Ref: ADD-GAP-ST-1.0

Amaris Data Diode For Air Gap (ADD-GAP) Security Target

DOCUMENT VERSION	**1.0**
DOCUMENT DATE	**05-JUNE-2020**

No. 209, Jalan Impian Emas 22, Taman Impian Emas,
81300 Skudai, Johor, Malaysia.
Email: leekp@biocryptodisk.com
Tel: (6012) 776 9949
Website: www.biocryptodisk.com

Prepared by:

ACROSS VERTICALS

DOCUMENT REVISION HISTORY

Version No.	Published Date	Description of changes	Author
0.1	30-OCT-2019	First release	Wilson Lim
0.2	09-DEC-2019	AVCC006-EOR001 Correction	Wilson Lim
0.3	14-FEB-2020	AVCC006-EOR002 Correction and TOE diagram update	Wilson Lim
0.4	26-MAY-2020	ISCB-3-CAR-C110-CAR_001-v1 and ISCB-3-CAR-C110-CAR_002-v1 Comments Update	Wilson Lim
1.0	05-JUNE-2020	Final Release	Wilson Lim

TABLE OF CONTENTS

1 Security Target Introduction

1.1 Security Target Reference

Security Target Title:	Amaris Data Diode For Air Gap (ADD-GAP) Security Target
Security Target Version:	1.0
Security Target Date:	05-JUNE-2020

Table 1 - ST Reference

1.2 TOE Reference

TOE Name & Version	**TOE NAME:**	**TOE VERSION:**
	Amaris Data Diode For Air Gap	v2.0.112
TOE Initial:	ADD-GAP	

Table 2 - TOE Reference

1.3 Terminology and Acronyms

Acronyms	Full Name
ADD-GAP	Amaris Data Diode For Air Gap
CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
SPI	Serial Peripheral Interface
SCK	Serial Clock
SDO	Serial Data Output
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements

ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
HID	Human Interface Device
USB	Universal Serial Bus

1.4 Product Overview

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.

Please refer to

- Table 3: ADD-GAP Product Specification
- Table 4: Hardware Picture with Casing
- Table 5: Hardware Picture without Casing

Table 3 – ADD-GAP Product Specification

Type	Version	Specification	Driverless
MASTER(Hardware)	1.0.118	• FAT32 8GB fake capacity • USB2.0 Mass Storage controller • Max size per file per transaction: 4GB • Data Transfer Rates: 10 Mbps – 40Mbps • Supports vendor specific command • Firmware Version can identified using "DiodeInfoVers1.0.exe" upon request from customer	Yes
SLAVE(Hardware)	2.0.112	• FAT32 8GB fake capacity, • USB2.0 composite device (HID + mass storage controller) • SLAVE drive is write-protected and read-only • Supports vendor specific command • Firmware Version can identified from the back of the hard metal case	Yes
DiodeCore.dll	20.1.16.1	All core functions used to communicate with Diode Devices. Function includes: • FindDevices • ConnectToken • ReleaseHandle • GetBCDInfo • SetParam • ReadSPI • SetTerminated • SendACK	Yes

DiodeDecode.dll	30.1.16.1	All sub-functions used to decode received packets and generate the specific file.Function includes: • SaveSlaveData • ProcessSlaveData • ClearAll • CreateEmpty	Yes
Diode Receiver (Windows Application)	1.0.107	• Tools used to receive data packets from MASTER SENDER. • Trace Log - Error<date>.log to take note of error - Diode<date>.log to display received filename list, summarize the total files received	Portable

Table 4 - ADD-GAP Hardware Picture with Casing

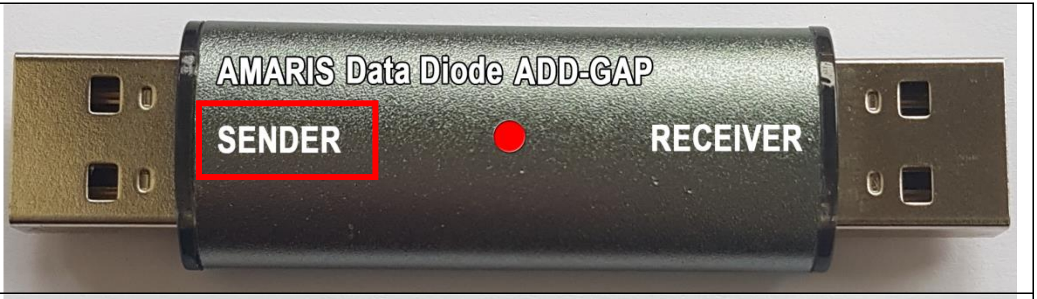
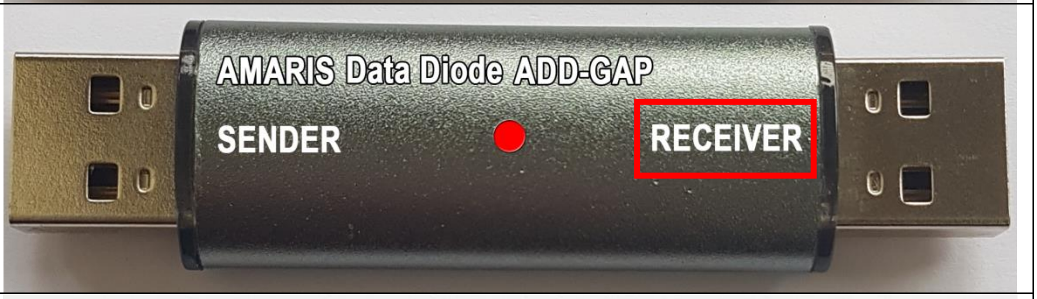
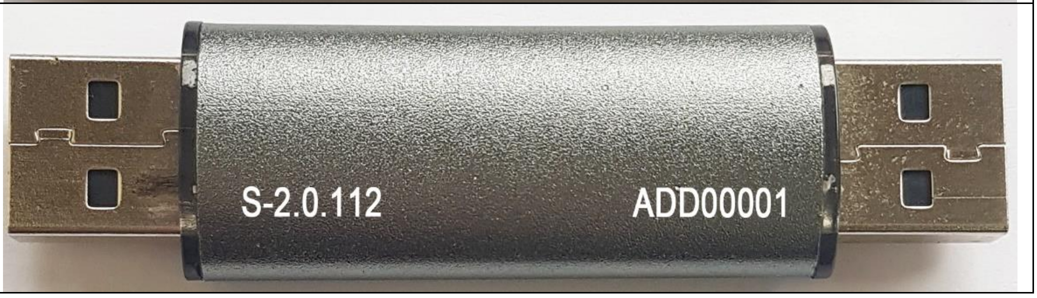
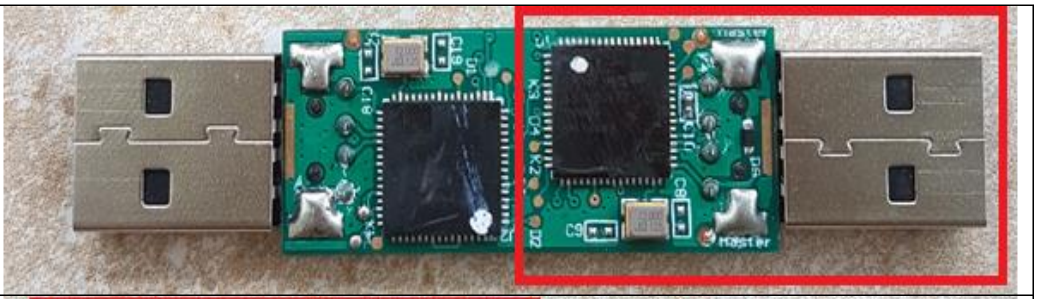
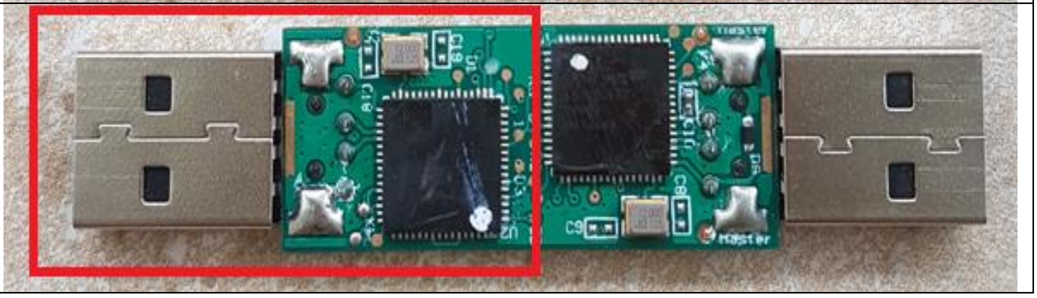
MASTER (Sender)	
SLAVE (Receiver)	
BACK	

Table 5 - ADD-GAP Hardware Picture without Casing

MASTER (Sender)	
SLAVE (Receiver)	

1.5 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

1.5.1 Usage and Major Security Feature of the TOE

Amaris Data Diode for Air Gap (ADD-GAP) is the product designed and manufactured by Advanced Product Design Sdn Bhd. This product 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.

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.

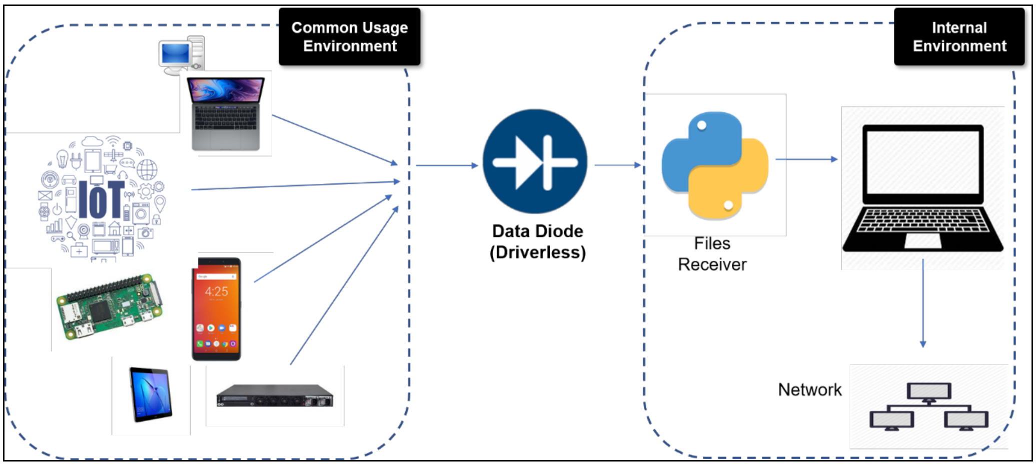


Figure 1 - ADD-GAP One-way unidirectional flow of data

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.

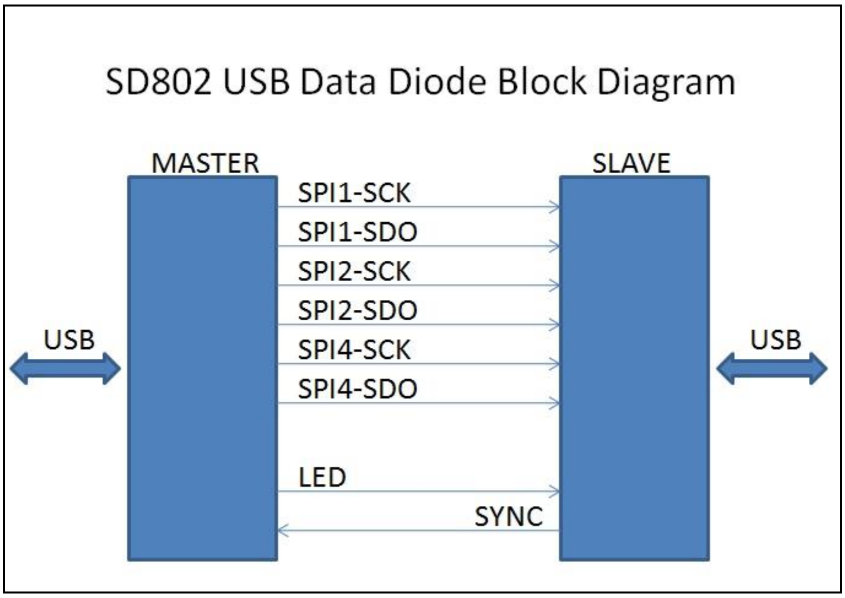


Figure 2 - TOE Block Diagram

- Master PC send data to Master controller
- Master controller sends data to slave through three SPI channels 1, 2 and 4.
- At the same time LED blinks on & off to signal data transfer.
- Slave receive data via three SPIs.
- Slave controller alert Slave PC that data is available.
- 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.

The ADD-GAP has two virtual drives, namely the MASTER drive (Sender-side) and the SLAVE drive (Receiver-side).

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.

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.

The major security feature of the TOE included in the evaluation is:

- One direction data transfer from one device to another device via USB

For more details, refer to Section Logical scope.

1.5.2 TOE Type

ADD-GAP is physical layer unidirectional USB data diode.

1.5.3 Non-TOE hardware/firmware/software required by the TOE

The following figure shows the typical operational environment of the TOE.

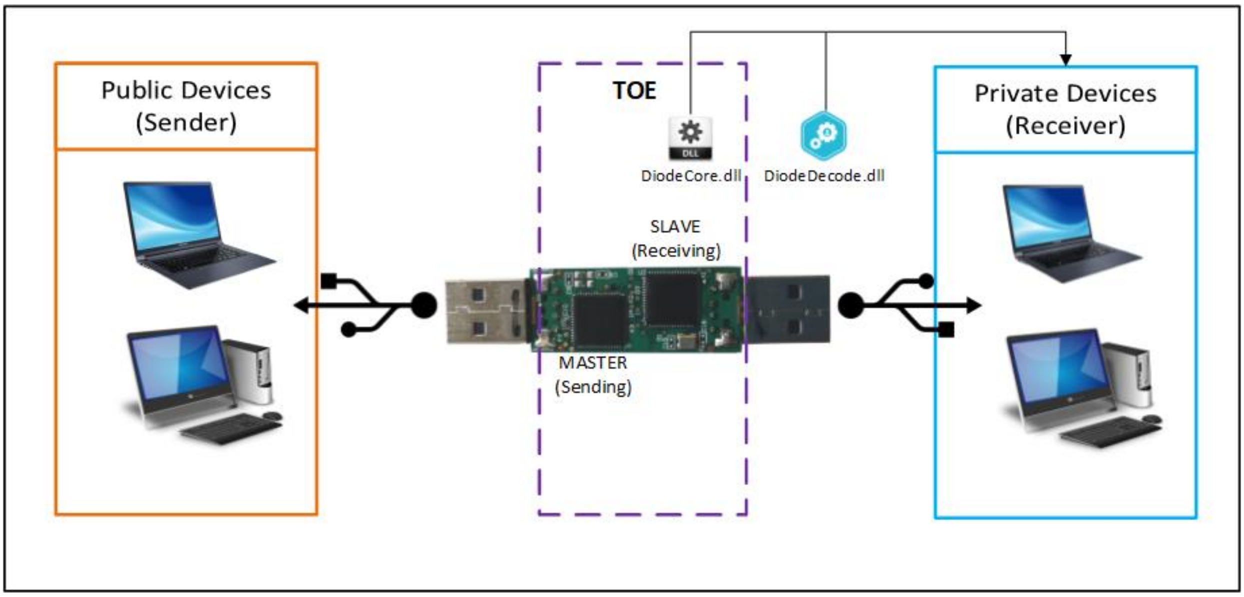


Figure 3 - TOE typical operational environment

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.

1.6 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.6.1 Physical Scope of the TOE

As illustrated in **Figure 3**, 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).

The guidance document is delivered together with the TOE on separate media support, in order to support the user in operating the TOE:

- Guidance documents
  - APD [ADD-GAP] Diode Receiver (DR) Software User Guideline-ver3.0
  - APD [ADD-GAP] Product Introduction-ver0.3

1.6.2 Logical Scope of the TOE

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

1.6.2.1 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.

1.6.2.1 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.

2 Conformance Claims

The following conformance claims are made for the TOE and ST:

CCv3.1 conformant	The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 5.
Part 2 conformant	The ST is Common Criteria Part 2 conformant.
Part 3 conformant	The ST is Common Criteria Part 3 conformant.
Package conformant	EAL 2.
Protection Profile conformance	None.

3 TOE Security Problem Definition

3.1 Assumption

The assumptions are to ensure the security of the TOE and its deployed environment.

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.

Table 6: Assumptions

3.2 Threats

This section describes the threats that are addressed by the TOE:

T.RCVDATALEAK	A user or process on the Private Device (Receiver) that accidentally or deliberately breaches the confidentiality of data by transmitting data through TOE to Public Device (Sender).
T.PHYTAMPER	An unauthorized personnel may attempt to peel or pry the physical protection (hard metal case and Epoxy Resins on the programming pin) of the TOE.

Table 7: Threats

3.3 Organizational Security Policies

There are no Organizational Security Policies that the TOE must comply to.

4 Security Objectives

Security objectives are formed to address the security problem definition defined in earlier section. The security implementation in TOE and its environment will meet these objectives.

4.1 Security Objectives for the TOE

The security objectives for the TOE as following:

O.ONEWAY	The TOE shall allow the data to flow from the Public Device (Sender) to the Private Device (Receiver) but not in the reverse direction i.e. Private Device to the Public Device.
O.PHYPROTECT	The TOE shall be covered with hard metal case from external and seal the programming pin on the PCB with Epoxy Resin.

Table 8: Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

The security objectives for the TOE operational environment as following:

OE.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 with the operating procedures stipulated in the user guidance.
OE.DATAFLOW	The information flow between Public Device (Sender) and Private Device (Receiver) shall pass through the TOE and there shall not be any other connectivity between Public Device (Sender)and Private Device (Receiver).

Table 9: Security Objectives for the Operational Environment

4.2.1 Security Objectives Rationale

Table 10 maps security objectives to threats and assumptions described in Section 4. The table illustrates that each threat is countered by at least one security objective, that each assumption is upheld by at least one security objective, and that each objective counters at least one threat or upholds at least one assumption.

Threats and Assumptions / Security Objectives	T.RCVDATALEAK	T.PHYTAMPER	A.USER	A.DATAFLOW
O.ONEWAY	✓			
O.PHYPROTECT		✓		
OE.USER	✓		✓	
OE.DATAFLOW	✓			✓

Table 10 - Security Objectives Rationale Mapping

5 Extended Components

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) applicable for the TOE.

5.1 Extended Security Functional Requirement (SFR)

There are no extended SFR components defined for this evaluation.

5.2 Extended Security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

6 TOE Security Requirements

This section provides the security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 Conventions

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

Assignment The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

Selection The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

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

Iteration The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing an acronym at the end of the component identifier as follows: FCS_COP.1 (SWP).

6.2 Security Functional Requirements (SFR)

This section contains the security functional requirements (SFRs) for the TOE. The summary of SFRs is listed in following table.

Component	Component Name
Class FDP: USER DATA PROTECTION	
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple Security Attributes
Class FPT: PROTECTION OF THE TSF	
FPT_PHP.1	Passive detection of physical attack

Table 11: Security Functional Requirements List

6.2.1 Class FDP: User Data Protection

FDP_IFC.2 Complete information flow control

Hierarchical FDP_IFC.1 Subset information flow control

Dependencies FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [**one-way data transmission via USB**] on [**any information from Public Device (Sender) to Private Device (Receiver) through the TOE**] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 Simple Security Attributes

Hierarchical No other components

Dependencies FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation[1]

FDP_IFF.1.1 The TSF shall enforce the [**one-way data transmission via USB**] based on the following types of subject and information security attributes: [

Subject: Public Device (Sender), Private Device (Receiver).

Information security attribute: Subject Identity[2]]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) **The TSF shall allow the data from Public Device (Sender) to flow to the Private Device (Receiver).**

b) **The TSF shall deny data from the Private Device (Receiver) to flow to Public Device (Sender).**

]

FDP_IFF.1.3 The TSF shall enforce the [**none**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**none**].

Application notes None

6.2.2 Class FPT: Protection of the TSF

FPT_PHP.1 Passive detection of physical attack

Hierarchical No other components

Dependencies No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

[1] FMT_MSA.3 is not applicable as there is no security attributes to initialise

[2] The subject identity is defined as the Public Device (Sender) and Private Device (Receiver)

6.3 Security Assurance Requirements

This ST claims compliance to the assurance requirements from the CC EAL2 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat and environment.

The following table summarized the TOE assurance requirements drawn from CC Part 3.

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

Table 12: Security Assurance Requirements for EAL2

7 TOE Summary Specifications

TOE addressed the security functional requirements as following:

7.1 User Data Protection

TOE shall enforce the Information flow control policy in transferring data from sender (MASTER) to receiver (SLAVE). The data need to be completely transferred from sender to receiver unidirectional via TOE.

TOE shall reset the USB storage (fake capacity) for Sender within 5 seconds once the data been completely transferred to the specified destination at receiver PC local storage.

Relevant SFR: FDP_IFC.2, FDP_IFF.1

7.2 Protection of the TSF

TOE shall provide 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.

Relevant SFR: FPT_PHP.1

8 Rationale

8.1 Protection Profile Conformance Claim Rationale

ST does not claim conformance to any Protection Profile. Hence, there are no elements to be covered in the conformance claim rationale.

8.2 Security Objectives Rationale

This section explains how threat, assumptions and OSP are related to each other. The following tables show threat, assumptions and organizational policy being mapped to security objectives.

8.2.1 Rationale of Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.RCVDATALEAK A user or process on the Private Device (Receiver) that accidentally or deliberately breaches the confidentiality of data by transmitting data through TOE to Public Device (Sender).	**O.ONEWAY** The TOE shall allow the data to flow from the Public Device (Sender) to the Private Device (Receiver) but not in the reverse direction i.e. Private Device to the Public Device.	This security objective counters threat because TOE shall prevent data leakage to be happened while transmitting data through TOE.
T.PHYTAMPER An unauthorized personnel may attempt to peel or pry the physical protection (hard metal case and Epoxy Resins on the programming pin) of the TOE.	**O.PHYPROTECT** The TOE shall be covered with hard metal case from external and seal the programming pin on the PCB with Epoxy Resin.	This security objective counters threat because TOE shall prevent physical tampering and access the internal physical components of TOE.

Table 13 - Rationale of Security Objectives Mapped to Threats

8.2.2 Rationale of Security Objectives Mapped to OSP

Not applicable since there is no OSP declared in ST.

8.2.3 Rationale of Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
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.	**OE.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 with the operating procedures stipulated in the user guidance.	This security objective upholds assumption because the users shall be non-hostile and follows guidance documentation accordingly; however, the user is not free from human error and mistakes.
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.	**OE.DATAFLOW** The information flow between Public Device (Sender) and Private Device (Receiver) shall pass through the TOE and there shall not be any other connectivity between Public Device (Sender) and Private Device (Receiver).	This security objective upholds assumption because the TOE shall provide only one-way direction (unidirectional) data transmission from sender to receiver.

Table 14 - Rationale of Security Objectives Mapped to Assumptions

8.3 Extended Security Functional Requirement Rationale

Not applicable since there is no Extended Security Functional Requirement (SFR) declared in ST.

8.4 Extended Security Assurance Requirement Rationale

Not applicable since there is no extended Security Assurance Requirement declared in ST.

8.5 Security Functional Requirements Rationale

This section provides the rationale of using SFRs to meet the security objectives for the TOE and justify the SFRs dependencies that have been satisfied or not satisfied.

8.5.1 Rationale for SFR Mapped to Security Objectives for TOE

Security Objectives	SFRs	Rationale
O.ONEWAY The TOE shall allow the data to flow from the Public Device (Sender) to the Private Device (Receiver) but not in the reverse direction i.e. Private Device to the Public Device.	FDP_IFC.2 FDP_IFF.1	This SFR requires the TOE to transmit the data in ONLY one direction (unidirectional) from sender to receiver. It traces back to this objective.
O.PHYPROTECT The TOE shall be covered with hard metal case from external and seal the programming pin on the PCB with Epoxy Resin.	FPT_PHP.1	This SFR requires the TOE to have feature to indicate when a TSF device or TSF element is subject to tampering. It traces back to this objective.

Table 15 - Rationale for SFR Mapped to Security Objectives for TOE

8.5.2 SFR Dependency Rationale

The following table provides a demonstration that all SFRs dependencies included in the ST have been satisfied.

SFR	Dependency	Dependency Met?	Justification
FDP_IFC.2	FDP_IFF.1	Yes	-
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Partially	FMT_MSA.3 is not applicable as there is no security attributes to initialise
FPT_PHP.1	-	Yes	-

Table 16 - SFR Dependencies