MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

C126 Certification Report

Argrace IoT Security Communication Module (BLE+ Wi-Fi) v2.0A-009

File name: ISCB-5-RPT-C126-CR-v1
Version: v1
Date of document: 25 May 2022
Document classification : PUBLIC

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

CyberSecurity Malaysia
(726630-U)

Best Brand Internet Security 2008 & 2009
CERTIFIED TO ISO/IEC 27001:2013 CERT. NO.: AR 4656
MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)
MSC MALAYSIA Status Company
Best Child Online Protection Website

T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Securing Our Cyberspace

C126 Certification Report

Argrace IoT Security Communication Module (BLE+ Wi-Fi) v2.0A-009

25 May 2022

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:	C126 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C126-CR-v1
ISSUE:	v1
DATE:	25 May 2022
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 7 June 2022, 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).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

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	10 May 2022	All	Initial draft
v1	25 May 2022	All	Final version

Executive Summary

The Target of Evaluation (TOE) is an IoT Security Communication Module (SCM), which consists of TOE dedicated software and TOE hardware. Generally, the IoT SCM is integrated into an IoT host device. This SCM is to enable the IoT host device to connect to the network, establish a secure communication network channel between the IoT device and other terminals (i.e., Cloud service, Mobile APP), encrypt the user data for the IoT Application of the IoT device, and store the encryption data. The software of the above features is called IoT Security Communication Embedded Software (IoT SCES).

The scope of the evaluation is defined by the Security Target (Ref[6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, 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 2 Augmented ALC_FLR.1. 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 TÜV AUSTRIA Cybersecurity Lab (TACSL) and the evaluation was completed on 13 April 2022.

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 Argrace IoT Secure Communication Module (BLE + Wi-Fi) V2.0A-009 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 Argrace IoT Secure Communication Module (BLE + Wi-Fi) V2.0A-009. The TOE is used for providing security assurance for IoT host devices and IoT users, including functions such as identity authentication, information encryption and decryption, confidential information management, and access control.

2 The Target of Evaluation (TOE) is an IoT Security Communications Module (SCM), which consists of TOE dedicated software and TOE hardware. Generally, the IoT SCM is integrated into an IoT host device. This SCM is to enable the IoT host device connection to network, establish secure communication network channel between the IoT device and other terminals (i.e. Cloud, Mobile APP.), encrypt the user data for the IoT Application of IoT device, and store the encryption data. The software of above features is called IoT Security Communication Embedded Software (IoT SCES).

3 TOE hardware is an IoT SCM, which is composed of I/O ports, physical memories (Flash and ROM), antenna connector and crystal oscillator. It provides the hardware functions required for operation of IoT dedicated software. In particular, the CPU that developed and provided by the third-party manufacturer is not in the scope of TOE hardware, which provides the security function of generating true random number.

4 The TOE dedicated software operating on IoT SCM is called IoT Secure Communication Embedded Software (IoT SCES), which to implement the IoT device connection to network, establish secure communication network channel between the IoT device and other terminals (i.e., Cloud, mobile APP), encrypt and decrypt the data stored in Flash, and verify the firmware update image.

The IoT Secure Communication Embedded Software comprises：

- IoT Secure Communication Embedded Software source code, which is stored in Flash.

- User data of the Composite TOE, especially personalization data and other data generated and used by the IoT Secure Communication Embedded Software, which is stored in Flash.

1.2 TOE Identification

5 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	C126
TOE Name	Argrace IoT Secure Communication Module (BLE + Wi-Fi)
TOE Version	V2.0A-009
Security Target Title	Security Target of Argrace IoT Secure Communication Module (BLE + Wi-Fi) V2.0A-009
Security Target Version	V1.5
Security Target Date	22 April 2022
Assurance Level	Evaluation Assurance Level 2 Augmented ALC_FLR.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 2 Augmented ALC_FLR.1
Sponsor	Hangzhou Yaguan Technology Co. LTD (HYT) 33rd Floor, T4 US Center, European and American Financial City, Yuhang District, Hangzhou, Zhejiang
Developer	Hangzhou Yaguan Technology Co. LTD (HYT) 33rd Floor, T4 US Center, European and American Financial City, Yuhang District, Hangzhou, Zhejiang
Evaluation Facility	TÜV AUSTRIA Cybersecurity Lab Sdn. Bhd. (TACSL) A-11-01, Empire Office Tower, Jalan SS16/1, Subang Jaya, 47500 Selangor, Malaysia.

1.3 Security Policy

6 There are two (2) organisational security policies defined in the security target regarding the use of TOE.

- P.SCM: FirmwareUpdate

  The TOE should provide functionality to securely update its firmware, protected concerning authenticity and confidentiality. Only authentic SCM firmware update images as provided by the developer of the TOE shall be accepted by the TOE. Non-authentic SCM firmware update images or those being issued by the TOE developer but modified thereafter shall be rejected by the TOE. The TOE shall not accept a SCM firmware update image, if its firmware version is older than the version of the latest successfully installed firmware.

- P.SCM: RNG

  The TOE should use and rely on the trusted true random number source to get true random numbers. Such random number source can be a separate random generator or a CPU providing true random number generation function.

1.4 TOE Architecture

7 The TOE consists of logical and physical boundaries which are described in Section 1.4 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

8 The logical scope of TOE is the security functions as follows:

- Cryptographic support (TSF_CST):

  The TOE can derive 128-bit AES keys from true random number generated by CPU using MD5 algorithm. The TOE supports 128-bit AES CBC mode encryption and decryption function.

- User data protection (TSF_UDP):

  The TOE can only connect to cloud with approved IP address. The TOE can only connect to mobile APP with mutually known initial key.

- Secure firmware update (TSF_SFU):

  The TOE verifies the MD5 value of firmware image. The approved MD5 values are delivered to TOE via trusted path from cloud.

- Trusted path (TSF_TPH):

  The TOE will establish secure communication channel with mobile APP via self-defined mechanism. All the data transferred is protected by 128-bit AES algorithm. The TOE will initiate TLS channel with cloud.

- Memory protection (TSF_MPN):

  The TOE will encrypt all the data stored in Flash by 128-bit AES algorithm.

1.4.2 Physical Boundaries

9 The physical boundaries of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

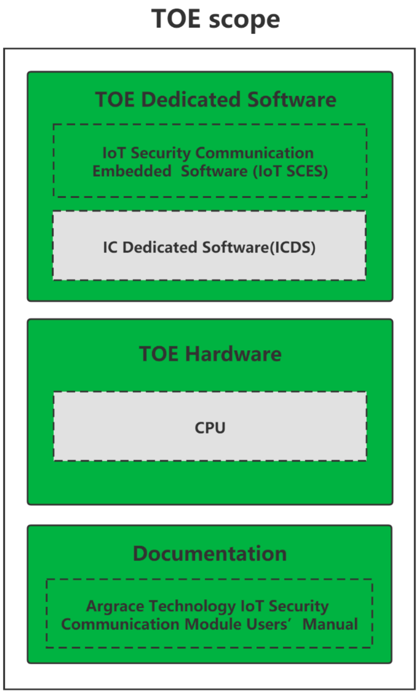

TOE scope
TOE Dedicated Software
IoT Security Communication Embedded Software (IoT SCES)
IC Dedicated Software(ICDS)
TOE Hardware
CPU
Documentation
Argrace Technology IoT Security Communication Module Users' Manual

Figure 1 – TOE Physical Scope (The green part)

1.4.2.1 TOE Hardware Description

10 In this ST, TOE hardware is an IoT SCM, which is composed of I/O ports, physical memories (Flash and ROM), antenna connector and crystal oscillator. It provides the hardware functions required for operation of IoT dedicated software. In particular, the CPU that developed and provided by the third-party manufacturer is not in the scope of TOE hardware, which provides the security function of generating true random number.

1.4.2.2 TOE Dedicated Software

11 The TOE dedicated software in this ST operating on IoT SCM is called IoT Secure Communication Embedded Software (IoT SCES), which to implement the IoT device connection to network, establish secure communication network channel between the IoT device and other terminals (i.e., Cloud, mobile APP), encrypt and decrypt the data stored in Flash, and verify the firmware update image.

12 The IoT SCES is embedded in the IoT SCM, which is the operational environment of the IoT SCES. However, due to different requirements and certification, other than IoT SCES, the other embedded software (embedded software to fulfil IoT host device functions, non-security related) in IoT SCM should be excluded and is not part of the TOE scope.

The IoT Secure Communication Embedded Software comprises :

- IoT Secure Communication Embedded Software source code, which is stored in Flash.

- User data of the Composite TOE, especially personalization data and other data generated and used by the IoT Secure Communication Embedded Software, which is stored in Flash.

1.4.2.3 Documentation

13 The "Argrace IoT Security Communication Module Users' Manual V1.0" is also part of the TOE which contains necessary description and guidance for users. In addition, the "Users' Manual" also includes guidance and requirements focused on security aspects.

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 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 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand the requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Operational Environmental assumptions

18 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 2: Assumptions for the TOE Environment

Environment	Statement
A.SCM:IoTManufacturer	It is assumed that the IoT device manufacturer understands which expected IoT host devices can be physically bound and integrated with the IoT SCM TOE, and this operation is not easy to implement. In addition,

	IoT device manufacturers can detect whether the device has been physically modified.
A.SCM:IoTApplication	It is assumed that the security requirements of the IOT application are consistent with the security functions provided by the IoT SCM TOE, and the IoT application uses the security functions provided by the IoT SCM TOE to protect the information received or sent, and to ensure that the data is sent to the expected device or from the expected device receiving data
A.SCM:Communication	It is assumed that IoT device manufacturers only use IoT SCM TOE as the only way for IoT host devices to communicate with external network devices, that is, IoT devices do not use other methods to communicate with external devices.

1.7 Evaluated Configuration

19 This section describes the evaluated configurations of the TOE that are included within the scope of the evaluation.

20 The TOE is available in two configurations, test configuration, and operational configuration.

21 The test configuration covers the functions of all TSF and non-TSF systems under the operational mode. Under this configuration, test interfaces (interfaces related to TSF and data) can be accessed via specific AT commands.

22 The operational configuration supports the user to use all functions of non-TSF and TSF modules provided by the system in a normal environment under the Operational mode. Under this mode, interfaces and data related to TSF functions cannot be accessed via serial ports.

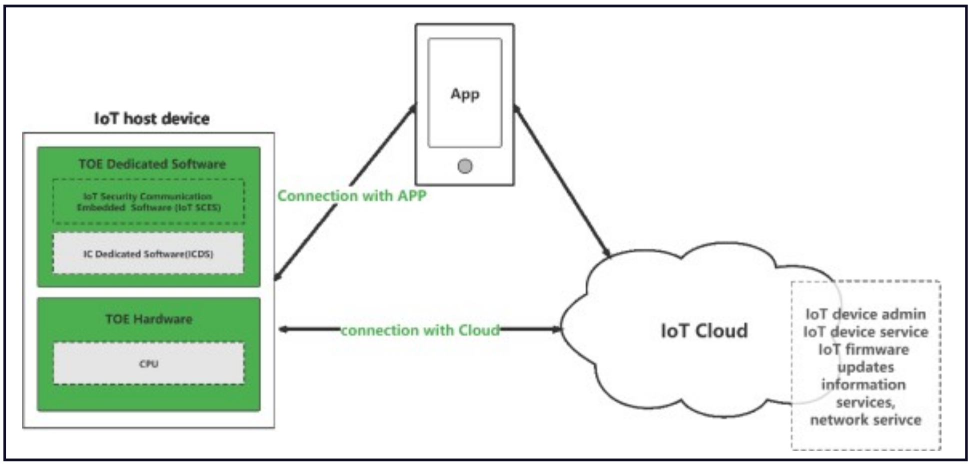


Figure 2 – Scope of TOE Evaluation

1.8 Delivery Procedures

23 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

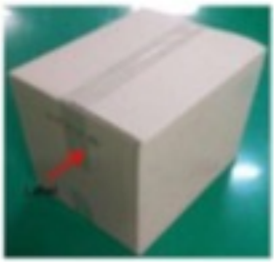
24 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

25 Several procedures are necessary to maintain security of the TOE during distribution including the procedures during the production, packaging, and release of the TOE.

26 Packaging

After firmware burning is completed for TOE products, the QC personnel will randomly sample 10% of products for examination. Such examination includes the confirmation of basic product information (including the category of IoT devices, firmware version, etc.) and routine functional testing. If examination results are positive, the products will be packaged by means of tape and reel and then delivered. Labels will be attached to the surface of the tape/reel to indicate product model, size, quantity and other basic information. The direction of product placement, the location of label and product package are in accordance with the packaging drawing



Each reel of carrier tape is sealed in a vacuum tin foil bag. 2 bags of 2g desiccant are put into each tin foil bag, together with 1 six-color humidity indicator. A label is attached to each tin foil bag. Carrier tapes in vacuum tin foil bags are put into small paper boxes, to the surface of which the same labels are attached. As the last step, 5 small paper boxes are put into a large carton. Both the small paper boxes and the carton are sealed with adhesive tape, with labels attached to the surface. Each reel accommodates 600 TOE (modules), each small paper box accommodates 1 reel, and each carton accommodates 5 small paper boxes. The total quantity of TOE is 3000 pieces/carton. Carton size: 375mm*285mm*365mm; box size: 355mm*355mm*55mm. Other packaging sizes may be customized according to the requirements of customers (IoT device manufacturers).

For orders from each customer (IoT device manufacturer), before delivery, the QC personnel verifies order information and put it into storage, with the Shipment Notice (put in an anti-tampering sealing bag) provided in one of the cartons. The Shipment Notice indicates the basic information such as TOE (module) model, quantity, receiver, batch, etc. After that, the sales order specialist submits the product outbound approval associated with the corresponding sales order on the internal OA platform and checks order information (model, quantity, etc.) in the approval process, before the warehouse manager ships the products upon approval.

Hangzhou Yaguan Technology Co., Ltd.
Model: xxxxx
Batch No.: xxxxxx
Quantity: xxx
TOE code: xxx
Labels on inner boxes (carrier tapes, tin foil bags, general labels for inner boxes)

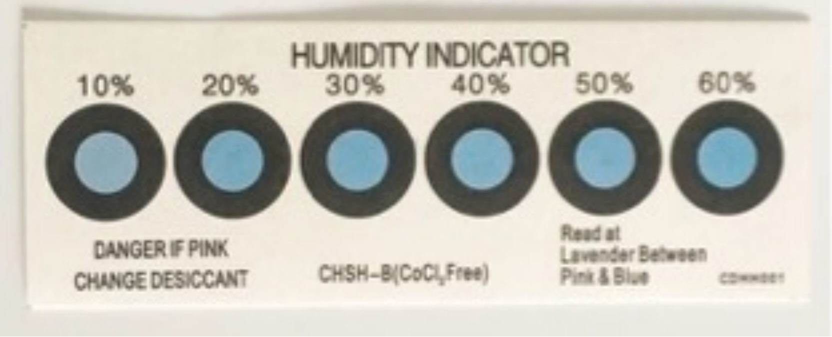
Hangzhou Yaguan Technology Co., Ltd.	
Model: xxxxx	
Batch No.: xxxxxx	
Quantity: xxx	Weight: kg/piece
TOE code: xxx	
Labels on cartons	

27 Distribution

TOE products will be transported by internationally and domestically well-known delivery companies (SF, DHL, etc.). Once the products are delivered, the receiver will receive a notice. The sender and receiver may track delivery information (the current location and the expected time of arrival of the parcel) via the delivery company's App or official website by entering the tracking number. They can also check the name and contact number of the delivery man in the delivery process once the parcel arrives at the destination. If necessary, the sender and receiver may forward the tracking number to a third party to follow up the delivery process.

28 Storage

During the delivery to the customer (IoT device manufacturer), TOE (modules) shall be stored in an environment with a temperature < 30℃ and a humidity < 70% RH. The customer (IoT device manufacturer) may check dampness of products, with the vacuum package removed, using the six-color humidity indicator (changing from blue to pink).



Surface mounting of TOE (modules) must be performed mechanically by an SMT machine. The process of surface mounting must be completed within 24 hours after the package is removed for firmware burning, otherwise the package must be vacuumized and the TOE (modules) must be baked again before surface mounting. The modules shall be baked for 2 hours at a temperature of 120℃±5℃. SMT can be carried out after the modules are naturally cooled down to < 36℃.

29 Additional procedure for overseas delivery

The Company will designate an international delivery company such as DHL, UPS, or FedEx to transport products abroad and ensure to provide delivery services with online parcel tracking and query.

2 Evaluation

30 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 2 Augmented ALC_FLR.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

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

2.1.1 Life-cycle support

32 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.

33 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Flaw Reporting Procedures

34 The evaluators have examined the flaw remediation procedures documentation and determined that it describes the procedures used to track all reported security flaws in each release of the TOE which would produce a description of each security flaw in terms of its nature and effects.

35 The evaluators have examined the flaw remediation procedures and determined that the application of the procedures would identify the status of finding a correction to each security flaw and identify the corrective action for each security flaw.

36 The evaluators have examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information on each security flaw.

37 The evaluators have examined the flaw remediation procedures and determined that it describes procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.

38 The evaluators have examined the flaw remediation procedures and determined that the application of the procedures would help to ensure every reported flaw is corrected and that TOE users are issued remediation procedures for each security flaw.

39 The evaluators have examined the flaw remediation procedures and determined that the application of the procedures would result in safeguards that the potential correction contains no adverse effects.

40 The evaluators have examined the flaw remediation guidance and determined that the application of the procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

2.1.3 Development

41 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).

42 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

43 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

44 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.4 Guidance documents

45 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 operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

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

2.1.5 IT Product Testing

47 Testing at EAL 2 Augmented ALC_FLR.1 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by TÜV AUSTRIA Cybersecurity Lab (TACSL). The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.5.1 Assessment of Developer Tests

48 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.5.2 Independent Functional Testing

49 At EAL 2 Augmented ALC_FLR.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.

50 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 3: Independent Functional Test

Test ID	Description	Security Function	Results
TSFI_GRD_01	□ To verify that the interface can generate true random arrays correctly	FCS_CKM.5 FDP_ACC.1/APP FDP_ACF.1/APP FTP_PHP.3	Passed.
TSFI_SCB_01	□ To verify that the interface can combine the string correctly	FCS_CKM.5 FDP_ACC.1/APP FDP_ACF.1/APP FTP_PHP.3	Passed.
TSFI_MD5_01	□ To verify that the interface can transform a string of a designated length to the 32-bit MD5 format	FCS_CKM.5 FDP_ACC.1/APP FDP_ACF.1/APP FDP_ACC.1/SCMFW FDP_ACF.1/SCMFW FPT_PHP.3	Passed.
TSFI_CBC/CS5PaddingEncrypt_01	□ To verify that the interface can encrypt correctly string via AES/CBC/PKCS5 Padding algorithm	FCS_CKM.5 FCS_COP.1 FDP_ACC.1/APP FDP_ACF.1/APP FDP_ACC.1/SCMFW FDP_ACF.1/SCMFW FPT_PHP.3	Passed.
TSFI_CBC/CS5PaddingDecrypt_01	□ To verify that the interface can correctly decrypt cipher text via AES/CBC/PKCS5 Padding algorithm	FCS_CKM.5 FCS_COP.1 FDP_ACC.1/APP FDP_ACF.1/APP FDP_ACC.1/SCMFW FDP_ACF.1/SCMFW FPT_PHP.3	Passed.

Test ID	Description	Security Function	Results
TSFI_ECB/ZeroPaddingEncrypt_01	□ To verify that the interface can correctly encrypt string via AES/ECB/ZeroPadding Algorithm	FCS_CKM.5 FCS_COP.1 FDP_ACC.1/APP FDP_ACF.1/APP FDP_ACC.1/SCMFW FDP_ACF.1/SCMFW FPT_PHP.3	Passed.
TSFI_ECB/ZeroPaddingDecrypt_01	□ To verify that the interface can correctly decrypt cipher text via AES/ECB/ZeroPadding Algorithm	FCS_CKM.5 FCS_COP.1 FDP_ACC.1/APP FDP_ACF.1/APP FDP_ACC.1/SCMFW FDP_ACF.1/SCMFW FPT_PHP.3	Passed.
TSFI_WFH_01	□ To verify that the interface can correctly encrypt the data blocks via AES/ECB/zeropadding algorithm and save them to the specified address area of flash	FPT_PHP.3	Passed.
TSFI_RFH_01	□ To verify that the interface obtain the encrypted data block stored in Flash and decrypt it via AES/ECB/zeropadding algorithm. Then, store the plain text into parameter data array	FPT_PHP.3	Passed.
TSFI_ERF_01	□ To verify that the interface implements the function of erasing encrypted data blocks of designated address and size in flash	FPT_PHP.3	Passed.
TSFI_CTA_01	□ To verify that the TOE is capable of establish connection to the Argrace Smart Application as documented by developer.	FDP_ACC.1/APP FDP_ACF.1/APP FTP_ITC.1	Passed.

Test ID	Description	Security Function	Results
TSFI_CTC_01	□ To verify that the TOE is capable of establish connection to the Argrace Smart Application as documented by developer.	FDP_ACC.1/Cloud FDP_ACF.1/Cloud FTP_ITC.1	Passed.

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

2.1.5.3 Vulnerability Analysis

52 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, functional specification, TOE design, and security architecture description.

53 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

2.1.5.4 Vulnerability testing

54 The penetration tests focused on:

a) Insecure Network Services

b) Lack of Secure Update Mechanism

c) Insufficient Privacy Protection

d) Insecure data transfer (Wireless + Bluetooth Sniffing)

e) Insecure data storage (via Memory analysis)

f) Bluetooth replay attack

g) Vulnerability Scanning

55 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]).

2.1.5.5 Testing Results

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

3 Result of the Evaluation

57 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 Argrace IoT Security Communication Module (BLE+ Wi-Fi) v2.0A-009 which is performed by TÜV AUSTRIA Cybersecurity Lab (TACSL).

58 TÜV AUSTRIA Cybersecurity Lab (TACSL) found that Argrace IoT Security Communication Module (BLE+ Wi-Fi) v2.0A-009upholds the claims made in the Security Target (Ref [6]) and supporting documentations and met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 Augmented ALC_FLR.1.

59 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

60 EAL 2 Augmented ALC_FLR.1 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

61 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 penetration attackers with a basic attack potential.

62 EAL 2 Augmented ALC_FLR.1 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

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

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable with the stated security objectives for the operational environment and it can be suitably addressed.

b) Potential purchasers should consider the usage, practicality and security considerations and best practices of the mobile application before deploying it in their intended environment.

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] Argrace IoT Security Communication Module (BLE + Wi-Fi) v2.0A-009 Security Target, Version 1.5, 22 April 2022.

[7] Evaluation Technical Report, Version 1.1, 28 April 2022.

A.2 Terminology

A.2.1 Acronyms

Table 4: 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 5: 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 ---