CSA
SINGAPORE

Cybersecurity
Certification Centre
CYBER SECURITY AGENCY OF SINGAPORE

Certificate Report

Version 1.1

17 August 2021

CSA_CC_21002

For

ADPICS Data Diode (ADPICS-DD) Version 1.0

From

Attila Cybertech Pte Ltd.

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	August 2021	Released
1.1	August 2021	Minor editorial changes

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the ADPICS Data Diode (ADPICS-DD) Version 1.0 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS).

The TOE consists of the following.

Name and version	Version
ADPICS Data Diode (ADPICS-DD) Hardware	1.0
Attila ADPICS Data Diode User Guidance	2.0

The ADPICS Data Diode (i.e. the TOE) is a network gateway that ensures physical layer one-way data transmission through the TOE. The TOE is used to connect two separate networks together, one being the Source Zone and the other being the Destination Zone. The TOE ensures that the data can only flow from the Source Zone to the Destination Zone but blocks data flow in the reverse direction.

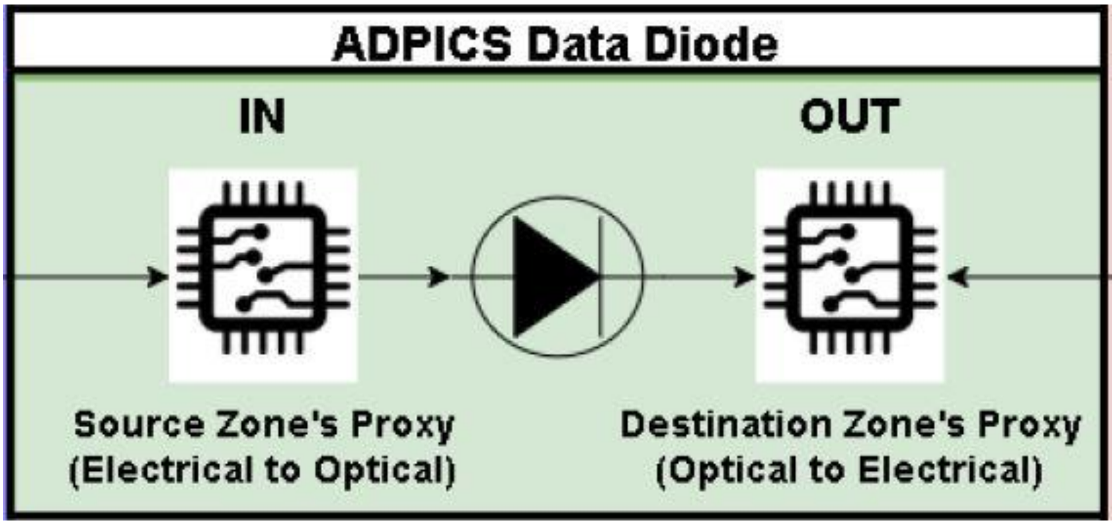
The evaluation of the TOE has been carried out by An Security, an approved CC test laboratory, at the assurance level CC EAL 1 and was completed on 27 July 2021.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality
Enforcing unidirectional data flow between two zones through physical disconnection of the reverse flow interfaces.

Table 1: TOE Security Functionality



Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 4 of the Security Target [1]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that it is in compliance with all the stipulations as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration.

Table of Contents

1 CERTIFICATION 8

1.1 PROCEDURE 8
1.2 RECOGNITION AGREEMENTS 8

2 VALIDITY OF THE CERTIFICATION RESULT 9

3 IDENTIFICATION 10

4 SECURITY POLICY 11

5 ASSUMPTIONS & SCOPE OF EVALUATION 11

5.1 ASSUMPTIONS 11
5.2 CLARIFICATION OF SCOPE 11
5.3 EVALUATED CONFIGURATION 12
5.4 NON-EVALUATED FUNCTIONALITIES 12
5.5 NON-TOE COMPONENTS 12

6 DOCUMENTATION 13

7 IT PRODUCT TESTING 13

7.1 EVALUATOR TESTING (ATE_IND) 13
7.1.1 Test Approach and Depth 13
7.1.2 Test Configuration 13
7.1.3 Test Results 13
7.2 PENETRATION TESTING (AVA_VAN) 13
7.2.1 Test Approach and Depth 13

8 RESULTS OF THE EVALUATION 14

9 OBLIGATIONS & RECOMMENDATIONS FOR USAGE OF THE TOE .. 14

10 ACRONYMS 15

11 BIBLIOGRAPHY 16

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is fully covered by the CCRA.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **03 August 2026**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: ADPICS Data Diode (ADPICS-DD) Version 1.0. The following table identifies the TOE deliverables.

Identifier	Version
ADPICS-DD Hardware	1.0

Table 2 - TOE Deliverable

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents.

Name and version	Version
Attila ADPICS Data Diode User Guidance	2.0

Table 3 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	ADPICS Data Diode (ADPICS-DD) v1.0
Security Target	ADPICS® Data Diode Security Target, Version 4.0, 22 July 2021
Developer	Attila Cybertech Pte. Ltd.
Sponsor	Attila Cybertech Pte. Ltd.
Evaluation Facility	An Security Pte Ltd
Completion Date of Evaluation	27 July 2021
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_21002
Certificate Validity	5 years from date of issuance

Table 4: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to security functional class "User Data Protection".

Specific details concerning the above mentioned security policy can be found in Chapter 5 of the Security Target [1].

5 Assumptions & Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Environmental Assumptions	Description
OE.PHYSICAL	The intended operation environment shall be capable of storing and operating the TOE in accordance with the requirements of the Source Zone.
OE.NETWORK	The TOE is the only method of interconnecting Source Zone to the Destination Zone.
OE.USER	The users are trusted; the users shall not maliciously compromise the security functionality of the TOE.

Table 5: Environmental Assumptions

Details can be found in section 3.1 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to the claims made in the Security Target [1].

5.3 Evaluated Configuration

The evaluated configuration in the Security Target [1] is as shown in Figure 2. The TOE enforces unidirectional data flow between the Source Zone and Destination Zone.

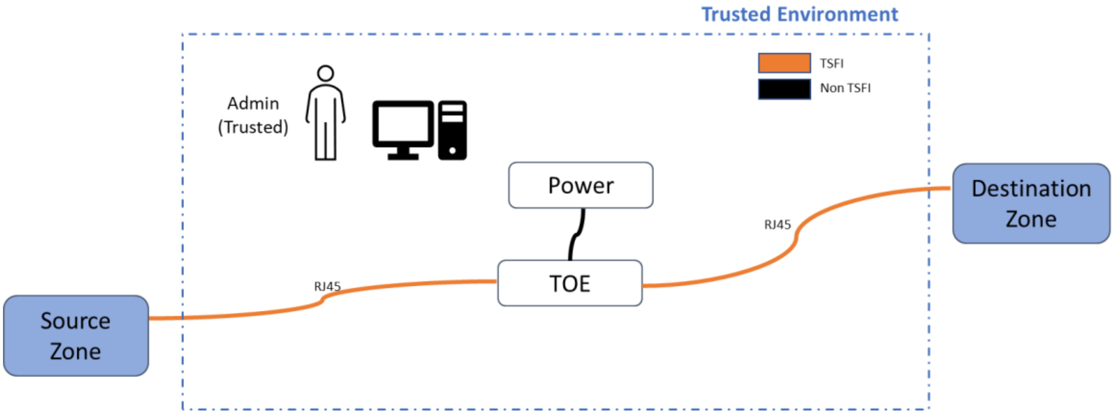


Figure 1: TOE Evaluated Configuration

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

5.5 Non-TOE Components

The TOE does not require additional components for its operation.

6 Documentation

The evaluated documentation as listed in Table 3 - Guidance Document is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

7 IT Product Testing

7.1 Evaluator Testing (ATE_IND)

7.1.1 Test Approach and Depth

As there are no required developer test plan, the evaluator decided to test the unidirectional property of the TOE following the steps in the user guidance to verify data unidirectional flow from IN PORT to OUT PORT.

7.1.2 Test Configuration

A detailed test description was provided in the ATE document. Prior to running tests, the evaluator performed identification of the test environment and verification of the TOE.

7.1.3 Test Results

The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

7.2 Penetration Testing (AVA_VAN)

7.2.1 Test Approach and Depth

The AVA_VAN.1 assurance class requires the evaluator to conduct a vulnerability survey based on publicly available source of information and based on structured examination of the evidence while performing previous evaluation activities (ASE, ADV, AGD, ATE). The evaluator then performs penetration testing to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE.

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.1) treating the resistance of the TOE to an attack with the Basic potential.

<u>The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration</u>. No residual risks were identified.

8 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 1 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

9 Obligations & Recommendations for Usage of the TOE

The documents as outlined in Table *3* - Guidance Document contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

No additional recommendation was provided by the evaluators.

10 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

11 Bibliography

[1] Attila Cybertech Pte Ltd, “ADPICS Data Diode Security Target, Version 4.0, 10 August 2021”.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[9] An Security, “Evaluation Technical Report EAL 1 CC Evaluation of ADPICS Data Diode, Version 1.0, 27 July 2021”.

[10] Attila Cybertech Pte Ltd, “Attila ADPICS Data Diode User Guidance, Version 2.0,” 2021.

---End of Report ---------------------------------------