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.1 / ASE_TSS.2
Project no./Ref. no.	PRC-160067
Date	June 27, 2018
Version	3.04
Author	Frans van Dorsselaer
Business Unit	High Assurance
Pages	22

for a more secure society

FOX-IT BV
Olof Palmestraat 6, Delft
PO BOX 638, 2600 AP Delft
The Netherlands

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
IBAN NL57ABNA0554697041
KVK Haaglanden 27301624

FOX-IT.COM

Fox-IT B.V.

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

Document Management

Version management

Project name:	Common Criteria FFHDD – EAL7+
Customer:	Fox-IT
Subject:	Security Target
Date:	June 27, 2018
Version:	3.04
Status:	Final
Author:	Frans van Dorsselaer

This version replaces all previous version of this document. Please destroy all previous copies!

Change management

Historical changes to this public document are recorded separately in a classified document [5].

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	3.04
ST Status	Final
ST Classification	Public
Author	Frans van Dorsselaer (Fox Crypto B.V.)
Evaluation Assurance Level	EAL7+, augmented with ASE_TSS.2 and ALC_FLR.3
Publication Data	June 27, 2018
Number of pages	22
Common Criteria Version	3.1, Revision 5, April 2017

1.2 TOE Reference

Developer Name	Fox Crypto B.V.
TOE Name	Fort Fox Hardware Data Diode
TOE Version Number	FFHDD3_1 FFHDD3_10

This Security Target covers both version FFHDD3_1 and version FFHDD3_10, collectively referred to as FFHDD3_1/10.

1.3 TOE Overview

The Target of Evaluation (TOE) is the Fort Fox Hardware Data Diode (version FFHDD3_1/10) developed by Fox Crypto B.V., 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 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.

Once manufactured, there is no way to alter the function of the TOE.

Example 1: Protecting downstream confidentiality

As an example, one practical deployment of the TOE is to protect a High Security Level downstream network from leaking information to a Low Security Level upstream network, as is indicated in Figure 1.

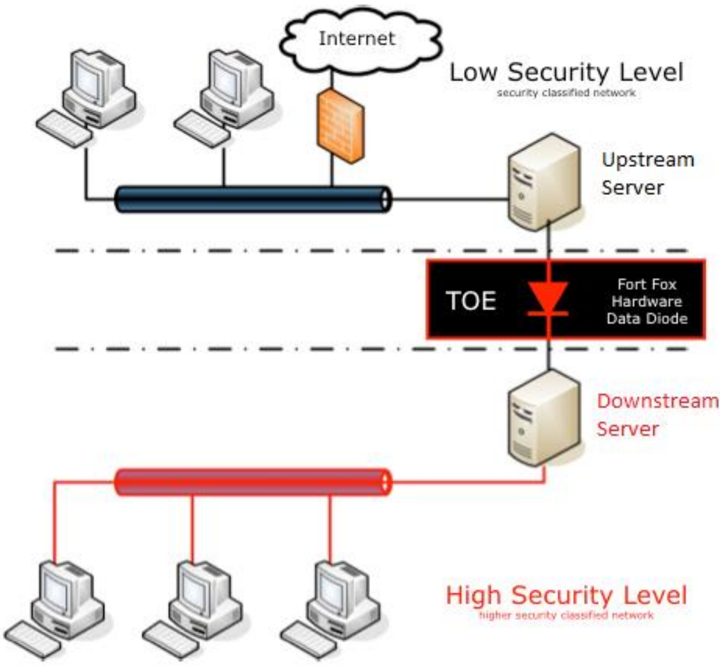

Figure 1: Protecting downstream confidentiality

This setup for using the TOE is used to allow an information flow into the protected downstream network while preventing information leaving the protected downstream network; the confidentiality of the downstream side is ensured. Examples of upstream data sources that can unidirectionally feed data into the protected downstream network include:

Internet Information from the upstream network (Internet) may be transferred to the protected downstream network enabling the gathering of information from around the world. This is achieved by using a standard file-transfer communication protocol.

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

Intercept Mobile telephone service providers are frequently required to intercept telecom traffic data. Intercepted signals on the upstream side are transformed into digital data and packaged in low-level UDP network packets which are transmitted to the protected downstream side for analysis by the police or intelligence agencies.

Updates Software updates can be deployed at the protected downstream side after being copied from the upstream side.

Printing Information located on the upstream side can be transmitted to a printer located on the protected downstream side.

Example 2: Protecting upstream integrity

As a second example, another practical deployment of the TOE is to protect a High Security Level upstream network from being tampered with by a Low Security Level downstream network as is indicated in Figure 2.

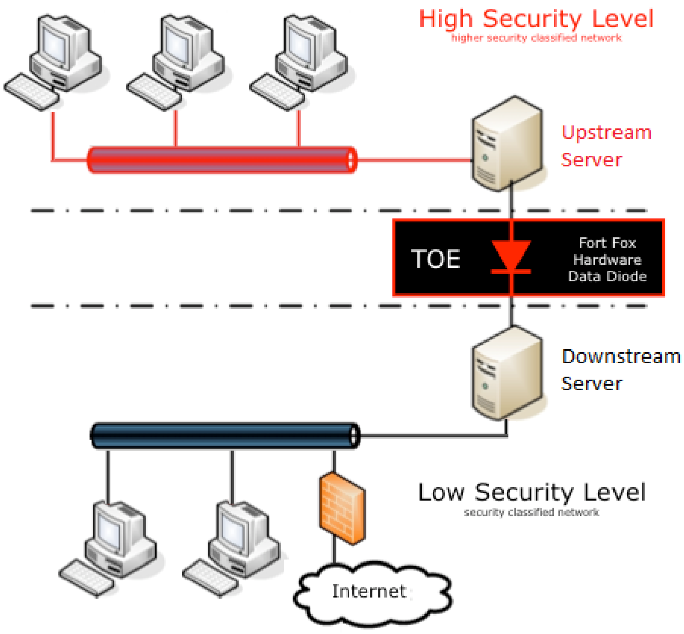

Figure 2: Protecting upstream integrity

This setup for using the TOE is used to allow an information flow from the protected upstream network while preventing information from the downstream network to influence the upstream side; the integrity of the upstream side is ensured. Examples of upstream data sources that can unidirectionally transmit data from the protected downstream network include:

Industrial Processes Processes on the protected upstream side provide the downstream side with real-time process information for monitoring purposes, without allowing downstream network users being able to influence these critical industrial processes on the protected upstream side.

In the first example, the High Security Level network (the network to protect) is positioned downstream and, within that scenario, only the confidentiality claim is used. In the second example, the High Security Level network (the network to protect) is positioned upstream and, within that scenario, only the integrity claim is used. In general, however, the TOE separates two distinct security domains and both the integrity of the upstream network and the confidentiality of the downstream network are ensured simultaneously.

1.4 TOE Description

1.4.1 Physical Scope

The Target of Evaluation (TOE) consists of a single hardware unit, see figure 2. The TOE contains only fixed-function physical hardware and does not contain any programmable logic, firmware, software, volatile memory, or persistent memory. The TOE allows information to flow through the device in a single direction from the bidirectional upstream transceiver to the unidirectional downstream transceiver. This is the only function performed by the TOE.

Figure 3: The TOE as a single hardware unit

The physical scope includes the OE.PHYSICAL environmental objective defined in Section 4.2 which applies to the entire lifecycle of the TOE, including storage and transport. It is required that the procedures as described in the User Guidance documentation [4] are followed; deviation from the procedures in the User Guidance documentation [4] invalidates the security claims in this document. The User Guidance documentation [4] is delivered separately from the TOE through a secure electronic channel directly from Fox Crypto B.V. to the customer.

The picture in Figure 2 is not normative for the identification of the TOE as color and print may differ. The User Guidance documentation [4] describes all necessary steps for secure accepting, identifying, and installing the delivered TOE.

The TOE has 3 interface ports. The Power port consists of 5 electrical connections: one ground pin and two sets of 24VDC input power pins. Either or both of the power inputs activate the TOE. The TOE has one bi-directional Upstream port used to connect the TOE to the upstream network with two optical fibers. The TOE has one unidirectional Downstream port used to connect the TOE to the downstream network with one optical fiber.

This ST will position the TOE in a standard setup where information flows from the upstream side, through the TOE, to the downstream side.

1.4.2 TOE Versions

The TOE comes in two versions that differ only in operating speed. The TOE versions each have a unique model number that is marked on the TOE casing, see Table 1. There are no further differences between the TOE versions with respect to this ST.

Table 1: TOE Versions

TOE Version	Model Number	Speed
FFHDD3_1	FDD1GI	1 Gbit/sec
FFHDD3_10	FDD10GI	10 Gbit/sec

1.4.3 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 Upstream port and Unidirectional Downstream port. At the upstream transceiver light is carried into the Bidirectional Upstream port and converted, with the aid of a photocell, into an electrical signal. The electrical signal spreads through the TOE to the downstream transceiver. The downstream transceiver 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. Consequently, an electrical signal is unable to propagate to the upstream transceiver and therefore incapable to create a covert channel.

Fiber 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 aluminum casing.

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.

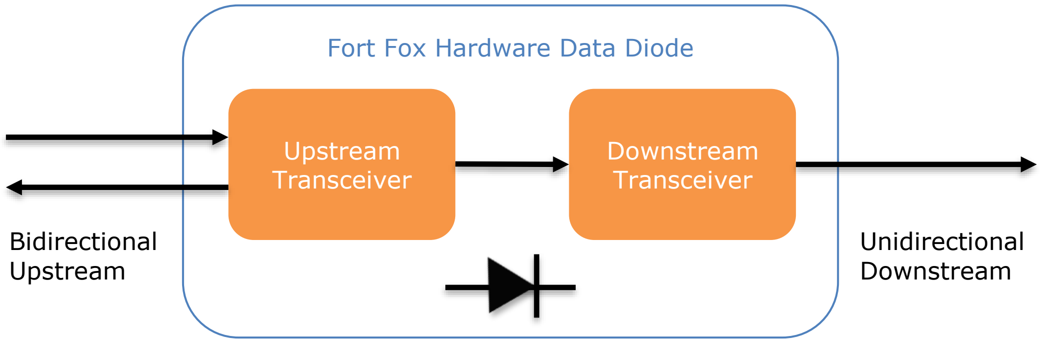

Figure 4: Fort Fox Hardware Data Diode Functional Block Diagram

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

Section 6 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 downstream side that either (a) accidentally or deliberately breaches the confidentiality of some downstream information by transmitting data through the TOE to the upstream side, or (b) accidentally or deliberately breaches the integrity of the upstream side by transmitting data through the TOE to the upstream side.

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 security levels known as the upstream network and the downstream 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 highest of each of the requirements of the upstream side and of the downstream side.

A.POWER The TOE shall be powered such that a user or process on the downstream side cannot control the power by means of the downstream network. This prevents a threat agent from using the power input as a covert channel by toggling the TOE power and, as a consequence, by controlling the signal carrier of the Bidirectional Upstream port.

A.NETWORK The only method of interconnecting the upstream network and downstream network is one or more units of the TOE, where all of the units are operating in the same data flow direction. 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 downstream side destination is kept confidential from the upstream source.
O.INTEGRITY	The information on the upstream side source is kept consistent, accurate, and trustworthy such that it cannot be modified by the downstream destination.

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 operational environment shall be capable of storing and operating the TOE in accordance with the highest of each of the requirements of the upstream side and of the downstream side.
OE.POWER	The intended operational environment shall provide power to the TOE such that the power to the TOE cannot be interfered with from the downstream network.
OE.NETWORK	The only method of interconnecting the upstream network and downstream network is one or more units of the TOE, where all of the units are operating in the same data flow direction.

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: Upstream and Downstream. 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.

The **FFHDD policy** is defined to be the compliancy to FPD_IFC.2 and FDP_IFF.1 as specified in sections 5.1.1 and 5.1.2.

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 **[[Upstream, Downstream], 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: **[[Upstream [], Downstream []], 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 Upstream to Downstream**.

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 shall not flow from Downstream to Upstream**.

[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 2: 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 (ASE_TSS.1 / ASE_TSS.2)

The TOE addresses two Security Functional Requirements, FDP_IFC.2 and FDP_IFF.1, which is described in section 1.4.3 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 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:

- Being the only connection between the upstream network and downstream 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 downstream interface), thus preventing bypass "through" the TOE (see **A.POWER**).

References

[1] Common Criteria for Information Technology Security Evaluation.
Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[2] Common Criteria for Information Technology Security Evaluation.
Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[3] Common Criteria for Information Technology Security Evaluation.
Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[4] FDDV3_MAN_FOX-CRYP_0001, Installation Manual, Fox Crypto B.V.
User Guidance, v1.0, 2018.

[5] FFHDD-ASE-Document-Management.pdf, Fox Crypto B.V.
Historical changes to this document, classified non-public.

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 3: Mapping Threats/Assumptions to Objectives

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

Table 4: Threats/Objectives Rationale

Threats	Objectives	Rationale
T.TRANSFER	O.CONFIDENTIALITY O.INTEGRITY OE.PHYSICAL OE.POWER	The threat that data will be transferred from the downstream network to the upstream network through the TOE is partially reduced by both O.CONFIDENTIALITY and O.INTEGRITY. Both O.CONFIDENTIALITY and O.INTEGRITY, simultaneously and independently, achieve this by explicitly prohibiting any flows from the downstream network through the TOE to the upstream network. OE.POWER ensures that the power provided to the TOE cannot be used as a covert channel by the downstream side. OE.PHYSICAL ensures that the TOE is operated and stored within a physically secure environment that, at minimum, meets the higher of each of the requirements of the upstream side and of the downstream side. This mitigates the risk that unauthorized personnel have access to the TOE at any time.

		O.CONFIDENTIALITY, O.INTEGRITY, OE.PHYSICAL, and OE.POWER collectively serve to counter the threat of T.TRANSFER throughout the operating life cycle of the TOE.

Table 5: 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 higher of each of the requirements of the upstream side and of the downstream side. Information systems have different requirements for the storage of computer equipment used for processing information of different security levels. There 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 higher of each of the requirements of the upstream side and of the downstream side. This mitigates the risk that unauthorized personnel have access to the TOE at any time.
A.POWER	OE.POWER OE.PHYSICAL	OE.POWER ensures that the power supplied to the TOE cannot be interfered with by a user or process on the downstream network. OE.PHYSICAL ensures that the TOE is operated and stored within a physically secure environment that, at minimum, meets the higher of each of the requirements of the upstream side and of the downstream side. This mitigates the risk that unauthorized personnel have access to the TOE at any time. OE.POWER and OE.PHYSICAL collectively ensure that the assumption A.POWER is met throughout the operating life cycle of the TOE.
A.NETWORK	OE.NETWORK OE.PHYSICAL	OE.NETWORK ensures that the TOE is the only method of interconnecting the upstream and downstream networks. If an untrustworthy product is used to connect the upstream and downstream networks it may result in a compromise of information flow and thus circumvent the security being provided by the TOE. OE.PHYSICAL ensures that the TOE is operated and stored within a physically secure environment that,

		at minimum, meets the higher of each of the requirements of the upstream side and of the downstream side. This mitigates the risk that unauthorized personnel have access to the TOE at any time. OE.NETWORK and OE.PHYSICAL collectively ensure the assumption A.NETWORK is met throughout the operating life cycle of 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 6: Mapping Requirements to Objectives

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

Table 7: 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 downstream port to the upstream port, while user data can flow from the upstream 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 upstream information be allowed to flow from the upstream input interface port to the downstream output interface port. Additionally, FDP_IFF.1 requires that no information flow from the downstream output interface port to the upstream input interface port. This is how the FDP_IFF.1 and FDP_IFC.2 help achieve the O.CONFIDENTIALITY objective.

O.INTEGRITY	FDP_IFC.2 Information flow control policy FDP_IFF.1 Simple Security Attributes	O.INTEGRITY 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 downstream port to the upstream port, while user data can flow from the upstream 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.INTEGRITY objective. FDP_IFF.1 requires that all upstream information be allowed to flow from the upstream input interface port to the downstream output interface port. Additionally, FDP_IFF.1 requires that no information flow from the downstream output interface port to the upstream input interface port. This is how the FDP_IFF.1 and FDP_IFC.2 help achieve the O.INTEGRITY objective.