FOX-IT
EXPERTS IN IT SECURITY

FORT FOX HARDWARE DATA DIODE

Security Target

Common Criteria FFHDD – EAL7+

Classification **PUBLIC**

Component: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.2

Project no./Ref. no.	TD-10-02-00103
Date	June 3, 2010
Version	2.04
Author	Bartek Gedrojc
Business Unit	Fox Crypto
Pages	18

Fox Crypto B.V.
Olof Palmestraat 6, 2616 LM
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: crypto@fox-crypto.com
Web: www.fox-crypto.com

ABN-AMRO
no. 61.01.62.179
Chamber of Commerce
Haaglanden no. 27262642

PUBLIC
This document is classified as Public and intended for Public Use Only.

Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. Fox-IT cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by its contained information.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

Table of Contents

List of Figures

List of Tables

1 Security Target Introduction (ASE_INT.1)

1.1 Security Target Reference

ST Title	Fort Fox Hardware Data Diode Security Target
ST Version	2.04
ST Status	Final
ST Classification	Public
Author	Bartek Gedrojc (Fox-IT)
Advisor	Dirk-Jan Out (Brightsight)
Evaluation Assurance Level	EAL7+, augmented with ASE_TSS.2 and ALC_FLR.3
Publication Data	June 3, 2010
Number of pages	18
Common Criteria Version	3.1, Revision 2, September 2007

1.2 TOE Reference

Developer Name	Fox-IT
TOE Name	Fort Fox Hardware Data Diode (FFHDD)
TOE Version Number	FFHDD2+

1.3 TOE Overview

The Target of Evaluation (TOE) is the Fort Fox Hardware Data Diode (FFHDD) developed by Fox-IT, and will hereafter be referred to as the TOE throughout this document. The TOE is a unidirectional network, as shown in figure 1, allowing data to travel only in one direction.

The one way physical connection of the TOE allows information to 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. 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.

Once manufactured, there is no way to alter the function of the TOE. When the TOE Low Security Level side is connected to a Low Security Level Server and the High Security Level side is connected to a High Security Level server as is indicated in figure 1 the TOE and corresponding servers can be deployed in the following scenarios:

Internet Information from the Low Security Level (Internet) may be transferred to the High Security Level enabling the gathering of information from around the world. This is achieved by using a standard file-transfer communication protocol.

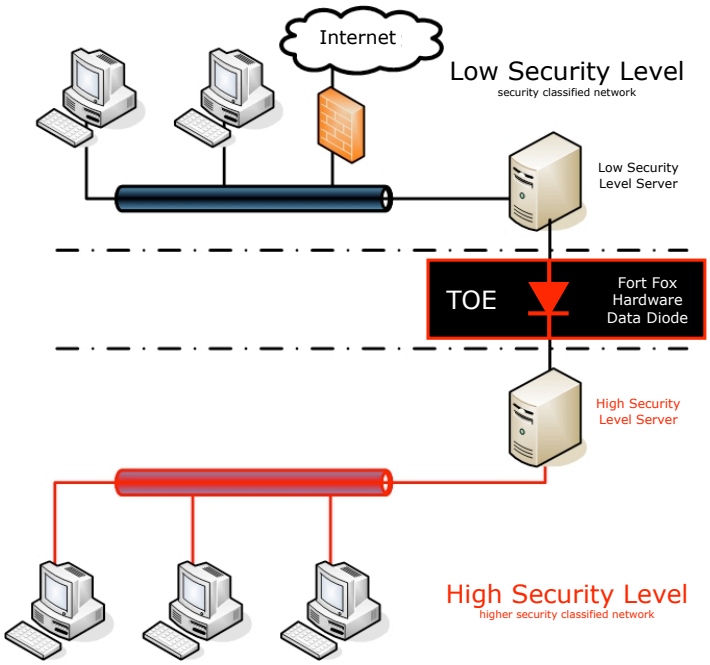

Figure 1: Fort Fox Hardware Data Diode Concept

E-mail Using a 'normal' electronic mail gateway, e-mails can be transmitted from the Low Security Level and received at the High Security Level. Therefore, users can read their emails without going to a different Security Level.

Intercept Mobile telephone service providers are frequently required to intercept telecom traffic data. Intercepted signals on the Low Security Level are transformed into digital data and packaged in low-level UDP network packets to the High Security Level for analysis by the police or intelligence agencies.

Updates Windows and virus updates can be deployed in a High Security Level after being copied from the Low Security Level.

Printing Information located on a Low Secure Level can be transmitted to a printer located in a High Secure Level.

The standard setup for using the TOE is to have an information flow from the Low Security Level side, through the TOE to the High Security Level side, but not the other way around. This enables users to write information on the High Security Level side without being able to extract information from the High Security Level side.

An alternative setup is to have an information flow from the High Security Level side, through the TOE to the Low Security Level side, but not the other way around. This enables users to read information from the High Security Level side without being able to control or input information on the High Security Level side. The following example describes a scenario based on an alternative setup:

Industrial Processes Processes on the High Security Level side that provide the Low Security Level side with real-time process information for monitoring purposes, without letting users being able to influence these critical industrial processes on the High Security Level side.

1.4 TOE Description

1.4.1 Physical Scope

The Target of Evaluation (TOE) consists of a single 19” rack component, see figure 2. 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.

Figure 2: The TOE as a single 19” rack component

Figure 3 shows the three available front panels for the TOE, the Fox-IT front panel, the SINA front panel and the Nexor front panel.

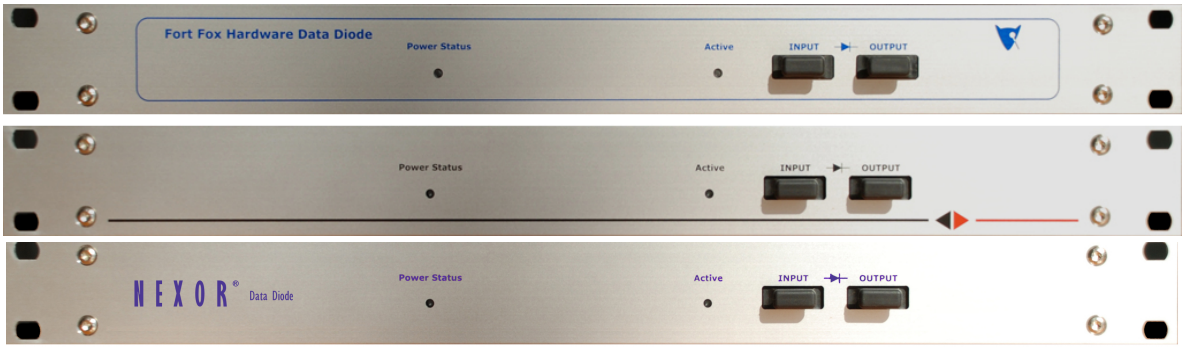

Figure 3: TOE front panel with Fox-IT logo (Top), SINA logo (Middle) and Nexor (Bottom)

The preparative procedures [4] describe all necessary steps for secure accepting and installing the delivered TOE.

This ST will position the TOE in a standard setup where information flows from the Low Security Level side, through the TOE, to the High Security Level side. Placing the TOE in an alternative setup will not change anything to the physical scope of the TOE nor will it change anything to the security function of the TOE.

By using a redundant power supply the Mean Time Between Failures (MTBF) for the TOE is 785,697 hours (89.69 years), based on MIL-HDBK-217F at 25° C.

1.4.2 Logical Scope

Figure 4 shows the TOE (Fort Fox Hardware Data Diode) functional block diagram consisting of two discrete fiber optical transceivers. The data transfer is implemented in hardware, of the physical Open System Interconnection (OSI) reference model, to guarantee complete unidirectionality.

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. The Unidirectional Output port is incapable of input and therefore lacks the ability of converting light into an electrical signal. Consequently, an electrical signal is unable to propagate to the Low Security Level Transceiver and therefore incapable to create a covert channel.

Fiber optics is used to transport signals from and to the TOE Bidirectional Input and Unidirectional Output ports. Electrical signals only transport signals inside the TOE, which is completely enclosed by an aluminum casing.

Unidirectional communication does not work with a network protocol that requires a handshake (acknowledgement). To establish a communication link between the Low Security Level side and the Low Security Level Transceiver, a Bidirectional Input port is initiated. Data, information, or communication originating at the Output (High Security Level) is physically unable to flow to the Bidirectional Input port (Low Security Level) 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.

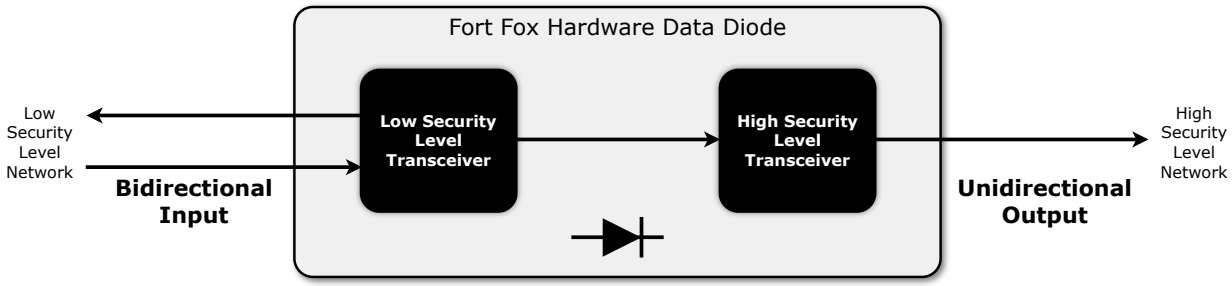

Figure 4: Fort Fox Hardware Data Diode Functional Block Diagram

1.5 Document Overview

The ST has been developed in accordance with the requirements of the Common Criteria (CC) part 3, Class ASE: Security Target Evaluation [3] and Annex A: Specification of Security Targets, of the CC part 1 [1]. The ST contains the following sections:

Section 1 ST introduction, provides the identification material for the ST and the TOE, it provides an overview and description of the TOE.

Section 2 Conformance claims, describes how the ST conforms to the CC.

Section 3 Security problem definition, defines the security problem that is to be addressed.

Section 4 Security objectives, are a concise and abstract statement of the intended solution to the problem.

Section 5 Extended components definition, describes new components if the security requirements are not based on components from the CC.

Section 6 Security requirements, describes the Security Functional Requirements (SFRs) and the Security Assurance Requirements (SARs).

Section 7 TOE summary specification, provides potential consumers of the TOE with a description of how the TOE satisfies all the SFRs.

2 Conformance Claim (ASE_CCL.1)

2.1 CC Conformance Claim

This Security Target and TOE claim conformance to [1,2,3]. This ST is CC Part 2 conformant and CC Part 3 conformant.

2.2 Protection Profile Claim, Package Claim

This Security Target claims conformance to assurance package EAL7 augmented by ASE_TSS.2 and ALC_FLR.3.

2.3 Conformance Rationale

None

3 Security Problem Definition (ASE_SPD.1)

3.1 Threats

The following threats are the assumed threat to the TOE, which could cause it to fail its security objective:

T.TRANSFER 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.

3.2 Organizational Security Policies

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

3.3 Assumptions

The TOE will be connected between two networks of different levels known as the High Security Level network and the Low Security Level network. The assumptions made about the intended environment are:

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

A.NETWORK 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.

4 Security Objectives (ASE_OBJ.2)

4.1 Security Objective for the Target Of Evaluation

The TOE is intended to protect the asset, of High Security Level information, in accordance with the following objectives:

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

4.2 Security Objectives for the Operational Environment

All of the secure usage assumptions are considered to be security objectives of the environment. These objectives are satisfied though the application of procedural or administrative measures.

OE.PHYSICAL The intended operation environment shall be capable of storing and operating the TOE in accordance with the requirements of the High Security Level side.

OE.NETWORK The TOE is the only method of interconnecting the Low Security Level network and High Security Level network.

4.3 Security Objective Rationale

Appendix A presents the security objective rationale.

5 Security Requirements (ASE_REQ.2)

5.1 Security Functional Requirements (SFRs)

The TOE uses two subjects: Input and Output. These represent the input and output of the TOE. These subjects have no attributes.

This statement of SFRs does not define other subjects, objects, operations, security attributes or external entities.

5.1.1 FDP_IFC.2 Complete Information Flow Control

Dependencies: FDP_IFF.1 Simple security attributes.

FDP_IFC.2.1 The TSF shall enforce the **FFHDD policy** on **[[Input, Output], all information]** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

5.1.2 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization[1]

FDP_IFF.1.1 The TSF shall enforce the **FFHDD policy** based on the following types of subject and information security attributes: **[[Input [], Output []], all information []]**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **information may flow from Input to Output**.

FDP_IFF.1.3 **<refined away>**

FDP_IFF.1.4 **<refined away>**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **information may not flow from Output to Input**.

[1] The dependency to FMT_MSA.3 is not applicable as there are no security attributes to initialize.

5.2 Security Assurance Requirements *(SARs)*

The security assurance requirements for the TOE are the Evaluation Assurance Level 7 (EAL 7 – Formally verified design and tested), augmented with the classes ASE_TSS.2 – TOE summary specification with architectural design summary and ALC_FLR.3 – Systematic flaw remediation is chosen while this is the highest evaluation level possible. For a detailed description of these components, please refer to the Part 3 of the Common Criteria [3] directly. These requirements are listed in the following table:

Table 1: Assurance Requirements

Assurance Class	**Assurance Component**
ADV: Development	ADV_ARC.1 – Security architecture description
	ADV_FSP.6 – Complete semi-formal functional specification with additional formal specification
	ADV_IMP.2 – Complete mapping of the implementation representation of the TSF
	ADV_INT.3 – Minimally complex internals
	ADV_SPM.1 – Formal TOE security policy model
	ADV_TDS.6 – Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 – Operational user guidance
	AGD_PRE.1 – Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 – Advanced support
	ALC_CMS.5 – Development tools CM coverage
	ALC_DEL.1 – Delivery procedures
	ALC_DVS.2 – Sufficiency of Security Measures
	ALC_FLR.3 – Systematic flaw remediation
	ALC_LCD.2 – Measurable life-cycle model
	ALC_TAT.3 – Compliance with implementation standards – all parts
ASE: 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.2 – TOE summary specification with architectural design summary
ATE: Tests	ATE_COV.3 – Rigorous analysis of coverage
	ATE_DPT.4 – Testing: implementation representation
	ATE_FUN.2 – Ordered functional testing
	ATE_IND.3 – Independent testing - complete
AVA: Vulnerability assessment	AVA_VAN.5 – Advanced methodical vulnerability analysis

As ADV_SPM.1.D contains an assignment, we therefore provide this element in full:

ADV_SPM.1.1.D The developer shall provide a formal security policy model for the **FFHDD policy**.

5.3 Extended Component Definition *(ASE_ECD.1)*

All security requirements in this ST are based on components from CC Part 2 [2] and CC Part 3 [3], therefore there are no Extended Component Definitions.

5.4 Security Requirements Rationale

Appendix B presents the security requirements rationale.

6 TOE Summary Specification with architectural Design Summary (ASE_TSS.2)

The TOE addresses two Security Functional Requirements, FDP_IFC.2 and FDP_IFF.1, which is described in section 1.4.2 of this document.

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 Low Security level interface: the TOE passes through all data received here without interpreting this data
    - The High Security level 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:

- Being the only connection between the Low Security Level network and High Security Level network (see **A.NETWORK**), thus preventing bypass "around" the TOE.
- Ensuring that all data flows must pass through a single SFR-enforcing component (which is the first component encountered from the High Security Level interface), thus preventing bypass "through" the TOE.

References

[1] Common Criteria for Information Technology Security Evaluation.
Part 1: Introduction and General Model, Version 3.1, Revision 1, September 2006.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf

[2] Common Criteria for Information Technology Security Evaluation.
Part 2: Security Functional Components, Version 3.1, Revision 2, September 2007.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf

[3] Common Criteria for Information Technology Security Evaluation.
Part 3: Security Assurance Components, Version 3.1, Revision 2, September 2007.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R2.pdf

[4] Common Criteria Fox-IT.
*Fort Fox Hardware Data Diode – Delivery Procedures, Preparative Procedures and Operational User Guidance (*AGD-ALC_DEL.1*)*, June, 2010.
FFHDD-AGD-ALC_DEL.1.pdf

APPENDIX

A Security Objective Rationale

This section presents the rationale for the matter in which the security objectives address the threats and assumptions associated with the TOE.

Table 2 demonstrates how all threats and assumptions are covered by at least one of the security objectives of the TOE, and that each security objective covers at least one threat or assumption.

Table 3 demonstrates how the objectives of the TOE and the TOE environment counter the threats identified in section 3.1.

Table 4 demonstrates how the objectives of the TOE and the TOE environment address the assumptions identified in section 3.3.

Table 2: Mapping Threats/Assumptions to Objectives

Threats and Assumptions / **Objectives**	T.TRANSFER	A.PHYSICAL	A.NETWORK
O.CONFIDENTIALITY	X		
OE.PHYSICAL	X	X	
OE.NETWORK			X

Table 3: Threats/Objectives Rationale

Threats	**Objectives**	**Rationale**
T.TRANSFER	O.CONFIDENTIALITY OE.PHYSICAL	The threat that data will be transferred from the High Security Level network to the Low Security Level network through the TOE is partially reduced by O.CONFIDENTIALITY O.CONFIDENTIALITY achieves this by explicitly prohibiting any flows from the High Security Level network through the TOE to the Low Security Level, including flows that might take place through the use of covert channel. Thus both explicit and implicit flows are covered. OE.PHYSICAL ensures that the TOE is operated and stored within a physically secure environment that, at minimum, meets the requirements for the High Security Level. This mitigates the risk that unauthorized personnel have access to the TOE at any time. O.CONFIDENTIALLY and OE.PHYSICAL collectively serve to counter the threat of T.TRANSFER.

Table 4: Assumptions/Objectives Rationale

Threats	Objectives	Rationale
A.PHYSICAL	OE.PHYSICAL	A.PHYSICAL assumes that the intended environment will be capable of storing and operating the TOE, in accordance with the requirements of the High Security Level network. Information systems have different requirements for the storage of computer equipment used for processing information of different security levels. They may also be a requirement for protecting critical system resources within secured rooms. The TOE is critical to all the users and requires no administrator control after is has been installed. It is the system management staff responsibility to protect it from accidental or deliberate tampering causing its functionality to be bypassed. OE.PHYSICAL ensures that the TOE is operated and stored within a physically secure environment that, at minimum, meets the requirements for the High Security Level side. This mitigates the risk that unauthorized personnel have access to the TOE at any time.
A.NETWORK	OE.NETWORK	OE.NETWORK ensures that the TOE is the only method of interconnecting the Low and High Security Level networks. If an untrustworthy product is used to connect the Low Security Level network to the High Security Level network it may result in a compromise of High Security Level information and thus circumvent the security being provided by the TOE.

B Security Requirements Rationale

Table 5 provides a mapping between the security requirements and the objectives that have been defined in section 4. Table 6 provides a detailed rationale of this mapping.

Table 5: Mapping Requirements to Objectives

Objectives / **SFRs**	O.CONFIDENTIALITY
FDP_IFC.2	X
FDP_IFF.1	X

Table 6: Security Requirements/Objectives Rationale

Objectives	**Security Functional Requirements**	**Rationale**
O.CONFIDENTIALITY	FDP_IFC.2 Information flow control policy FDP_IFF.1 Simple Security Attributes	O.CONFIDENTIALITY is achieved through the diode functionality implemented in the TOE, which serves to enforce the FDP_IFC.2 and FDP_IFF.1 requirements. FDP_IFC.2 defines that the policy of the *Unidirectional flow SFP*: User data cannot flow from the High Security Level port to the Low Security level port, while user data can flow from the Low Security Level port via the TOE. FDP_IFF.1 identifies the rules for the TOE that is required to enforce the *Unidirectional Flow SFP*. FDP_IFF.1 is based on the TOE interface port attributes and user data security attributes. These attributes are defined through FDP_IFF.1 and are required to achieve the SFP rules and the O.CONFIDENTIALITY objective. FDP_IFF.1 requires that all Low Security Level information be allowed to flow from the Low Security Level input interface port to the High Security Level output interface port. Additionally, FDP_IFF.1 requires that no information flow from the High Security Level output interface port to the Low Security Level input interface port. This is how the FDP_IFF.1 and FDP_IFC.2 help achieve the O.CONFIDENTIALITY objective.