MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C110 Certification Report

Amaris Data Diode for Air Gap (ADD-GAP) v 2.0.112

File name: ISCB-5-RPT-C110-CR-v1
Version: v1
Date of document: 17 June 2020
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
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

C110 Certification Report

Amaris Data Diode for Air Gap (ADD-GAP) v 2.0.112

17 June 2020

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:	C110 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C110-CR-v1
ISSUE:	v1
DATE:	17 June 2020
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. 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 25 June 2020 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	9 June 2020	All	Initial draft
v1	17 June 2020	All	Final Released

Executive Summary

The Target of Evaluation (TOE) is a Amaris Data Diode For Air Gap (ADD-GAP) offers end users a means to convey user data across the communication interface from the ADD-GAP Send-Only circuit to the ADD-GAP Receive-Only circuit and the data's target destination.

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 (EAL2). 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 Cybertronics Lab and the evaluation was completed on 5 June 2020.

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 Amaris Data Diode For Air Gap (ADD-GAP) v2.0.112 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

Document Authorisation ii
Copyright Statement iii
Foreword iv
Disclaimer v
Document Change Log vi
Executive Summary vii
Index of Tables ix
Index of Figures ix
1 Target of Evaluation 1
1.1 TOE Description 1
1.2 TOE Identification 3
1.3 Security Policy 4
1.4 TOE Architecture 4
1.4.1 Logical Boundaries *4*
1.4.2 Physical Boundaries *4*
1.5 Clarification of Scope 5
1.6 Assumptions 5
1.6.1 Environmental assumptions *5*
1.7 Evaluated Configuration 6
1.8 Delivery Procedures 8
1.8.1 TOE Delivery Procedures 8
2 Evaluation 10
2.1 Evaluation Analysis Activities 10
2.1.1 Life-cycle support *10*
2.1.2 Development *10*
2.1.3 Guidance documents *11*
2.1.4 IT Product Testing *11*

3 Result of the Evaluation 15

3.1 Assurance Level Information 15

3.2 Recommendation 15

Annex A References 17

A.1 References 17

A.2 Terminology 17

A.2.1 Acronyms 17

A.2.2 Glossary of Terms 18

Index of Tables

Table 1: TOE identification 3

Table 2 : Assumptions for the TOE environment 6

Table 3 : Independent Functional Test 12

Table 4 : List of Acronyms 17

Table 5 : Glossary of Terms 18

Index of Figures

Figure 1 - ADD-GAP One-way unidirectional flow of data 1

Figure 2 - TOE Block Diagram 2

Figure 3 - Independent TOE Testing Environment 7

Figure 4 - Microchip Firmware Tampering Environment 8

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is an Amaris Data Diode For Air Gap (ADD-GAP) offers end users a means to convey user data across the communication interface between the SEND-ONLY circuit as MASTER and RECEIVE-ONLY circuit as SLAVE. ADD-GAP was designed as USB 2.0 mass storage controller with standard USB 2.0 Specification for both MASTER and SLAVE drive, it has fake capacity of 8GB only, support plug & play feature and not need any additional driver to be installed on the PC.

2 (ADD-GAP) is the product designed and manufactured by Advanced Product Design Sdn Bhd. ADD-GAP provides an absolute deterministic one-way unidirectional flow of any data and information between a source domain, the USB sending host system; tablet; android; laptop; PDA; network to a destination domain, the USB or host system/network that identified in this Security Target (Ref [6]).

3 There is no storage on the device itself and it only acts as a gateway to send data over from sender to receiver side. The MASTER drive is a write only fake USB storage drive whereas the SLAVE drive is a read only USB storage device with HID interface.

4 ADD-GAP is driverless which means no software is required on the sender side. Only a receiver program on the receiver side is required to handle the file transfers and destination folder.

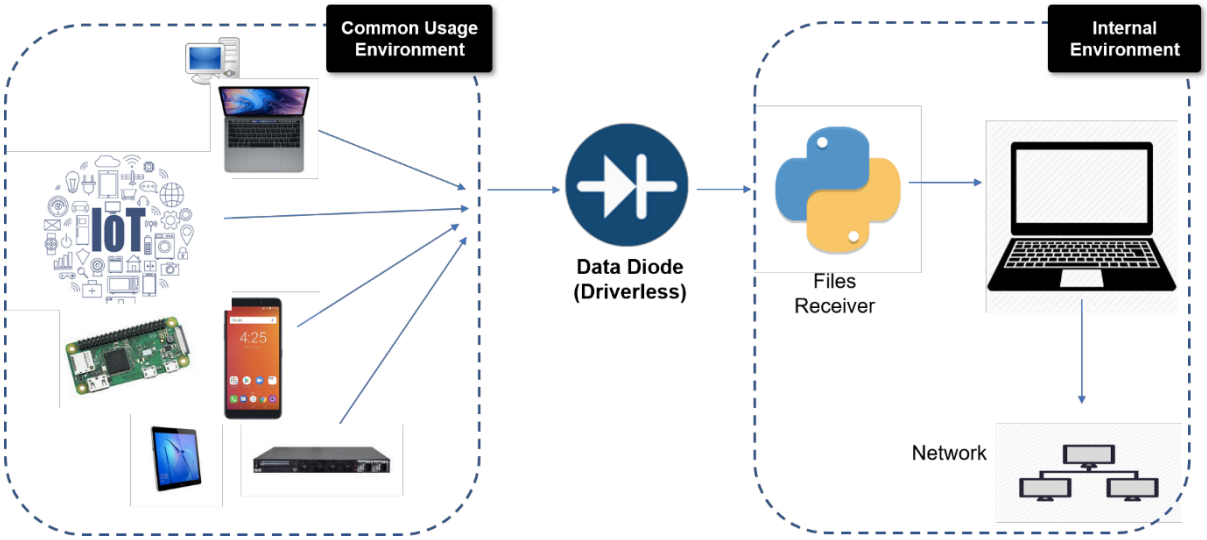

Figure 1 - ADD-GAP One-way unidirectional flow of data

5 The data diode's one-way policies which are implemented with a hardware pipeline cannot be reconfigured by any software configuration. Specifically, the hardware is designed to be contained within the data diode casing with CPU compliant USB 2.0 interface.

a. Master PC send data to Master controller.

b. Master controller sends data to slave through three SPI channels 1, 2 and 4.

c. At the same time LED blinks on & off to signal data transfer.

d. Slave receive data via three SPIs.

e. Slave controller alert Slave PC that data is available.

f. Slave PC Acknowledge to Master through SYNC pin. SYNC is just a low to high and then high to low pulse for synchronization only. This is to tell MASTER that we are ready to accept more data.

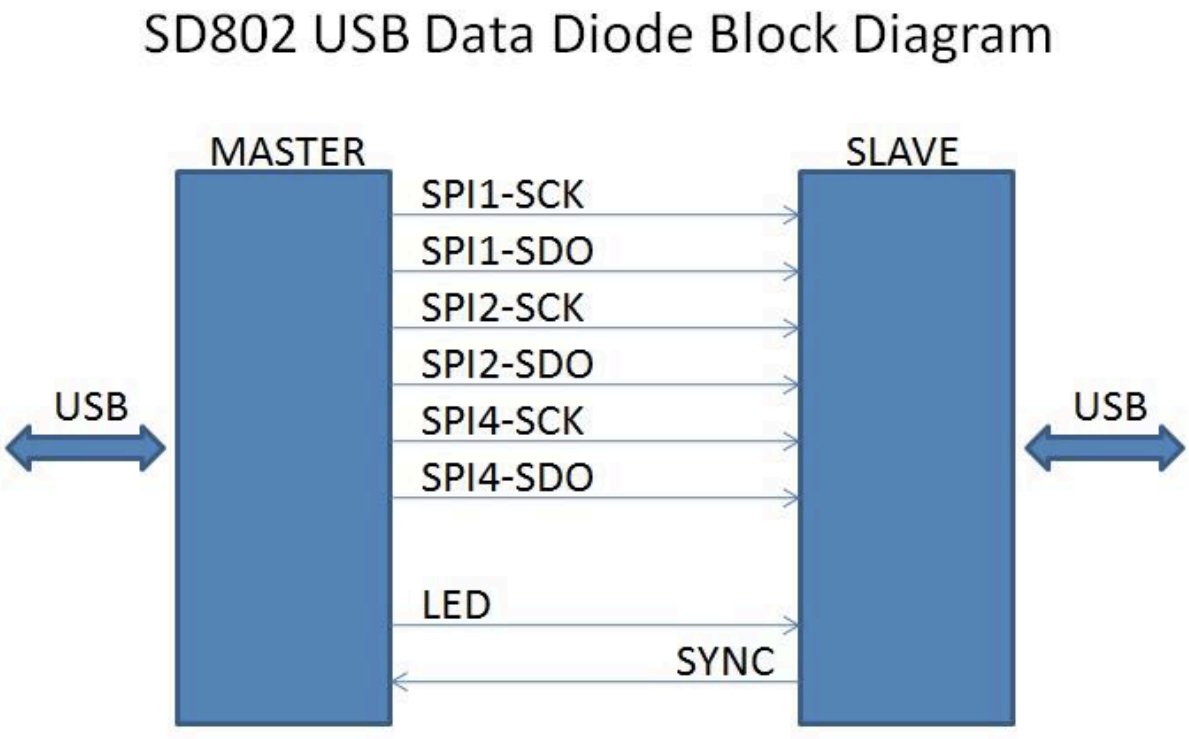

Figure 2 - TOE Block Diagram

1.2 TOE Identification

6 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C110
TOE Name	Amaris Data Diode For Air Gap (ADD-GAP)
TOE Version	V2.0.112
Security Target Title	Amaris Data Diode For Air Gap (ADD-GAP) Security Target
Security Target Version	V1.0
Security Target Date	5 June 2020
Assurance Level	Evaluation Assurance Level 2
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
Sponsor	Advanced Product Design Sdn Bhd No. 209, Jalan Impian Emas 22, Taman Impian Emas, 81300 Skudai, Johor, Malaysia.
Developer	Advanced Product Design Sdn Bhd No. 209, Jalan Impian Emas 22, Taman Impian Emas, 81300 Skudai, Johor, Malaysia.
Evaluation Facility	Cybertronics Lab C-5-15, Centum @ Oasis Corporate Park No 2, Jalan PJU 1A/2, Ara Damansara 47301 Selangor, Malaysia

1.3 Security Policy

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

1.4 TOE Architecture

8 The TOE consist of logical and physical boundaries which are described in Section 1.6 of the Security Target (Ref[6]).

1.4.1 Logical Boundaries

9 The logical scope of TOE is described based on one security functional requirement.

- User Data Protection

  ADD-GAP offers end users a means to convey user data across the communication interface from the ADD-GAP Send-Only circuit to the ADD-GAP Receive-Only and the data's target destination. Since we have established that the TOE provides an absolute deterministic one-way unidirectional flow of any data and information between two devices, there is no way to extract the data from the ADD-GAP Receive-Only side, thus achieving user data protection.

- Protection of the TSF

  ADD-GAP offers passive detection of physical attack, it provides for features that indicate when a TSF device or TSF element is subject to tampering. However, notification of tampering is not automatic; an authorised user must perform manual physical inspection to determine if tampering has occurred.

1.4.2 Physical Boundaries

10 The TOE consists of two microchips i.e. Sender and Receiver. These two microchips are physically connected to each other on a printed circuit board (PCB).

11 The supporting hardware and software for TOE are as following:

a) Universal serial bus (USB)

   Universal serial bus, USB is a plug and play interface that allows a computer to communicate with peripheral and other devices.

b) Computers/ Laptops/ Servers (Private Devices)

   The TOE will connect public and private devices for data transfer purpose. The connection will be established via USB port of the computer/ Laptops/ Servers. The

private device will be the machine to receive data and must running in Microsoft Windows based operating system.

c) Computers/ Laptops/ Servers (Public Devices)

The TOE will connect public and private devices for data transfer purpose. The connection will be established via USB port of the computer/ Laptops/ Servers. The public device will be the machine to send data.

d) DiodeCore.dll

The core engine that consists all the core functions for Diode Receiver (Windows application) to communicate with ADD-GAP.

e) DiodeDecode.dll

All sub-functions used to decode received packets and generate the specific file.

1.5 Clarification of Scope

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

13 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]).

14 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

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

1.6.1 Environmental assumptions

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

Table 2 : Assumptions for the TOE environment

Assumption	Statements
A.USER	The users are trusted; the users shall not maliciously compromise the security functionality of the TOE. The users are well-trained; the user shall comply to the operating procedures stipulated in the user guidance.
A.DATAFLOW	The data flow between Public Device and Private Device must pass through the TOE and there will be no other connection between Public Device and Private Device.

1.7 Evaluated Configuration

17 ADD-GAP may be deployed in a number of configurations consistent with the requirements as below:

a) Domain Separation

The TOE does not provide security domains to potentially-harmful entities. The TOE management functionality described does not provide security domains, but is a direct implementation of the security requirements. In short, security domains are not applicable for this TOE.

b) Initialisation

After the TOE securely delivered to the customer, the TOE will be usable directly based on the Operation Steps in APD [ADD-GAP] Diode Receiver (DR) Software User Guideline-ver3.0.

c) Protection from Tampering

- Physical Protection: ADD-GAP come with a hard metal case to protect the microchip and circuit board of the TOE. Additionally, the programming pin of the microchip is sealed with Epoxy Resins.
- Logical: Logical protection is not applicable for the TOE device. This is due to no authentication feature been implemented at the TOE.

d) Protection from Bypassing

TSF ensures that the security functionality is always invoked and hence, with the self-protection (as described earlier in this document) and correct functional behaviour (as described in the FSP/TDS evaluation evidence), the SFRs are always enforced.

18 Figure 3 shows the testing environment to test the TOE. The TOE establish a communication bridge between two test machines via the Universal Serial Bus (USB) interface. The TOE consists of two microchips which is MASTER and SLAVE. These two microchips are logically connected to each other on a printed circuit board (PCB). MASTER is connected to the sender device while SLAVE is connected to the receiver device. "DiodeCore.dll" is the core library file for "DiodeReceiver.exe", which will be used to control the file transfer process.

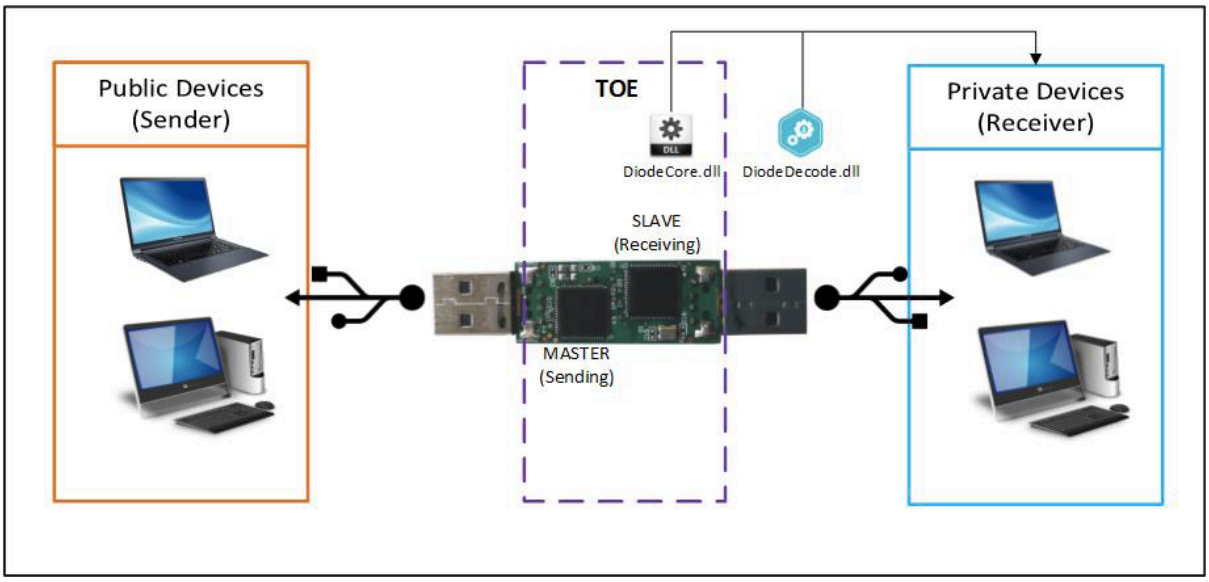

Figure 3 - Independent TOE Testing Environment

19 Figure 4 shows the testing environment for microchip firmware testing. Test jig is connected to the test machine via USB port and the application named MPLAB Integrated Programming Environment (IPE) is loaded in the test machine. Test jig is used to connect the programming pin on the TOE to the test machine thus allow MPLAB Integrated Programming Environment (IPE) to read the microchip firmware.

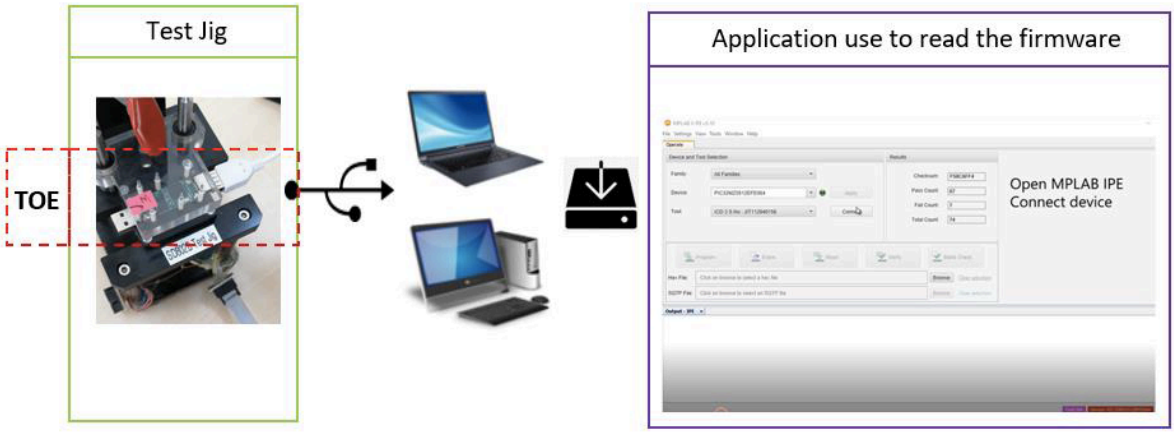

Figure 4 - Microchip Firmware Tampering Environment

1.8 Delivery Procedures

20 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.

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

1.8.1 TOE Delivery Procedures

22 The TOE is delivered by Advanced Product Design personnel to the customer.

23 Advanced Product Design personnel will prepare the User Guide document for ADD-GAP and deliver through E-mail to the customers.

24 Advanced Product Design personnel will label the ADD-GAP device with ADD-GAP identification and serial number.

25 The TOE is wrap with protective sponge foam and package it with a box.

26 The TOE packaging box will be sealed with security tape to avoid the product being tampered during delivery to the customer.

27 The product will be hand-delivered to customer.

28 Once the package is delivered, the customer is expected to perform the following measures:

a. Receive the package.

b. Acknowledge received items receipt as per Appendix A.

29 Advanced Product Design personnel will keep the Acknowledge received items as proof of product receipt. Acceptance of product will be based on customer's selection of product functionalities

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. 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 Development

34 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).

35 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.

36 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.

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

2.1.3 Guidance documents

38 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.

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

2.1.4 IT Product Testing

40 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Cybertronics Lab. 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 Assessment of Developer Tests

41 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.

2.1.4.2 Independent Functional Testing

42 At EAL 2, 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.

43 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	Results
AVCC006-FT001	To ensure the data transmission is operate in a desire manner.	Passed.
AVCC006-FT002	To ensure the TSF deterministic ONE-WAY unidirectional flow of information.	Passed.
AVCC006-FT003	To ensure the data diode is capable of transfer data within the designed fake storage capacity.	Passed.
AVCC006-FT004	To ensure the fake capacity in the data diode will wipe the storage after file successfully transferred.	Passed.
AVCC006-FT005	To ensure the data diode will not perform data transfer without user control or intention.	Passed.
AVCC006-FT006	To ensure the data diode microchip firmware is protected by Epoxy seal.	Passed.
AVCC006-FT007	To ensure the Epoxy sealant cannot be removed from the PCB.	Passed.

Test ID	Description	Results
AVCC006-FT008	To ensure the data diode hard metal case will not easily pry open.	Passed.

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

2.1.4.3 Vulnerability Analysis

45 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.

46 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) Any public knowledge of the vulnerability or known exploit;

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.

2.1.4.4 Vulnerability testing

47 The penetration tests focused on:

a) Code Tempering and Reverse Engineering

b) Extraneous Functionality

c) Client Code Quality

48 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]).

2.1.4.5 Testing Results

49 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. Therefore, the certifiers confirmed that all the test conducted were PASSED as expected.

3 Result of the Evaluation

50 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 Amaris Data Diode for Air Gap (ADD-GAP) v 2.0.112 which is performed by Cybertronics Lab.

51 Cybertronics Lab found that Amaris Data Diode for Air Gap (ADD-GAP) v 2.0.112 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 2.

52 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

53 EAL 2 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.

54 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.

55 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

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

a) A strict adherence to guidance documentations and procedures provided by the developer are highly recommended.

b) The TOE users should be aware and implement available security or critical updates related to the TOE security features and its supporting hardware, software, firmware or relevant guidance documents.

c) Users are advice to seek assistance or guidance directly from the developer of the TOE if specific requirements shall be configured or implemented by the TOE to meet certain policies, procedures and security enforcement within the users' organization. This is important in order to reduce operational error, misconfiguration, malfunctions or insecure operations of the TOE that may compromise the confidentiality, integrity and availability of the assets that is protected by the TOE.

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), v2, December 2019.

[6] Amaris Data Diode For Air Gap (ADD-GAP) Security Target, Version 1.0, 5 June 2020.

[7] Evaluation Technical Report, Version 2.0, 9 June 2020.

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
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme

Acronym	Expanded Term
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 ---