Certification Report

Fort Fox Hardware Data Diode FFHDD3_1/10

Sponsor and developer:	***Fox Crypto B.V.*** **Olof Palmestraat 6** **2616 LM Delft** **The Netherlands**
Evaluation facility:	***Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-163925-CR**
Report version:	**1**
Project number:	**163925**
Author(s):	**Twan van der Schoot**
Date:	**11 July 2018**
Number of pages:	**11**
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-18-163925**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Fox Crypto B.V.** **Olof Palmestraat 6, 2616 LM Delft, The Netherlands**
Product and assurance level	**Fort Fox Hardware Data Diode FFHDD3_1/10** Assurance Package: ▪ EAL7 augmented with ASE_TSS.2 and ALC_FLR.3
Project number	**163925**
Evaluation facility	**Riscure B.V. located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of 1st issue : **11-07-2018** Certificate expiry : **11-07-2023**

PRODUCTS RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license 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, TÜV Rheinland Nederland 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, 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 or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

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

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.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 Target of Evaluation – TOE (i.e., Fort Fox Hardware Data Diode FFHDD3_1/10) is a hardware-only device that allows data to travel only in one direction. The purpose of the TOE is to allow information to be transferred optically from one network (the upstream network) to another network (the downstream network). The unidirectional data flow ensures the integrity of the upstream network against threats from the downstream network, and simultaneously ensures the confidentiality of the downstream network.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 11-07-2018 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 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 it 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]*.

TÜV Rheinland Nederland 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. It should be noted that the certification results only apply to the specific version of the product as evaluated.

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

2 Certification Results

2.1 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 a single hardware unit:

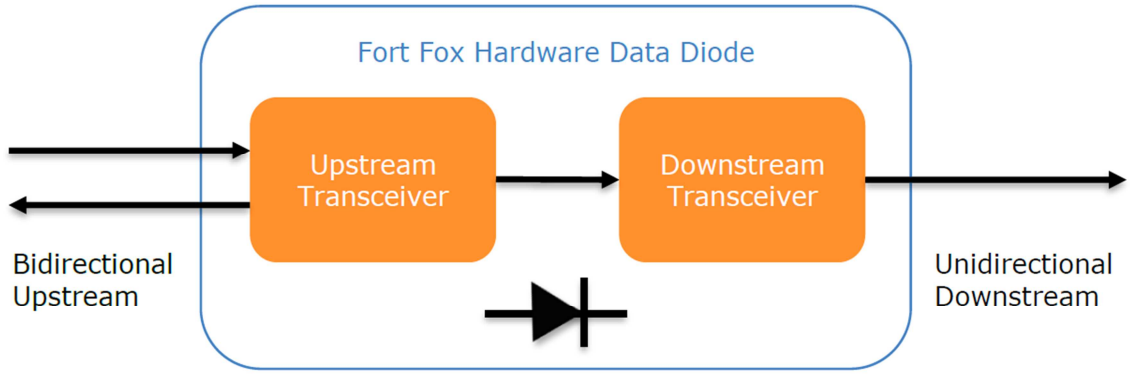
Delivery item type	Identifier	Version	Model number
Hardware (metal enclosure containing PCB with electronic components)	Fort Fox Hardware Data Diode	FFHDD3_1	FDD1GI
		FFHDD3_10	FDD10GI

The TOE is assembled, tested and packaged for delivery to Fox Crypto B.V. by TBP Electronics in Dirksland, The Netherlands. Before the TOE is packaged and dispatched to Fox Crypto B.V. a Fox Crypto B.V. employee performs several tests visual as well as electronic tests at the site of TBP Electronics. When the TOE arrives at Fox Crypto B.V. visual checks are performed on the integrity of the packaging and documentation, as well as functional testing.

To ensure secure usage a set of guidance documents is provided together with the Fort Fox Hardware Data Diode FFHDD3_1/10. Details can be found in section 2.5 of this report.

2.2 Security Policy

The TOE is a hardware data diode that 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. Once manufactured, there is no way to alter the function of the TOE.



2.3 Assumptions and Clarification of Scope

2.3.1 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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

There are no defined threats for the TOE that require additional measures in the environment; they are all met by the TOE. The Security Target *[ST]* assumes an operational environment such that threats

could come only from the attached networks. The evaluation did not reveal any functionality in the TOE that was excluded from the TOE evaluated configuration.

2.4 Architectural Information

The Target of Evaluation (TOE) consists of a single hardware unit, see figure 1. The TOE Fort Fox Hardware Data Diode is a unidirectional network and only allows data to flow in one direction. 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. To ensure signals can only pass in one direction, and not vice versa, the TOE deploys a single light source as the only connection to the downstream network. Fiber-optic cables are used to connect the TOE to both the upstream and downstream networks in order to minimize electromagnetic coupling. Physical restrictions on the environment ensure that the unidirectionality of the dataflow cannot be bypassed.

Figure 1: The TOE as a single hardware unit

The system design decomposes the TOE in two subsystems, "Power" and "Data Diode", as presented in blue and orange in Figure 2. In this diagram, the four TSFIs of the system are visible: power, LEDs, Upstream and Downstream. The security function is implemented by the Downstream interface in the Data Diode subsystem. There is no electrical path for the Downstream interface to present data to the Upstream interface.

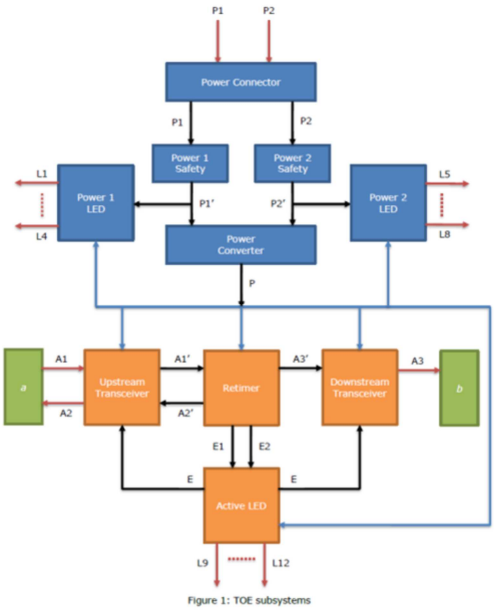


Figure 2: TOE subsystems extract

The TOE protects itself against interference and logical tampering by:

- Consisting of hardware only with no memory, settings, or other parameters that can be changed.
- Having only two interfaces that are accessible to attackers, which allow only very limited interaction:
    - The upstream interface: the TOE passes through all data received here without interpreting this data;
    - The downstream interface: the TOE ignores all data received here so that even if there were memory, settings or other parameters that could be changed in the TOE, there would be no way to tamper or interfere with these settings.

The TOE protects itself against bypass by ensuring that all data flows must pass through a single SFR-enforcing component (which is the first component encountered from the downstream interface), thus preventing bypass “through” the TOE.

2.5 Documentation

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

Identifier	Version
Installation Manual for the Fox Data Diode version 3 Rackmount Products FDDv3-1r-F and FDDv3-10r-F	2018-06-27, V1.0 Final

2.6 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.

2.6.1 Testing approach and depth

The developer defined three test scopes "Design Scope", "Unit Scope" and "Batch" scope:

- The "Design Scope" tests are applied to verify the correct functioning according to design rationale and functional specification.
- The "Unit Scope" tests are applied to each manufactured unit and confirm TOE integrity and function.
- The "Batch Scope" tests are applied to samples of manufactured batches, and verify correct functionality under abnormal operating conditions.

The evaluator confirmed that the developer is testing all TSF and related security mechanisms, subsystems and modules in order to assure complete coverage of all SFR.

Amount of testing performed by the developer:

- The tests are performed on security mechanisms and on subsystem and module level.
- As demonstrated by ATE_COV.3 the developer has tested all security mechanisms and TSFIs.
- As demonstrated by ATE_DPT.4 the developer has tested all the TSF subsystems and modules against the TOE design and against the security architecture description.

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 independent testing includes one evaluator test, to determine the correct function of the power converter module.

2.6.2 Independent Penetration Testing

At the start of the test the TOE is identified by means of visual inspection of the internal components and comparison to the implementation representation.

The evaluator independent penetration tests were conducted according to the following testing approach:

- During evaluation of the ADV, ATE and ALC classes the evaluators have not identified potential vulnerabilities.
  The analysis in AVA used the design knowledge gained in particular from the analysis in ADV_IMP.
- Next, the evaluator analysed the TOE design and implementation for resistance against all known attack techniques, similar to what is found in *[JIL-AM]* although the TOE is clearly not a smart card or similar device. This resulted in one potential vulnerability to be tested.
- The evaluator made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis in ADV_ARC has assessed all information.

2.6.3 Test Configuration

The evaluator has used a test setup and tools described in Appendix A.1 Test environment configurations of the *[ETR]*.

There are two variants of the TOE, which differ only in the maximum transfer rate. There are no tests defined in the vulnerability analysis AVA_VAN, or independent testing ATE_IND, where test results would depend on the TOE variant.

2.6.4 Testing 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.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Fort Fox Hardware Data Diode FFHDD3_1/10. The TOE is marked by a *model number* corresponding to the TOE name and version as documented in table 1 TOE Versions in section 1.4.2 of the *[ST]*.

The developer issues with each TOE a *user installation manual [UM]* providing the customer with detailed instructions on how to assess the integrity of the TOE upon delivery.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references an ASE Intermediate Report and other evaluator documents

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 conformant, 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 the Security Target *[ST]*.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 *[UM]* contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance 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 need to be fulfilled by the operational environment of the TOE.

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

The customer or user of the product shall consider the results of the certification within his system risk management process. In order 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.

It should be noted that the TOE can be delivered to the customer already mounted in a single unit 19”-rack mount. This configuration still allows the customer to verify the integrity of the TOE upon delivery as per the installation instructions provided by the developer.

3 Security Target

The Fort Fox Hardware Data Diode Security Target, version 3.04, 2018-06-27 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms 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 Fort Fox Hardware Data Diode FFHDD3_1/10, version 1.1, 2018-07-10.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.
[ST]	Fort Fox Hardware Data Diode Security Target, version 3.04, 2018-06-27.
[JIL-AM]	Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013.
[UM]	Fox Crypto B.V., Installation Manual for the Fox Data Diode version 3 Rackmount Products FDDv3-1r-F and FDDv3-10r-F, version 1.0.

(This is the end of this report).