Swedish Certification Body for IT Security

Certification Report Arbit Data Diode 2.0

Issue: 1.0, 2016-okt-13

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary

The Target of evaluation, TOE, is a one-way data diode for optical information.

The TOE implements the one-way data diode through a repeater, where a fiber optic network cable is connected to the LOW port and a fiber optic network cable is connected to the HIGH port.

Information can only be received from the LOW network connected on the LOW port, and no light can spill over to the LOW port from the HIGH port.

Information received on the LOW port is allowed to exit through the HIGH port, without further processing.

The TOE design is presented solely using modules. The abstraction level of subsystems was not found to be required due to the simple design of the TOE.

The TOE consists of one module, the PCBA module. It represents the populated printed circuit board. The PCBA module has seven interfaces, two of which are TSF interfaces.

The TOE is a static hardware-only product, and consists of a printed circuit board.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT Security Evaluation, version 3.1, release 4.

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 is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL5 + AVA_VAN.5 and ALC_FLR.1

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	CSEC2015011
Name and version of the certified IT product	Arbit Data Diode 2.0
Security Target Identification	Arbit Data Diode Security Target, version 4.0, 2016-09-05
EAL	EAL5 +AVA_VAN.5 and ALC_FLR.1
Sponsor	Eurotempest AB, Teknikringen 10, Linköping. Sweden
Developer	Eurotempest AB, Teknikringen 10, Linköping. Sweden
ITSEF	atsec information security AB, Svärdvägen 3C, S-182 33 Danderyd, Sweden
Common Criteria version	3.1 release4
CEM version	3.1 release 4
Certification date	2016-10-13

3 Security Policy

The TOE implements the One-Way information flow control policy (One-Way SFP), which is defined as:

Subjects:

- LOW port
  The input interface of the data diode.
- HIGH port
  The output interface of the data diode.

Information:

- An optical signal that can traverse the HIGH or LOW port.

Policy:

- Information is allowed to enter the TOE through the LOW port and may leave through the HIGH port.
- Information is not allowed to leave the TOE through the LOW port.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes one assumption on the usage of the TOE.

A.INTEGRATOR - The integrator who is performing the installation of the TOE is well-trained and competent in the prevention of signal leakage, and will properly adhere to the TOE guidance.

4.2 Environmental Assumptions

One assumption on the environment is made in the Security Target.

A.PHYSICAL - The TOE and its interfaces will be physically protected from unauthorized access and mechanical, electrical, optical, radiation or any other form of physical influence.

4.3 Clarification of Scope

The Security Target [ST] contains one threat, which have been considered during the evaluation.

T.DATA_LEAK - TA-LOW and/or TA-HIGH threat agents may be able to cause HIGHINFO to exit the TOE through the LOW port.

The Security Target [ST] contains one organisational security policies:

P.ONE_WAY_FLOW - The TOE shall allow information to enter through the LOW port and then leave through the HIGH port.

5 Architectural Information

The TOE is a one-way data diode for optical information. It can be the connection point between a high security and low security network. The actual transmission is handled by two dedicated servers, with the data diode in between them. The data diode ensures that information can only flow from the pitcher to the catcher, but not the other way. This allows for automated information transfer from the low security network to the high security network without manual intervention, while preventing the opposite ow direction. Another usage scenario is the export of information from a protected network to a more open environment. The security goal is in this case to allow the export, while preventing any potential attacks from reaching the protected network.

The TOE implements the one-way data diode by repeating the signal emitted by the pitcher (part of the LOW network) to the catcher (part of the HIGH network). The optical fiber from the pitcher connects to the LOW port of the TOE. The optical fiber to the catcher connects to the HIGH port of the TOE. The only allowed information flow is therefore from the LOW to the HIGH side. The HIGH port has a physical light emitter. The LOW port has a physical light receiver and has no light emitting capability. The TOE implementation is only utilizing the physical property of the LOW port and is not dependent on any software.

All signal processing in the TOE is performed in hardware at the Physical Medium Dependent sublayer in Ethernet [IEEE 802.3]. The TOE does not perform any higher layer signal parsing such as Ethernet frames or TCP/IP processing.

The TOE supports a range of light signals up to 10.3125 Gbps. The specific supported light range of each TOE is determined during production based on customer requirements.

6 Documentation

Arbit Data Diode Integrator Guide v2.0 [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

7.2.1 Testing Effort

The TOE is a one-way data diode for optical information, which ensures that the information flow through the data diode is one-way only. It is hardware-only, and consists of a printed circuit board. Due to its simplicity, the TOE is solely described at the module level. One module is defined, which has seven module interfaces. Two of the seven interfaces are TSFIs.

The developer devised four test cases to test the TOE. Each test case consists of several test steps, and each test step contains one specific task to perform, e.g. connecting a cable between the TOE and the testing equipment. All the tests are manually executed and do not need any automatic testing scripts.

7.2.2 Results

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

7.3 Evaluator Testing Effort

7.3.1 Testing Effort

Since the TOE is fairly simple and its functionality is straightforward, the developer devised four test cases to test every instance of the TOE. Therefore, the evaluator decided to re-run all the four developer tests instead of using a sampling strategy.

Furthermore, the evaluator supplemented the developer testing strategy by adding new tests in order to provide better coverage and depth in the TOE testing. Four evaluator tests were added.

7.3.2 Results

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

7.4 Evaluator Penetration Testing

In order to identify potential vulnerabilities in the TOE, the evaluator performed an independent methodical analysis and a search of public domain sources. The vulnerability analysis did not reveal any potential vulnerability in the TOE. The evaluator also concluded that the tests already performed were sufficient and no further penetration testing was required

8 Evaluated Configuration

The TOE is a static hardware product, and consists of a printed circuit board. 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 Enhanced-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 respective 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 semi-formal functional specification with additional error information	ADV_FSP.5	PASS
Implementation representation of the TSF	ADV_IMP.1	PASS
Well-structured internals	ADV_INT.2	PASS
Semiformal modular design	ADV_TDS.4	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
Development tools CM coverage	ALC_CMS.5	PASS
Delivery procedures	ALC_DEL.1	PASS
Identification of security measures	ALC_DVS.1	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Compliance with implementation standards	ALC_TAT.2	PASS
Security Target evaluation	ASE	PASS
ST introduction	ASE_INT.1	PASS
Conformance claims	ASE_CCL.1	PASS
Security problem definition	ASE_SPD.1	PASS
Security objectives	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Derived security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE	PASS

Analysis of coverage	ATE_COV.2	PASS
Testing: modular design	ATE_DPT.3	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Methodical vulnerability analysis	AVA_VAN.5	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
Catcher	The entity receiving information from the data diode. It resides on the HIGH network.
Data diode	A device that allows information to flow from the input to the output, but not the other way.
HIGH network	The network which is to receive information from the LOW network, through the TOE.
HIGH port	The output interface of the data diode. HIGH devices and networks are connected to this interface.
HIGH system	Any system residing on the HIGH network, excluding the TOE.
Information	An optical signal that can traverse the HIGH or LOW port.
LOW network	The network from which information is to be sent to the HIGH network, through the TOE.
LOW port	The input interface of the data diode. LOW devices and networks are connected to this interface.
LOW system	Any system residing on the LOW network, excluding the TOE.
Pitcher	The entity sending information to the data diode. It resides on the LOW network.
Port	The physical interface by which the optical cables are connected to the TOE.

12 Bibliography

[ST] Arbit Data Diode Security Target, version 4.0, 2016-09-05

[IGUIDE] Arbit Data Diode Integrator Guide, version 2.0, 2016-09-05

[IEEE 802.3] IEEE Standard for Ethernet
http://standards.ieee.org/about/get/802/802.3.html

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1, revision 4, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, revision 4, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, version 3.1, revision 4, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version 3.1, revision 4, September 2012, CCMB-2012-09-004

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

Version	Introduced	Impact of changes
1.19.3	2016-06-02	No impact
1.19.2	2016-04-28	No impact
1.19.1	2016-03-07	No impact
1.19	2016-02-05	No impact
1.18.1	Application	Original version

A.2 Scheme Notes

Version	Introduced	Impact of changes
4.0	Application	Original version