Swedish Certification Body for IT Security

Certification Report - Owl XDE Radium v1.3

Issue: 1.0, 2022-sep-19

Authorisation: Helén Svensson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is Owl XDE Radium V1.3 module providing an absolute one-way connection between a Source domain – the sending host system or network, and a Destination domain - a receiving host system or network. Information is permitted to flow from the sending host system or network to the receiving host system or network. Data, information, or communications originating at the receiving host system or network are not allowed to flow to the sending host system or network through the XDE Radium.

The Target of Evaluation (TOE) is Owl XDE Radium v1.3 with the following elements:

- Owl XDE Radium v1.3 optical module
- Owl XDE Radium v1.3 digital module
- TOE Documentation

It is envisioned that up to 10 TOE XDE Radium modules will be packed into a single product box. More than one product box may be packed into a product carton for shipment.

Each TOE will have a unique serial number attached to the board itself. There will be a bill of lading inside or attached to each product box listing the TOEs and their associated serial numbers. Customers will be able to compare the Invoice, Bill of Lading, and TOE serial numbers to validate the authenticity of the delivered Owl products. Product boxes will be sealed with tape in a manner that will make obvious any post-shipment attempt at tampering, product modification, or substitution. The secure packaging is done to give customers confidence that they are receiving unaltered, certified Owl products.

Owl works with trusted carriers to ensure accurate tracking and delivery of product boxes/cartons to customers' delivery destination. Standard carriers like FedEx will forward tracking information and delivery notifications to the customer including an ETA and the last known location of the TOE or solution that was sent. If another carrier is used, Owl will confirm with the customer point of contact a shipment's ETA. These methods are employed by Owl to limit the opportunity an untrustworthy individual could modify or substitute the TOE or solution. This would virtually guarantee the TOE or solution received by the customer came directly from Owl and has not been tainted or altered.

TOE documentation will be delivered to customer separately from the physical products via secure electronic means. Firmware or software updates to deployed systems will be signed and accompanied by a valid X.509 certificate to ensure the firmware/software provenance. All updates will be delivered via secure electronic means.

No PP claims are being made.

The evaluation has been performed by atsec information security AB in Danderyd, Sweden. All evaluator testing was performed in Danderyd, Sweden, and the site visit was executed remotely through video link between atsec in Danderyd, Sweden and Owl in Connecticut, USA.

The evaluation was completed on 2022-09-02. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports, and by observing site-visit and testing. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 4 augmented by AVA_VAN.4

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by atsec information security AB.

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	CSEC2021009
Name and version of the certified IT product	Owl XDE Radium v1.3 Major components: • Firmware Version: 1.4.0.15 • HW Version: Rev. B-01 RW-02 • XD Manager Version: 1.0.0.2 • User Guide Version: V1.3_r02a TOE Hardware Models: • Owl XDE Radium V1.3 Optical Isolator module (XDE-RAD-OWT-OI-XX) • Owl XDE Radium V1.3 Digital Isolator module (XDE-RAD-OWT-DI-XX)
Security Target Identification	Owl XDE Radium V1.3 One-Way Transfer (OWT) Data Diode Module, Security Target, Owl Cyber Defense Solutions, LLC, 11 February 2022, document version 1.3
EAL	EAL4 + 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	2.2
Scheme Notes Release	19.0
Recognition Scope	CCRA, SOGIS and EA/MLA
Certification date	2022-09-19

3 Security Policy

The TOE provides the following TOE security functionality:

- User data protection
- Protection of the TSF

3.1 User data protection

The Owl XDE Radium module passes data from the Send-Only side to the Receive-Only side and provides the following security features:

- Information Flow Control - The TOE directly interfaces with the source host and the destination host to transmit information in a unidirectional flow through a hardware isolator (optical or digital). The module's Send-Only side of the TOE is only capable of transmitting information and conversely the module's Receive-Only side is only capable of receiving information.
- Residual Information - The TOE stores no user data in the board's data handling components. Intentional or unplanned power loss to the Source side will result in immediate dropping of all buffered user data, leaving no residual user information on the board. Intentional or unplanned power loss to the Destination side will likewise result in immediate dropping of all buffered user data, leaving no residual user information on the board. Simultaneous loss of power to both sides results in complete loss of any residual data, and prevents the TOE from passing and user data from Source to Destination networks.

3.2 Protection of the TSF

The design feature has been incorporated in the Owl XDE Radium module to ensure the integrity, reliability, and security of the TOE:

- Fail Secure - XDE Radium's components and overall physical board architecture enforces one-way data flow from Source to Destination. Any major component failure in the TOE will stop data flow entirely, thus preventing unintended information flow from bypassing the TSF.

4 Assumptions and Clarification of Scope

4.1 Usage and Environmental Assumptions

The Security Target [ST] makes six 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.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.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.

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.

4.2 Clarification of Scope

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

T.FAILURE

The TOE has a hardware failure that allows access to confidential or proprietary information on the source side through the TOE.

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 source host or network back through the TOE to the originating source host or network.

The Security Target contains one 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.

5 Architectural Information

The TOE is Owl XDE Radium V1.3 module providing an absolute one-way connection between a Source domain – the sending host system or network, and a Destination domain - a receiving host system or network. Information is permitted to flow from the sending host system or network to the receiving host system or network. Data, information, or communications originating at the receiving host system or network are not allowed to flow to the sending host system or network through the XDE Radium.

The XDE Radium is a relatively simple device. It has no Central Processor Unit (CPU), and thus no Operating System (OS). The major security components are two Field Programmable Gate Arrays (FPGAs) and either an optical or digital isolator. The FPGAs and Isolator (optical or digital) working together, and aided by the overall board architecture, perform packet-by-packet header filtering and enforce strict one-way transfer (OWT) between the Source and Destination networks.

XDE Radium will be a primary security component within host devices such as industrial servers, edge computers, gateways, sensors, programmable logic controllers (PLC), Perimeter Defense Systems (PDS), etc. It is expected that XDE Radium will be implemented in host devices that connect two dissimilar networks, zones, or enclaves.

6 Documentation

The following guidance documents is available:

- XDE Radium Version 1.3 User Guide [GUIDE]

7 IT Product Testing

7.1 Developer Testing

The developer devised ten 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 by use of common tools and a few simple scripts to facilitate the process.

Both models of the TOE (Optical and Digital Isolator) have been tested.

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

7.2 Evaluator Testing

The evaluator started with analysis of the developer test evidence, which provides information on how the TSF documented in the [ST] has been tested by the developer.

Based on the analysis, the evaluator decided to re-run a part of the developer's test and suggested to add additional tests as part of developer tests.

The tests were performed on both versions of the TOE (Optical and Digital Isolator).

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

7.3 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

XDE Radium uses a software Configuration Utility application for setting Source and Destination network whitelisted connections. The Configuration Utility runs on Windows and Linux operating systems, and the configuration workstation/laptops connects to the circuit board's Source and Destination serial UART connectors to download network configuration policy prior to normal operations. Once configurations are downloaded to the FPGAs, the Configuration Utility's workstation/laptop will be disconnected from the circuit board and will not be used during normal operation.

During the normal operation, the TOE is a static product. 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 Moderate.

The certifier reviewed the work of the evaluators 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	Component	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, document describing the methodology used in Common Criteria evaluations
Destination Field Programmable Gate Array (FPGA)	The XDE Radium's Destination FPGA interfaces with the module's isolator on one side and the Destination Network on the other side. The Destination FPGA contains firmware logic which enables it to rebuild packet headers and deliver packets to pre-defined network destinations while simultaneously preventing data flow from Destination to Source networks.
Destination Domain or Destination	The destination host system or network to receive the information transmitted through the TOE.
EAL	Evaluation Assurance Level
FPGA	Field Programmable Gate Array is a COTS semiconductor device containing programmable logic components, interconnects, and memory. FPGAs include high level functionality fixed into the silicon but are also configurable by loading application programs to perform complex functions such as packet segmentation, framing or reassembly. FPGA are "deterministic," in that they only perform the functions for which they are programmed.
Isolator	XDE Radium V1.3uses either an optical or digital isolator to impose physical oneway flow control restrictions on data flowing through the device.
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
PP	Protection Profile (Does not exist for one-way packet transfer systems)
Source Field Programmable Gate Array (FPGA)	The XDE Radium's Source FPGA interfaces with the Source network on one side and the modules optical or digital isolator on the other side. The Source FPGA contains firmware logic which enables it to evaluate and deconstruct packet headers before delivering packets to the isolator for one-way transfer.
Source or Source Domain	The originating network and / or source host system whence information is transmitted through the TOE.
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation – XDE Radium V1.3module
TSF	TOE Security Function
XDE	An Owl product brand acronym representing the term, "Cross-Domain Embedded"

12 Bibliography

ST	Owl XDE Radium V1.3 One-Way Transfer (OWT) Data Diode Module, Security Target, Owl Cyber Defense Solutions, LLC, 11 February 2022, document version 1.3
GUIDE	XDE Radium Version 1.3 User Guide, Owl Cyber Defense Solutions, LLC, 2022-05-25, document version r02a
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
EP-002	EP-002 Evaluation and Certification, CSEC, 2021-10-26, docu-ment version 34.0

Appendix A Scheme Versions

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

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.2	2022-06-27	New procedure for search in public vulnerability databases
2.1.1	2022-02-25	None
2.1	2022-01-18	None
2.0	2021-11-24	None
1.25	Application	Original version

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 11 - Methodology for AVA_VAN 4 and 5
- Scheme Note 15 – Testing
- Scheme Note 16 - Additional planning requirements
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 27 - ST requirements at the time of application for certification
- Scheme Note 28 - Updated procedures for application, evaluation and certification
- Scheme Note 31 - New procedures for site visit oversight and testing oversight