Certification Report

Fort Fox Hardware Data Diode FFHDD3_1/10

Sponsor and developer: ***Fox Crypto B.V.***
Olaf Palmestraat 6
2616 LM Delft
The Netherlands

Evaluation facility:

Riscure B.V.
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-2300039-01-CR**
Report version:	**1**
Project number:	**NSCIB-2300039-01**
Author(s):	**Wim Ton**
Date:	**19 September 2023**
Number of pages:	**10**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, 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 or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Fort Fox Hardware Data Diode FFHDD3_1/10. The developer of the Fort Fox Hardware Data Diode FFHDD3_1/10 is Fox Crypto B.V. located in Delft, the Netherlands and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a unidirectional network, allowing data to travel only in one direction (data-diode).

The one-way physical connection of the TOE allows information to be transferred optically from one network (the upstream network) to another network (the downstream network). The unidirectionality of the data flow ensures the integrity of the upstream network against threats from the downstream network, and simultaneously ensures the confidentiality of the downstream network.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in the Installation manual chapters 4 and 7. As such it is vital that meticulous adherence to the user guidance of the TOE is maintained.

The TOE was previously evaluated by Riscure B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 2018-07-11 (CC-18-163925). The current evaluation of the TOE has also been conducted by Riscure B.V. and was completed on 2023-09-19 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The changes from previous evaluations are: updates in the documentation and the replacement of some mechanical and non-TSF electronic components.

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Fort Fox Hardware Data Diode FFHDD3_1/10, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Fort Fox Hardware Data Diode FFHDD3_1/10 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL7 augmented (EAL7+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (TOE summary specification with architectural design summary), and ALC_FLR.3 (Systematic flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific versions of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Fort Fox Hardware Data Diode FFHDD3_1/10 from Fox Crypto B.V. located in Delft, the Netherlands.

The TOE is evaluated in 2 versions:

Delivery item type	Identifier	Version
Hardware	Fort Fox Hardware Data Diode FDD1GI	FFHDD3_1
	Fort Fox Hardware Data Diode FDD10GI	FFHDD3_10

To ensure secure usage, a guidance document is provided, together with the Fort Fox Hardware Data Diode FFHDD3_1/10. For details, see section 2.4 “Documentation” of this report.

2.1 Security Policy

The TOE allows all data from an optical fibre network to travel from the physical “Upstream” interface to the physical “Downstream” interface.

The TOE does not allow any data from an optical fibre network to travel from the physical “Downstream” interface to the physical “Upstream” interface.

2.2 Assumptions and Clarification of Scope

2.2.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.2.2 Clarification of scope

The certificate covers 2 versions of the TOE, the Fort Fox Hardware Data Diode FFHDD3_1 and the Fort Fox Hardware Data Diode FFHDD3_10, for the sake of conciseness called Fort Fox Hardware Data Diode FFHDD3_1/10 in this evaluation. The only difference is the speed of the fibre optic transceivers: 1 GB/s or 10 GB/s.

2.3 Architectural Information

The TOE operates on the physical layer of the Open System Interconnection (OSI) reference model. This ensures demonstrable complete unidirectionality.

The TOE has two operational interfaces to establish one-way communication, the Bidirectional Upstream port and Unidirectional Downstream port. At the upstream receiver light is carried into the Bidirectional Upstream port and converted, with the aid of a photodiode, into an electrical signal. The electrical signal is connected inside the TOE to the downstream transmitter. The downstream transmitter receives the electrical signal and converts this, using a light source, into light. Finally, the light is offered, through the Unidirectional Downstream port, to the downstream network. The Unidirectional Downstream port is incapable of input and therefore lacks the ability of converting light into an electrical signal. Furthermore, the electrical signal from the downstream receiver is not connected and therefore incapable to create a covert channel.

Fibre optics is used to transport signals from and to the Bidirectional Upstream port, and from the Unidirectional Downstream port. Electrical signals only transport signals inside the TOE, which is completely enclosed by an aluminium casing.

The TOE does not contain any software.

Unidirectional communication does not work with a network protocol that requires a handshake (acknowledgement). To establish a communication link between the upstream side and the upstream transceiver, a Bidirectional Upstream port is initiated. Data, information, or communication originating at the downstream side is physically unable to flow to the Bidirectional Upstream port via the TOE, therefore there is no back channel which could be used as a covert channel. Any network protocol could be used to implement the communication if no handshaking across the TOE is required, e.g., the User Datagram Protocol (UDP) can provide a unidirectional flow of information.

2.4 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Installation Manual	1.3

2.5 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.5.1 Testing approach and depth

For the testing performed by the evaluators, the developer provided samples. The evaluators reproduced a selection of the developer tests.

2.5.2 Independent penetration testing

The evaluators verified that no signal from the downstream network can reach the other interfaces of the TOE. Both hardware versions were tested.

The total test effort expended by the evaluators was 10 days. During that test campaign, 100% of the total time was spent on Perturbation attacks.

2.5.3 Test configuration

The evaluators used a 2 port Vector Network Analyzer to measure the attenuation of a signal from the downstream receiver to the internal and external power-supply interfaces.

2.5.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

2.6 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Fort Fox Hardware Data Diode FFHDD3_1/10. Both hardware versions are evaluated. Chapter 4 of the installation manual describes the process to verify the integrity of the TOE.

2.8 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. The development site and the production site were audited for this evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Fort Fox Hardware Data Diode FFHDD3_1/10, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 7 augmented with ASE_TSS.2 and ALC_FLR.3**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.4 "Documentation" contains necessary information about the usage of the TOE.

This TOE is critically dependent on delivery process as described in [IM] chapter 4 and on the operational environment as described in the *[ST]* chapter 4.2 to provide countermeasures against specific attacks. Therefore, it is vital to maintain meticulous adherence to the user guidance of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The TOE does not contain any cryptographic functionality.

3 Security Target

The Fort Fox Hardware Data Diode Security Target, Version 3.3, 7 August 2023 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report for Fort Fox Hardware Data Diode FFHDD3_1/10, 20220141-D, 1.2, 19 Sep 2023
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Fort Fox Hardware Data Diode Security Target, Version 3.3, 7 August 2023
[IM]	Installation Manual for the Fox Data Diode version 3 Rackmount Products FDDv3, FDDV3_MAN_FOX-CRYP_0001, Version 1.3, 8 March 2023

(This is the end of this report.)