TNO CERTIFICATION

Date
June 16, 2010

Reference
NSCIB-CC-09-11025-CR2

Subject

Project number
11025

NSCIB-CC-09-11025

Certification Report

Fort Fox Hardware Data Diode, version FFHDD2+

TNO CERTIFICATION

TNO CERTIFICATION
HEREBY DECLARES THAT EVALUATION
HAS DEMONSTRATED THAT THE PRODUCT

Fort Fox Hardware Data Diode, version FFHDD2+,
Assurance Package: EAL7 augmented with ALC_FLR.3 and
ASE_TSS.2

Product and version

FROM

Fox-IT BV located in Delft, the Netherlands

Sponsor's name and address

COMPLIES WITH THE

Common Criteria for Information Technology Security
Evaluation (CC), Version 3.1 Revision 2

Certification guidelines or standards

AS DEMONSTRATED BY / EVALUATION PERFORMED BY

Brightsight BV located in Delft, the Netherlands

Testing Laboratory

APPLYING THE

Common Methodology for Information Technology
Security Evaluation (CEM), Version 3.1 Revision 2

NSCIB-CC-09-11025-CR2

Certification Report number

THE CERTIFICATE HAS BEEN ISSUED ON

September 7, 2009

1st Issue Date

June 16, 2010

Revision Date

September 7, 2019

Expiry Date

ISSUED IN: Apeldoorn, the Netherlands

DIRECTOR TNO CERTIFICATION

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 2 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 2. 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 TNO Certification or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Table of contents

Document Information

Date of issue	16 June 2010
Author	R.T.M. Huisman
Version of report	2
Certification ID	NSCIB-CC-09-11025
Sponsor and Developer	Fox-IT BV
Evaluation Lab	Brightsight BV
TOE name	Fort Fox Hardware Data Diode, version FFHDD2+
Report title	Certification Report
Report reference name	NSCIB-CC-09-11025-CR2

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, TNO Certification has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations in the Netherlands are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TNO Certification 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 TNO Certification 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, TNO Certification 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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European Recognition Agreement approved by the SOG-IS in April 1999 provides mutual recognition of ITSEC and Common Criteria certificates for all evaluation levels (E6, resp. EAL7). This agreement was originally signed by Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Fort Fox Hardware Data Diode, version FFHDD2+. The developer of the FFHDD2+ is Fox-IT BV 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 FFHDD2+ is evaluated on the assurance level EAL7+ and builds on the evaluation results of the recently performed evaluation of the Fort Fox Hardware Data Diode, version FFHDD2. This previous version was certified on September 7th 2009 on the assurance level EAL4+ under the same certification identifier NSCIB-09-11025 with an certification report identified as 'version 1'. Version FFHDD2+ of the TOE is identical to the previous version FFHDD2 except for the addition of a new front panel and the guidance documentation describing this additional front panel. The original certification report NSCIB-CC-09-11025 version 1 has now been extended to cover the Fort Fox Hardware Data Diode, version FFHDD2+ as described in this document, certification report NSCIB-CC-09-11025 version 2.

The Target of Evaluation – TOE (i.e., Fort Fox Hardware Data Diode) is a hardware-only device that allows data to travel only in one direction. The intention of is to let information be transferred optically from a low security classified network (Low Security Level) to a higher security classified network (High Security Level), without compromising the confidentiality of the information on the High Security Level. Once manufactured, there is no way to alter the function of the TOE.

The TOE has been re-evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 10 June 2010. The evaluation builds upon the EAL4+ evaluation that was completed on 21 August 2009 as described in version 1 of this Certification Report. 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 certification was completed on 16 June 2010 with the preparation of version 2 of this Certification Report.

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, 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 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 Evaluation Assurance Level (EAL) 7 assurance requirements augmented with ALC_FLR.3 and ASE_TSS.2 for the evaluated security functionality. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 2 *[CC]*.

TNO Certification, as the NSCIB Certification Body, declares that the Fort Fox Hardware Data Diode, version FFHDD2+ 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 Assurance Level (EAL) 7 augmented with ALC_FLR.3 and ASE_TSS.2 evaluation is the Fort Fox Hardware Data Diode, version FFHDD2+ from Fox-IT BV located in Delft, the Netherlands.

This report pertains to the TOE comprised of the following main component:

Item	Identifier	Version	Medium
Hardware	Fort Fox Hardware Data Diode	FFHDD2+	single 19-inch rack component

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

2.2 Security Policy

The TOE is the Fort Fox Hardware Data Diode (FFHDD) and allows data to travel only in one direction. The intention of is to let information be transferred optically from a low security classified network (Low Security Level) to a higher security classified network (High Security Level), without compromising the confidentiality of the information on the High Security Level. Once manufactured, there is no way to alter the function of the TOE.
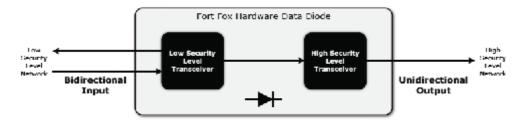

Figure 1, Overview of the TOE.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

There are no usage assumptions identified in the Security Target that are of relevance to the TOE.

2.3.2 Environmental assumptions

The following assumptions about the environmental aspects defined by the Security Target have to be met (for the detailed and precise definition of the assumptions refer to the *[ST]*, chapter 3.3):

Ø The intended operation environment shall store and operate the TOE in accordance with the requirements of the High Security Level side.

Ø The TOE is the only method of interconnecting the Low Security Level network and High Security Level network. This prevents a threat agent from circumventing the security being provided by the TOE through an untrustworthy product.

2.3.3 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 TOE is a single 19" rack component, a hardware-only device. To ensure signals can only pass in one direction, but not vice versa, the TOE deploys a light source and corresponding photocell. The data transfer is implemented in hardware, of the physical Open System Interconnection (OSI) reference model, to guarantee complete unidirectionality. Fiber-optic cables are used to minimize the electromagnetic radiation when the TOE input is connected to the Low Security Level Server and the TOE output is connected to the High Security Level Server.

The TOE has two operational interfaces to establish one-way communication, the Bidirectional Input and Unidirectional Output port. At the Low Security Level Transceiver light is carried into the Bidirectional Input port and converted, with the aid of a photocell, into an electrical signal. The electrical signal spreads through the TOE to the High Security Level Transceiver. The High Security Level Transceiver receives the electrical signal and converts this, using a light source, into light. Finally, the light is offered, through the Unidirectional Output port, to the High Security Level Network.

Figure 2 The TOE

Figure 3 Three variants for the front panels of the TOE

2.5 Documentation

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

Identifier	Version
Fox-IT BV, FFHDD, Delivery Procedures, Preparative Procedures and Operational User Guidance, CC EAL7+	2.02, June 3, 2010

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

The evaluator has tested all interfaces of the TOE and tested all six tests defined by the developer. In addition four tests are defined to extend the rigor of testing done by the developer.

Before these tests were conducted it was verified that the TOE was suitable for testing and has a unique reference number as identified in the ST introduction.

2.6.2 Test Configuration

The test configuration for the independent testing comprised of two configurations. The non-TOE servers for the High Security Level side and Low Security Level side were included in both test setups.

Ø   Test configuration 1 was the configuration as delivered to a customer and was used for testing the external interfaces for all TSFI.

Ø   Test configuration 2 was using an additional Fort Fox Hardware Data Diode of which the output side was connected to the output of the TOE. This setup was used to test the interfaces of the SFR-enforcing module.

2.6.3 Depth

For this evaluation, the depth of testing relates to the TSF modules and the SFR-enforcing module in the TOE design. The TOE Design defines two simple sets of modules for the TOE. The first set concerns the power supply; the second concerns the data diode.

All modules are SFR-supporting, except for one security-enforcing module in the data diode set of modules and this module has been tested.

In one of the tests it is checked that all the components in the design documentation are indeed implemented in FFHDD2+. In this test the implementation representation is tested exhaustively.

2.6.4 Independent Penetration Testing

The evaluators considered the following possible attacks:

1.   Attack from the low security level network trying to compromise the TOE such that it passes information through from the high security level network;

2.   Attack from the high security level network trying to compromise the TOE such that it passes information through from the high security level network;

3.   Attack from bystanders by the TOE to eavesdrop information passing through the TOE;

4.   Trying to cause TOE failure such that the TOE comes in a state that it passes information through from the high security level to the low security level.

The TOE design shows that one electronic component is essential in the realisation of ensuring that signals can only pass in one direction, and not vice versa. The evaluators have chosen to test the resistance of the TOE against the introduction of light signals at the Output port. If these signals would pass through the TOE, they could influence the signals as emitted by the bi-directional Input. This

attack relates to the possible attacks 1, 3 and 4 listed above. Attack 2 is out of scope due to the objectives of the environment.

2.6.5 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. No residual vulnerabilities were found.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Fort Fox Hardware Data Diode, version FFHDD2+ and can be identified by its identification at the backside.

The TOE needs no specific configuration settings because there is only one configuration defined.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* [2] which references several Intermediate Reports. The verdict of each claimed assurance requirement is given in the following table:

Security Target		Pass

Development		Pass
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.6	Pass
Implementation representation	ADV_IMP.2	Pass
Internals	ADV_INT.3	Pass
Security Policy Model	ADV_SPM.1	Pass
TOE design	ADV_TDS.6	Pass

Guidance documents		Pass
Operational	AGD_OPE.1	Pass
Preparative	AGD_PRE.1	Pass

Life cycle support		Pass
Configuration Management Capabilities	ALC_CMC.5	Pass
Configuration Management Scope	ALC_CMS.5	Pass
Delivery	ALC_DEL.1	Pass
Development Security	ALC_DVS.2	Pass
Flaw remediation	ALC_FLR.3	Pass

---

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

| Lifecycle definition | ALC_DEL.2 | Pass |
| Tools and Techniques | ALC_TAT.3 | Pass |

Tests		**Pass**
Coverage	ATE_COV.3	Pass
Depth	ATE_DPT.4	Pass
Functional	ATE_FUN.2	Pass
Independent	ATE_IND.3	Pass

Vulnerability assessment		**Pass**
Vulnerability analysis	AVA_VAN.5	Pass

Based on the above evaluation results the evaluation lab concluded the Fort Fox Hardware Data Diode, version FFHDD2+, to be **CC Part 2 conformant**, **CC Part 3 conformant**, and to meet the requirements of **EAL 7 augmented with ALC_FLR.3 and ASE_TSS.2**. This implies that the product satisfies the security technical requirements specified in Security Target FFHDD, CC EAL7+, version 2.04, June 3, 2010. The Security Target does not claim conformance to any Protection Profile.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

Based on the insights gained during the evaluation the evaluator recommends for the protection of configuration items at Fox-IT to extend the current anti-virus measures in a similar way to non-Windows platforms.

2.9.2 Recommendations and hints for the customer

The TOE is normally delivered together with the two servers. These servers are connected to the network that the TOE connects. These servers are not considered during the evaluation.

3 Security Target

The Security Target FFHDD, CC EAL7+, version 2.04, June 3, 2010 is included here by reference. Please note that for the need of publication a public version has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

CC	Common Criteria
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PP	Protection Profile
TNO	Netherlands Organization for Applied Scientific Research
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, Part I version 3.1 revision 1, and Parts II and III, version 3.1 revision 2.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 2, September 2007
[ETR]	Evaluation Technical Report, Fort Fox Hardware Data Diode FFHDD2+ - EAL7+, Version 2.0, June 10, 2010.
[NSCIB]	Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.
[ST]	Fox-IT BV, FFHDD, Security Target, CC EAL7+, version 2.04, June 3, 2010.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.