Certification Report

Version 1.0

23 March 2020

CSA_CC_19004

for

Fort Fox Hardware Data Diode
Version: FFHDD3_1 & FFHDD3_10

From

Fox Crypto B.V.

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	23 March 2020	Released

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is a Fort Fox Hardware Data Diode, Version: FFHDD3_1 and FFHDD3_10. The TOE has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

- Fort Fox Hardware Data Diode (FFHDD3_1 and FFHDD3_10)
- Fort Fox Hardware Data Diode FDDV3_MAN_FOX-CRYP_0001, Installation Manual, Fox Crypto B.V. User Guidance, v1.0, 2018.

The TOE is a unidirectional network that allows data to travel only in one direction. The one-way physical connection of the TOE allows for information to be transferred optically from a low security classified network (Low Security Level) to a higher security classified network (High Security Level).

The TOE comes in two versions (Version: FFHDD3_1 and FFHDD3_10) with the only difference being the transceiver model: 1 Gbps vs. 10 Gbps operating speed:

TOE Version	Model Number	Speed
FFHDD3_1	FDD1GI	1 Gbit/sec
FFHDD3_10	FDD10GI	10 Gbit/sec

The evaluation of the TOE has been carried out by Riscure, an approved CC test laboratory, at the assurance level CC EAL4+AVA_VAN.5 and completed on 6 January 2020. The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The Security Target [1] is the basis for this certification. It is not based on a certified Protection Profile.

The Security Assurance Requirements (SARs) are based entirely on the assurance components defined in Part 3 of the Common Criteria [2]. The TOE meets the assurance requirements of the Evaluation Assurance Level EAL4+AVA_VAN.5.

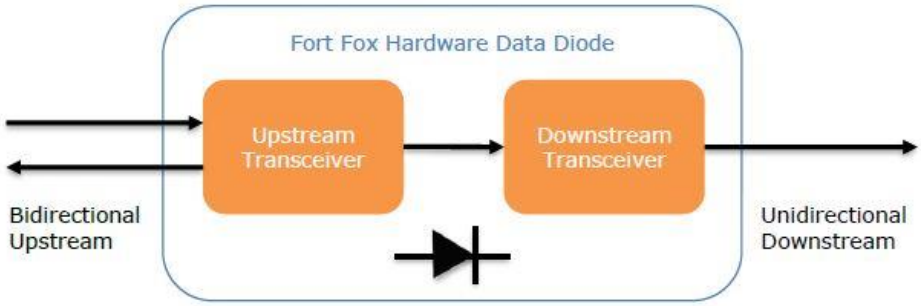
The Security Functional Requirements (SFRs) relevant for the TOE are outlined in Chapter 5 of the Security Target [1]. The Security Target claims conformance to CC Part 2 [3].

The SFRs are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed Issue
Unidirectional Network	Light signal sent via fibre optic cable from the Upstream (Sending) Network will flow

	through the Bidirectional Upstream Input port connecting to the Upstream Transceiver. The photocell within the Upstream Transceiver will convert the received light signal into electrical signal and the electrical signal will flow through the TOE, received by the Downstream (Receiving) Transceiver. The received electrical signal will be converted to light signal and flow to the Downstream Network via the Downstream Unidirectional output port. **The Unidirectional output port is incapable to convert light signal into electrical signal and therefore unidirectionality of the data transmission within the TOE is ensured**.

Table 1: TOE Security Functionalities



Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats, and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1].

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [4] [3] [2];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is covered partially by the CCRA for the components up to EAL2.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **22 March 2025**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: Fort Fox Hardware Data Diode (FFHDD)

Version: FFHDD3_1 and FFHDD3_10

The following table identifies the TOE deliverables.

Type	Name	Version
HW	Fort Fox Hardware Data Diode	FFHDD3_1 FFHDD3_10
DOC	FDDV3_MAN_FOX-CRYP_0001, Installation Manual, Fox Crypto B.V. User Guidance, 2018	Version 1.0

Table 2: Deliverables of the TOE

The guide for receipt and acceptance of the above mentioned TOE are described in the set of guidance documents.

Additional identification information relevant to this Certification procedure as follows:

TOE	Fort Fox Hardware Data Diode (FFHDD) Version FFHDD3_1 and FFHDD3_10
Security Target	Fort Fox Hardware Data Diode Security Target Version 3.04, 27 June 2018
Developer	Fox-IT BV
Sponsor	Fox-IT BV
Evaluation Facility	Riscure
Completion Date of Evaluation	6 January 2020
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_19004
Certificate Validity	5 years from date of issuance

Table 3: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to security functional class "User Data Protection".

Specific details concerning the above mentioned security policy can be found in Chapter 5 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Environmental Assumptions	Description
OE.PHYSICAL	The intended operational environment shall be capable of storing and operating the TOE in accordance with the highest of each of the requirements of the upstream side and of the downstream side.
OE.POWER	The intended operational environment shall provide power to the TOE such that the power to the TOE cannot be interfered with from the downstream network.
OE.NETWORK	The only method of interconnecting the upstream network and downstream network is one or more units of the TOE, where all of the units are operating in the same data flow direction.

Table 4: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to those claims made in the Security Target [1], comprising only the unidirectional data flow. The Operating System and software are outside the scope of the certification.

5.3 Evaluated Configuration

The TOE comes in two versions (Version: FFHDD3_1 and FFHDD3_10) with the only difference being the transceiver model: 1 Gbps vs. 10 Gbps operating speed:

TOE Version	Model Number	Speed
FFHDD3_1	FDD1GI	1 Gbit/sec
FFHDD3_10	FDD10GI	10 Gbit/sec

The evaluated configuration (as shown in Figure 1 below) is a hardware data diode that provides a unidirectional information flow from the Upstream network to the Downstream network.

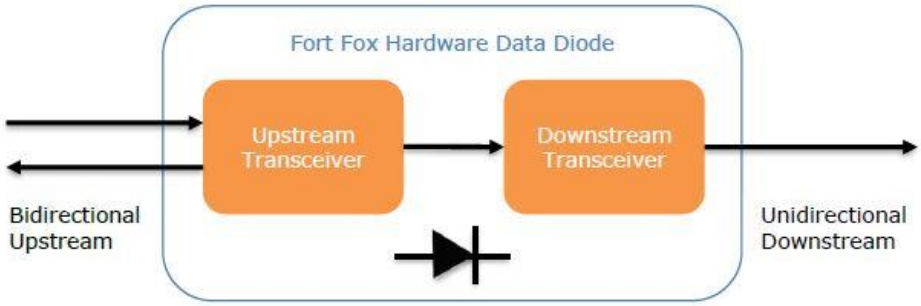


Figure 1: TOE Evaluated Configuration

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

5.5 Non-TOE Components

The TOE does not require additional components for its operation.

6 Architecture Design Information

The TOE is a Fort Fox Hardware Data Diode (version FFHDD3_1 and FFHDD3_10) network gateway that ensures physical layer one-way data transmission through the TOE.

The TOE only allows one-way flow of information from the Upstream Network to the Downstream Network, without compromising the confidentiality of the information on the Downstream Network. The reverse flow of data is not allowed as the TOE Receiver's transmitter port is being terminated. Fibre-optic cables are used to minimize the electromagnetic radiation when the TOE input port is connected to the Upstream Sever and the TOE output port is connected to the Downstream Server.

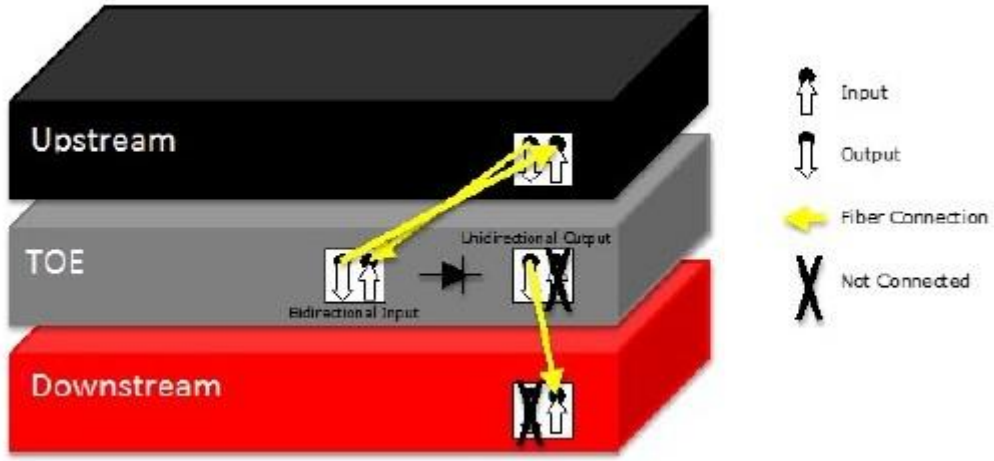


Figure 2: Fort Fox Hardware Data Diode Concept

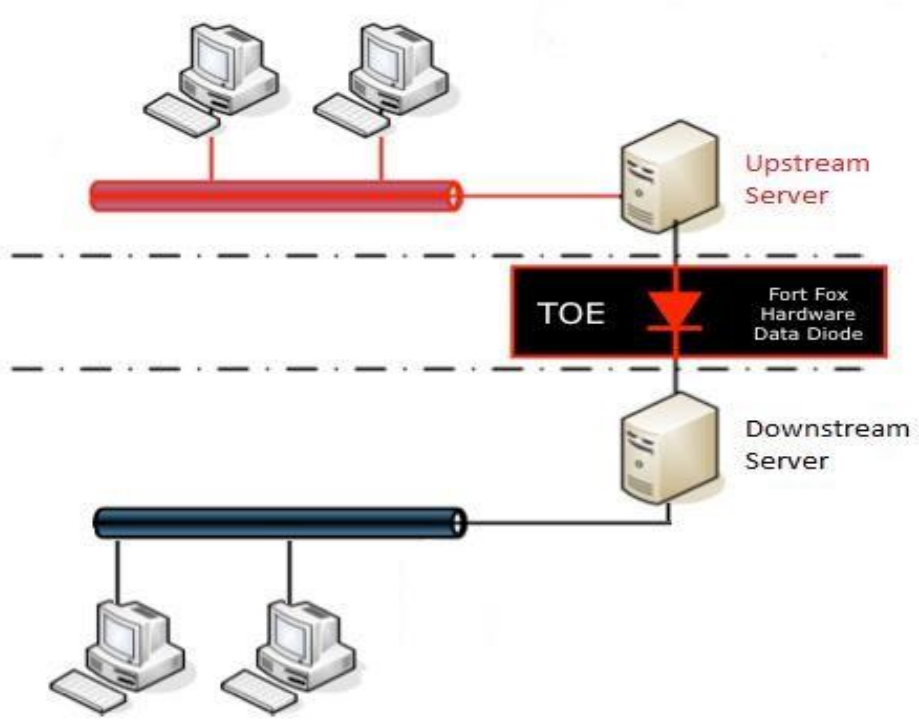


Figure 3: Fort Fox Hardware Data Diode Concept

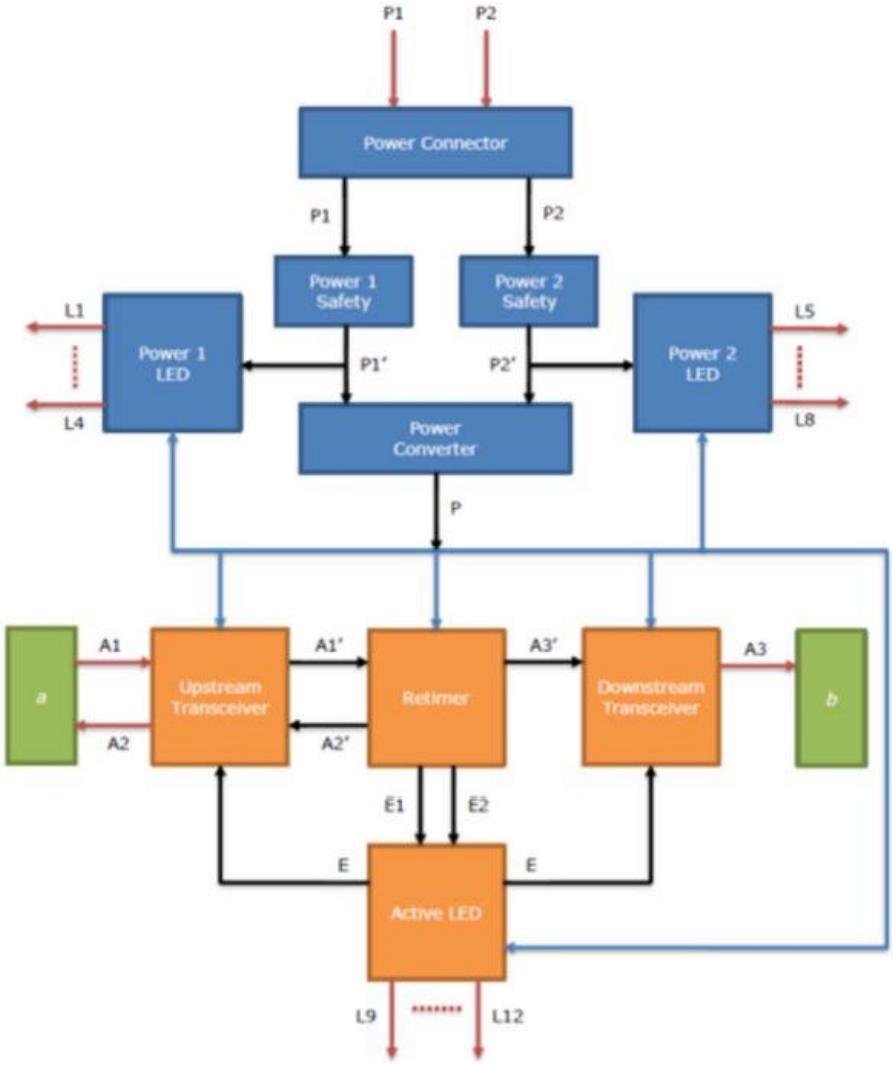


Figure 4: TOE Subsystem Extract

The TOE has two operational interfaces, the Bidirectional Input and Unidirectional Output port. Light received from the Bidirectional input is converted into electrical signal with the aid of a photocell at the Upstream Transceiver. The electrical signal spreads through the TOE to the Downstream Transceiver and gets converted into light using a light source. Light signal leaves the TOE via the Downstream Unidirectional Output port and to the Downstream Network.

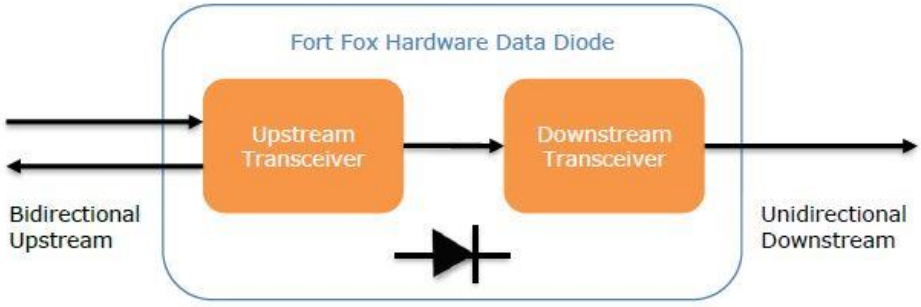


Figure 5: TOE Functional Block Diagram

The TOE setup allows data to flow from the Upstream Network passing through the TOE to the Downstream Network and the reverse flow is disallowed. The user from the Upstream Network is unable to extract data from the Downstream Network when sending a data from the Upstream Network to the Downstream Network.

Table 5: TOE Versions

Figure 6: Image of the TOE

Figure 7: 'Input' and 'Output' Interfaces, and Activity LEDs

The TOE consists of purely hardware, is not configurable and therefore is always in a permanently secure state.

7 Documentation

The evaluated documentation as listed in

Type	Name	Version
HW	Fort Fox Hardware Data Diode	FFHDD3_1 FFHDD3_10
DOC	FDDV3_MAN_FOX-CRYP_0001, Installation Manual, Fox Crypto B.V. User Guidance, 2018	Version 1.0

Table 2: Deliverables of the TOE is being provided with the product to the customer. These documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The developer performed testing only with the FFHDD3_10 model as the difference (transceiver operating speed 10Gpbs versus 1Gpbs) between the two versions are has no impact on the security of the TOE. The developer defined the test plans for numberous tests divided over 3 test scopes:

a. Design Scope to verify correct functionality according to the design rationale and functional specification
b. Unit Scope to verify each unit of the TOE for correct functionality under normal operating conditions
c. Batch Scope to verify correct functionality under abnormal conditions

8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [9].

8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluator analysed the developer's test coverage, test plans and procedures, expected and actual test results.

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.The evaluator decided to devise one additional test case for the TOE to determine the correct function of the power converter module.

8.2.2 Test Configuration

A detailed test description was provided in the ATE document. In summary, the test consists of measuring the internal 3.3V power output of the Power Converter while varying the input power.

8.2.3 Test Results

The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

The evaluator's additional test case verified that the power convertor only outputs 3.3V or 0V, and no other voltage levels.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the TOE and to demonstrate that the vulnerabilities were not exploitable in the intended environment of the TOE.

The general approach for the vulnerability analysis is based on the following:

- All applicable attack techniques known by the lab
- Analysis of the TOE deliverables (ARC, TDS, FSP, AGD, etc).
- Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices (although the TOE does not belong to the cartegory of a smartcard)

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL4+AVA_VAN.5 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in

Type	Name	Version
HW	Fort Fox Hardware Data Diode	FFHDD3_1 FFHDD3_10
DOC	FDDV3_MAN_FOX-CRYP_0001, Installation Manual, Fox Crypto B.V. User Guidance, 2018	Version 1.0

Table *2* contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

No additional recommendation was provided by the evaluators.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] Fox-IT BV., “Fort Fox Hardware Data Diode Security Target Version 3.04 June 27, 2018”.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[9] Fox Crypto B.V. , “FDDV3_MAN_FOX-CRYP_0001, Installation Manual, User Guidance, Version 1.0,” 2018.

----------End of Report ----------