CSEC

Swedish Certification Body for IT Security

Certification Report - Owl DualDiode Communication Cards 10G, 2.5G, 1.0G v.7 & v.7t Models

Issue: 1.0, 2019-Sep-11

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the Owl DualDiode Communication Cards (DDCC) which consists of the 10G v.7 DualDiode Communication Card, the v.7 Standard Capacity 2.5G Communication Cards, and the v.7 and v.7t Standard Capacity 1.0G Communication Cards, which are designed and manufactured by Owl Cyber Defense Solutions, LLC (Owl).

The DDCC provide an absolute one-way unidirectional flow of any data and information between a source domain, the sending host system or network to a destination domain, the receiving host system or network. Thereby protecting the destination host or network from any potential leaks of information or potential network probing attacks.

The Security Target [ST] is the basis for this evaluation. It does not claim conformance to any Protection Profile.

The whole TOE (hardware products and the guidance document on a disc) is packaged and secured with security tape, which is delivered to Owl's consumer by commercial couriers (e.g. FebEx). Owl sends a shipment notification to the customer as an additional security delivery measure. The shipment notification tells the customer when the TOE is shipped and alerts them of the impending arrival date.

Each TOE component can be uniquely identified by its PCB (Printed Circuit Board) version and the firmware version. The TOE guidance can also be uniquely identified by its title and version.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden and the developer's premises in Danbury, Connecticut, USA, and was completed on the 1st of July 2019.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation conforms to evaluation assurance level EAL 4, augmented by AVA_VAN.4.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2018006
Name and version of the certified IT product	• Owl DualDiode 10G v.7 Communication Cards, Firmware Revision V39 • Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards in Commercial Variation, Firmware Revision V77 • Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards in Industrial Variation, Firmware Revision V77 • Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards in Commercial Variation, Firmware Revision V77 • Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards in Industrial Variation, Firmware Revision V77 • Owl DualDiode v.7t Commercial 1.0G Communication Cards, Firmware Revision V75 • Owl DualDiode v.7t Industrial 1.0G Communication Cards, Firmware Revision V75
Security Target Identification	DualDiode Communication Cards 10G, 2.5G, 1.0G v.7 & v.7t Models, Security Target, version 01m, June 2019
EAL	EAL 4+ AVA_VAN.4
Sponsor	Owl Cyber Defense Solutions, LLC
Developer	Owl Cyber Defense Solutions, LLC
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.22.3
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2019-09-11

3 Security Policy

The TOE provides the following TOE security functionality:

- User data protection (one-way information flow) The TOE provides unconditional and unidirectional information flow control between two separate host systems. Please note that the "two separate host systems" are the Sending Host System and the Receiving Host System in the TOE environment. Information that comes from the Sending Host System goes one-way only through the TOE and then reaches the Receiving Host System.
- Protection of the TSF (hardware failure detection) Any component failure in the TOE will prevent any means of unintended information flow from bypassing the TSF.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes two assumptions on the usage of the TOE.

A.ADMIN Authorized personnel that are used to install, administer and use the TOE are trustworthy, competent and follow the guidance regarding the usage of the TOE.

A.GUIDE Authorized personnel shall ensure that the TOE has been delivered, installed and is administered in accordance with security guidance, in a manner that maintains security. The appropriate security authority shall accredit the installation of the TOE before taking it into operation.

4.2 Environmental Assumptions

The Security Target [ST] makes four assumptions on the operational environment of the TOE.

A.CONNECTION The TOE must be installed so all relevant network traffic will only flow through the TOE and hence be subject to the organizational security policy.

A.EMISSION The TOE must be installed and operated in an environment where physical or other security measures prevent any Emissions Security attacks or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions attacks.

A.NETBREAK The operational environment of the TOE shall ensure that information cannot flow between the source network and destination network without going through the TOE. This prevents a threat agent from circumventing the security provided by the TOE.

A.PHYSICAL The TOE must be operated in a protected environment prevents unauthorized physical access to the TOE.

4.3 Clarification of Scope

The Security Target contains four threats, which have been considered during the evaluation.

T.FAILURE The TOE has a hardware failure that allows access to confidential information on the destination side through the TOE.

T.OLD_INF An attacker may gather residual information by monitoring the IP stack at the Transport Layer from previous information transmissions or from internal TOE data.

T.TAMPER An attacker tampers with the TOE to in order to bypass the unidirectional interface of the TOE or otherwise compromise or influence the behavior of the TOE.

T.WRONGWAY An attacker or process, e.g. “Trojan Horse”, deliberately or accidentally transfers information from the destination host or network back through the TOE to the originating source host or network.

The Security Target contains two Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.ONEWAY Information from the source host must only flow one-way to the attached destination host.

P. SEALS The installation of the TOE in its operational environment shall be done with visible tamper detection markings that can be manually inspected to detect any tampering.

5 Architectural Information

The TOE is the Owl DualDiode Communication Cards (DDCC) providing an absolute one-way unidirectional flow of any data and information between a source, the Sending Host System, and a destination domain, the Receiving Host System.

The whole physical boundary of the TOE is covered by the two modules:

- The Send-Only DDCC module
  - 1. Receiving electrical signals from the Sending Host System through the PCI Express (PCIe) interface (information entering the Send-Only DDCC module);
  - 2. The on-board FPGA segmenting the information (packages) received from the PCIe interface to fragments according to the Owl proprietary transfer protocol;
  - 3. The transmitting part of the optical transceiver converting electrical signals to optical signals (information leaving the Send-Only DDCC module).
- the Receive-Only DDCC module
  - 1. The receiving part of the optical transceiver receiving optical signals and converting them into electrical signals (information entering the Receive-only DDCC module);
  - 2. The on-board FPGA reassembling the received fragments (coded in Owl's proprietary transfer protocol) to packages;
  - 3. Passing the packages to the Receiving Host System through the PCIe interface (information leaving the Receive-Only DDCC module).

The TSF is enforced by the TOE hardware design together with the Owl's proprietary transfer protocol. The former one makes sure that there is only one way electrically/optically that information can travel through the TOE. The latter one is in place to verify that what received at the Receive-Only DDCC module is consistent to what is expected to be received using checksum. In case of hardware component failures in the TOE, the broken data fragments will be discarded.

6 Documentation

The following guidance documents is available

- Owl Version 7 Card (Type 7000) Installation Manual v.05a [IGUIDE]

7 IT Product Testing

7.1 Test Configuration

Since the TOE is a static hardware product, no configuration of the TOE is needed during the testing.

7.2 Developer Testing

The developer devised nine test cases to test the TOE. The evaluator determined that the first six test cases have already been sufficient to fulfill the ATE test requirements.

Each test case consists of a number of test steps, and each test step contains one specific task to perform. All the tests are manually executed and do not need any automatic testing scripts.

The developer has tested the TOE directly at the module and module interface level.

The developer has provided the results of all test cases that were performed. All tests were successful.

7.3 Evaluator Testing

The evaluator repeated all the developer's tests on two TOE variations using a sampling strategy. Furthermore, the evaluator decided not to add any additional tests based on a justified rationale.

The tests were performed directly on the module and module interface level.

Regarding the testing environment, the evaluator used the same test equipment as the ones used by the developer for the testing.

The re-run of the developer tests was performed by the evaluator successfully. The expected tests results and the actual test results were consistent.

7.4 Penetration Testing

The evaluator performed a search of public domain sources and a methodical analysis on the evaluation evidences, in the end concluded that no potential vulnerability was identified to be applicable to the TOE. Therefore, the evaluator determined that penetration tests are not necessary.

8 Evaluated Configuration

The TOE is a static hardware product with firmware loaded. No configuration is needed or possible.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance	Class/Family	Short name	Verdict
Development		ADV	PASS
	Security architecture description	ADV_ARC.1	PASS
	Complete functional specification	ADV_FSP.4	PASS
	Implementation representation of the TSF	ADV_IMP.1	PASS
	Basic modular design	ADV_TDS.3	PASS
Guidance documents		AGD	PASS
	Operational user guidance	AGD_OPE.1	PASS
	Preparative procedures	AGD_PRE.1	PASS
Life-cycle support		ALC	PASS
	Production support, acceptance procedures and automation	ALC_CMC.4	PASS
	Problem tracking CM coverage	ALC_CMS.4	PASS
	Delivery procedures	ALC_DEL.1	PASS
	Identification of security measures	ALC_DVS.1	PASS
	Developer defined life-cycle model	ALC_LCD.1	PASS
	Well-defined development tools	ALC_TAT.1	PASS
Security Target evaluation		ASE	PASS
	Conformance claims	ASE_CCL.1	PASS
	Extended components definition	ASE_ECD.1	PASS
	ST introduction	ASE_INT.1	PASS
	Security objectives	ASE_OBJ.2	PASS
	Derived security requirements	ASE_REQ.2	PASS
	Security problem definition	ASE_SPD.1	PASS
	TOE summary specification	ASE_TSS.1	PASS
Tests		ATE	PASS
	Analysis of coverage	ATE_COV.2	PASS
	Testing: basic design	ATE_DPT.1	PASS
	Functional testing	ATE_FUN.1	PASS
	Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment		AVA	PASS
	Methodical vulnerability analysis	AVA_VAN.4	PASS

10 Evaluator Comments and Recommendations

None

11 Glossary

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security,
Destination Domain or Destination	The final destination host system or network to receive the information transmitted through the TOE. Part of the TOE; the Owl Receive-Only DDCC must be integrated into a receiving host system. See Receiving Host.
DualDiode	Deployment of two Data Diode protection mechanisms to enforce one-way transfer security policy at either end of cross-domain connection.
DDCC	DualDiode Communications Card:
EAL	Evaluation Assurance Level
FPGA	Field Programmable Gate Array
Host or Host System	A general term for a computer system that has been allocated for the installation and operation of the Owl DDCC. Once the Owl DDCC hardware is installed in a host it assumes the role of DualDiode host, gateway, receiving host of the destination domain and sending host of the source domain.
ITSEF	IT Security Evaluation Facility,
PCIe	Peripheral Component Interface Express,
Receive-Only DDCC	The Receive-Only DDCC only allows information for transfer to flow from its optical interface across the Receive-Only DDCC and to the host system. All information presented for transfer to the Receive-Only DDCC is subject to the unconditional unidirectional information flow. No information is able to flow from the host system across the Receive-Only DDCC and through the optical interface of the Receive-Only DDCC. This non-bypassability of the TOE is enforced at the physical level.
Receiving Host	The host system or network in which a Receive-Only DDCC is installed. The Receiving Host is to receive information through the Receive-Only DualDiode Communication Card.
Sending Host	A host system or network in which a Send-Only DDCC is installed. The Sending Host is to send information through the Send-Only DualDiode Communication Card. See Source Domain.
Source or Source Domain	The originating network and / or source host system whence information is transmitted through the TOE. The Source or Source Domain must have a host system with an Owl Send-Only DualDiode Communication Card installed. See Sending Host.
Send-Only DDCC	The Send-Only DDCC only allows information for transfer to flow from the host system across the DDCC through the optical interface. All information presented to the Send-Only DDCC is subject to the unconditional unidirectional information flow. No information is able to flow from out-

	side the Send-Only DDCC through the optical interface across the Send-Only DDCC and into the host system. This non-bypassability of the TOE is enforced at the physical level.
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

12 Bibliography

ST	DualDiode Communication Cards 10G, 2.5G, 1.0G v.7 & v.7t Models, Security Target, version 01m, June 2019
IGUIDE	Owl Version 7 Card (Type 7000) Installation Manual v.05a, 2019-06-11
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-01-21, document version 30.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used.

A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.21.5 valid from 2018-11-19

QMS 1.22 valid from 2019-02-01

QMS 1.22.1 valid from 2019-03-08

QMS 1.22.2 valid from 2019-05-02

QMS 1.22.3 valid from 2019-05-20

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.22.3". The certifier concluded that, from QMS 1.21.5 to the current QMS 1.22.3, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment