CSA SINGAPORE

Cybersecurity Certification Centre

CYBER SECURITY AGENCY OF SINGAPORE

Certificate Report

Version 1.0

8 July 2022

CSA_CC_21006

For

ST Engineering Data Diode model 5282, version 2.2.1055, model 5283 version 2.2.1055

From

ST Engineering

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorising 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	8 July 2022	Released

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 ST Engineering Data Diode model 5282, version 2.2.1055 and model 5283 version 2.2.1055, and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS).

The Target of Evaluation (TOE) is defined as a network gateway that ensures physical layer one-way data transmission through the TOE. The TOE is used to connect two separated networks together, one being the Sending Network and the other being the Receiving Network. The TOE ensures that the data can only flow from the Sending Network to the Receiving Network but blocks data flow in the reverse direction.

All TOE versions i.e., models 5282 and 5283 share the same security functionality, which is to provide unidirectional data flow between the Sending Network and Receiving Network.

The difference between the two models being that the 5282 model consist of 1 set of data diode while the 5283 model consist of 2 sets of data diodes within the chassis.

The TOE comprises of the following components:

Type	Name	Identifier
Hardware	ST Engineering Data Diode model 5282	version 2.2.1055
	ST Engineering Data Diode model 5283	version 2.2.1055
Documentation	ST Engineering Data Diode Model 5282 version 2.2 Setup Guide	v2.3.2
	ST Engineering Data Diode Model 5283 version 2.2 Setup Guide	v2.3.2
	ST Engineering Data Diode Model 328X, 5282 and 5283 Acceptance Test	V2.2
	ST Engineering Data Diode Model 328X, 5282 and 5283 Management Portal User Guide	v2.6.1

Table 1: TOE Deliverables Overview

The evaluation of the TOE has been carried out by An Security, an approved CC test laboratory at the assurance level CC EAL, augmented by AVA_VAN.5 and completed on 23 June 2022. The certification body monitored each evaluation to ensure proper, consistent 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	Addressed Issue
Unidirectional Network	The TOE ensures data can only flow from the Sending Network to the Receiving Network and not vice-versa

Table 2: TOE Security Functionality

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

The assets to be protected by the TOE have 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 3 of the Security Target.

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 all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

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

- Common Criteria for IT Security Evaluation (CC) Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5, ISO/IEC 18045
- SCCS scheme publications

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.

Singapore is authorised to issue CC certificates recognised widely through the Common Criteria Recognition Arrangement (CCRA) by the member nations. Hence, the certification for this TOE is partially covered by the CCRA.

The Common Criteria Recognition Arrangement Logo printed on this certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (http://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 **7 July 2027**[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 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 . Potential users should check the SCCS website (https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/csa-common-criteria/product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is the the **ST Engineering Data Diode model 5282 and 5283, version 2.2.1055**. The following table identifies the TOE deliverables.

Type	Name	Identifier	Form of Delivery
Hardware	ST Engineering Data Diode model 5282	version 2.2.1055	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery.
	ST Engineering Data Diode model 5283	version 2.2.1055	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery.
Documentation	ST Engineering Data Diode Model 5282 version 2.2 Setup Guide	v2.3.2	PDF format delivered via email.
	ST Engineering Data Diode Model 5283 version 2.2 Setup Guide	v2.3.2	PDF format delivered via email.
	ST Engineering Data Diode Model 328X, 5282 and 5283 Acceptance Test	V2.2	PDF format delivered via email.
	ST Engineering Data Diode Model 328X, 5282 and 5283 Management Portal User Guide	v2.6.1	PDF format delivered via email.

Table 3: Deliverables of the TOE

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents [2] [3] [4] [5].

Additional identification information relevant to this Certification procedure as follows:

TOE	ST Engineering Data Diode model 5282 and 5283, version 2.2.1055
Security Target	ST Engineering Data Diode model 5282 and 5283 Security Target Version 4.0
CC Scheme	Singapore Common Criteria Scheme (SCCS)
Methodology	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Assurance Level/cPP	EAL 4 augmented AVA_VAN.5
Developer	ST Engineering
Sponsor	ST Engineering
Evaluation Facility	An Security Pte Ltd
Certification Body	Cyber Security Agency of Singapore (CSA)
Certification ID	CSA_CC_21006
Certificate Validity	**8 July 2022** till **7 July 2027**

Table 4: Additional Identification Information

4 Security Policy

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

The TOE implements policies pertaining to the following security functional classes:

- User Data Protection

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

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target 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:

Security Objectives	Description
OE.PHYSICAL	The TOE shall be installed and operated in a physically secure environment which prevents unauthorized physical access.
OE.USER	The users are trusted; the users shall not maliciously compromise the security functionality of the TOE. The users are well-trained; the user shall comply to the operating procedures stipulated in the user guidance.
OE.NETWORK	The information flow between Sending Network and Receiving Network shall pass through the TOE and there shall not be any other network connectivity between Sending Network and Receiving Network.

Table 5: Objectives for the Operational Environment

Details can be found in Chapter 4.2 of the Security Target [1].

5.2 Clarification of Scope

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

5.3 Evaluated Configuration

The Target of Evaluation (TOE) is a network gateway that ensures physical layer one-way data transmission through the TOE.

The TOE is used to connect two independent networks together, denoted as the Sending Network and Receiving Network. Sending Network connects to TOE via InterfaceLAN (Sender) interface while Receiving Network connects to TOE via the InterfaceLAN (Receiver) interface.

Figure 1: TOE Network Configuration illustrates the network configuration which is also the evaluated TOE configuration.

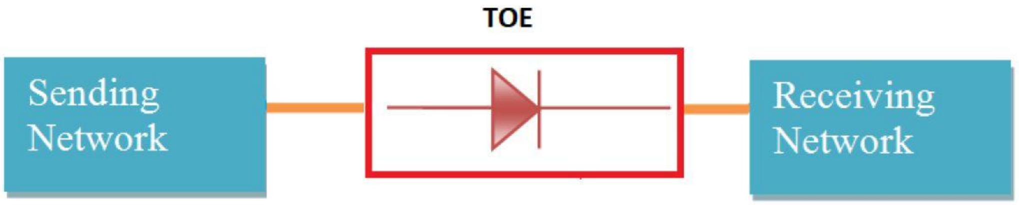

Figure 1: TOE Network Configuration

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 Architecture Design Information

The TOE consists of two subsystems i.e., the Sender Motherboard and Receiver Motherboard. The Sender Motherboard and Receiver Motherboard are physically separated from each other and are only connected to each other via a customised SFP+-pair.

The customised SFP+-pair is implemented such that:

- Sender Motherboard’s customised SFP+ can only allow optical signals to be transmitted to because it contains an optical transmitter. There are no optical sensor to receive optical signals.
- Receiver Motherboard’s customised SFP+ can only receive optical signals because it contains only an optical sensor to receive optical signal. There are no optical transmitter to transmit optical signals.

Together, the customised SFP+-pair on the Sender Motherboard and Receiver Motherboard physically enforces the unidirectional data flow property of the TSF. In addition, the unidirectional data flow property is enforced whenever the TOE is powered.

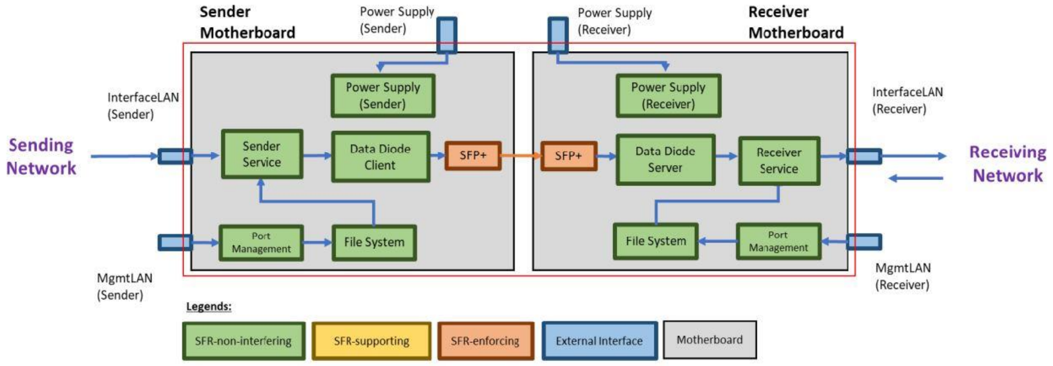

Figure 2: TOE Subsystems

7 Documentation

The evaluated documentation as listed in Table *3*: Deliverables of the TOE is provided with the product to the customer. The documentation contains the required information for secure usage of the TOE in accordance with the Security Target. The documentation is provided via an email from the developer to the customer.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

- The developer performed extensive tests to verify the functionality of the TOE. All SFRs that could be invoked by the TSFI were tested

Test Configuration

The test configuration is as described below.

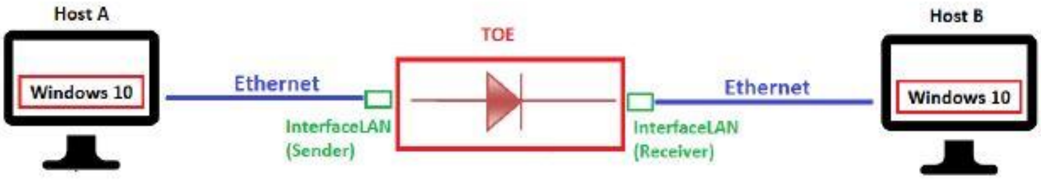

Figure 3: Test Setup 1

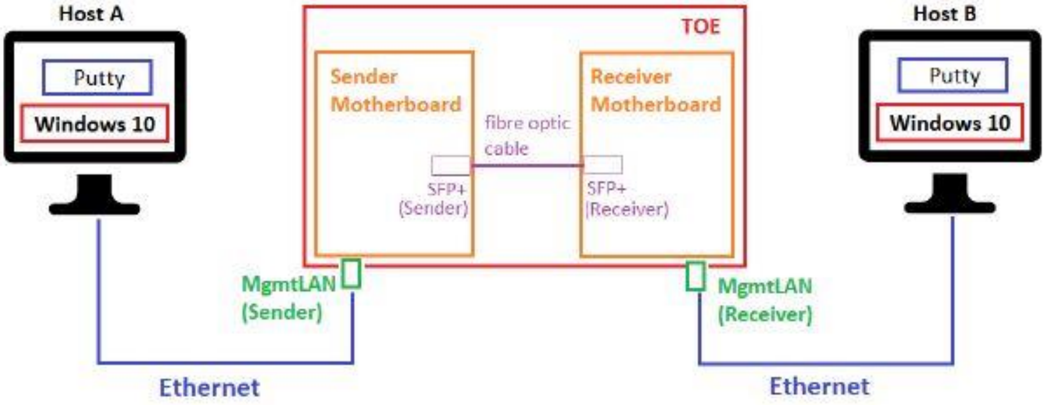

Figure 4: Test Setup 2

8.1.2 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1]. All actual test results from all tested environments are identical to the expected test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluator analysed the developer's test coverage, test plans and procedures, expected and actual test results.

The evaluator repeated all of the developer's tests and verified the accuracy of the developer's test results.

The evaluator decided to devise one additional test case for the TOE:

- IND1 – This test case augments developer's test cases. The objective of this test case is to provide assurance that the one-way unidirectional data flow policy cannot be circumvented by power supply disruption; both power sources to both Sender Motherboard and Receiver Motherboard must be available before data is allowed to flow through the TOE.

8.2.2 Test Configuration

The same test configuration as shown in Figure 3: Test Setup 1.

8.2.3 Test Results

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

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN) treating the resistance of the TOE to an attack with the **high** attack potential. i.e. amongst other that the evaluator used sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator analysed which potential vulnerabilities are not applicable to the TOE in its operational environment

For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluator devised the attack scenarios where these potential vulnerabilities could be exploited. For each such attack scenario he firstly performed a theoretical analysis on the related attack potential. Where the attack potential was **high** or near to **high**, the evaluator conducted penetration tests for such attack scenarios. He analysed then the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential **high** was successful.

The approach chosen by the evaluator is appropriate for the assurance component chosen (AVA_VAN.5), treating the resistance of the TOE to an attack with **high attack** potential.

Test ID	Description
AS1	The LED optical output on the InterfaceLAN (Receiver) is measured to verify whether it does not contain data leakage from the Receiving Network.
AS2	The internal power supply rails in the TOE is measured to verify there is no leakage of data via modulation of the power supply

Table 6: Penetration Test Cases

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

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM, 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 4 + AVA_VAN.5 assurance package

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

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] ST Engineering, "ST Engineering Data Diode model 5282 and 5283 Security Target Version 4.0," 2022.

[2] ST Engineering, "ST Engineering Data Diode Model 5282 v2.2 Setup Guide v2.3," 2021.

[3] ST Engineering, "ST Engineering Data Diode Model 5283 v2.2 Setup Guide v2.3," 2021.

[4] ST Engineering, "ST Engineering Data Diode Model 328X, 5282 and 5283 Acceptance Test v2.2," 2020.

[5] ST Engineering, "ST Engineering Data Diode Model 3282, 3283, 3284, 5282 and 5283 Management Portal User Guide v2.6," 2021.

[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] 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.

[10] 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.

[11] 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.

[12] 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.

[13] An Security, "ETR-00032-ST-CC EAL4+ ST Engineering Data Diode model 528X-v1.0," 2022.

--End of Report --