DATAFLOWX

Data Diode Modules
Security Target v1.1 - LITE

19.02.2020

Document History

Sürüm	Tarih	Değişiklik Nedeni	Değişikliği Yapan	Değişikliği Onaylayan
1.1 Lite	09.03.2020	Lite version create according to CCDB-2006-04-004	Soner GÜLEÇ/ Project Manager	Soner GÜLEÇ/ Project Manager

Contents

List of Tables

List of Figures

1 ST INTRODUCTION

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization.

The Target of Evaluation (*TOE*) is the ***DataFlowX Data Diode Modules*** and will hereafter be referred to as the TOE throughout this document.

1.1 ST Organization

This ST is divided into 8 sections, as follows:

- **Section 1 ST Introduction:** Provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- **Section 2 Conformance Claims:** Provides the identification of Common Criteria (*CC*), Protection Profile, and Evaluation Assurance Level (*EAL*) package claims.
- **Section 3 Security Problem:** A security environment description in terms of assumptions, threats and organizational security policies.
- **Section 4 Security Objectives:** Identifies the security objectives that are satisfied by the TOE and its environment. It also presents the rationale for the security objectives.
- **Section 5 Extended Components:** Identifies new components (*extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)*) that are not included in CC Part 2 or CC Part 3.
- **Section 6 Security Requirements:** Presents the SFRs and SARs met by the TOE. It also presents the rationale for the security objectives.
- **Section 7 TOE Summary Specification:** Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- **Section 8 Acronyms**: Defines the acronyms used within this ST.

1.2 ST Reference

Title:	DataFlowX Data Diode Modules Security Target
Version:	1.1 - Lite
Status:	Released
Date:	19.02.2020
Developer:	Bilge SGT Corp.
Keywords:	Data Diode, Boundary Protection, One-Way Gateway

1.3 TOE Reference

TOE Identification:	DataFlowX Data Diode Modules
TOE Version	v1.0.0
CC Identification:	Common Criteria for Information Technology Security Evaluations, Version 3.1R5

1.4 TOE Overview

This part of the ST describes the TOE with its intended usage, general IT features and major security features.

The TOE provides a unidirectional data path between a source (*untrusted network*) and destination (*trusted network*) and allows information to flow from an untrusted network to a trusted network, without compromising the confidentiality of the information on the trusted network.

The TOE consists of hardware components (***TX Module and RX Module***) and software components (***DataFlowX Sender and DataFlowX Receiver***). The TOE components are located on the two different Application Servers (*as shown in the Figure 1*).

Both of the TX Module and RX Module have two external interfaces. One external interface of these modules is connected to the PCI bus of the Application Server on which they are installed. Other external interfaces (*SFP Fiber Optic Interface*) of the TX Module and the RX Module are physically connected each other with as single fiber optic cable.

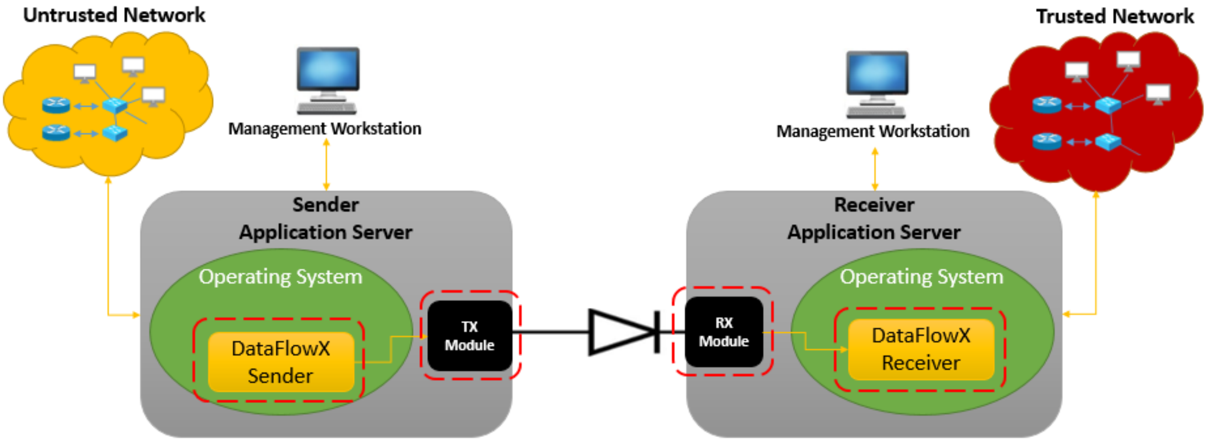

Figure 1: *DataFlowX Data Diode Modules and General TOE Environment*

DataFlowX Data Diode Modules (*TOE*) consists of the components shown in Figure 1 with red dashed frame.

The connection between ***TX Module and RX Module*** allows data to flow from the Sender Application Server to the Receiver Application Server but does not allow data to flow in the reverse direction (*prevents information leak from Receiver Application Server to Sender Application Server*) by property of the physical implementation of TX Module and RX Module. The one-way data transmission property between TX Module and RX Module is implemented at the physical layer of the OSI reference model (*no software and firmware*).

DataFlowX Sender constantly monitors specific predefined file directory in the file system. If it detects a new file that is transferred via SFTP (*Secure File Transfer Protocol*) to the Sender Application Server from the Untrusted Network, it immediately converts the file as data packets in order to send to the TX Module.

All data packets calculated meta information of the file are forwarded according to the below order (*as shown in Figure 1*):

- ✓ From the DataFlowX Sender to the TX Module,
- ✓ From the TX Module to the RX Module,
- ✓ From the RX Module to the DataFlowX Receiver.

DataFlowX Receiver receives all data packets and calculated meta information of the file from the DataFlowX Sender via RX Module and TX Module. And it merges all data packets and checks the integrity of the file using its hash value. According to the hash control result, the file is stored in specific predefined file directory in the file system. All stored files on the Receiver Application Server are shared with the Trusted Network.

1.4.1 Major Security Features of the TOE

User Data Protection: The User Data Protection function implements functionality necessary to protect the Trusted Network information. The TOE applies a set of rules (*One-Way Information Flow SFP*) to provide a unidirectional (*One-way*) data path from an untrusted network and trusted network and allows information to flow from an untrusted network to a trusted network, without compromising the confidentiality of the information on the trusted network.

1.4.2 Non-TOE Hardware/ Software/ Firmware

Application Servers: All parts of the TOE are located in the Application Servers (*Receiver and Sender Application Servers*). Receiver and Sender Application Servers are physically separated from each other and powered by independent power supplies. This approach has been implemented to minimize the TEMPEST security threat. These Application Servers are generally planned to be deployed in a physically secure cabinet or data center with the appropriate level of physical access control and physical protection.

Power Supply: It is components that provide power for the Application Servers (*Receiver and Sender*).

Operating System and File System: Both the DataFlowX Sender and DataFlowX Receiver operates on Linux operating system File System stores the required configuration and log files that is read and generated by the DataFlowX Sender and DataFlowX Receiver.

Management Workstation: It is any PC running an operating system on it and that can establish a TCP/IP connection. It is used to manage the DataFlowX Sender/DataFlowX Receiver via LAN Interface of the Receiver Application Server/Sender Application Server. The TOE management functionalities are used through CLI commands.

Devices in Networks: Devices in trusted network and untrusted network such as Switch, Router, and PC that may change depend on the deployment of the TOE in the network environment.

1.4.3 TOE Type

TOE is a collection of embedded application software and hardware modules installing on the Application Servers that act as a unidirectional (*one-way*) gateway at the physical network layer.

1.5 TOE Description

This part of the ST describes the physical and logical scopes of the TOE as an aid to the understanding security capabilities of the TOE and to the separation of the TOE from non-TOE entities.

1.5.1 Physical Scope of TOE

The physical scope of the TOE is a DataFlowX Data Diode Modules to be installed in two separated Application Servers (*as shown in the Figure 1*) and TOE Documentation.

- ❖ DataFlowX Data Diode Modules consist of:
  - ➢ Hardware Modules:
    - ✓ TX Module
    - ✓ RX Module
  - ➢ Software Modules:
    - ✓ DataFlowX Sender
    - ✓ DataFlowX Receiver

DataFlowX Sender

- ✓ Constantly monitors specific predefined file directory in the file system to detect a new file transferred via SFTP to the Sender Application Server from the Untrusted Network
- ✓ After detection, calculates the hash value of the file and converts the file as data packets
- ✓ Sends all data packets and calculated meta information of the file to the DataFlowX Receiver via TX Module and RX Module
- ✓ is configured via the LAN Interface of the Sender Application Server using the CLI commands

DataFlowX Receiver

- ✓ Receives all data packets and calculated meta information of the file from DataFlowX Sender via RX Module and TX Module
- ✓ Merges the all data packets and checks the integrity of the file using its hash value
- ✓ Stores the file in specific predefined file directory according to the hash control result
- ✓ is configured via the LAN Interface of the Receiver Application Server using the CLI commands

TX Module

- ✓ Special Ethernet Card with customized SFP
- ✓ Located in the Sender Application Server
- ✓ Has only an optical transmitter
- ✓ Has no external interface to receive optical signal (*optical sensor*)
- ✓ Is implemented at the physical layer of the OSI reference model (*no software and firmware*).

RX Module

- ✓ Special Ethernet Card with customized SFP
- ✓ Has only an optical sensor
- ✓ Has no an optical transmitter, therefore, it is physically not possible for data to flow from the Trusted Network to the Untrusted Network via the TOE
- ✓ Is implemented at the physical layer of the OSI reference model (*no software and firmware*).

Data can only be optically transmitted from SFP Fiber Optic Interface of the TX Module to the *SFP Fiber Optic Interface* of the RX Module (*not vice versa*) by property of the physical implementation. They are considered part of the TOE.

TOE Documentation consists of:

- ❖ The TOE Operational Guidance
- ❖ The TOE Preparative Procedures

All parts of the TOE including software parts and hardware parts are, installed on the Application Servers. The TOE is delivered to the customer’s address by the company staff. The TOE is installed by DataFlowX personnel. DataFlowX customers may contact DataFlowX support to request a copy of the guidance, which provides instructions and cautions for operating the product in its evaluated configuration.

1.5.2 Logical Scope of TOE

This section describes the logical security features of the TOE.

***Table 1**- Logical Scope of TOE*

TOE Security Function	Description
User Data Protection	The User Data Protection function implements functionality necessary to protect confidentiality of the information on the Trusted Network. The TOE enforces a One-Way Information Flow SFP that applies a set of rules to provide a unidirectional data path from an Untrusted Network and Trusted Network. It explicitly deny any information attempting to leave through the RX Module and any information attempting to enter to the TX Module from the RX Module. It also allows any information generated from an Untrusted Network and coming from the TX Module to the RX Module can enter the Trusted Network.

2 CONFORMANCE CLAIMS

2.1 CC Conformance Claim

This ST claims conformance to

- ❖ Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, (CC Part 1)
- ❖ Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, (CC Part 2)
- ❖ Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, (CC Part 3)

as follows

- Part 2 conformant
- Part 3 conformant

- ❖ The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [CEM] has to be taken into account.

2.2 PP and Package Claim

2.2.1 Protection Profile (PP) Claim

This ST does not claim conformance to any protection profile.

2.2.2 Package Claim

This ST is conforming to assurance package EAL4 augmented with AVA_VAN.5 defined in CC part 3.

2.3 Conformance Rationale

This ST does not claim conformance to any protection profile. Thus, this section is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 Threats

This section identifies the threats to the assets against which protection is required by the TOE or by the security environment.

Attackers: They are not TOE user and have public knowledge of how the TOE operates.

Primary Assets (User Data): The primary asset is the Trusted Network Information that must be prevented being transmitted during the communication between the untrusted network and trusted network.

Table 2*- Threats*

Threats	Definition
T.Data_Leak	An attacker may breach the confidentiality of data on the trusted network by using a malicious software infected by attacker into devices in the trusted network with the aim of providing data leakage from the trusted network.
T.Physical_Manipulation	The hardware parts of the TOE may be subject to physical attack by an attacker, which may compromise security of the user data.

3.2 Organizational Security Policies

The Organizational Security Policies identified in the following subsections are addressed by the TOE and the environment of the TOE.

The Organizational Security Policies for the operational environment are given in Table 3.

Table 3*- Organizational Security Policies*

Policies	Definition
P.One_Way_Flow	The TOE shall provide one-way data path from the SFP Fiber Optic Interface of the TX Module to the SFP Fiber Optic Interface of the RX Module.
P. Standart	TX and RX modules of TOE should be installed by NATO SDIP-29 "Installation of Electrical Equipment for the Processing of Classified Information" standard or MST 401-1(A) “Turkish Armed Forces TEMPEST Standards” standard.

3.3 Assumptions

These assumptions are made on the operational environment in order to be able to ensure that the security functionality can be provided by the TOE. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

The assumptions for the operational environment are given in Table 4.

Table 4*- Assumptions for the Operational Environment*

Assumption	Definition
A.Personnel	***It is assumed that*** the personnel with authorized physical access to the TOE is well-trained and will not at-tempt to circumvent the TOE's security functionality.
A.Network	Apart from transmitting information through the TOE, ***It is assumed that*** there are no channels for the information to flow between the untrusted network and the trusted network.
A.Environment	***It is assumed that*** the TOE environment provides stable network connectivity for the TOE to perform its intended function.

4 SECURITY OBJECTIVES

The security objectives identify the responsibilities of the TOE and its environment, in meeting the security needs.

4.1 Security Objectives of the TOE

The TOE must satisfy the following objectives of the TOE.

***Table** 5- Security Objectives of the TOE*

Objective	Definition
O.No_Data_Leak	The TOE must ensure that no information that may exit the Receiver Application Server through RX Module to enter the Sender Application Server through TX Module.
O.One_Way_Flow	TOE must provide one-way data path from the SFP Fiber Optic Interface of the TX Module to the SFP Fiber Optic Interface of the RX Module. For this purpose: ✓ *The TOE must allow any information sent to the RX Module to exit the TX Module.* ✓ *The TOE must allow any information coming from TX Module to enter to the RX Module.* ✓ *The TOE must ensure that no information that may enter to the Sender Application Server through TX Module.*

4.2 Security Objectives of the Operational Environment

The TOE's IT environment must satisfy the following objectives.

Table 6*- Security Objectives for the Operational Environment*

Objective	Definition
OE.Physical_Security	The TOE and its interfaces shall be physically protected from unauthorized access and mechanical, electrical, optical, radiation or any other form of physical influence.
OE.Personnel	Personnel with authorized physical access to the TOE shall be well-trained and will not attempt to circumvent the TOE's security functionality.
OE.Network	Apart from transmitting information through the TOE, there shall be no channels for the information to flow between the untrusted network and the trusted network.
OE. Standart	TX and RX Modules of TOE shall be installed by NATO SDIP-29 "*Installation of Electrical Equipment for the Processing of Classified Information*" standard or MST 401-1(A) "*Turkish Armed Forces TEMPEST Standards*" standard.
OE.Environment	TOE environment shall provide stable network connectivity for the TOE to perform its intended function.

4.3 Security Objective Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target.

4.3.1 Security Objectives Rationale Relating to Threats

The following tables describe the rationale for Threats, Assumptions and Organizational Security Policies (*OSPs*) to security objectives mapping.

Table 7*- Objectives Mapping for Threats, Assumptions and OSPs*

	T.Data_Leak	**T.Physical_Manipulation**	**A. Personnel**	**A.Network**	**A.Environment**	**P.One_Way_Flow**	**P. Standart**
O.No_Data_Leak	✓						
O.One_Way_Flow						✓	
OE.Physical_Security		✓					
OE.Personnel			✓				
OE.Network	✓			✓			
OE. Standart							✓
OE.Environment					✓		

Table 8*- Security Objectives Rationale for Threats*

Threats	Objectives	Rationale
T.Data_Leak	**O.No_Data_Leak**	***O.No_Data_Leak*** counters this threat by ensuring that no information is able to exit the RX Module.
	OE.Network	***OE.Network*** ensures that there are no channels for the information to flow between the untrusted network and the trusted network, apart from transmitting information through the TOE.
T.Physical_Manipulation	**OE.Physical_Security**	***OE.Physical_Security*** ensures that the TOE and its interfaces are physically protected from unauthorized access and mechanical, electrical, optical, radiation or any other form of physical influence.

4.3.2 Security Objectives Rationale Relating to Assumptions

The following table describes the rationale for the assumption.

Table 9- *Objectives Rationale for Assumptions*

Assumptions	Objectives	Rationale
A. Personnel	**OE.Personnel**	***OE.Personnel*** upholds this assumption by ensuring that Personnel with authorized physical access to the TOE is well-trained and is not attempt to circumvent the TOE's security functionality.
A.Network	**OE.Network**	***OE.Network*** upholds this assumption by ensuring that there are no channels for the information to flow between the untrusted network and the trusted network, apart from transmitting information through the TOE.
A.Environment	**OE.Environment**	***OE.Environment*** upholds this assumption by ensuring that TOE environment is provide stable network connectivity for the TOE to perform its intended function.

4.3.3 Security Objectives Rationale Relating to Policies

The following table describes the rationale for OSPs.

Table 10- *Objectives Rationale for OSPs*

Security Policies	Objectives	Rationale
P.One_Way_Flow	**O.One_Way_Flow**	***O.One_Way_Flow*** fulfils this Security Policies by ensuring that the TOE is provide one-way data path from the SFP Fiber Optic Interface of the TX Module to the SFP Fiber Optic Interface of the RX Module.
P. Standart	**OE.Standart**	***OE.Standart*** fulfils this Security Policies by ensuring that TX and RX Modules of TOE are installed by NATO SDIP-29 "*Installation of Electrical Equipment for the Processing of Classified Information*" standard or MST 401-1(A) "*Turkish Armed Forces TEMPEST Standards*" standard.

5 EXTENDED COMPONENTS DEFINITION

There are no extended SFRs and extended SARs for this TOE.

6 SECURITY REQUIREMENTS

6.1 Security Functional Requirements

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Section 8.1 of Common Criteria Part1 [17]. The following operations are used in the ST.

- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out.~~
- The **selection** operation is used to select one or more options provided by the CC instating a requirement. Selections having been made are denoted as underlined text.
- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments are denoted by *italicized* text.
- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1.1 Class FDP: User Data Protection

6.1.1.1 FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes **fulfilled** by FDP_IFF.1

FDP_IFC.2.1 The TSF shall enforce the *One-Way Information Flow SFP* on

Subjects: Trusted Network and Untrusted Network

Information: Any optical signal that wants to traverse to the trusted network or untrusted network through the Interface between the TX and RX Module

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.

6.1.1.2 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control **fulfilled** by FDP_IFC.2

FMT_MSA.3 Static attribute initialization **not fulfilled** but justified

Justification: *The TOE configuration is static and has no concept of manageable security attributes. Therefore, this dependency SFR is not required, nor meaningful.*

FDP_IFF.1.1 The TSF shall enforce the *One-Way Information Flow SFP* based on the following types of subject and information security attributes:

Subjects: Sender Network and Receiver Network

Information: Any optical signal that wants to traverse to the trusted network or untrusted network through the Interface between the TX and RX Module

Subject Attributes: Trusted Network and Untrusted Network

Information Attributes: Trusted Network Information and Untrusted Network 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: *no security attribute-based rules.*

FDP_IFF.1.3 The TSF shall enforce the *none.*

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules:

i. *Any information coming from the SFP Fiber Optic Interface of the TX Module and attempting to enter to the SFP Fiber Optic Interface of the RX Module.*

ii. *Any information attempting to exit from the SFP Fiber Optic Interface of the TX Module in order to enter the SFP Fiber Optic Interface of the RX Module.*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

i. *Any information attempting to leave through the SFP Fiber Optic Interface of the RX Module.*

ii. *Any information attempting to enter to the SFP Fiber Optic Interface of the TX Module from the SFP Fiber Optic Interface of the RX Module.*

6.2 Security Assurance Requirements

For the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level (*EAL4*) and augmented by taking the following component: AVA_VAN.5.

The security assurance requirements are listed in Table 11 below.

Table 11*- Security Assurance Requirements Table*

Assurance Classes	Assurance Components
ADV: 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
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DVS.1 Identification of security measures
	ALC_TAT.1 Well-defined development tools
	ALC_DEL.1 Delivery procedures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability Assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

Table 12*- Security Functional Requirements Rationale*

Objective	SFRs	Rationale
O.No_Data_Leak	FDP_IFC.2 Complete information flow control	This requirement meets the objective by ensuring that any information flow in the TOE is covered by the "*One-Way Information Flow SFP*".
	FDP_IFF.1 Simple security attributes	This requirement meets the objective by denying any information attempting to leave through the SFP Fiber Optic Interface of the RX Module.
O.One_Way_Flow	FDP_IFC.2 Complete information flow control	This requirement meets the objective by ensuring that any information flow in the TOE is covered by the "*One-Way Information Flow SFP*".
	FDP_IFF.1 Simple security attributes	This requirement meets the objective by allowing any information sent to the RX Module to exit the SFP Fiber Optic Interface of the TX Module and allowing any information coming from the SFP Fiber Optic Interface of the TX Module to enter to the SFP Fiber Optic Interface of the RX Module. This requirement also meets the objective by denying any information that may enter to the Sender Application Server through the SFP Fiber Optic Interface of the TX Module.

6.3.2 Security Assurance Requirements Rationale

EAL4 is chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources.

EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

The underlying EAL4 assurance level is augmented by AVA_VAN.5 (*Advanced methodical vulnerability analysis*).

The component AVA_VAN.5 augmented to EAL4 has no dependencies to other security requirements.

7 TOE SUMMARY SPECIFICATION

7.1 TOE Security Functionality

This chapter provides a description of the Security Functionality of the TOE, which show how the TOE meets each Security Functional Requirement.

7.1.1 User Data Protection

All parts of the TOE are located in the Application Servers (*Sender and Receiver*). Both the Sender Application Server and Receiver Application Server are entirely independent, each with its own independent power and network interfaces, each enclosed in enclosure that does not admit electrical or optical signals via any other than the described interfaces. The Sender Application Server is only connected to the Untrusted Network and is not connected to the Trusted Network. Conversely, the Receiver Application Server is connected only to the Trusted Network.

The Sender Application Server and Receiver Application Server are connected by only a single fiber-optic cable. This fiber-optic cable is connected to each of the Sender Application Server and Receiver Application Server via their respective TX Module and RX Module. This ensures that all data flowing through the TOE must flow through the fiber-optic cable and are thereby covered by the *One-Way Information Flow SFP*.

This SFP contains following rules:

- It allows any information coming from the SFP Fiber Optic Interface of the TX Module and attempting to enter to the SFP Fiber Optic Interface of the RX Module.
- It allows any information attempting to exit from the SFP Fiber Optic Interface of the TX Module in order to enter the SFP Fiber Optic Interface of the RX Module.
- It denies any information attempting to leave through the SFP Fiber Optic Interface of the RX Module.
- It denies any information attempting to enter to the SFP Fiber Optic Interface of the TX Module from the SFP Fiber Optic Interface of the RX Module.

This SF is mapped to the following SFRs: *FDP_IFC.2, FDP_IFF.1*

8 Acronyms

CLI	Command Line Interface
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement