MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C116 Certification Report

Huawei AppGallery v10.4.0.301

File name: ISCB-5-RPT-C116-CR-V1
Version: v1
Date of document: 15 April 2021
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

C116 Certification Report

Huawei AppGallery v10.4.0.301

15 April 2021

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C116 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C116-CR-V1
ISSUE:	v1
DATE:	15 April 2021
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (726630-U)

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 20 April 2021 and the Security Target (Ref [6])The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	7 April 2021	All	Initial draft
V1	15 April 2021	All	Final Release

Executive Summary

The Target of Evaluation (TOE) is Huawei AppGallery v10.4.0.301. The TOE is an official Huawei product which is a mobile application that has the capability as a mobile distribution channel for applications. The TOE provides users with a secure portal to buy, download, install, view list (sort/search), monitor, update and delete all registered third-party mobile apps inside the Huawei mobile devices. The TOE also enables TOE users access to all registered 3rd party mobile applications as application distribution platform with all relevant security features. The TOE provides several security functionalities such as Identification and Authentication, Security Management and Secure Communication.

The scope of the evaluation is defined by the Security Target (Ref[6]) which identifies security objectives for the environment, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 1 (EAL1). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by CyberSecurity Malaysia MySEF (CSM MySEF) and the evaluation was completed on 23 March 2021.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that Huawei AppGallery v10.4.0.301 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 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.

2 Below are the key features of the TOE:

a) TOE have access to catalogue of carefully selected android apps;

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

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

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

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

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

3 The following list highlights the range of security functions implemented by the TOE:

I. Identification and Authentication

II. Security Management

III. Secure Communication

1.2 TOE Identification

4 The details of the TOE are identified in Table 1: TOE Identification below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C116
TOE Name	Huawei AppGallery
TOE Version	V10.4.0.301
Security Target Title	Huawei AppGallery Security Target
Security Target Version	V1.0
Security Target Date	17 March 2021
Assurance Level	Evaluation Assurance Level 1
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 1
Sponsor	Huawei Technologies (Malaysia) Sdn Bhd Suite 32.01, Level 34, Integra Tower The Intermark, No 348, Jalan Tun Razak 50400 Kuala Lumpur, Malaysia
Developer	Huawei Technologies (Malaysia) Sdn Bhd Suite 32.01, Level 34, Integra Tower The Intermark, No 348, Jalan Tun Razak 50400 Kuala Lumpur, Malaysia
Evaluation Facility	CyberSecurity Malaysia MySEF (CSM MySEF) Level 7, Tower 1 Menara Cyber Axis Jalan Impact 63000 Cyberjaya Selangor Malaysia

1.3 Security Policy

5 There is no organisational security policy defined regarding the use of TOE.

1.4 TOE Architecture

6 The TOE consist of logical and physical boundaries which are described in Section 1.5 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

7 The logical boundary of the TOE is summarized below.

- 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-order, 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.

- 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 applications(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 the TOE user with registered account with Huawei.

- Security Management

  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.

1.4.2 Physical Boundaries

8 A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

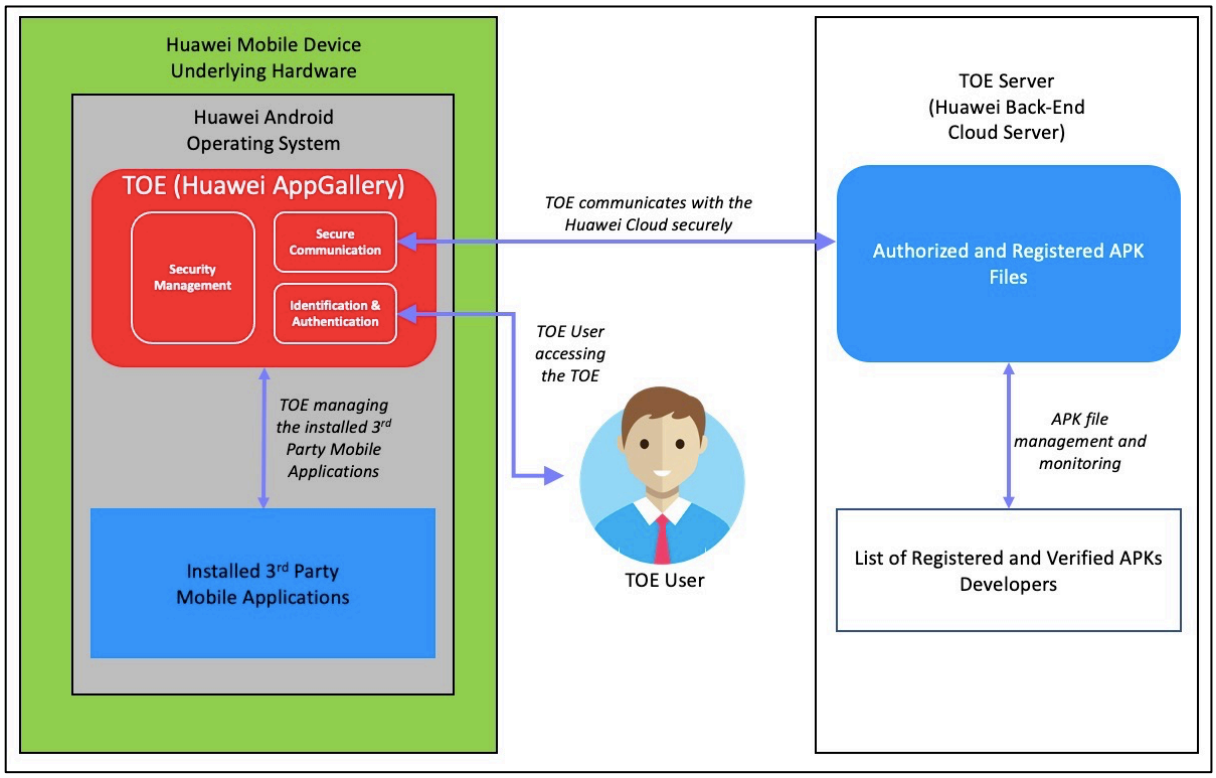

Figure 1 – TOE in Red Box

9 Huawei AppGallery as the TOE is designed specifically for Huawei mobile devices and Huawei mobile operating system to play role as applications distribution platform for other mobile application APK file to initiate TOE functions as stated below:

- Purchase, download, and install the paid 3rd party mobile application(s);
- Monitor and update the 3rd party mobile application(s) has been notified by the TOE upon update available;
- Remove selected 3rd party mobile application(s) selected by TOE user
- Receiving rewards;
- Managing gifts (claim and redeem);

- Writing comment/remark; and
- Perform pre-orders.

10 These TOE functions are secure operates within Huawei mobile device Android operating system.

11 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.

12 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.

13 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.

1.5 Clarification of Scope

14 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

15 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

16 Potential consumers of the TOE are advised that some functions and services of the overall product have not have been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

17 There is no assumptions defined regarding the use of TOE.

1.7 Evaluated Configuration

18 The TOE is delivered to the users in its operational state (Mobile Application) and no additional configuration is required.

1.8 Delivery Procedures

19 Huawei AppGallery is delivered to the customer via pre-installed in Huawei mobile devices.

20 However for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, the evaluators did not verify any TOE delivery process.

2 Evaluation

21 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

22 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

23 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

2.1.2 Development

24 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

25 The evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

26 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and

administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operative guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

27 The evaluators confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

28 Testing at EAL 1 consists of performing independent functional test and conducting penetration tests. The TOE testing was conducted by CyberSecurity Malaysia MySEF (CSM MySEF). The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Independent Functional Testing

29 At EAL 1, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

30 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 2: Independent Functional Test

Test Title	Description	Security Function	TSFI	Results
Test Group A Identification and Authentication				
A.1 Registration Process Require Credentials	This test group consist of a series of test cases on user registration, user identification and authentication.	FIA_ATD.1	Secure Communication with TOE Server and TOE User Credential Management	Passed.
A.2 Login Using Email and Password		FIA_UAU.2 FIA_UID.2		

Test Title	Description	Security Function	TSFI	Results
A.3 Login Using Email and Without Password		FIA_ATD.1	Administrator 3rd Party Mobile Application Manager, Secure Communication with TOE Server and TOE User Credential Management	
A.4 Login Without Email and Without Password				
A.5 Login Using Phone Number and Verification Code				
A.6 Login Using Phone Number and without Verification Code				
A.7 Login Without Phone Number and with Verification Code				
A.8 Login Without Phone Number and without Verification Code				
A.9 Login Using Phone Number and wrong Verification Code				
Test Group B Security Management				
B.1 Purchase 3rd Party Mobile Application – With Login	This test group consists of a series of test cases on TOE security functions of how security permission and capability being managed for TOE user.	FIA_ATD.1 FIA_UID.2 FIA_UAU.2 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT SMR.1 FDP_ACC.1 FDP_ACF.1	3rd Party Mobile Application Manager, Secure Communication with TOE Server and TOE User Credential Management	Passed.
B.2 Download and Install 3rd Party Mobile Application – With Login				
B.3 Update and Monitor 3rd Party Mobile Application – With Login				
B.4 View (Sort/Search) 3rd Party Mobile Application – With Login				
B.5 Remove 3rd Party Mobile Application – With Login				
B.6 Managing Gifts – With Login				
B.7 Access Rewards – With Login				

Test Title	Description	Security Function	TSFI	Results
B.8 Write and View Comments – With Login				
B.9 Perform Pre-Order and Managing Wish – With Login				
B.10 Purchase 3rd Party Mobile Application – Without Login		FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT SMR.1 FDP_ACC.1 FDP_ACF.1	3rd Party Mobile Application Manager	
B.11 Managing Gifts – Without Login				
B.12 Access Rewards – Without login				
B.13 Write and View Comments – Without login				
B.14 Perform Pre-Order and Managing Wish – Without login				
B.15 Manage Profile		FIA_ATD.1 FIA_UID.2 FIA_UAU.2 FDP_ACC.1 FDP_ACF.1	3rd Party Mobile Application Manager, Secure Communication with TOE Server and TOE User Credential Management	
B.16 Manage Credential				
Test Group C Secure Communication				
C.1 User Interactive Session Termination	This test group consists of a series of test cases on secure communication between TOE as mobile application and TOE server manage by TOE			Passed.
C.2 User Interactive Secure Communication Session Termination by Closing TOE.		FTA_SSL.4	Secure Communication with TOE Server	
C.3 User Interactive Secure Communication Session Termination using Clear All function.		FTA_SSL.4 FTP_ITC.1		

Test Title	Description	Security Function	TSFI	Results
C.4 User Interactive Secure Communication Session Termination using Force Stop function.	developer and the capability of TOE user to terminate his/her interactive session.			

31 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.2 Vulnerability Analysis

32 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation and functional specification.

33 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

2.1.4.3 Vulnerability testing

34 The penetration tests focused on:

a) Attack on TLS Version: Insecure Communication

b) Insecure Application Data Storage: Insecure Data Storage

c) Insecure Disclosure Through Logcat : Insecure Data Storage

35 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

36 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all the test conducted were PASSED as expected.

3 Result of the Evaluation

37 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Huawei AppGallery v10.4.0.301 which is performed by CyberSecurity Malaysia MySEF (CSM MySEF).

38 CyberSecurity Malaysia MySEF (CSM MySEF) found that Huawei AppGallery v10.4.0.301 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 1.

39 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

40 EAL 1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

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

42 EAL 1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

43 This EAL provides a meaningful increase in assurance over unevaluated IT.

3.2 Recommendation

44 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) Developer is recommended to ensure that TOE user needs to be identified and authenticated before able to access the TOE and perform any activities inside the TOE.
b) Developer is recommended to use latest version of TLS which is TLS1.2 and above, while, the use of TLS version 1.1 and 1.0 are generally discouraged as suggested by the NIST Guideline for TLS Implementations.

c) Developer is recommended to provide FAQ documentation based on the TOE version.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2020.

[6] Huawei AppGallery Security Target, Version 1.0, 17 March 2021.

[7] Evaluation Technical Report, Version 1.1, 2 April 2021.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---