Certification Report

Data Diode

Author: Eugenia Ana CAPOTA

Table of Contents

[1 Certification Statement 3](#_Toc157770499)

[2 Executive Summary 3](#_Toc157770500)

[2.1 Introduction 3](#_Toc157770501)

[2.2 Evaluated product 3](#_Toc157770502)

[2.3 TOE scope 4](#_Toc157770503)

[2.4 Protection Profile Conformance 4](#_Toc157770504)

[2.5 Assurance Level 4](#_Toc157770505)

[2.6 Security Policy 4](#_Toc157770506)

[2.7 Security Claims 4](#_Toc157770507)

[2.8 Threats Countered 4](#_Toc157770508)

[2.9 Threat Countered by the TOE’s environment 4](#_Toc157770509)

[2.10 Threats and Attacks not Countered 4](#_Toc157770510)

[2.11 Environmental Assumptions and Dependencies 4](#_Toc157770511)

[2.12 Security Objectives for the TOE 5](#_Toc157770512)

[2.13 Security Objectives for the TOE’s Environment 5](#_Toc157770513)

[2.14 Security Functional Requirements 5](#_Toc157770514)

[2.15 Security Function Policy 5](#_Toc157770515)

[2.16 Evaluation Conduct 5](#_Toc157770516)

[2.17 General Points 5](#_Toc157770517)

[3 Evaluation Findings 5](#_Toc157770518)

[3.1 Introduction 6](#_Toc157770519)

[3.2 Misuse 6](#_Toc157770520)

[3.3 Vulnerability Analysis 7](#_Toc157770521)

[3.4 Evaluator’s Tests 7](#_Toc157770522)

[4 Evaluation Outcome 7](#_Toc157770523)

[4.1 Certification Result 7](#_Toc157770524)

[4.2 Recommendations 7](#_Toc157770525)

[5 References 8](#_Toc157770526)

[Annex A: Evaluated Configuration 9](#_Toc157770527)

[TOE Documentation 9](#_Toc157770528)

[TOE Configuration 10](#_Toc157770529)

# Certification Statement

The Data Diode is a unidirectional network allowing data to travel only in one direction. The TOE comes in three versions, each with a unique model number. The only difference between the TOE versions, with respect to the tests performed by the evaluators, is the operating speed.

|  |  |  |
| --- | --- | --- |
| **TOE Version** | **Model Number** | **Speed** |
| 1 | TP-Link MC200CM | 1 Gbit/sec |
| 1b | TP-Link MC100CM | 100 Mbit/sec |
| 1c | TP-Link MC200CM-MC100CM with slower (fast ethernet) receiver | 100 Mbit/sec |

The two versions tested by the evaluators are TP-Link MC200CM (1Gbit/sec) and TP-Link MC100CM with slower (fast ethernet) receiver (100 Mbit/sec).

The Data Diode has been evaluated and has met the security assurance requirements of 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.

# Executive Summary

## Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of the Data Diode, and is intended to assist prospective users when judging the IT security of the product.

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

## Evaluated product

The product evaluated is the Data Diode and it is also described in this report as the Target of Evaluation (TOE).

The TOE allows data to travel only in one direction. The purpose of the TOE is to transfer information 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.

Annex A contains details of the evaluated configuration and any additional TOE documentation.

## TOE scope

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

## Protection Profile Conformance

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

## Assurance Level

The Security Target [1] specifies the assurance requirements for the evaluation. The assurance incorporates predefined evaluation assurance level EAL7 (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. The assurance given by levels EAL1 to EAL2 is described in Part 3 of the Common Criteria Part 3 [2]. An overview of Common Criteria is given in Part 1 of the Common Criteria [3].

## Security Policy

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

## Security Claims

The TOE threats, assumptions, security objectives, security requirements and security assurance requirements are fully specified in the Security Target [1]. The Security Functional Requirements (SFRs) are taken from Part 2 of the Common Criteria [4].

## Threats Countered

A user or process on the downstream network that either (a) accidentally or deliberately breaches the confidentiality of some downstream information by transmitting data through the TOE to the upstream network, or (b) accidentally or deliberately breaches the integrity of the upstream network by transmitting data through the TOE to the upstream network.

## Threat Countered by the TOE’s environment

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

## Threats and Attacks not Countered

This certification report does not describe any threats or attacks which are not countered.

## Environmental Assumptions and Dependencies

The following assumptions exist in the TOE environment:

* The intended operation environment shall store and operate the TOE in accordance with the highest of each of the requirements of the upstream network and the downstream network.
* The TOE must be powered in such a way that users or processes on the downstream side cannot control power through the downstream network. This prevents unauthorized agents from controlling the signal carrier of the Bidirectional Upstream port, by toggling the TOE power.
* The only method of interconnecting the upstream network and downstream network is one or more units of the TOE, with all of the units operating in the same data flow direction. This prevents an unauthorized agent from using an untrustworthy product to circumvent the security provided by the TOE.

## Security Objectives for the TOE

* The information on the downstream network is kept confidential from the upstream network.
* The information on the upstream network cannot be altered by the downstream network.

## Security Objectives for the TOE’s Environment

* The intended operational environment shall be capable of storing and operating the TOE according to the requirements of the upstream network and of the downstream network.
* The intended operational environment shall provide power to the TOE such that the TOE power cannot be evaluated or interfered with from the downstream network.
* The only method to interconnect the upstream network and the downstream network is by using one or more units of the TOE. All the units must operate in the same data flow direction.

## Security Functional Requirements

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

* Information Flow Control FDP\_IFC.2.
* Simple Security Attributes FDP\_IFF.1.

## Security Function Policy

The TOE’s information flow security function policy is defined in FDP\_IFC.2 and FDP\_IFF.1.

## Evaluation Conduct

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting it’s Security Target [1].

The evaluation was completed on the 17.05.2024. This Certification Report was produced as a result.

## General Points

The evaluation addresses 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 is specified in Annex A.

Certification does not guarantee that the product is free from security vulnerabilities. This Certification Report and the belonging documents only reflect the view of the evaluators at the time of certification. It is the responsibility of users to verify whether any security vulnerabilities have been discovered since the date of this Certification Report.

# Evaluation Findings

The security assurance requirements for the TOE are those of 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. These components are explained in Part 3 of the Common Criteria [2].

|  |  |
| --- | --- |
| **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 |

|  |  |
| --- | --- |
| ADV\_SPM.1.1.D | The developer shall provide a formal security policy model for the **FFHDD policy**. |

## Introduction

The requirements specified in the Security Target [1] were addressed in this evaluation. The following sections contain considerations relevant to either users or those involved in subsequent assurance maintenance and re-evaluation of the TOE.

## Misuse

A risk of intentional and unintentional misconfigurations that could compromise confidential information always exists. In order to ensure that the TOE operates in a secure manner, users should follow the adequate guidance documents [1].

The guidance documents outline how to operate the TOE, the assumptions about the intended environment and all the requirements for external security. There is sufficient guidance for the user to effectively administer and use the TOE.

## Vulnerability Analysis

The TOE, in its intended environment, should be resistant to attackers. This Certification Report addresses all the potential exploitable vulnerabilities of the TOE.

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

## Evaluator’s Tests

The independent testing performed by the evaluators focused on the Security Functional Requirements (SFR) of the TOE and on the TOE Security Functionality Interface (TSFI).

The mathematical model used by the evaluators is a directed graph with 2 nodes. The graph contains a directed edge from node A to node B. Tests were conducted to confirm that a transfer cannot occur from node B to node A. In this sense a few algorithms were applied: Prim’s algorithm [5], Depth-First Search (DFS) [5] and Breadth-First Search (BFS) [5].

The evaluators considered the network under node B as a graph with undirected edges (bidirectional). The network above node A is considered the same.

The security models implemented over the directed graph are Biba and Bell-LaPadula [6]. Biba is a model focused on integrity and Bell-LaPadula is focused on confidentiality. These models describe information flow between different subjects.

Tests were also conducted on the Data Diode with a hardware enforced one-way communication channel. As expected, Ethernet frames (ARP, ARPING and PING packets) can only be transferred in one direction, according to the TX-RX connections on the media convertors of the Data Diode. The media convertors tested were: TP-Link MC200CM (1Gbit/sec) and TP-Link MC100CM with slower (fast ethernet) receiver (100 Mbit/sec).

# Evaluation Outcome

## Certification Result

According to the results produced by the evaluators and the conduct of the evaluation, the Data Diode meets the security assurance requirements of 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. These security assurance requirements are explained in Part 3 of the Common Criteria [2].

## Recommendations

Prospective users of the Data Diode should understand the specific scope of the certification by reading this report and the Security Target [1]. The TOE should be used according to the environmental considerations specified in the Security Target [1].

# References

1. Security Target - Data Diode. Internal document.
2. 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>
3. 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>
4. 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>
5. Even, S. (2011). *Graph algorithms*. Cambridge University Press.
6. Balon, N., & Thabet, I. (2004). The biba security model.

# Annex A: Evaluated Configuration

Figure 1 shows the TOE (Data Diode) functional block diagram consisting of two discrete fiber optical transceivers. The data transfer is implemented in hardware to guarantee complete unidirectionality.

The TOE has two operational interfaces to establish one-way communication, the Bidirectional Upstream port and the 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.

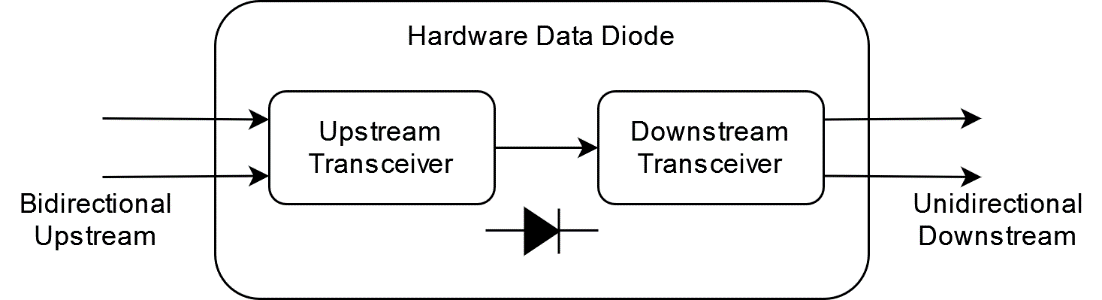


Figure 1. Hardware Data Diode functional block diagram.

# TOE Documentation

The supporting document evaluated was the Security Target for the Data Diode.