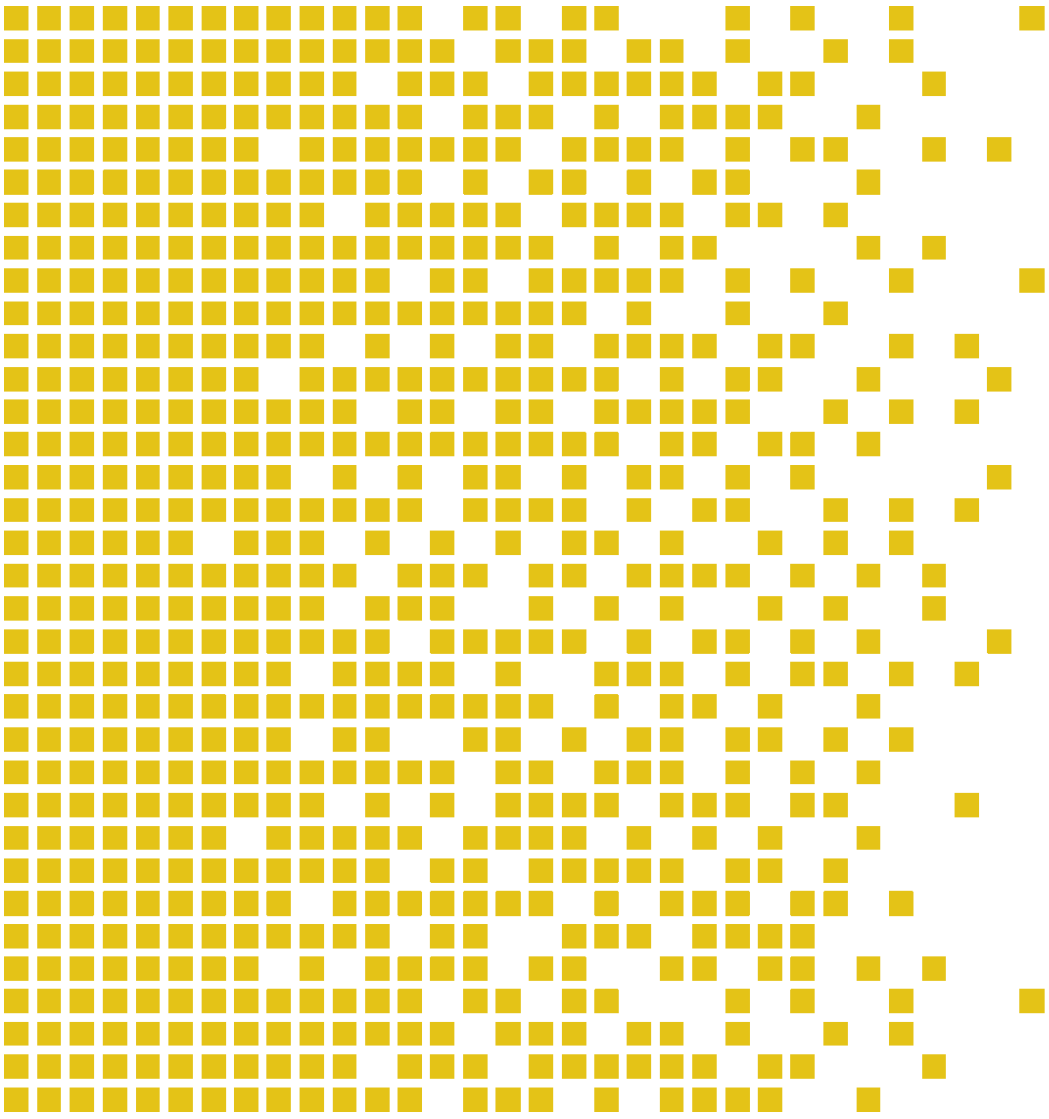
SERTIT-014 CR Certification Report

Issue 1.0 3 March 2010

Fort Fox Hardware Data Diode FFHDD2



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

* Mutual Recognition under the CC recognition arrangement applies to EAL 4 but not to AVA_VAN.5 and ALC_DVS.2.

Contents

1 Certification Statement

Fox-IT BV Fort Fox Hardware Data Diode (FFHDD) is a unidirectional network allowing data to travel only in one direction.

Fort Fox Hardware Data Diode (FFHDD) version FFHDD2 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL 4+ (AVA_VAN.5 and ALC_DVS.2) for the specified Common Criteria Part 2 conformant functionality in the specified environment as described in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	3 March 2010

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
FFHDD	Fort Fox Hardware Data Diode
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT/ITSEF	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
OSP	Organisational Security Policy
OSI	Open System Interconnection
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF interfaces
TSP	TOE Security Policy

3 References

[1] Security Target, Fox-IT BV, Fort Fox Hardware Data Diode security target, version 1.07 public, January 29, 2009.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 7.0, 28 March 2008.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1, July 2009.

[7] Evaluation Technical Report Common Criteria EAL4+ Evaluation of Fort Fox Hardware Data Diode FFHDD2, 20100128, ed. 3.0.

[8] Fox-IT BV, FFHDD, Delivery Procedure, Preparative Procedure and Operational User Guidance, CC EAL4+, Version 1.04, May 7, 2009

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Fort Fox Hardware Data Diode (FFHDD) version FFHDD2 to the Sponsor, Fox-IT BV, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was Fort Fox Hardware Data Diode (FFHDD), version FFHDD2.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Fox-IT BV.

The TOE is the Fort Fox Hardware Data Diode (FFHDD). The TOE 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.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The scope of the TOE is described in the ST[1], chapter 1.4.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 4 augmented with AVA_VAN.5 and ALC_DVS.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats, OSP's and assumptions which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

A user or process on the High Security Level network that accidentally or deliberately breaches the confidentiality of some High Security Level information by transmitting data through the TOE to the Low Security Level network.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

The following assumptions are assumed to exist in the environment:

- The intended operation environment shall store and operate the TOE in accordance with the requirements of the High Security Level side.
- The TOE is the only method of interconnecting the Low Security Level network and High Security Level network.

4.12 IT Security Objectives

- The information on the High Security Level side destination is kept confidential from the Low Security Level source.

4.13 Non-IT Security Objectives

- The intended operation environment shall be capable of storing and operating the TOE in accordance with the requirements of the High Security Level side.
- The TOE is the only method of interconnecting the Low Security Level network and High Security Level network.

4.14 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- Complete Information Flow Control FDP_IFC.2
- Simple Security Attributes FDP_IFF.1

4.15 Security Function Policy

The TOE's information flow security function policy is defined in FDP_IFC.2 and FDP_IFF.1.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight BV Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 20100128. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 4 assurance package augmented with AVA_VAN.5 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
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
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

Delivery procedures for the TOE are described in the developer's delivery procedure[8].

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in Fox-IT BV, FFHDD, Delivery Procedure, Preparative Procedure and Operational User Guidance[8].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Administrators should follow the guidance [8] for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively administer and use the TOE's security functions.

5.5 Vulnerability Analysis

The evaluators' assessments of potential exploitable vulnerabilities in the TOE have been addressed, and the TOE in its intended environment should be resistant to attackers with a high attack potential.

The TSF is resistant against known attacks at the given time of evaluation, but this could change in the future as attack techniques become more sophisticated.

5.6 Developer's Tests

The testing results from the developer show that the TOE exhibits the expected behaviour at TSFI and SFR enforcing module level. The developers test specification are directly linked to its corresponding functional specification, and passing one test shows that that specific functional specification works according to the documentation.

The depth and coverage analysis shows that the developers' tests cover all TSF, and that the TOE has been extensively tested against its functional specification. The developer's testing results lead either to a test is passed, or the test is failed and an error report is created for that error.

The results show that the developer testing requirements is extensive and that the TSF satisfies the TOE security functional requirements.

5.7 Evaluators' Tests

The independent testing performed by the evaluators focused on the only SFR-enforcing module, and the retesting tested all of all of the interfaces of the TOE as the TOE is a simple TOE with only four TSFIs.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Fort Fox Hardware Data Diode (FFHDD) version FFHDD2 meets the specified Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL 4+ [AVA_VAN.5 and ALC_DVS.2] for the specified Common Criteria Part 2 conformant functionality, in the specified environment.

6.2 Recommendations

Prospective consumers of Fort Fox Hardware Data Diode (FFHDD) version FFHDD2 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with the environmental considerations as specified in the Security Target.

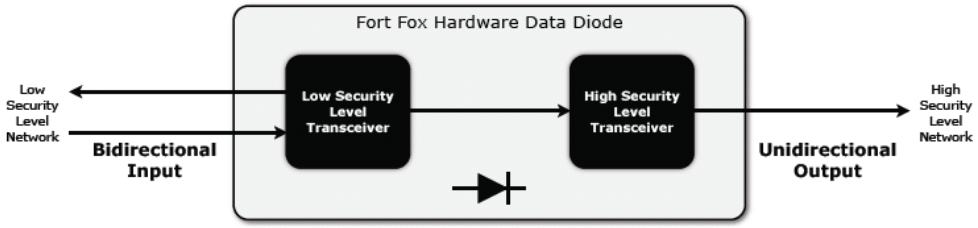
Only the evaluated TOE configuration should be installed. This is specified in Annex A.

Annex A: Evaluated Configuration

TOE Identification

The Target of Evaluation (TOE) consists of a single 19" rack component. The TOE contains physical hardware and does not contain any logic, firmware or software. The TOE allows information to flow through the device in a single direction from the Bidirectional Input (Low Security Level Transceiver) to the Unidirectional Output (High Security Level Transceiver). This is the only function performed by the TOE.

The intention of the TOE 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.



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. Fibre-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.

TOE Documentation

The supporting guidance documents evaluated were:

[a] Security Target, Fox-IT BV, Fort Fox Hardware Data Diode security target, version 1.07 public, January 29, 2009 [1]

[b] Fox-IT BV, FFHDD, Delivery Procedure, Preparative Procedure and Operational User Guidance [8]

TOE Configuration

The following configuration was used for testing:

Item	Identifier	Version
Hardware	Fort Fox Hardware Data Diode (single 19-inch rack component)	FFHDD2
Manuals	Fox-IT BV, FFHDD, Delivery Procedures, Preparative Procedures and Operational User Guidance, CC EAL4+	Version 1.04, May 7, 2009