL2.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 5), April 2017.
- This ST and TOE did not conformance to any Protection Profiles.

3 SECURITY PROBLEM DEFINITION

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,
b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and
c) any relevant ***organisational security policies*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The TOE addresses the following threats.

Table 3: TOE Threats

Identifier	Threat statement
T.AUDIT	Actions may not be accountable because of the audit records are not reviewed, thus allowing an attacker to modify the behaviour of TSF data without being detected.
T.MGMT	Attacker may attempt to change the data inside the smartphone by gaining unauthorised access to the smartphone by dictionary brute forcing the PIN code or Password on the smartphone lock screen.
T.PHYSICAL	The attacker may attempt to break the protective casing and bypass the encapsulation materials, which is injected into the metal shielding chambers, in which protecting all the hardware components of the TOE device, with the objective of access the hardware chips, electronics board, ROM and RAM, by gaining access physically to the data stored inside the hardware .
T.THERMAL	Attacker may attempt to heat up the smartphone to certain temperature or hitting certain temperature threshold of the smartphone to create system malfunction.

Identifier	Threat statement
T.ACCESS	Attacker may have access to the data/file(s) physical or content without having permission from the authorized TOE user (in which the person who owns, or is responsible for, the information). This threat is applicable if the device installed with the TOE got stolen or falls into the hands of an attacker, who then attempts to gain unauthorized access to the device protected by the TOE.
T. MALWARE	Any 3rd party mobile applications installed or loaded onto the TOE device may include malicious or exploitable code. This code could be included intentionally or unknowingly by the developer, perhaps as part of a software library. Malicious apps may attempt to exfiltrate data to which they have access. They may also conduct attacks against the platform's system software, which will provide them with additional privileges and the ability to conduct further malicious activities. Malicious applications may be able to control the device's sensors (GPS, camera, microphone) to gather intelligence about the user's surroundings even when those activities do not involve data resident or transmitted from the device. Flawed applications may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.

3.3 Organisational Security Policies

No organisational security policies have been defined regarding the use of the TOE in specific for this ST. Nonetheless, there few recommendations on the TOE operations in the aspects of organization measures. This is to ensure the TOE is operated in the way it has been evaluated, whilst the TOE User has to ensure the following configuration has been enabled. The configuration can be also enforced by a respective Mobile Device Management profile.

i. Lock Screen configuration:
   - Enforce lock screen password.
   - Enable time-out.

ii. Thermal Monitoring configuration:
   - Enable thermal monitoring.

iii. Device Management profiles configuration:
   - Enable security audit logging.
   - Configure multi-user profiles, if applicable.

iv. Log Management configuration: Disable log capturing including bug report collection.

v. Mobile Application Management Configuration: Disable installation of applications through sideload.

vi. Cryptography configuration: Ensure that only mobile applications and services are used, that make use of the cryptographic algorithms recommended by TOE developer and as per mentioned in this ST. In addition, it is recommended to refer the list of deprecated cryptographic algorithms published by NIST (NIST Special Publication 800-131A Revision 2) and permanently disable all deprecated algorithms.

vii. The Diagnostic Mode port is being disable as a mechanism to protect the TOE device from possible unauthorised access from external with intern to perform unauthorised access and modification on the TOE operations, data and configuration.

viii. The Bootloader Mode and OEM Locking are mechanism enabled in the TOE device with objective to protect the TOE from possible attack in aspects of tampering with the TOE data and configuration set by TOE Developer.

3.4 Assumptions

The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 4: TOE Assumptions

Identifier	Assumption statement
A.TOE_USER	TOE User can access the files and folders of the TOE that is been installed in the device, in which they can be trusted and shall not be considered to be hostile, are not careless (aware of the surrounding to prevent any social engineering attacks) and understood the importance of keeping information of data/files plus password in private (securely).
A.NOEVIL	TOE User that are responsible for configuring, installing and removing the TOE Mobile Apps, whilst managing the TOE Mobile Apps data and communication with the Developer Management System for updates or upgrades. It is assumed that this person, is not hostile and is competent. Note that, the Developer Management System is a system deployed by the TOE Developer to push updates on the underlying Android OS and push updates on the TOE Mobile Apps.
A.PASSWD	TOE User are recommended to enable complex password protected or biometric access protection on the smartphone lock screen.
A.CONFIG	It is assumed that the TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable based on the usage of the TOE device.

4 SECURITY OBJECTIVES

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

Table 5: Security Objective for the TOE

Identifier	Objective statements
O.AUDIT	The TSF shall provide a means to record a readable audit trail of information of every file access by different applications, moving of information to the external devices, file ownership, and blocked operations.
O.MGMT	The TSF shall enforced protection on the data stored inside the smartphone (including all TSF data) and prevent any unauthorised access from external.
O.PHY_PROTECT	The TSF shall ensure all TOE files and its resources are not being tampered or modified due to the physical hacking, cracking and breaking the physical protection of the TOE casing performed by unauthorized individual.
O.THML_PROTECT	The TSF shall ensure all TOE files and its resources are not being tampered or modified due to the physical hacking, cracking and breaking the thermal sensors of the device performed by unauthorized individual.
O.MANAGE	The TOE shall allow TOE user to manage the TOE and its security functions, whilst ensure that only authorized TOE user is able to access TOE functionality.
O.STORE	To address the issue of loss of confidentiality of user data in the event of loss of the TOE device, it is conformant that the TOE will use data-at-rest protection. The TOE will be capable of encrypting data and keys stored on the device and will prevent unauthorized access to encrypted data reside in the TOE device.

Identifier	Objective statements
O.INTEGRITY	To ensure the integrity of the TOE is maintained by performing self-tests to ensure the integrity of critical functionality, software/firmware and data has been maintained. The user shall be notified of any failure of these self-tests.

4.3 Security Objectives for the TOE Operational Environment

Table 6: Security Objective for the TOE Operational Environment

Identifier	Objective statements
OE.USER_GUIDANCE	Those responsible for the TOE must provide documentation for TOE user that are containing information sufficient to guide in operating the TOE by enable complex password/PIN code protection, and/or enable biometric access controls protection.
OE.NO_EVIL	The TOE user roles should be adequately trained, responsible and honest individuals who are not motivated to disable, degrade or subvert the operation of the TOE in the environment for personal gain or other purposes that contradict the security policies of the organization.
OE.CONFIG	TOE Developer and TOE User will configure the TOE security functions correctly to create the intended security policy.

4.4 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

Table 7: Security Objective Rational Mapping

THREATS/ ASSUMPTIONS / OBJECTIVES	T.AUDIT	T.MGMT	T.PHYSICAL	T.THERMAL	T.ACCESS	T.MALWARE	A.TOE_USER	A.NOEVIL	A.PASSWD	A.CONFIG
O.AUDIT	☒	☒								
O.MGMT	☒	☒								
O.PHY_PROTECT			☒							
O.THML_PROTECT				☒						
O.MANAGE					☒	☒				
O.STORE					☒	☒				
O.INTEGRITY						☒				
OE.USER_GUIDANCE							☒	☒	☒	
OE.NO_EVIL							☒	☒		
OE.CONFIG										☒

4.4.1 TOE Security objectives rationale

The following table demonstrates that all security objectives for the TOE are trace back to the threats in the security problem definition.

Table 8: Security Objective Rationale Justification

Threats	Objectives	Rationale
T.AUDIT	O.AUDIT	O.AUDIT counter the threat T.AUDIT by providing a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
	O.MGMT	O.MGMT counter the threat T.AUDIT by providing a means to managing all the data of the TSF inside the smartphone securely and maintained integrity from any forms of modification by unauthorised user, through the support of readable and reliable audit trail.
T.MGMT	O.MGMT	O.MGMT counter the threat T.MGMT by providing a means to managing all the data of the TSF inside the smartphone securely and maintained integrity from any forms of modification by unauthorised user.
	O.AUDIT	O.AUDIT counter the threat T.MGMT by providing a means to managing all the data of the TSF inside the smartphone securely and maintained integrity from any forms of modification by unauthorised user, through the support of readable and reliable audit trail.
T.PHYSICAL	O.PHY_PROTECT	O.PHY_PROTECT counter the threat T.PHYSICAL by providing a means to protect the TSF data by providing reliable forms of encapsulation materials protection, which is injected into the metal shielding chambers, in which protecting all the hardware components of the TOE device that supported by TOE Mobile Apps that monitors the status with triggering alerts.

Threats	Objectives	Rationale
T.THERMAL	O.THML_PROTECT	O.THML_PROTECT counter the threat T.THERMAL by providing a means to protect the TSF data and the device by providing reliable forms of temperature sensors supported by TOE Mobile Apps that monitors the status with triggering alerts.
T.ACCESS	O.MANAGE	O.MANAGE counter the threat T.ACCESS by providing a means protection of data of the TOE functionality by enabling preventive measures of secure identification and authentication mechanisms.
	O.STORE	O.STORE counter the threat T.ACCESS by providing a means protection of data of the TOE functionality by enabling preventive measures of secure data storage by cryptographic functionalities.
T.MALWARE	0.MANAGE	O.MANAGE counter the threat T.MALWARE by providing a means protection of data of the TOE functionality by enabling preventive measures of secure identification and authentication mechanisms. Any means of installing new mobile apps required proper identification and authentication mechanisms triggered by the TOE User.
	O.STORE	O.STORE counter the threat T.MALWARE by providing a means protection of data of the TOE functionality by enabling preventive measures of secure data storage by cryptographic functionalities.
	O.INTEGRITY	O.INTEGRITY counter the threat T.MALWARE by providing a means protection of data of the TOE functionality by enabling self-test of the device during device turn on and reboot. To ensure the data stored in the TOE mobile device are maintained of its integrity.

4.4.2 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment are trace back to assumptions in the security problem definition.

Table 9: Environment Security Objective Rationale Justification

Assumptions	Objective	Rationale
A.TOE_USER	OE.USER_GUIDANCE	OE.USER_GUIDANCE counter the threat A.TOE_USER by providing a means education and trust on the TOE User by understanding the usage and operations of the TOE Mobile Apps and overall functions/features of the smartphone that holds the TSF data.
	OE.NO_EVIL	OE.NO_EVIL counter the threat A.TOE_USER by providing a means education and trust on the TOE User by the assumption that the TOE User is hostile and is competent.
A.NO_EVIL	OE.USER_GUIDANCE	OE.USER_GUIDANCE counter the threat A.NO_EVIL by providing a means education and trust on the TOE User by understanding the usage and operations of the TOE Mobile Apps and overall functions/features of the smartphone that holds the TSF data.
	OE.NO_EVIL	OE.NO_EVIL counter the threat A.NO_EVIL by providing a means education and trust on the TOE User by the assumption that the TOE User is hostile and is competent.
A.PASSWD	OE.USER_GUIDANCE	OE.USER_GUIDANCE counter the threat A.PASSWD by providing a means education and trust on the TOE User by understanding the usage and operations of the TOE Mobile Apps and overall functions/features of the smartphone that holds the TSF data.

Assumptions	Objective	Rationale
A.CONFIG	OE.CONFIG	OE.CONFIG counter the threat A.CONFIG by enforcing secure development and secure production of the TOE on the TOE Device by following all security policies plus guidance as per instructed defined in the documentation in ensuring the TOE able to be operated in secure manner.

5 EXTENDED COMPONENTS DEFINITION

No extended components have been defined for this ST.

6 SECURITY REQUIREMENTS

6.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows **[assignment].**
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows ***[selection]*.**
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using underlined and bolded text, for additions (e.g., **additions**), and strike-through, for deletion (e.g., ~~deletions)~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter/word at the end of the component identifier as given example as such: FDP_IFF.1a, FDP_IFF.1b, FIA_UID.1/ENTRY and FIA_UID.1/OUT_TO.

6.2 Security functional requirements

6.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 6.1 above and are itemised in the table below.

Table 10: SFRs

No.	Identifier	Title
	FAU: Security audit	
1.	FAU_ARP.1	Security alarms
2.	FAU_GEN.1	Audit data generation
3.	FAU_SAA.1	Potential violation analysis
4.	FAU_STG.1	Protected audit trail storage

No.	Identifier	Title
5.	FAU_STG.4	Prevention of audit data loss
	FCS: Cryptographic Support	
6.	FCS_CKM.1	Cryptographic key generation
7.	FCS_CKM.4	Cryptographic key destruction
8.	FCS_COP.1/ENC_DEC	Cryptographic operation (Encrypt and Decrypt Function)
9.	FCS_COP.1/HASH	Cryptographic operation (Hash Function)
10.	FCS_COP.1/SIGN	Cryptographic operation (Digital Signature or Signing Function)
	FDP: User data protection	
11.	FDP_ACC.1	Subset access control
12.	FDP_ACF.1	Security attribute based on access control
13.	FDP_ITC.1	Import of user data without security attributes
14.	FDP_SDI.1	Stored data integrity monitoring
15.	FDP_SDI.2	Stored data integrity monitoring and action
	FIA: Identification and authentication	
16.	FIA_AFL.1	Authentication failure handling
17.	FIA_ATD.1	User attribute definition
18.	FIA_SOS.2	TSF Generation of secrets
19.	FIA_UAU.2	User authentication before any action
20.	FIA_UAU.4	Single-use authentication mechanisms
21.	FIA_UAU.6	Re-authenticating
22.	FIA_UAU.7	Protected authentication feedback
23.	FIA_UID.2	User identification before any action

No.	Identifier	Title
	FMT: Security management	
24.	FMT_MOF.1	Management of security functions behaviour
25.	FMT_MSA.1	Management of security attributes
26.	FMT_MSA.3	Static attribute initialisation
27.	FMT_SMF.1	Specification of management function
28.	FMT_SMR.1	Security roles
	FPT: Protection of the TSF	
29.	FPT_PHP.1	Passive detection of physical attack
30.	FPT_PHP.3	Resistance to physical attack
31.	FPT_STM.1	Reliable time stamps
32.	FPT_TST.1	TSF testing
	FTA: TOE Access	
33.	FTA_SSL.1	TSF-initiated session locking
34.	FTA_SSL.3	TSF-initiated termination
35.	FTA_TAB.1	Default TOE Access banners

6.2.2 FAU_ARP.1 Security alarms

Hierarchical to:	No other components.
Dependencies:	FAU_SAA.1 Potential violation analysis
FAU_ARP.1.1	The TSF shall take **[assignment: Notification on the eIS that monitors the data from various thermal sensors]** upon detection of a potential security violation.
Notes:	The features can be turn off and turn on based on the organisation security policy implementation through the configuration performed by TOE Device Administrator or requested by the TOE User. By default, this feature is enable unless being turn off.

6.2.3 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **[*selection: minimum*]** level of audit; and **c) [assignment: All administrative actions, start-up and shutdown of the OS, insertion or removal of external media (e.g., SD card, SIM Card), enrolment/activation of eSIM, auditable events generated by TOE Mobile Apps and auditable events generated by the OS, Invocation of ECOMS SDK APIs (kindly refer to Appendix A)].**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**assignment: none].**
Notes:	The following are auditable events recorded by TOE as stated below. These audit event logs are being captured by TOE Mobile Apps based on individual features and functions.

In addition, there are several modules in the TOE that supporting the audit functions which are: Android SELinux, Android Secure Boot and DM Verify.

The retention period of the audit logs only applicable during the phone online (power on) and accessible through relevant interface(s) approved by the TOE Developer. Once the TOE restarted, the existing log will be override.

Table 11: Auditable events

LOG TYPE	SUBJECT/ COMPONENT TOE	DETAILS
Log 1	**Device Thermal Sensors (related to eIS)**	**Device temperature exceeds the threshold (temperature acceptance (Ta) range accepted: -20 °C ≤ Ta ≤ +60 °C).**
Log 2	**Battery Model**	**Unapproved battery detected.**
Log 3	**Administrative Actions**	**Logs generated by OS and mobile apps triggered by the actions performed by TOE User.**
Log 4	**Start-Up and Shutdown**	**Logs generated by OS based on the actions requested by TOE User to turn on or turn off the TOE.**
Log 5	**Insertion of External Media**	**Logs generated by OS based on the actions requested by TOE User to insert or remove external media.**
Log 6	**OS and Pre-Installed Mobile Apps**	**Logs generated by OS and TOE Mobile Apps based on actions performed/requested by TOE User.**
Log 7	**Rooting of Device**	**Logs generated by OS based on attempt to root the device by TOE User.**
Log 8	**Harmful App Installed**	**Logs generated by eXTEND when any platform signed app that is considered risky is installed by TOE User.**

	Log 9	**Security Event**	**Logs generated by security event in the device.**	

6.2.4 FAU_SAA.1 Potential violation analysis

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of **[assignment: subset of defined auditable events in Table 11]** known to indicate a potential security violation; b) **[assignment: none].**
Notes:	In addition, there are several modules in the TOE that supporting the audit functions which are: Android SELinux, Android Secure Boot and DM Verify.

6.2.5 FAU_STG.1 Protected audit trail storage

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [***selection: detect***] unauthorised modifications to the stored audit records in the audit trail.
Notes:	In addition, there are several modules in the TOE that supporting the audit functions which are: Android SELinux, Android Secure Boot and DM Verify. The audit trails (also known as audit logs and event logs) are being managed by Android OS and may be collected by the TOE Mobile Apps based on their features and functions as either requested by TOE User or TOE Developer.

6.2.6 FAU_STG.4. Prevention of audit data loss

Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall [***selection, choose one of: "overwrite the oldest stored audit records"***] and [**assignment: circular log buffer size function**] if the audit trail is full.
Notes:	In addition, there are several modules in the TOE that supporting the audit functions which are: Android SELinux, Android Secure Boot and DM Verify.

6.2.7 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**assignment: AES, SHA, ECDSA**] and specified cryptographic key sizes [**assignment: AES (256-bit), SHA (256/384/512-bit keys), ECDSA (256-bit keys)**] that meet the following: [**assignment: FIPS 140-2**].
Notes:	All the stated key generation schemes used for the key establishment and entity authentication. Furthermore, this SFRs are meant to protect data in the TOE through the process of cryptographic functions upon unlocked and locked of the TOE on login page screen. Additional Notes: i. Cryptographic on Software Level: Android verified boot2.0 Cryptographic authentication of high-level operating system (HLOS) images. ii. Cryptographic on Hardware Core: AES, SHA cryptographic algorithms implemented in device hardware.

	iii. Crypto Engine: Hardware engine for encrypting and decrypting storage devices. iv. Fuse Memory: One-time programmable QFPROM fuse memory and automatic programming via sec-partition. v. Management Master Key: Hardware-backed (KeyStore services supporting public and private key generation, management, signing, and verification. vi. Android OS Crypto Function: Verified Boot is Google's defined mechanism for the Android boot loader to verify the integrity of Android boot and recovery images before bootup. ASN1Dxe – Contains the implementation of routines required to parse ASN1 X509 data, such as Android Verified Boot Signature and Certificate. In addition, the usage of the cryptographic algorithms and key sizes are depending on the need of the TOE User(s) organisational security policies based on the usage and deployment environment. The possible use of deprecated algorithms are not recommended but depends on the risk assessment and risk appetite of the TOE User(s) organisation requirements.

6.2.8 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**assignment: overwrite**] that meets the following: [**assignment: none**].
Notes:	None.

6.2.9 FCS_COP.1/ENC_DEC Cryptographic operation (Encrypt and Decrypt Function)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or

	FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1 /ENC_DEC	The TSF shall perform [**assignment: encrypt/decrypt**] in accordance with a specified cryptographic algorithm [**assignment: AES, SHA, ECDSA**] and cryptographic key sizes [**assignment: AES (256-bit), SHA (256/384/512-bit keys), ECDSA (256-bit keys)**] that meet the following: [**assignment: FIPS 140-2**].
Notes:	All the stated key generation schemes used for the key establishment and entity authentication. Furthermore, this SFRs are meant to protect data in the TOE through the process of cryptographic functions upon unlocked and locked of the TOE on login page screen. Additional Notes: i. Cryptographic on Software Level: Android verified boot2.0 Cryptographic authentication of high-level operating system (HLOS) images. ii. Cryptographic on Hardware Core: AES, SHA cryptographic algorithms implemented in device hardware. iii. Crypto Engine: Hardware engine for encrypting and decrypting storage devices. iv. Fuse Memory: One-time programmable QFPROM fuse memory and automatic programming via sec-partition. v. Management Master Key: Hardware-backed (KeyStore services supporting public and private key generation, management, signing, and verification. vi. Android OS Crypto Function: Verified Boot is Google's defined mechanism for the Android boot loader to verify the integrity of Android boot and recovery images before bootup. ASN1Dxe – Contains the implementation of routines required to parse ASN1 X509 data, such as Android Verified Boot Signature and Certificate.

6.2.10 FCS_COP.1/HASH Cryptographic operation (Hash Function)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1 /HASH	The TSF shall perform [**assignment: hashing**] in accordance with a specified cryptographic algorithm [**assignment: SHA**] and cryptographic key sizes [**assignment: 256-bits, 384-bits, 512-bits**] that meet the following: [**assignment: FIPS 180-4**].
Notes:	The hash selection must support any operations for security validation or security checks. The hash selection should be consistent with the overall strength of the algorithm used (for example, SHA 256 for 128-bit keys). Additional Notes: i. Cryptographic on Software Level: Android verified boot2.0 Cryptographic authentication of high-level operating system (HLOS) images. ii. Cryptographic on Hardware Core: AES, SHA cryptographic algorithms implemented in device hardware. iii. Crypto Engine: Hardware engine for encrypting and decrypting storage devices. iv. Fuse Memory: One-time programmable QFPROM fuse memory and automatic programming via sec-partition. v. Management Master Key: Hardware-backed (KeyStore services supporting public and private key generation, management, signing, and verification. vi. Android OS Crypto Function: Verified Boot is Google's defined mechanism for the Android boot loader to verify the integrity of Android boot and recovery images before bootup. ASN1Dxe – Contains the implementation of routines required to parse ASN1 X509 data, such as Android Verified Boot Signature and Certificate.

6.2.11 FCS_COP.1/SIGN Cryptographic operation (Digital Signature or Signing Function)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 /SIGN	The TSF shall perform [**assignment: generation and verification based on signing mechanism**] in accordance with a specified cryptographic algorithm [**assignment: RSA**] and cryptographic key sizes [**assignment: 2048-bits or greater**] that meet the following: [**assignment: FIPS PUB 186-4**].
Notes:	The algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement should be iterated to specify the functionality. Additional Notes: i. Cryptographic on Software Level: Android verified boot2.0 Cryptographic authentication of high-level operating system (HLOS) images. ii. Cryptographic on Hardware Core: AES, SHA cryptographic algorithms implemented in device hardware. iii. Crypto Engine: Hardware engine for encrypting and decrypting storage devices. iv. Fuse Memory: One-time programmable QFPROM fuse memory and automatic programming via sec-partition. v. Management Master Key: Hardware-backed (KeyStore services supporting public and private key generation, management, signing, and verification. vi. Android OS Crypto Function: Verified Boot is Google's defined mechanism for the Android boot loader to verify the integrity of Android boot and recovery images before bootup. ASN1Dxe – Contains the implementation of routines required to parse ASN1 X509 data, such as Android Verified Boot Signature and Certificate.

6.2.12 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the **[assignment: access control SFP, as in Table 12]** on **[assignment: list of subjects, objects, and operations components among subjects and objects covered by the SFP as stated below.** Table 12: Access Control SFP

SUBJECT	OBJECT	OPERATION COMPONENTS
TOE Mobile Apps (eDIAGNOSTICS and eIS)	Battery Hardware Sensors (device temperature and battery health)	PCB temperature, Battery Health, and Alerts (temperature acceptance (Ta) range accepted: -20 °C ≤ Ta ≤ +60 °C).
TOE Mobile Apps (eDIAGNOSTICS)	Hardware Sensors (Accelerometer, Gyroscope, Compass, Proximity, Light, Magnetic)	Hardware Status, Monitor Status, Detection Status and Alerts.
Input Devices	Microphone and Camera	Configuration of Hardware components related to the object mentioned.
Device Location	GPS	Configuration of Hardware components related to the object mentioned.
TOE User Credentials	System Wide Credentials	Configuration, data and files stored inside the TOE related to the object mentioned.
Content of TOE Mobile Apps	Pictures, text messages, emails and documents stored in the TOE	Configuration, data and files stored inside the TOE related to the object mentioned.
Information	Device Identifier	Configuration of Hardware components related to the object mentioned.
Network Access	Wireless Adapter, Mobile Adapter, Bluetooth Adapter and NFC Adapter	Configuration of Hardware components related to the object mentioned.

].

Notes:	None.

6.2.13 FDP_ACF.1 Security attribute based on access control

<table>
<tr><td>Hierarchical to:</td><td>No other components.</td></tr>
<tr><td>Dependencies:</td><td>FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation</td></tr>
<tr><td>FDP_ACF.1.1</td><td>The TSF shall enforce the [assignment: access control SFP, as in Table 12] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, as in Table 12].</td></tr>
<tr><td>FDP_ACF.1.2</td><td>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects as stated below.
Table 13: Access Control SFP Rules
<table>
<tr><th>SUBJECT</th><th>OBJECT</th><th>RULES</th></tr>
<tr><td>Input Devices</td><td>Microphone and Camera</td><td>Allow access as per requested by TOE User or TOE Mobile Apps.</td></tr>
<tr><td>Device Location</td><td>GPS</td><td>Allow access as per requested by TOE User or TOE Mobile Apps.</td></tr>
<tr><td>Content of TOE Mobile Apps</td><td>Pictures, text messages, emails and documents stored in the TOE</td><td>Allow access as per requested by TOE User or TOE Mobile Apps.</td></tr>
<tr><td>Information</td><td>Device Identifier</td><td>Allow access as per requested by TOE User or TOE Mobile Apps.</td></tr>
<tr><td>Network Access</td><td>Wireless Adapter, Mobile Adapter, Bluetooth Adapter and NFC Adapter</td><td>Allow access as per requested by TOE User or TOE Mobile Apps.</td></tr>
</table>
].</td></tr>
</table>

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: none]**.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: none]**.
Notes:	None.

6.2.14 FDP_ITC.1 Import of user data without security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1	The TSF shall enforce the [**assignment: access control SFP(s) based on Table 12 and Table 13**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**assignment: none**].
Notes:	None.

6.2.15 FDP_SDI.1 Stored data integrity monitoring

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDI.1.1	The TSF shall monitor user data stored in containers controlled by the TSF for [**assignment: integrity errors**] on all objects, based on the following attributes: [**assignment: TOE User data attributes related to the evaluated configuration of TOE Mobile Apps, evaluated configuration of Android OS and evaluated configuration of Hardware**].

Notes:	None.

6.2.16 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for [**assignment: integrity errors**] on all objects, based on the following attributes: [**assignment: TOE User data attributes related to the security configuration, files, hardware, OS configuration and TOE Mobile Apps configuration**].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [**assignment: alert TOE User**].
Notes:	None.

6.2.17 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [***selection: [assignment: value configured by TOE User]***] unsuccessful authentication attempts occur related to [**assignment: PIN code login screen, Pattern, Password Based, Biometric fingerprint login screen**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***selection: met***], the TSF shall [**assignment: lockout and prevent to login on the screen with the timeout set by TOE User**].
Notes:	Note that it is possible the TOE User and TOE Developer to enable Android Password Requirements function. It is recommended for TOE User to set the value “3” for unsuccessful authentication attempts. In addition, the configurable value that is recommended are based on the TOE User organisational security policies through the results of the risk assessment and risk appetite of the TOE User(s) organisation requirements.

	Additional notes that the as for the biometric fingerprint sensor, the configuration recommended as in: False Acceptance Rate (FAR) for fingerprint shall not exceed [1:X].

6.2.18 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment: login screen access credentials consist of PIN code login screen, Pattern, Password Based, Biometric fingerprint login screen**].
Notes:	Note that it is possible the TOE User and TOE Developer to enable Android Password Requirements function. It is recommended for TOE User to set the value "3" for unsuccessful authentication attempts. In addition, the configurable value that is recommended are based on the TOE User organisational security policies through the results of the risk assessment and risk appetite of the TOE User(s) organisation requirements. Additional notes that the as for the biometric fingerprint sensor, the configuration recommended as in: False Acceptance Rate (FAR) for fingerprint shall not exceed [1:X].

6.2.19 FIA_SOS.2 TSF Generation of secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.2.1	The TSF shall provide a mechanism to generate secrets that meet [**assignment: a defined quality metric configured by the TOE User**].
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for [**assignment: encryption/decryption function, password management function, access control function, biometric security function, access to configuration of hardware, access to configuration of OS, access to configuration of TOE Mobile Apps, PKI key management function**].

Notes:	Note that it is possible the TOE User and TOE Developer to enable Android Password Requirements function.

6.2.20 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Notes:	Note that it is possible the TOE User and TOE Developer to enable Android Password Requirements function. It is recommended for TOE User to set the value "3" for unsuccessful authentication attempts. In addition, the configurable value that is recommended are based on the TOE User organisational security policies through the results of the risk assessment and risk appetite of the TOE User(s) organisation requirements. Additional notes that the as for the biometric fingerprint sensor, the configuration recommended as in: False Acceptance Rate (FAR) for fingerprint shall not exceed [1:X].

6.2.21 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [**assignment: PIN code login screen and Password Based].**
Notes:	Note that it is possible the TOE User and TOE Developer to enable Android Password Requirements function. It is recommended for TOE User to set the value "3" for unsuccessful authentication attempts. In addition, the configurable value that is recommended are based on the TOE User organisational security policies through the results of the risk assessment and risk appetite of the TOE User(s) organisation requirements.

	Additional notes that the as for the biometric fingerprint sensor, the configuration recommended as in: False Acceptance Rate (FAR) for fingerprint shall not exceed [1:X].

6.2.22 FIA_UAU.6 Re-authenticating

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [**assignment: session lock-out of TOE Mobile Apps or exiting TOE Mobile Apps or exiting any configuration functions on the TOE**].
Notes:	None.

6.2.23 FIA_UAU.7 Protected authentication feedback

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_UAU.7.1	The TSF shall provide only [**assignment: obscured feedback to the device's display**] to the user while the authentication is in progress.
Notes:	All authentication methods specified in FIA_ATD.1. The TSF may not display each character and will not provide an option to allow the TOE User to unmask the password; however, the password must be obscured (mask) by default.

6.2.24 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Notes:	Note that it is possible the TOE User and TOE Developer to enable Android Password Requirements function.

	It is recommended for TOE User to set the value "3" for unsuccessful authentication attempts. In addition, the configurable value that is recommended are based on the TOE User organisational security policies through the results of the risk assessment and risk appetite of the TOE User(s) organisation requirements. Additional notes that the as for the biometric fingerprint sensor, the configuration recommended as in: False Acceptance Rate (FAR) for fingerprint shall not exceed [1:X]. Note: The False Acceptance Rate (FAR) in fingerprint biometric systems measures how often unauthorized users are mistakenly granted access, and it is crucial to ensure this rate does not exceed [1:X] to maintain security and prevent unauthorized access while balancing usability. The value set [1:X] is recommended that X not goes beyond 5 to ensure the value still protecting from attempt of bypassing the protection. This is subject to the TOE User demand or organisation demand on specific configuration.

6.2.25 FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to [***selection: disable, enable***] the functions [**assignment: list of object in Table 12 and Table 13**] to [**assignment: TOE User**].
Notes:	None.

6.2.26 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1	The TSF shall enforce the **[assignment: access control SFP(s), as stated in Table 12 and Table 13]** to restrict the ability [***selection: change_default, query, modify, delete, [assignment: enable, disable***] the security attributes **[assignment: TOE Mobile App]** to **[assignment: TOE User, TOE Developer]**.
Notes:	Note that, TOE Developer only has access to the TOE upon approval of the TOE User based on situation if the TOE mobile device require new updates, new upgrade, forensic study upon incident and troubleshooting the device via remote access.

6.2.27 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the **[assignment: access control SFP]** to provide ***[selection, choose one of: permissive]]*** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the **[assignment: TOE User, TOE Developer]** to specify alternative initial values to override the default values when an object or information is created.
Notes:	Note that, TOE Developer only has access to the TOE upon approval of the TOE User based on situation if the TOE mobile device require new updates, new upgrade, forensic study upon incident and troubleshooting the device via remote access.

6.2.28 FMT_SMF.1 Specification of management function

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[assignment: All administrative actions related to the TOE Mobile Apps, configuration of security function of the OS and configuration of security functions of the hardware]**.

Notes:	In addition, the TOE User or TOE Developer can enable the Android OS underlying operating system security capabilities and functionality as follows. i. Android Secure Boot Feature. ii. DM Verity. iii. Security Compatibility Test Suite (CTS) includes kernel address space layout randomization (KASLR).

6.2.29 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles **[assignment: TOE User, TOE Developer**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Notes:	Note that, TOE Developer only has access to the TOE upon approval of the TOE User based on situation if the TOE mobile device require new updates, new upgrade, forensic study upon incident and troubleshooting the device via remote access.

6.2.30 FPT_PHP.1 Passive detection of physical attack

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.1.2	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
Notes:	The TOE has the capability of providing a means to protect the TSF data by providing reliable forms of encapsulation materials protection, which is injected into the metal shielding chambers, in which protecting all the hardware components of the TOE device that supported by TOE Mobile Apps that monitors the status with triggering alerts.

6.2.31 FPT_PHP.3 Resistance to physical attack

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist **[assignment: protection casing being compromised or broken, hardware sensor**] to the **[assignment: physical protection casing, hardware consist of PCB motherboard, RAM, ROM and other hardware in the mobile device]** by responding automatically such that the SFRs are always enforced.
Notes:	The TOE has the capability of providing a means to protect the TSF data by providing reliable forms of encapsulation materials protection, which is injected into the metal shielding chambers, in which protecting all the hardware components of the TOE device that supported by TOE Mobile Apps that monitors the status with triggering alerts.

6.2.32 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Notes:	None.

6.2.33 FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests ***[selection: during initial start-up]*** to demonstrate the correct operation of ***[selection: the TSF].***
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of ***[selection: TSF data]***.

FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of ***[selection: TSF]***.
Notes:	In addition, the TOE User or TOE Developer can enable the Android OS underlying operating system security capabilities and functionality as follows. i. Android Secure Boot Feature. ii. DM Verity. iii. Security Compatibility Test Suite (CTS) includes kernel address space layout randomization (KASLR).

6.2.34 FTA_SSL.1 TSF-initiated session locking

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FTA_SSL.1.1	The TSF shall lock an interactive session after [**assignment: time interval configured by TOE User of inactivity**] by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session.
FTA_SSL.1.2	The TSF shall require the following events to occur prior to unlocking the session: [**assignment: successful authentication on the lock screen with identified correct TOE User credential**].
Notes:	This function can be trigger by the mechanism of smart-lock features of Android OS configuration. In addition, the usage of this mechanism are depends on the need of the TOE User(s) organisational security policies based on the usage and deployment environment.

6.2.35 FTA_SSL.3 TSF-initiated termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FTA_SSL.3.1	The TSF shall terminate an interactive session after a **[assignment: time interval configured by TOE User of inactivity]**.
Notes:	This function can be trigger by the mechanism of smart-lock features of Android OS configuration. In addition, the usage of this mechanism are depends on the need of the TOE User(s) organisational security policies based on the usage and deployment environment.

6.2.36 FTA_TAB.1 Default TOE access banners

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TAB.1.1	Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.
Notes:	None.

6.3 TOE Security assurance requirements

EAL2 requires evidence relating to the design information and test results but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description on the architecture of the TOE, to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to attackers with basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Table 14: SARs

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.4 Security requirements rationale

6.4.1 Dependency rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL2, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

Table 15: SFRs Justification

SFR	Dependency	Inclusion
FAU_ARP.1	FAU_SAA.1 Potential violation analysis	FAU_SAA.1
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAA.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.4	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2 FCS_COP.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1 FDP_ITC.1

SFR	Dependency	Inclusion
FCS_COP.1/ ENC_DEC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FDP_ITC.1 FCS_CKM.4
FCS_COP.1/ HASH	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FDP_ITC.1 FCS_CKM.4
FCS_COP.1/ SIGN	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FDP_ITC.1 FCS_CKM.4
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FDP_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FDP_SDI.1	No dependencies.	None.
FDP_SDI.2	No dependencies.	None.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2

SFR	Dependency	Inclusion
FIA_ATD.1	No dependencies.	None.
FIA_SOS.2	No dependencies.	None.
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2 (Hierarchical to FIA_UID.1)
FIA_UAU.4	No dependencies.	None.
FIA_UAU.6	No dependencies.	None.
FIA_UAU.7	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_UID.2	No dependencies.	None.
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No dependencies.	None.
FMT_SMR.1	FIA_UID.1 Timing of identification	None.
FPT_PHP.1	No dependencies.	None.
FPT_PHP.3	No dependencies.	None.
FPT_STM.1	No dependencies.	None.
FPT_TST.1	No dependencies.	None.

SFR	Dependency	Inclusion
FTA_SSL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2 (Hierarchical to FIA_UAU.1)
FTA_SSL.3	No dependencies.	None.
FTA_TAB.1	No dependencies.	None.

6.4.2 Mapping of SFRs to security objectives for the TOE

Table 16: SFRs Mapping to Security Objectives

Security objective	Mapped SFRs	Rationale
O.AUDIT	FAU_ARP.1	FAU_ARP.1 enforces that the detection of any security violation such as broken protection casing, device and/or battery heating up beyond threshold and malfunction of hardware shall trigger the TSF and recorded the alerts via audit trails for future investigation.
	FAU_GEN.1	FAU_GEN.1 enforces to generate reliable audit log trails recorded and stored securely in Android OS, managed by the TOE Mobile Apps without any means of tampering or modification.
	FAU_SAA.1	FAU_SAA.1 enforces to generate reliable audit log trails recorded and stored securely inside Android OS and managed by the TOE Mobile Apps without any means of tampering or modification, based on the triggered events such as device and/or battery heating up beyond threshold and malfunction of hardware.
	FAU_STG.1	FAU_STG.1 enforces the TOE capabilities to protected audit data loss within the TOE and securely managed inside the TOE devices.
	FAU_STG.4	FAU_STG.4 enforces the TOE capabilities to prevent audit data by overwriting the oldest data with new data in the event of the TOE storage are in full capacity within the TOE and securely managed inside the TOE devices.

Security objective	Mapped SFRs	Rationale
	FPT_STM.1	FPT_STM.1 enforces the TOE capabilities in providing reliable time stamps to support audit functionality.
O.MGMT	FDP_ACC.1	FDP_ACC.1 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it.
	FDP_ACF.1	FDP_ACF.1 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it.
	FDP_ITC.1	FDP_ITC.1 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it when being imported.
	FDP_SDI.1	FDP_SDI.1 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it through the mechanism of data integrity monitoring.
	FDP_SDI.2	FDP_SDI.2 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it through the mechanism of data integrity monitoring with action.
	FMT_MSA.1	FMT_MSA.1 enforces the actions made by the TOE User and TOE Developer are authenticated and identified using correct credentials, before allowing access to the TSF data managed by the TOE Mobile App.
	FMT_MSA.3	FMT_MSA.3 enforces the actions made by the TOE User and TOE Developer are authenticated and identified using correct credentials, before allowing access to the TSF data managed by the TOE Mobile App.
	FMT_SMF.1	FMT_SMF.1 enforces the actions made by the TOE User and TOE Developer are authenticated and identified using correct credentials, before allowing access to the TSF data managed by the TOE Mobile App.

Security objective	Mapped SFRs	Rationale
	FMT_SMR.1	FMT_SMR.1 enforces to identified and authenticated any actions performed on the TOE and TSF data by authorised TOE User and TOE Developer.
O.PHY_PROTECT	FAU_ARP.1	FAU_ARP.1 enforces that the detection of any security violation such as device and/or battery heating up beyond threshold and malfunction of hardware shall trigger the TSF and recorded the alerts via audit trails for future investigation.
	FPT_PHP.1	FPT_PHP.1 enforces that the detection of any physical tampering are being detected, alerts and recorded by the TOE Mobile App. Whilst, the TSF data generated by the TOE Mobile App send back to the Developer Web Application Management System for record purposes.
	FPT_PHP.3	FPT_PHP.3 enforces that the detection of any physical tampering are being detected, alerts and recorded by the TOE Mobile App. Whilst, the TSF data generated by the TOE Mobile App send back to the TOE Developer for record purposes.
	FPT_TST.1	FPT_TST.1 enforces self-testing on the sensors and operations of the TSF as in the whole start-up/boot up sequence of the smartphone to check for any issues related to physical protection and battery status.
O.THML_PROTECT	FAU_ARP.1	FAU_ARP.1 enforces that the detection of any security violation such as device and/or battery heating up beyond threshold and malfunction of hardware shall trigger the TSF and recorded the alerts via audit trails for future investigation.
	FPT_PHP.1	FPT_PHP.1 enforces that the detection of any thermal issues on the device and/or battery are being detected, alerts and recorded by the TOE Mobile App. Whilst, the TSF data generated by the TOE Mobile App send back to the Developer Web Application Management System for record purposes.

Security objective	Mapped SFRs	Rationale
	FPT_PHP.3	FPT_PHP.3 enforces that the detection of any thermal issues on the device are being detected, alerts and recorded by the TOE Mobile Apps. Whilst, the TSF data generated by the TOE send back to the TOE Developer for record purposes.
	FPT_TST.1	FPT_TST.1 enforces self-testing on all the hardware components and Android OS operations of the TSF as in the whole start-up/boot up sequence of the smartphone to check for any issues.
	FMT_MSA.3	FMT_MSA.3 enforces the actions made by the TOE Developer are authenticated and identified using correct credential (such as: PIN code login screen, Pattern, Password Based, Biometric fingerprint login screen), before allowing access to the TSF data managed by the TOE Mobile App.
	FMT_SMF.1	FMT_SMF.1 enforces the actions to the management functions made by the TOE Developer are authenticated and identified using correct credential (such as: PIN code login screen, Pattern, Password Based, Biometric fingerprint login screen), before allowing access to the TSF data managed by the TOE Mobile App.
	FMT_SMR.1	FMT_SMR.1 enforces to identified and authenticated any actions performed on the TOE and TSF data by authorised TOE User and TOE Developer.
O.MANAGE	FMT_MOF.1	FMT_MOF.1 enforces the actions made by the TOE Developer are authenticated and identified using correct credential (such as: PIN code login screen, Pattern, Password Based, Biometric fingerprint login screen), before allowing access to the TSF data managed by the TOE Mobile App.
	FMT_MSA.1	FMT_MSA.1 enforces the actions made by the TOE User and TOE Developer are authenticated and identified using correct credentials, before allowing access to the TSF data managed by the TOE Mobile App.

Security objective	Mapped SFRs	Rationale
	FMT_MSA.3	FMT_MSA.3 enforces the actions made by the TOE User and TOE Developer are authenticated and identified using correct credentials, before allowing access to the TSF data managed by the TOE Mobile App.
	FMT_SMF.1	FMT_SMF.1 enforces the actions made by the TOE User and TOE Developer are authenticated and identified using correct credentials, before allowing access to the TSF data managed by the TOE Mobile App.
	FMT_SMR.1	FMT_SMR.1 enforces to identified and authenticated any actions performed on the TOE and TSF data by authorised TOE User and TOE Developer.
	FTA_SSL.1	FTA_SSL.1 enforces to identified and authenticated any actions performed on the TOE and TSF data by authorised TOE User and TOE Developer through session security management (locking, termination and access).
	FTA_SSL.3	FTA_SSL.3 enforces to identified and authenticated any actions performed on the TOE and TSF data by authorised TOE User and TOE Developer through session security management (locking, termination and access).
	FTA_TAB.1	FTA_TAB.1 enforces to identified and authenticated any actions performed on the TOE and TSF data by authorised TOE User and TOE Developer through session security management (locking, termination and access).
O.STORE	FDP_ACC.1	FDP_ACC.1 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it.
	FDP_ACF.1	FDP_ACF.1 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it.
	FDP_ITC.1	FDP_ITC.1 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it when being imported.

Security objective	Mapped SFRs	Rationale
	FDP_SDI.1	FDP_SDI.1 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it through the mechanism of data integrity monitoring.
	FDP_SDI.2	FDP_SDI.2 enforces to ensure all TSF operations are bounded to the protection of TSF data from any means of attempt of compromising it through the mechanism of data integrity monitoring with action.
	FIA_AFL.1	FIA_AFL.1 enforces to ensure all TSF operations and TSF data are secure access, stored and managed, all actions shall be authenticated and identified with the correct TOE User credential.
	FIA_ATD.1	FIA_ATD.1 enforces to ensure all TSF operations and TSF data are secure access, stored and managed, all actions shall be authenticated and identified with the correct TOE User credential.
	FIA_SOS.2	FIA_SOS.2 enforces to ensure all TSF operations and TSF data are secure access, stored and managed, all actions shall be authenticated and identified with the correct TOE User credential with enforcement of secure secret access configuration.
	FIA_UAU.2	FIA_UAU.2 enforces to ensure all TSF operations and TSF data are secure access, stored and managed, all actions shall be authenticated and identified with the correct TOE User credential.
	FIA_UAU.4	FIA_UAU.4 enforces to ensure all TSF operations and TSF data are secure access, stored and managed, all actions shall be authenticated and identified with the correct TOE User credential.
	FIA_UAU.6	FIA_UAU.6 enforces to ensure all TSF operations and TSF data are secure access, stored and managed, all actions shall be authenticated and identified with the correct TOE User credential if require re-authenticating.

Security objective	Mapped SFRs	Rationale
	FIA_UAU.7	FIA_UAU.4 enforces to ensure all TSF operations and TSF data are secure access, stored and managed, all actions shall be authenticated and identified with the correct TOE User credential.
	FIA_UID.2	FIA_UAU.4 enforces to ensure all TSF operations and TSF data are secure access, stored and managed, all actions shall be authenticated and identified with the correct TOE User credential.
O.INTEGRITY	FCS_CKM.1	FCS_CKM.1 enforces to ensure all TSF operations and TSF data with cryptographic processes enabled within the operations of the TOE through implementation cryptography algorithms.
	FCS_CKM.4	FCS_CKM.4 enforces to ensure all TSF operations and TSF data with cryptographic processes enabled within the operations of the TOE through implementation cryptography algorithms.
	FCS_COP.1/ENC_DEC	FCS_COP.1/ENC_DEC enforces to ensure all TSF operations and TSF data with cryptographic processes enabled within the operations of the TOE through implementation cryptography algorithms. Furthermore, this SFRs are meant to protect data in the TOE through the process of cryptographic functions upon unlocked and locked of the TOE on login page screen.

Security objective	Mapped SFRs	Rationale
	FCS_COP.1/HASH	FCS_COP.1/HASH enforces to ensure all TSF operations and TSF data with cryptographic processes enabled within the operations of the TOE through implementation cryptography algorithms. The hash selection must support any operations for security validation or security checks such as during the TOE self-test. This is to ensure relevant data and configuration in the TOE operations are being hashed to ensure data integrity preventing from any possible modification. Example, the mobile device evaluated configuration need to be hashed and being checked during TOE mobile device boot up via self-test in preventing the configuration being modified.
	FCS_COP.1/SIGN	FCS_COP.1/SIGN enforces to ensure all TSF operations and TSF data with cryptographic processes enabled within the operations of the TOE through implementation cryptography algorithms. Furthermore, this SFRs are meant to protect data in the TOE through the process of cryptographic functions upon unlocked and locked of the TOE on login page screen. All the stated key distribution schemes used for the selected cryptographic protocols and any operations of cryptographic processes requires cipher suites that use RSA-based key establishment schemes. This is to ensure relevant data and configuration in the TOE operations are being signed digitally to ensure data integrity preventing from any possible modification. Example, the mobile device evaluated configuration need to be sign digitally and being checked during TOE mobile device boot up via self-test in preventing the configuration being modified.
	FPT_TST.1	FPT_TST.1 enforces self-testing on all the hardware components and Android OS operations of the TSF as in the whole start-up/boot up sequence of the smartphone to check for any issues.

6.4.3 Explanation for selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2).

The TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

7 TOE SUMMARY SPECIFICATION

7.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE actually implements the claimed security functional requirements.

The TOE security functions include the following:

i. Security Audit;

ii. Cryptographic Function;

iii. User Data Protection;

iv. Identification and Authentication;

v. Security Management;

vi. Physical Tampering and Fault Tolerance; and

vii. TOE Access.

7.2 Security Audit

The TOE provides the capability to enforce audit log trails collection, stored and maintained on the smartphone to collect, stored and maintained data collected by thermal sensors, hardware components, Android OS configurations, hardware configuration and relevant operations linked to the TSF.

In the aspects of smart battery operations, the sensors are collecting data from variety of aspects, to ensure the smartphone operates securely and operation able on a good conditions in the area that are hazardous condition, heavy duty and dangerous environment.

Furthermore, the underlying operating system which is Android OS also generating relevant audit event logs in specific to security events that are related to TOE configuration that triggers the TSF. Added to that, the hardware components that linked to the operations of TSF also generating relevant audit event logs that crucial to the operations of the TOE related TSF.

These audit logs are securely stored and maintained within the TOE device so that they can be accessed by TOE Developer and/or exported to an EMM system.

All these audit event logs are being processed by the Android OS through the management of TOE Mobile Apps pre-installed by TOE Developer in the device. Plus, there are several modules in the TOE that supporting the audit functions which are: Android SELinux, Android Secure Boot and DM Verify.

Furthermore, the TOE are remotely access by the TOE Developer via TOE Developer MDM Web App server that have access to audit logs that allow TOE Developer to retrieve relevant audit logs from the TOE operations, in assisting TOE User understanding their mobile device operations in the aspects of possible damage, sensor activities and others relevant operations.

Security Functional Requirements: FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FAU_STG.1, FAU_STG.4, FDP_ACC.1, FDP, ACF.1, FDP_ITC.1, FDP_SDI.1, FDP_SDI.2, FPT_STM.1 and FCS_CKM.4.

7.3 Cryptographic Function

The TOE has the capabilities to perform cryptographic functionality and processing capabilities in protecting the data reside inside the TOE in specific of data, files and library related to the configuration of the TOE Mobile Apps, Android OS and Hardware components. Cryptographic processes such as hashing, signing, encrypt and decrypt that are operations under Android OS in which being trigger upon the successfully identified and authenticated TOE User.

The objective of this function are mainly to protect the data, files and library based on the configuration reside under the management of TOE through the secure operations of Android OS. These operations under Android OS through secure configuration applied by the TOE Developer on the TOE device are to secure data stored inside the TOE device and processes securely without any potential unauthorised modification or tampering or data theft.

In addition, further explanation on the Android OS secure configuration that support the operations of the cryptographic functions as follows.

i. Cryptographic on Software Level: Android verified boot2.0 Cryptographic authentication of high-level operating system (HLOS) images.
ii. Cryptographic on Hardware Core: AES, SHA and ECDSA cryptographic algorithms implemented in device hardware.
iii. Crypto Engine: Hardware engine for encrypting and decrypting storage devices.
iv. Fuse Memory: One-time programmable QFPROM fuse memory and automatic programming via sec-partition.
v. Management Master Key: Hardware-backed (KeyStore services supporting public and private key generation, management, signing, and verification.
vi. Android OS Crypto Function: Verified Boot is Google's defined mechanism for the Android boot loader to verify the integrity of Android boot and recovery images before bootup. ASN1Dxe – Contains the implementation of routines required to parse ASN1 X509 data, such as Android Verified Boot Signature and Certificate.

Furthermore, the usage of the cryptographic algorithms and key sizes are depends on the need of the TOE User(s) organisational security policies based on the usage and deployment environment. The possible use of deprecated algorithms are not recommended but depends on the risk assessment and risk appetite of the TOE User(s) organisation requirements.

In the aspects of communication between TOE and TOE Developer Mobile Device Management (MDM) system, it uses the cryptographic key distribution methods in which PKI system that operates by the MDM system through TOE Developer MDM Web App server via VPN secure communications.

The TOE Developer MDM Web App server enable TOE Developer to remotely access audit logs from the TOE to retrieve crucial info about the device in assisting TOE User to operate the TOE securely within its operations. Note that, the TOE Developer MDM Web App server is not part of TOE scope of evaluation.

Security Functional Requirements: FCS_CKM.1, FCS_CKM.4, FCS_COP.1/ENC_DEC, FCS_COP.1/HASH and FCS_COP.1/SIGN.

7.4 User Data Protection

In support of TOE Mobile Apps (which are: eDIAGNOSTICS, eIS, eLOGKIT, ecomManagerService and eXTEND), Android OS and Hardware components, in which these data collected, stored and managed through the underlying Android OS shall be protected from changes of modification, data deletion and data modification stored inside the device, whilst maintaining the integrity of the TOE.

Thus, mechanism of protection are being in place to ensure these data are protected inside the smartphone under management of TOE Mobile Apps, Android OS and Hardware component processing.

The following are additional information related to capabilities of security protection on data storage in Android OS, as follows.

i. Android User Data Encryption.

ii. File based encryption (FBE).

iii. Metadata Encryption.

iv. New FBE - Android R.

With the pre-installed mobile apps in which developed by the TOE Developer, known in this document as TOE Mobile Apps, make use of the implemented sensors that relates to the performance data generated by the Android OS , underlying hardware that shall be requested by the TOE User or TOE Developer. With that, the access to these data are being controlled by the TOE User and TOE Developer. The functions of the TOE Mobile Apps as defined below.

i. eDIAGNOSTICS: Allows TOE user to check the device and platform functions accordingly and to collect information of the TOE mobile device. Data accessible and functional checks are available for e.g., but not limited to: battery hardware sensors (device temperature and battery health), accelerometer, gyroscope, compass, proximity, microphone, camera, GPS, content of the TOE (e.g., pictures, test messages, emails and documents), device identifier and adapters (wireless, mobile, Bluetooth and NFC). The diagnostics data collected can be sent by the user to customer support or to developer support. No remote access is possible by the TOE Developer.

ii. eIS: eIS is a redundant layer of SW based protection on top of a design inherent temperature monitoring and cut-off mechanism. The hardware based thermal monitoring is designed into monitor various energy islands of the device to ensure thermal explosion protection. The tripping points of this hardware mechanism can't be changed by software.

    eIS is able to capture and pull thermal data from various explosion protection sensor zones and notify the same to the framework/application layer to show a notification when it approaches a particular threshold value. An early notification can be presented to the users when temperature is rising for a particular explosion protection zone. This enables users to take an appropriate action ahead of time.

iii. ecomManagerService: provides set of additional APIs as mentioned in Appendix A to configure and manage the device either via an EMM system or privileged apps on the device. The privileged apps are the ones that have the public key of certificate used to sign the application included in the knownCerts of ecomManagerService. KnownCerts in Android system is a list containing the signing certificate digests to be granted this permission when using the knownSigner protection flag and in this case ecomManagerService. This is to ensure the TOE integrity in protecting from any possible modifications related to the evaluated configuration of TOE Mobile Apps, evaluated configuration of Android OS and evaluated configuration of Hardware.

iv. eXTEND: eXTEND is the user-experience enhancement application that provides access to TOE user to configure ECOM defined extensions in forms of additional features above and beyond Android OS available on the device. This application is integrated with the Settings App and does not have a dedicated front end. Furthermore, there are logs generated by eXTEND when any platform signed app that is considered risky is installed by TOE User.

v. eLOGKIT: eLOGKIT is a passcode protected hidden application. The application allows the TOE User to capture and pull of relevant software event logs and to send these logs to TOE Developer support.

The TOE facilitates device configurations managed by user through the EMM in segregating the data between professional and personal usage. It leverages the Android OS standard multi-user setup to accommodate multiple users, each corresponding to a natural person. Users are linked to an account and may have multiple profiles, all tied to a parent profile. This profile structure ensures the segregation of user data, even as users share system resources and global settings such as wireless configurations. TOE mobile applications and system applications adhere to the Android standard "Application Sandboxing" concept, enhancing data security and protection. Additionally, TOE offers display time-out functions that require activation by the TOE User.

Each function of TOE Mobile Apps protects the data collected within secure manner.

Security Functional Requirement: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FDP_SDI.1, FDP_SDI.2, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7 and FIA_UID.2.

7.5 Identification and Authentication

In any processes of operations performed within the TOE and in device, the operations shall be first identified and authenticated by the TOE User with correct credential through validation of PIN Code, Pattern, Password or biometric security verification (fingerprint). TOE User required to be successfully identified and authenticated by the TOE and then able to access main security functions available in the devices which are also access to the TOE Mobile Apps, Android OS functions and Hardware components.

Furthermore, TOE Developer also shall require to be successfully identified and authenticated before having access to all the TSF capabilities. This shall be trigger based on the requirement set by TOE user via Android Password Requirements.

In the event of the screen lock due to session timeout (in the event of obscured feedback on the TOE mobile device display), exiting any TOE Mobile Apps (that required identification and authentication), or exiting any configuration function of the TOE, TOE User is required to re-login using correct credentials through validation of PIN Code, Pattern, Password or biometric security verification (fingerprint).

Plus, it is possible the TOE User and TOE Developer to enable Android Password Requirements.

Security Functional Requirement: FIA_AFL.1, FIA_ATD.1, FIA_SOS.2, FIA_UAU.2, FIA_UAU.4, FIA_UAU.6, FIA_UAU.7 and FIA_UID.2.

7.6 Security Management

The TOE in the smartphone is equipped with security management functions that capture, manage, operates, monitors, record and track all relevant hardware, sensors, OS operations and TOE Mobile Apps in the smartphone to ensure all main security components are operate in a good condition as defined by the configuration made by TOE developer.

These security management functions are performed and enforced by the TOE and TOE Mobile Apps (which are: eIS, eLOGKIT, eDIAGNOSTICS, eXTEND and ecomManagerService) operate inside the smartphone that continuously collect data and logs in the device. Further information can be refer to Section 7.4 (User Data Protection) regarding the operations of eIS, eLOGKIT, eDIAGNOSTICS, eXTEND and ecomManagerService that clearly defined the management of security attributes and static attribute initialisation, as in defined also on Table 12 and Table 13.

As such the following scenarios of operations as stated below.

i. eIS capture and pull data from thermal sensors.
ii. eLOGKIT capture and pull relevant software event logs.
iii. eDIAGNOSTICS to check the device and platform functions accordingly.
iv. eXTEND is a front end-users to configure ECOM defined extensions.

v. ecomManagerService is to provide additional APIs to configure and manage the device.

In addition, the data can be shared upon TOE User authorization via email, file sharing and manual data transfer using cable to TOE Developer Support team for data processing, data analysis and data analytics.

Access to the smart battery functions, underlying configuration of Android OS and hardware components configuration required TOE User and TOE Developer first to be successfully identified and authenticated using legitimate credentials.

In addition, the TOE User or TOE Developer can enable the Android OS underlying operating system security capabilities and functionality as follows.

i. Android Secure Boot Feature.

ii. DM Verity.

iii. Security Compatibility Test Suite (CTS) includes kernel address space layout randomization (KASLR).

Security Functional Requirements: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FIA_UAU.2 and FIA_UID.2.

7.7 Physical Tampering and Fault Tolerance

The TOE operates through the monitoring, alerts and prevention capabilities via TOE Mobile Apps (which are: eIS, eDIAGNOSTICS, and eLOGKIT) are to track, monitors and record data generated by the relevant sensors equipped inside the smartphones. These sensors are temperature sensors across the main board, smart battery functions, Android OS and hardware components, in which generated all data that are collected based on the usage, behaviours and conditions react by the TOE User and environment around the smartphone towards the smartphone during usage.

These sensors are specific being developed to track, monitors and record data being generated through the usage of the smartphone by the TOE User that being collected by TOE Mobile App. The following are the data collected by the sensors send to the TOE Mobile Apps, as stated below.

i. Thermal Sensors:

   a. Detect device temperature exceeds the threshold (temperature acceptance (Ta) range accepted: -20 °C ≤ Ta ≤ +60 °C)).

   b. Detect unauthorized battery being used in the device.

   c. Detect battery temperature exceeds the threshold.

ii. Hardware Sensors:

   a. Check hardware status and health.

b. Detect malfunction on certain part of hardware inside the smartphone such as Speaker, Display, RAM, ROM and other hardware in the mobile device.

Furthermore, these physical casing and hardware sensors mechanism are being designed and implemented in the TOE as part of the smartphone security functionality to ensure the components inside the smartphone are being protected by the rigged design of TOE casing supported with reinforced frames, strengthened glass, and shock-absorbing materials, making the smartphone highly resistant to physical shocks, falls, or rough handling. In the event of physical tampering, the TOE hardware sensor or battery sensor will be triggered and alert the TOE User.

Thus, if the TOE mobile device are not safe to be use, TOE User will be alert and prevented to start the device (if auto turn off) or login to the TOE mobile device, preventing any further issues related to safety of the TOE User. Self-test of the TOE mobile device will check the TOE condition during start-up of the TOE.

Plus, as for the thermal sensors the TOE is built to ensure the temperature of both battery and hardware are good condition physically, feasible temperature of operations and well performed through all the operations and usage of the TOE.

As depicted in above, the thermal protection of the device consists of two layers of protection. Temperature thresholds are monitored by device hardware (hardware coded, thus can't be influenced by software) and will make sure the device is not functional anymore if these thresholds are exceeded. The software base protection (eIS) monitors the temperature behaviour, alerts the user and/or generates audit trails if temperature thresholds are crossed and/or if tampering is suspected. In the event the battery is not feasible to be used or operated, TOE User is prevented from using the TOE mobile device and device will turn off automatically. Note that the temperature threshold: temperature acceptance (Ta) range accepted: -20 °C ≤ Ta ≤ +60 °C.

Note that, the device may turn off or automatically fail to operate below the acceptable threshold such as example: the device turn off or broken around 30 °C or the device may not response to any input when it state temperature around below -10 °C. This is because the wear and tear component(s) in the device are not able to cope with the harsh operations due to its daily use and these electronic components are deprecated through its lifetime usage.

Thus, Android OS are main components that operates the communication data between hardware components such as sensors, with the TOE Mobile Apps. By apply secure evaluated configurations of all parts from the TOE Mobile Apps, TOE Android OS and TOE Hardware components, allowing the possible of secure operations of the TOE. By enabling self-test during the initial start-up and boot-up to check the integrity of the TOE in ensuring the physical and logical of the TOE mobile device are operate accordingly and securely without any integrity issues.

Furthermore, the TOE as a mobile device are also protected from possible access via the Diagnostic Mode via Diagnostic Port in preventing the attempt of accessing by unauthorised personnel with intention of possible threats or attacks. In additional, the Bootloader Mode and OEM locking are also implemented with the same objective as prevention from possible threats and attacks.

Security Functional Requirements: FPT_PHP.1, FPT_PHP.3 and FPT_TST.1.

7.8 TOE Access

By being the TSF that support other TSFs operations, this TSF has the capabilities of performing security operation in limiting the access to the TOE by enforcing access control on the TOE for TOE User and TOE Developer. This is to prevent any potential threats accessing the TOE TSFs without proper security credentials and proper identification and authentication.

Based on the time interval set by TOE User on the inactivity, if being met, the TOE mobile device will enforced locked screen mechanism and required correct credential to login back to the TOE. If the credential provided is wrong, the TOE mobile device will triggered advisory warning and prevent from accessing the TOE.

Security Functional Requirement: FTA_SSL.1, FTA_SSL.3 and FTA_TAB.1.

8 APPENDIX A

The following are the table elaborate the API ECOM SDK as for reference.

Table 17: API ECOM SDK List

ECOM SDK API	Platform signed Apps	Apps with known Certs*
getNTPServerDetails	Y	N
assignKeysToApps	Y	N
configureInternetBrowser	Y	N
enableRecoveryMode	Y	N
disableRecoveryMode	Y	N
enableScreenLockSettings	Y	N
disableScreenLockSettings	Y	N
setNFCAlwaysOn	Y	N
setNFCAlwaysOff	Y	N
getNFCState	Y	N
setNetworkModeAlwaysOn	Y	N
getNetworkMode	Y	N
setDoNotDisturbIPCallAlwaysOn	Y	Y
getDoNotDisturbIPCall	Y	Y
setMobileDataSettingsAlwaysOn	Y	N
setMobileDataSettingsAlwaysOff	Y	N
getMobileDataSettings	Y	N

enableWifiPassPoint	Y	N
disableWifiPassPoint	Y	N
enableHardwareKeys	Y	N
disableHardwareKeys	Y	N
enableOTAUpdates	Y	N
disableOTAUpdates	Y	N
enableAdministratorMenu	Y	N
disableAdministratorMenu	Y	N
blockOpenWifiSSIDs	Y	N
lockHardwareKeys	Y	N
unlockHardwareKeys	Y	N
enablePocketMode	Y	N
disablePocketMode	Y	N
enableTorch	Y	N
disableTorch	Y	N
enableNotificationLED	Y	N
disableNotificationLED	Y	N
setNoiseCancellationMode	Y	N
enableSoftKeypad *	Y	N
disableSoftKeypad *	Y	N

disableTurnOffWorkMode	Y	N
lockAllHardwareKeys	Y	N
unlockAllHardwareKeys	Y	N
setNTPServer	Y	N
setAutoAcceptRejectIncomingCalls	Y	Y
isOTAUpdateDisabled	Y	N
configureLTEDrx	Y	Y
getLTEDrx	Y	Y
isTorchOn	Y	Y
toggleTorchInNonCameraMode	Y	Y
setBlockUninstall	Y	N
setOneTouchPttEnabled	Y	N
isOneTouchPttEnabled	Y	Y
getImei*	Y	Y
getDeviceSerialNumber*	Y	Y
getProgrammableKeyInfo*	Y	Y
setProgrammableKeyEnabled	Y	N
isProgrammableKeyEnabled	Y	N
swapPttCameraKey	Y	N
isPttCameraKeySwapped	Y	N

setDoubleTapLockEnabled	Y	N
isDoubleTapLockEnabled	Y	N
setAccessoryNotificationEnabled	Y	N
isAccessoryNotificationEnabled	Y	N
setSmartCallHandlingEnabled	Y	N
isSmartCallHandlingEnabled	Y	N
setLogCapturingEnabled	Y	N
isLogCapturingEnabled	Y	N
setAutoDataSwitchEnabled	Y	N
isAutoDataSwitchEnabled	Y	N
enableRRO	Y	N
setWifiCallingEnabled	Y	N
isWifiCallingEnabled	Y	N
setPsimEnabled	Y	N
isPsimEnabled	Y	Y
setEsimEnabled	Y	N
isEsimEnabled	Y	Y
allowOnRestrictedNetworks	Y	Y
showBluetoothDevicesWithoutNames	Y	N
setGloveMode	Y	N

getGloveMode	Y	N
getTouchMode	Y	N
setUsbMode	Y	N
getUsbMode	Y	N