Autek Ingeniería S.L.
Avda. de Burgos 9, oficina 1
28036 Madrid
t 91 597 46 29 **f** 91 597 20 67
www.autek.es

PSTdiode ATKDDL
Security Target Lite

27/06/2019
Ref. 0555-24 R1.3

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Security Target Reference

1 **Title**: PSTdiode ATKDDL Security Target

2 **Security Target Version**: 1.3

3 **Author**: Autek Ingeniería, S.L.

4 **Security Target Date**: 27/06/2019

1.2. TOE Reference

5 **TOE Name**: PSTdiode ATKDDL.

6 **TOE Version**: 1.0.0

7 **Manufacturer:** Autek Ingeniería, S.L.

1.3. TOE Overview

8 The TOE is composed of two PCI-Express cards. One of the cards is equipped with a fibre optic transmitter, referred to as TX card (ATKDDL_TX). The other card is equipped with a fibre optic receiver, referred to as RX card (ATKDDL_RX). The set supports unidirectional data transfers of 1 Gbps.

1.3.1. TOE Use

9 The TOE has been designed to be installed in two standard PCs. The forseen use for the TOE is unidirectional data transmission from the PC hosting the TX card to the PC hosting the RX card. The TOE design guarantees that there is no information flow in the reverse direction, making it adequate for all uses in which a physically assured one-way information flow is required.

1.3.2. Type of TOE

10 The TOE is a hardware set (two PCI-Express cards) that constitute the core to build a unidirectional transmission system between two networks not connected by any other means.

1.3.3. Required Hardware and Software

11 The TOE needs two standard computers (not considered part of the TOE) with a PCI-Express bus 2.1 or higher.

12 The operating system (not considered part of the TOE) of the computers can be Windows (7 or higher) o Linux (Debian 9 or higher is recommended).

13 Two software components, at a minimum, developed specifically to build a system to allow data transmission and reception using the TOE.

1.4. TOE Description

14 The TOE is composed of two PC expanssion cards, PCI-Express. One of the cards is exclussivelly a transmitter and the other is exclussivelly a receiver.

15 The set has been designed to be used as the core componenent to build a unidirectional data transmission system, normally known as 'Data diode'. The TOE physically guarantees a unidirectional communication.

16 The transmission speed of PSTdiode ATKDDL is 1 Gbps.

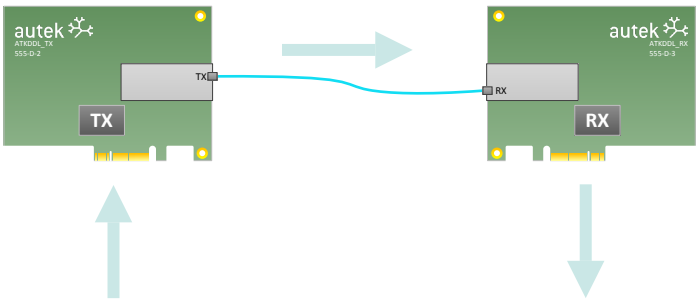

Figure 1. TOE Overview

1.4.1. Physical Scope

17 The TOE components are hand delivered by personnel from *Autek Ingeniería S.L.*

18 The TOE is composed of the following components:

- Transmitter card (ATKDDL_TX 1.0.0)
- Receiver card (ATKDDL_RX 1.0.0)

19 And by the CD-ROM ‘Software and Documentation’, containing:

- The 'User Manual' in PDF format (um_0555-10_r4.pdf).

1.4.2. Logical Scope

20 The TOE provides the following functionality:

- Unidirectional type of information transmission. Meaning that it guarantees that all the information transferred between the transmitter card and the receiver card flows in one unique direction, from the transmitter card to the receiver card.

1.5. Product Description

21 The TOE enables building a unidirectional transmission system.

1.5.1. Use Cases

22 The use of a unidirectional transmission system built using the TOE is applicable to several secure information exchange scenarios. Two of the most typical uses are described in the following sections. In all cases, the unidirectional transmission system must be the only connection path between the isolated security domains.

1.5.1.1. Confidentiality Guarantee

Security Properties	Typical Use	Description
Confidentiality	Classified networks	Introduction of information in a network with a higher classification level than that of the origin network. Guarantees that there is no information flow in the reverse direction, from the network of higher classification or security level to the lower one.

Table 1. Confidentiality Guarantee

1.5.1.2. Integrity and Availability Guarantee

Security Properties	Typical Use	Description
Integrity Availability	Isolated control networks	Extraction of information to monitor an isolated industrial control network. Precludes introduction of malware which may affect the integrity or availability of the industrial control network.

Table 2. Integrity and Availability Guarantee

1.5.2. Product Content

23 The product is composed of the TOE and a fibre optic cable (LC-LC simplex) which provides the physical connection between the transmitter card, TX card, and the receiver card, RX card, of the TOE.

24 Additionally, the product includes the following software components:

- Windows drivers to access the TOE.
- Libraries and TOE access application samples, as C++ source code, that facilitate the development of unidirectional transmission systems.

2. Conformance Claims

2.1. CC Conformance Claim

25 This Security Target is conformant with sections 2 and 3 of the CC v. 3.1, rev 5 standard and defines an evaluation assurance level EAL4 augmented with ALC_FLR.3 and AVA_VAN.5.

2.2. PP Conformance Claim

26 This Security Target has been developed specifically for PSTdiode ATKDDL system's security problem and does not claim conformance with any protection profile.

3. Security Problem Definition

3.1. Assets

27 There is only one asset to be protected by the TOE: the unidirectionality of the data sent from the transmitter card to the receiver card.

3.2. Threats

28 The following threats are considered:

3.2.1. Information flow

29 **T.R_TO_T_TRANSFER.**

1. A remote user (without physical access to the PC hosting the transmitter card, but with nework connectivity to it), manages to obtain, through the system, information from the receiver PC or other systems conncected to it.

2. A remote user (without physical access to the PC hosting the receiver card, but with network connectivity to it), manages to transmit any kind of information through the system, from the receiver PC to the transmitter PC.

3.3. Assumptions

30 **A.PHYSEC.** Both PCs hosting the transmitter and receiver cards (TOE hardware), shall be deployed in a physically controlled environment.

31 **A.LOCNOEVIL.** Authorized administrators with physical access to the TOE will not try to bypass the security functionality of the TOE.

32 **A.SINGLECHAN.** There are no other channels, apart from the TOE, through which information can flow between both PCs in which the transmitter and receiver cards are installed.

3.4. Organisational Policies

33 There are no organisational policies to be enforced by the TOE or its operational environment.

4. Security Objectives

4.1. Security Objectives for the TOE

34 **O.FLOW.** The TOE implements the following information flow policy:

1. There are no restrictions on the information transmitted from transmitter to receiver.

2. There must be no information flowing from receiver to transmitter.

4.2. Security Objectives for the Operational Environment

35 **OE.PHYSEC.** The PCs where both (transmitter and receiver) cards will be installed, will be placed in a physically controlled environment with access restrictions. Obvious ways to bypass the system (such as directly connecting both computers with a network cable) will be prevented by the organizational or physical measures of the operational environment.

36 **OE.LOCNOEVIL.** The TOE will be installed and administered by authorized administrators with physical access, and they will follow the TOE's secure use procedures.

37 **OE.TOPOLOGY.** The only possible way to connect the transmitter to receiver PC is through the TOE.

4.3. Justification of Security Objectives

	O.FLOW
T.R_TO_T_TRANSFER	X

Table 3. Security Objectives for the TOE

38 Flow control objective O.FLOW counters the T.R_TO_T_TRANSFER threat.

	OE.PHYSEC	**OE.LOCNOEVIL**	**OE.TOPOLOGY**
A.PHYSEC	X		
A.LOCNOEVIL		X	
A.SINGLECHAN			X

Table 4. Security Objectives for the Operational Environment

39 The security objective for the operational environment OE.PHYSEC ensures that the the A.PHYSEC assumption is directly fullfilled.

40 The security objective for the operational environment OE.LOCNOEVIL directly upholds the assumption A.LOCNOEVIL.

41 The security objective for the operational environment OE.TOPOLOGY directly upholds the assumption A.SINGLECHAN.

5. TOE Security Requirements

5.1. Security Functional Requirements

42 **This note applies to all security functional requirements:** The TOE uses two subjects: 'Input' and 'Output'. These subjects represent the information flowing into the transmitter part and the information leaving the receiver part. These subjects have no attributes.

43 **Note:** Despite the existence of a dependency, the FMT_MSA.3 requirement is not included because there are no security attributes.

5.1.1. FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

5.1.1.1. FDP_IFC.2.1

44 The TSF shall enforce the *[assignment: information transfer policy]* on *[assignment: 'Input', 'Output', all information]* and all operations that cause that information to flow to and from subjects covered by the SFP.

5.1.1.2. FDP_IFC.2.2

45 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

5.1.2.1. FDP_IFF.1.1

46 The TSF shall enforce the *[assignment: information transfer policy]* based on the following types of subject and information security attributes: *[assignment: 'Input', 'Output', all information]*.

5.1.2.2. FDP_IFF.1.2

47 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *[assignment: Information flow from 'Input' to 'Output' is permitted]*.

5.1.2.3. FDP_IFF.1.3

48 The TSF shall enforce the *[assignment: N/A]*.

5.1.2.4. FDP_IFF.1.4

49 The TSF shall explicitly authorise an information flow based on the following rules: *[N/A]*.

5.1.2.5. FDP_IFF.1.5

50 The TSF shall explicitly deny an information flow based on the following rules: *[assignment: Information flow from 'Output' to 'Input' is denied]*.

5.2. Security Assurance Requirements

51 TOE development and evaluation will be done in conformity with the following assurance level:

- EAL4 + ALC_FLR.3 + AVA_VAN.5

52 The security assurance requirements corresponding to this level with the cited enhancements are shown in Table 5, "Security Assurance Requirements". Part 3 of Common Criteria *for Information Technology Securtiy Evaluation* contains the detailed description of these components.

Assurance Class	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_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
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

Assurance Class	Assurance components
	ASE_SPD.1 Security problem definition
	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

Table 5. Security Assurance Requirements

5.3. Security Functional Requirements Rationale

	O.FLOW
FDP_IFC.2	X
FDP_IFF.1	X

Table 6. Security Requirements Rationale

5.3.1. Non Satisfied Dependencies Justification

53 FMT_MSA.3 dependency has not been satisfied because there are no security attributes.

5.3.2. Security Functional Requirements Rationale

54 The flow objective O.FLOW is met due to the existence of a complete flow control policy FDP_IFC.2 between 'Input' and 'Output' subjects, managed in accordance with the restrictions established in FDP_IFF.1.

5.4. Security Assurance Requirements Rationale

55 The desired security assurance for the TOE is the one provided by the evaluation level EAL4 + ALC_FLR.3 + AVA_VAN.5.

56 This security assurance level has been chosen to assure the final user that the product has been developed following a systematic engineering approach and development best practices, beeing capable of resisting attacks of adversaries with high attack potential.

6. TOE Summary Specification

57 The product *PSTdiode ATKDDL* guarantees compliance with security functional requirements: FDP_IFC.2 and FDP_IFF.1. The information flow control policy is complete and it explicitly applies in all cases.

58 The following sections detail the ways in which *PSTdiode ATKDDL* guarantees that it explicitly allows the flow from 'Input' to 'Output' and explicitly denies any information flow from 'Output' to 'Input'.

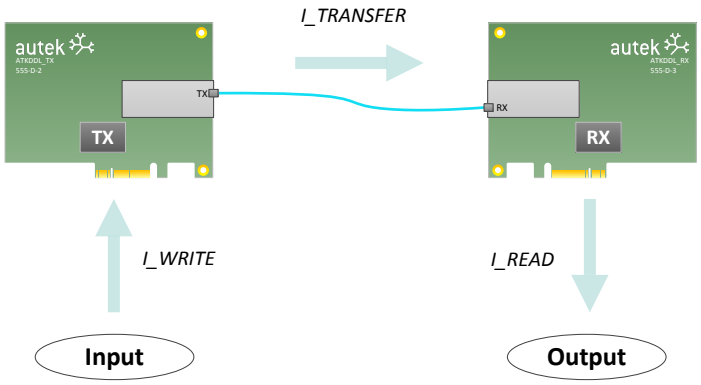

Figure 2. TOE Interfaces and Information Flow

6.1. Hardware Design

59 *PSTdiode ATKDDL* is composed of one transmitter card (TX) and one receiver card (RX). The information flow allowed is the one flowing from the transmitter card (TX) to the receiver card (RX).

60 The hardware design of the product guarantees there cannot be an information flow in the reverse direction, from the 'Output' to the 'Input':

- The transmitter card (TX) hardware lacks the components that would be necessary to receive any information flow from the receiver card (RX).
- The receiver card (RX) hardware lacks the components that would be necessary to transfer any information flow to the transmitter card (TX).

6.1.1. Interfaces

61 The TOE implements the hardware interfaces that allow data to enter the transmitter card (TX), to be sent from the transmitter card (TX) to the receiver card (RX) and to exit the receiver card (RX):

- The data input interface (I_WRITE) allows data to be sent to the transmitter card (TX), through the PCI-Express bus, to be transferred in a unidirectional manner to the receiver card (RX).
- The unidirectional data transfer interface (I_TRANSFER) allows transfer of information from the transmitter card (TX) to the receiver card (RX) via fiber optics.

- The data output interface (I_READ) allows reading the data received by the receiver card (RX), through the PCI-Express bus.