17 March 2021

Document Version 1.0

HUAWEI APPGALLERY SECURITY TARGET

HUAWEI

Document management

Document identification

Document title	Huawei AppGallery Security Target
Document date	17 March 2021
Prepared by	Securelytics
Release Authority	Huawei
Product version	10.4.0.301

Document history

Version	Date	Description
0.1	10 June 2020	Initial Released.
0.2	13 June 2020	Content Updated.
0.3	15 June 2020	Content Updated based on Evaluation Test Lab feedback.
0.4	7 July 2020	Content Updated based on Evaluation Test Lab feedback.
0.4.1	10 July 2020	Minor content Updated based on Evaluation Test Lab feedback.
0.5	23 July 2020	Update based on EOR.
0.6	13 Aug 2020	Update based on EOR.
0.7	28 Aug 2020	Update based on EOR.
0.8	4 Sept 2020	Update based on EOR.
0.9	5 Nov 2020	Content Updated.
0.10	19 Nov 2020	Update based on EOR.
0.11	30 Nov 2020	Content Updated.
0.12	10 Feb 2021	Update identification and Authentication operation.
0.13	24 Feb 2021	Content Updated.

Version	Date	Description
0.14	8 Mar 2021	Content Updated
1.0	17 Mar 2021	Final.

Table of Contents

1 Security Target Introduction 1

1.1 ST Reference 1

1.2 TOE Reference 1

1.3 Document Organization 1

1.4 TOE overview 2

1.4.1 TOE usage and major security functions 2

1.4.2 TOE Type 3

1.4.3 Supporting Hardware, software and/or firmware 4

1.4.4 Excluded from the TOE 4

1.5 TOE description 5

1.5.1 Physical scope of the TOE 5

1.5.2 Logical scope of the TOE 6

2 Conformance Claim 8

3 Security objectives 9

3.1 Overview 9

3.2 Security objectives for the Environment 9

4 Security requirements 10

4.1 Overview 10

4.2 Security Functional Requirements (SFR) 11

4.2.1 User attribute definition (FIA_ATD.1) 11

4.2.2 User authentication before any action (FIA_UAU.2) 11

4.2.3 User identification before any action (FIA_UID.2) 11

4.2.4 Management of security attributes (FMT_MSA.1) 11

4.2.5 Static attribute initialisation (FMT_MSA.3) 12

4.2.6 Specification of Management Functions (FMT_SMF.1) 12

4.2.7 Security roles (FMT_SMR.1) 13

4.2.8 Security attribute based access control (FDP_ACF.1) 13

4.2.9 Complete access control (FDP_ACC.1) 14

4.2.10 User-initiated termination (FTA_SSL.4) 15

4.2.11 Inter-TSF trusted channel (FTP_ITC.1) 15

5 TOE Security Assurance Requirements 16

6 TOE Summary Specification 17

6.1.1 Overview 17

6.1.2 Mapping of TOE Logical Scope towards the SFRs 17

1 Security Target Introduction

1.1 ST Reference

Table 1: Security Target (ST) Reference

ST TITLE	Huawei AppGallery Security Target
ST VERSION	1.0
ST DATE	17 March 2021

1.2 TOE Reference

Table 2: Target of Evaluation (TOE) Reference

TOE TITLE	Huawei AppGallery
TOE VERSION	10.4.0.301

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 defines the security objectives for the TOE and the operational environment (ASE_OBJ.1).
- Section 4 contains the security functional and assurance requirements derived from the Common Criteria Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.1).
- Section 5 contains the security assurance requirements derived from the Common Criteria, Part 3 (ASE_REQ.1).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 TOE overview

1.4.1 TOE usage and major security functions

The Target of Evaluation (TOE) is Huawei AppGallery version 10.4.0.301. The TOE is a mobile application that equipped with the capability as mobile applications distribution platform, as official app of Huawei. The TOE also known as Huawei AppGallery features with assurance of providing secure platform for user to purchase, download, install, view list (sort/search), monitor, update and remove all registered 3rd party mobile applications. The TOE user able to use the TOE for other functions such as receiving reward, managing gift (claim and redeem), writing comment/remark on 3rd party mobile application page, perform pre-orders and managing wish list.

The Huawei AppGallery as the TOE is designed specifically for Huawei mobile devices and Huawei mobile operating system to allow user experience of purchase, download, install, view list (sort/search), monitor, update and remove all type of registered 3rd party mobile applications, reward, gift and remark, pre-orders, wish list and comment notification in Huawei mobile devices platform.

The following is the list of key features of the TOE, as stated below:

i. TOE have access to catalogue of carefully selected android apps;

ii. Enable security with quad-layer security mechanism that includes Huawei's unique security manual verification check and validation;

iii. User reward and benefits upon usage of the Huawei AppGallery as mobile application manager platform;

iv. Smart search feature for user experience in exploring all types of mobile application varieties registered with Huawei, developed by authorised app developer by Huawei;

v. Auto-update applications for all mobile application under management of Huawei AppGallery via Wi-Fi for optimise mobile application updates; and

vi. User experience in application discovery upon different region stores with local varieties of mobile application for selection.

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

Table 3: TOE Security Features

SECURITY FEATURE	DESCRIPTION
Identification and Authentication	User of Huawei mobile devices requires to perform successful identification and authentication with the TOE before any information flows are permitted. In this process, TOE user is requiring to be authentication to allow any actions made in the TOE operations.
Security Management	The TOE provides security management functions that allow the TOE user to manage the TOE, 3rd party mobile applications and TOE security functions.

SECURITY FEATURE	DESCRIPTION
Secure Communication	The TOE is able to protect the user data from disclosure and modification using a secure communication between TOE as mobile application and TOE server managed by TOE developer. In the event of the TOE are close or exit or send to background process performed by the TOE user, the communication between TOE and TOE server will be terminated.

1.4.2 TOE Type

The TOE type is a mobile application that provides TOE users access to all registered 3rd party mobile applications as application distribution platform with all relevant security features as per mentioned in the TOE logical scope.

1.4.3 Supporting Hardware, software and/or firmware

The underlying hardware and software that is used to support the TOE are as follows. These two models and specifications of Huawei mobile devices are been used as TOE underlying operating platform and shall be consider not part of TOE scope.

Table 4: Non-TOE Hardware and Software Specification

NON-TOE HARDWARE AND SOFTWARE SPECIFICATION		
Huawei Android operating system (EMUI)	EMUI 9.1 (Based on Android 9)	EMUI 9.1.1 (Based on Android 9)
Processor	HUAWEI Kirin 710F	Hisilicon Kirin 710
Memory	RAM: 4GB Internal Memory: 64GB	RAM: 4GB Internal Memory: 128GB

The TOE also able to operate within the following list of underlaying operating system as per mentioned below. The listed below is the minimum requirements for AppGallery. However, it is not part of the TOE configuration evaluated for the certification.

i. Huawei Android operating system (EMUI) versions: 3.1, 4.0, 4.1, 5.0 and 8.1.

ii. Android OS versions: 5.0, 6.0, 7.0 and 8.1.

1.4.4 Excluded from the TOE

The only security functionality addressed by the evaluation is the functionality specified by the security functional requirements, and does not include additional platforms or specifications as stated below, such as:

i. Huawei mobile devices inclusive of its hardware and physical characteristics;

ii. All pre-install application comes with the Huawei mobile devices upon purchasing of the device or first starting up of the Huawei mobile devices;

iii. All installed 3rd party mobile applications performed by TOE user in the Huawei mobile devices inclusive of any 3rd party APK files and/or comes from Huawei AppGallery;

iv. TOE back-end server managed by the TOE developer (Huawei) that hosted all the 3rd party mobile applications for TOE as application distribution platform; and

v. Type of network connectivity used by the TOE such as Wi-Fi and mobile data network.

1.5 TOE description

1.5.1 Physical scope of the TOE

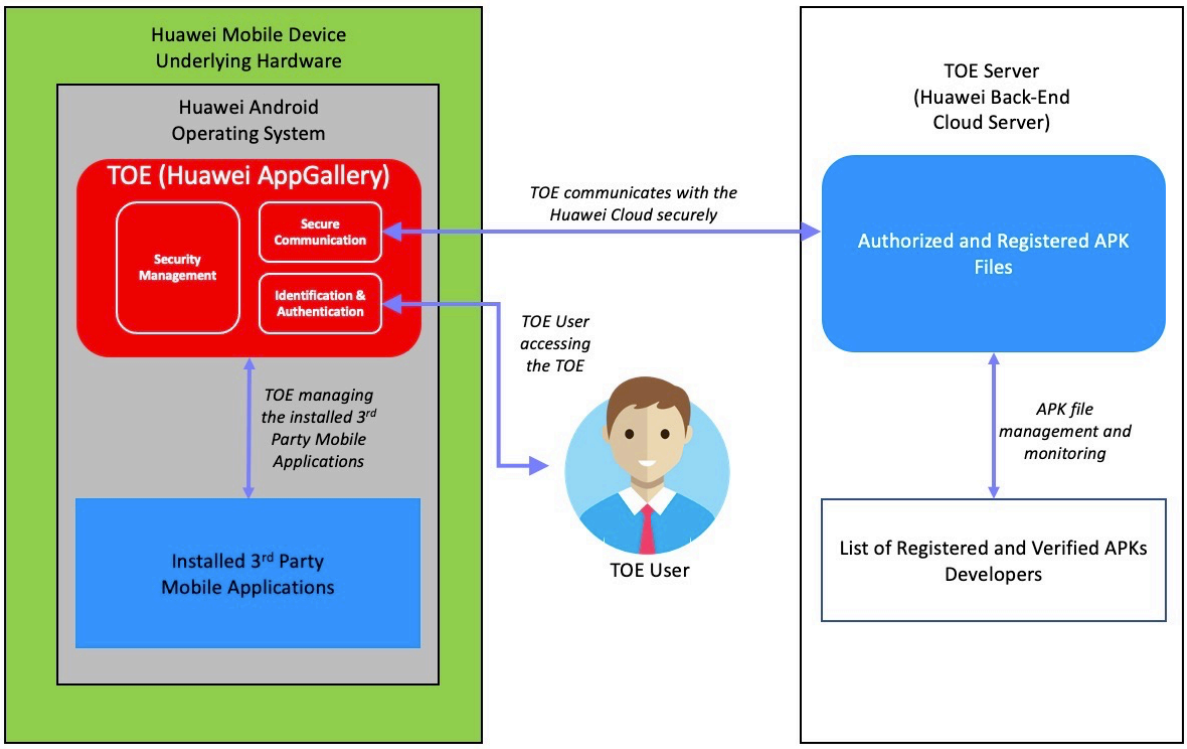

Figure 1: TOE Physical Scope

Note that, the RED box is the scope evaluation of the TOE.

The TOE is a mobile application that played role as applications distribution platform for other mobile application APK file to initiate TOE functions as stated below:

a. Purchase, download, and install the paid 3rd party mobile application(s);

b. Monitor and update the 3rd party mobile application(s) has been notified by the TOE upon update available;

c. Remove selected 3rd party mobile application(s) selected by TOE user

d. Receiving rewards;

e. Managing gifts (claim and redeem);

f. Writing comment/remark; and

g. Perform pre-orders.

These TOE functions are secure operates within Huawei mobile device Android operating system. Note that, third party components listed in Section 1.4.3 and Section 1.4.4 are not part of the TOE as scope of evaluation.

Aside of operate as applications distribution platform in the Huawei mobile device Android operating system, the TOE communicates with the TOE server to perform the following TOE functions as listed

above. Whilst, to ensure its secure operating environment are enforce through continuous usage by the TOE user and ensuring the 3rd party mobile applications are up to date via constant updates. The Huawei back-end cloud server (also known as TOE server) is not part of the TOE. TOE user able to perform TOE management functions based on the listed TOE functions listed above.

Before the TOE is operates as application distribution platform manager, TOE required to be identified and authenticated before any relevant actions are allowed by the TOE to be performed by TOE user on the TOE.

Between TOE and TOE server are communicates using secure communication protocols. The secure communication channel is secured by using international standards or industry-recognized security protocols that supports the following secure protocols: TLS v1.0, v1.1, v1.2 and v1.3. Likewise, the TOE also enables secure operations in the Huawei mobile device Android operating system to ensure all 3rd party mobile applications managed by the TOE are securely operates within the Android operating system operational environment. Note that, TOE server that hosting all registered developer mobile applications are not part of TOE scope.

Note that, all operations of the TOE inclusive of its installation process, delivery of the TOE, management of the TOE and handling of the TOE shall be elaborate further in the Guidance (AGD) documentation. TOE shall be accessible through download in form of APK file (such APK format example: com.huawei.appmarket.apk or com.huawei.appmarket.2007011605.apk) from the Huawei portal as mentioned below.

https://consumer.huawei.com/my/mobileservices/appgallery/

To download the TOE with this version 10.4.0.301, kindly refer to below link.

https://huawei-appgallery.en.uptodown.com/android/download/2209976

All underlying operating system and the hardware components describe in this document shall be treated as not part of the TOE scope. The components are not part of the TOE scope defined in Section 1.4.3 and 1.4.4.

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. **Identification & Authentication.** The TOE requires that TOE user is successfully identified and authenticated before any interactions with protected resources (registered APKs) which allow TOE user to purchase and download the 3rd party mobile applications, reward, gift and remark, pre-orders, wish list and comment notification. Additionally, TOE user requires to be identified and authenticated (via login into the Huawei registered account) before accessing the TOE as applications distribution platform.

B. **Security Management:** The TOE provides security management functions that allow the TOE user to manage the TOE functions as the following stated below.

    a. Purchase, download, and install the paid 3rd party mobile application(s);

b. Monitor and update the 3rd party mobile application(s) has been notified by the TOE upon update available;

c. Remove selected 3rd party mobile application(s) selected by TOE user

d. Receiving rewards;

e. Managing gifts (claim and redeem);

f. Writing comment/remark; and

g. Perform pre-orders.

The TOE restricts access to the management functions applicable for TOE user with registered account with Huawei.

C. Secure Communication: The TOE is able to protect the user data from disclosure and modification using a secure communication between TOE and TOE server for mobile APK file download and updates. If the TOE exit, close or send to background processes by the underlying operating system, the communication between TOE and TOE server will be terminated.

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 TOE and 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. There is not extended security functional requirements declared in this document.
- **Part 3 conformant, EAL1.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 5), April 2017. Evaluation is EAL1.

3 Security objectives

3.1 Overview

The objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition. The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

3.2 Security objectives for the Environment

Table 5: Security Objectives for the Environment

IDENTIFIER	OBJECTIVE STATEMENTS
OE.INSTALL	The TOE shall be delivered, installed, configured and set up in accordance with installation procedures defined in the guidance documentation.
OE.OS	The Huawei Android operating system are continuously hardened by Huawei to counter the perceived threats. The server-side hardening includes establish a secure configuration to the OS, configure OS audit logs, configure proper OS authentication and permission, and ensure legacy services are not enabled.
OE.UPDATE	Huawei shall provide updates of the TOE on a regular basis.

4 Security requirements

4.1 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:

i. **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**].

ii. **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***].

iii. **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

iv. **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

4.2 Security Functional Requirements (SFR)

4.2.1 User attribute definition (FIA_ATD.1)	
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a. Email Address and password, or** **b. Phone Number and verification code**].
Dependencies	No dependencies
Hierarchical to:	No other components.
4.2.2 User authentication before any action (FIA_UAU.2)	
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.
Dependencies:	FIA_UID.1 Timing of identification
Hierarchical to:	FIA_UAU.1 Timing of authentication
4.2.3 User identification before any action (FIA_UID.2)	
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.
Dependencies:	No dependencies.
Hierarchical to:	FIA_UID.1 Timing of identification
4.2.4 Management of security attributes (FMT_MSA.1)	
FMT_MSA.1.1	The TSF shall enforce the [**access control SFP (HAG)**] to restrict the ability to [**a. Purchase, download, and install the paid 3rd party mobile application(s);** **b. Monitor and update the 3rd party mobile application(s) has been notified by the TOE upon update available;** **c. Remove selected 3rd party mobile application(s) selected by TOE user;** **d. Receiving rewards;**

	e. **Managing gifts (claim and redeem);** f. **Writing comment/remark; and** g. **Perform pre-orders**] the security attributes [**object defined in the table of FDP_ACF.1.1]** to [**TOE user**].
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 Function
Hierarchical to:	No other components.
4.2.5 Static attribute initialisation (FMT_MSA.3)	
FMT_MSA.3.1	The TSF shall enforce the [**access control SFP (HAG), based on the information stated in the table of FDP_ACF.1.1**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**the authorised identified roles**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Hierarchical to:	No other components.
Application Notes:	HAG stands for "Huawei AppGallery". The initial been used for only labelling purpose.
4.2.6 Specification of Management Functions (FMT_SMF.1)	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**as requested by the TOE User in the TOE, listed below:** a. **Purchase, download, and install the paid 3rd party mobile application(s);** b. **Monitor and update the 3rd party mobile application(s) has been notified by the TOE upon update available;**

<table>
<tr><td></td><td>c. Remove selected 3rd party mobile application(s) selected by TOE user;
d. Receiving rewards;
e. Managing gifts (claim and redeem);
f. Writing comment/remark; and
g. Perform pre-orders].</td></tr>
<tr><td>Dependencies:</td><td>No dependencies.</td></tr>
<tr><td>Hierarchical to:</td><td>No other components.</td></tr>
<tr><td colspan="2">4.2.7 Security roles (FMT_SMR.1)</td></tr>
<tr><td>FMT_SMR.1.1</td><td>The TSF shall maintain the roles [TOE user].</td></tr>
<tr><td>FMT_SMR.1.2</td><td>The TSF shall be able to associate users with roles.</td></tr>
<tr><td>Dependencies:</td><td>FIA_UID.1 Timing of identification</td></tr>
<tr><td>Hierarchical to:</td><td>No other components.</td></tr>
<tr><td colspan="2">4.2.8 Security attribute based access control (FDP_ACF.1)</td></tr>
<tr><td>FDP_ACF.1.1</td><td>The TSF shall enforce the [access control SFP (HAG)] to objects based on the following: [information stated in the table below:
Table 6: TOE Security Attribute of the SFP (HAG)
<table>
<tr><th>SUBJECT</th><th>OBJECT</th><th>OPERATION/RULES</th></tr>
<tr><td>TOE user</td><td>Mobile Application</td><td>a. Purchase, download, and install the paid 3rd party mobile application(s);
b. Monitor and update the 3rd party mobile application(s) has been notified by the TOE upon update available;
c. Remove selected 3rd party mobile</td></tr>
</table></td></tr>
</table>

	<table><tr><td></td><td></td><td>**application(s) selected by TOE user;** **d. Receiving rewards;** **e. Managing gifts (claim and redeem);** **f. Writing comment/remark; and** **g. Perform pre-orders.**</td></tr><tr><td>**TOE user**</td><td>**User Account**</td><td>**Manage profile and credentials.**</td></tr></table>].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**operations/rules based on the information stated in the table of FDP_ACF.1.1**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**None**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control. FMT_MSA.3 Static attribute initialization
Hierarchical to:	No other components.
Application Notes:	HAG stands for “Huawei AppGallery”. The initial been used for only labelling purpose.
4.2.9 Complete access control (FDP_ACC.1)	
FDP_ACC.1.1	The TSF shall enforce the [**access control SFP (HAG)**] on [**operations/rules based on the information stated in the table of FDP_ACF.1.1**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Hierarchical to:	No other components.

Application Notes:	HAG stands for “Huawei AppGallery”. The initial been used for only labelling purpose.
4.2.10 User-initiated termination (FTA_SSL.4)	
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.
Dependencies:	No dependencies.
Hierarchical to:	No other components.
Application Notes:	None.
4.2.11 Inter-TSF trusted channel (FTP_ITC.1)	
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [**secure communication with TOE server**].
Dependencies:	No dependencies.
Hierarchical to:	No other components.
Application Notes:	None.

5 TOE Security Assurance Requirements

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

EAL1 provides a basic level of assurance by a limited Security Target (ST) and an analysis of the SFRs in that Security Target (ST) using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents. Below is the listed of security assurance requirements defined by EAL1.

Table 7: SAR

ASSURANCE CLASS	ASSURANCE COMPONENTS
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing – conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

6 TOE Summary Specification

6.1.1 Overview

This section provides the TOE summary specification in which, illustrates the mapping of justifications on the TOE security functions in achieving the consistency with the logical scope of the TOE. Thus, the following mapping that leads with the scope of TOE shall justify the requirements of SFRs defined.

6.1.2 Mapping of TOE Logical Scope towards the SFRs

The following the descriptions of mapping between TOE logical scope with the list of Security Functional Requirements (SFRs) defined in this document. Whilst this mapping shall elaborate the components of the TOE defined in the Logical Scope are meeting the SFRs as per required by the CEM.

Table 8: Mapping between Logical Scope and SFRs

LOGICAL SCOPE	SECURITY FUNCTIONAL REQUIREMENT (SFR)
Identification and Authentication	FIA_ATD.1 FIA_UAU.2 FIA_UID.2
Security Management	FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FDP_ACC.1 FDP_ACF.1
Secure Communication	FTA_SSL.4 FTP_ITC.1

6.1.2.1 Identification and Authentication

The TOE shall enforce security login through the identification and authentication processes where TOE user shall provide valid email address and password or phone number and verification code as login credential. The TOE protects all relevant data and configuration related to TOE operations as well TOE user in the TOE registration database, whilst enforcing secure authentication through the credential.

The TOE interacts with TOE server from Huawei Cloud to process the incoming request from the TOE and TOE user. The TOE implements access control and authentication measures to ensure that TOE

data and functionality is not misused by unauthorised 3rd parties. Note that, the TOE server is not part of the TOE scope of evaluation.

Each TOE login process supported through secure communication in between TOE and TOE server hosted by Huawei Cloud. Details of the TOE operations of the identification and authentication functions of the TOE kindly refer to TOE Guidance documentations. Note that, the TOE server is not part of TOE scope.

6.1.2.2 Security Management

TOE user shall have accessed the TOE using registered and verified credential in protecting the TOE from illegitimate access and outside threats. Any accessibility channel to the TOE shall be within approve and secure operational environment of the TOE and its underlying operating system, Huawei Android operating system.

Through the TOE, the TOE user shall manage the operations of the TOE by managing each functions of the TOE which are the following, as stated below.

a. Purchase, download, and install the paid 3rd party mobile application(s);
b. Monitor and update the 3rd party mobile application(s) has been notified by the TOE upon update available;
c. Remove selected 3rd party mobile application(s) selected by TOE user
d. Receiving rewards;
e. Managing gifts (claim and redeem);
f. Writing comment/remark; and
g. Perform pre-orders.

Detail operations of the security management functions of the TOE, kindly refer to TOE Guidance documentations.

6.1.2.3 Secure Communication

TOE initiate secure communication with the TOE server (managed by Huawei Cloud) and vice versa, with the objective of ensuring the TOE as whole solution are not being compromise or the transmitted data were not being tampered in its operations along the way. Transmission of data request by the TOE especially for 3rd party mobile application download and updates shall be in a secure communication channel approved by Huawei Cloud operations. This is to preventing attacker from access the TOE and made unauthorized changes.

Any activities performed by the TOE user on the TOE such as download and updating 3rd party mobile application are terminated (disconnected from secure communication session) if the TOE user exiting the TOE through force exit (using method of “Clear All” functions) through the push button “switch application” of the navigation menu.

In the event of the TOE user exit or close or in certain case of the TOE process are put in the background mode by the underlying operating system, the secure communication between TOE and TOE server will be disconnected to protect the communication from communication threats and risk. Once the TOE is re-open back by the TOE user, the TOE will initiated secure communication with the TOE server.

The secure communication channel is secured by using international standards or industry-recognized security protocols that supports the following secure protocols: TLS v1.0, v1.1, v1.2 and v1.3.

END OF DOCUMENT