Certification Report

Version 1.0

10 June 2020

CSA_CC_20002

for

Data Diode model 328X
(3282, 3283, 3284)

From

ST Electronics (Info-Security) 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	10 June 2020	Released

<div style="border:1px solid black; padding:10px;">

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.

</div>

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 Data Diode model 328X. The TOE has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Hardware
- Data Diode model 3282
- Data Diode model 3283
- Data Diode model 3284

TOE preparative and operative guidance (in PDF format and provided via email)
- Data Diode Model 3282 version 2.2 Setup Guide v2.3
- Data Diode Model 3283 version 2.2 Setup Guide v2.3
- Data Diode Model 3284 version 2.2 Setup Guide v2.3
- Data Diode Model 328X Acceptance Test v2.0
- Data Diode Model 328X Management Portal User Guide v2.2

The TOE is a network gateway that ensures physical layer one-way data transmission through the TOE. The TOE is used to connect two separated networks (sending network and receiving network) together. The TOE ensures that the data can only travel through the TOE from the sending network to the receiving network and not vice-versa.

The physical layer one-way data transmission property addresses two security problems:
- Prevents information leakage from the receiving network to the sending network
- Prevents the integrity of the data residing in the sending network from being compromised by the receiving network

The evaluation of the TOE has been carried out by An Security Pte Ltd, an approved CC test laboratory, at the assurance level CC EAL4+AVA_VAN.5 and completed on 22 May 2020. The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The Security Target [1] is the basis for this certification. It is not based on a certified Protection Profile.

The Security Assurance Requirements (SARs) are based entirely on the assurance components defined in Part 3 of the Common Criteria [2]. The TOE meets the assurance requirements of the Evaluation Assurance Level EAL4+AVA_VAN.5.

The Security Functional Requirements (SFRs) relevant for the TOE are outlined

in Chapter 5 of the Security Target [1]. The Security Target claims conformance to CC Part 2 [3].

The SFRs are implemented by the following TOE Security Functionality:

TOE Security Functionality	
Unidirectional Network	The TOE ensures that data can only flow from the Sending Network to the Receiving Network and not vice-versa.

Table 1: TOE Security Functionalities

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 3 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 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 Information Technology Security Evaluation, Version 3.1 Revision 5 [4] [3] [2];

- 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 covered partially by the CCRA for the components up to EAL2.

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 **9 June 2025[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: Data Diode model 328X

The following table identifies the TOE deliverables.

Type	Name	Version	Form of Delivery
Hardware	Data Diode model 3282		In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery.
Hardware	Data Diode model 3283		In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery.
Hardware	Data Diode model 3284		In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery.
Software	Data Diode Model 3282 version 2.2 Setup Guide	2.3	PDF format delivered via email.
Software	Data Diode Model 3283 version 2.2 Setup Guide	2.3	PDF format delivered via email.
Software	Data Diode Model 3284 version 2.2 Setup Guide	2.3	PDF format delivered via email.
Software	Data Diode Model 328X Acceptance Test	2.0	PDF format delivered via email.
Software	Data Diode Model 328X Management Portal User Guide	2.2	PDF format delivered via email.

Table 2: Deliverables of the TOE

The guide for receipt and acceptance of the above mentioned TOE are described in the set of guidance documents [9] [10] [11] [12] [13].

Additional identification information relevant to this Certification procedure as follows:

TOE	Data Diode model 328X
Security Target	ST Engineering Data Diode model 328X Security Target, version 2.0
CC Scheme	Singapore Common Criteria Scheme (SCCS)
Methodology	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Assurance Level/cPP	EAL4+AVA_VAN.5
Developer	ST Electronics (Info-Security) Pte Ltd
Sponsor	ST Electronics (Info-Security) Pte Ltd
Evaluation Facility	An Security Pte Ltd
Certification Body	Cyber Security Agency of Singapore (CSA)
Certification ID	CSA_CC_20002
Certificate Validity	**10 June 2020** till **9 June 2025**

Table 3: 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 and 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:

Usage Assumptions	Description
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.

Table 4: Usage Assumptions

Environmental Assumptions	Description
OE.PHYSICAL	The TOE shall be installed and operated in a physically secure environment which prevents unauthorized physical access.
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: Environmental Assumptions

Details can be found in section 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], comprising only the unidirectional data flow. The Operating System and software are outside the scope of the certification.

5.3 Evaluated Configuration

The evaluated configuration is as shown in Figure 1 below. The TOE is a data diode that enforces unidirectional data flow between the Sending Network and the Receiving Network.
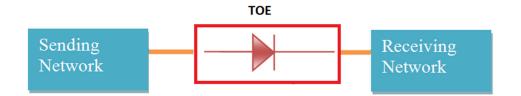

Figure 1: TOE Evaluated Configuration

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 Architecture Design Information

The 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 which are denoted as the Sending Network and Receiving Network. The TOE ensures that the data can only travel from the sending network to the receiving network and not vice-versa.

The TOE consists of 2 subsystems (i.e. the Sender Motherboard, and the Receiver Motherboard). The Sending Network is connected to the Sender Motherboard, and the Receiving Network is connected to the Receiver Motherboard. The two subsystems (Sender and Receiver motherboards) are physically separated, and are only connected via a pair of customised enhanced small form-factor pluggable (SFP+) fibre transceiver modules which provides the unidirectional network security functionality.
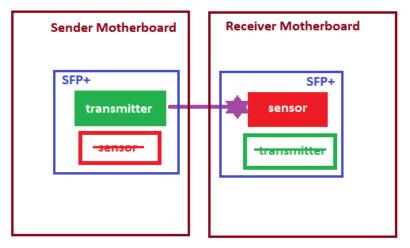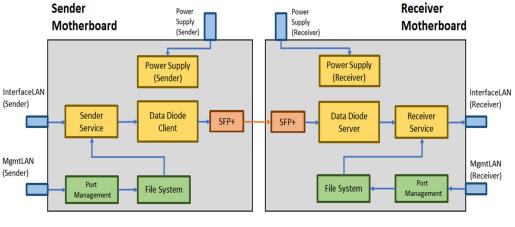

Figure 2: TOE Subsystems

The SFP+ fibre transceiver module located on the Sender Motherboard is customised to only contain an optical transmitter and not an optical sensor. As such, it can transmit optical signals to the Receiver Motherboard but not receive them.

Correspondingly, the SFP+ fibre transceiver module located on the Receiver Motherboard is customised to only contain an optical sensor and not an optical transmitter. It can only receive optical signals from the SFP+ fibre transceiver module located on the Sender Motherboard but not send them.

Together, as depicted in Figure 2, the customised pair of SFP+ fibre transceiver modules located on both the Sender Motherboard and Receiver Motherboard enforces the unidirectional data flow property of the TSF. The unidirectional data flow property is enforced whenever the TOE is powered.

Figure 3: TOE Subsystems and Modules

Figure 3 depicts how the TOE is connected to the Sending and Receiving Networks, and how data flows through the TOE. The following sequence describes the data flow through the TOE.

1. The Sender Motherboard receives data from the Sending Network via the InterfaceLAN (Sender) interface.

2. The Sender Motherboard subsystem (Sender Service module and Data Diode Client module) converts the data packets from a standard networking protocol to a proprietary protocol. The converted data packets are then forwarded to the Receiver Motherboard via the customised SFP+ fibre transceiver modules.

3. The Receiver Motherboard subsystem (Data Diode Server module and Receiver Service module) receives the data packets and converts them back to the standard networking protocol before forwarding it to the Receiving Network via the InterfaceLan (Receiver) interface.

The TOE is available in 3 models; model 3282, model 3283, and model 3284. The following table depicts the differences among the 3 versions. There is no difference in the adopted security architecture (depicted in Figure 3) among the 3 models of the TOE.

TOE Model	Picture of TOE	Description
3282		Both the Sender Motherboard and the Receiver Motherboard are enclosed within a single housing. The pair of customised SFP+ fibre

		transceiver modules are located within the housing.
3283		Both the Sender Motherboard and the Receiver Motherboard are enclosed within a single housing. The pair of customised SFP+ fibre transceiver modules are external interfaces.
3284		The Sender Motherboard and Receiver Motherboard are enclosed in 2 separate units. The two units are connected via the pair of customised SFP+ fibre transceiver modules which are external interfaces.

Table 6: TOE Versions

7 Documentation

The evaluated documentation as listed in Table 2: Deliverables of the TOE is being provided with the product to the customer. These 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 testing only with the model 3283 as the differences between the different models (i.e. model 3282 and 3284) are only related to the provided hardware environment that has no impact on the security of the TOE.

8.1.2 Test Configuration

Figure 4 describes the base setup used for both developer's and evaluator's testing. Some tests required additional network interfaces (e.g. ManagementLAN interface for configuration of the TOE).
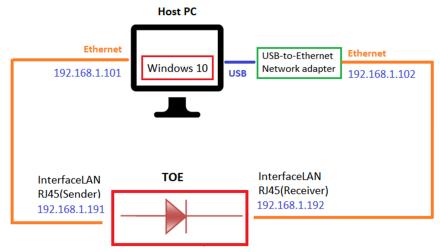
Figure 4: Developer's Base Test Setup

The TOE used for testing is configured according to the TOE guidance document [10].

8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual 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.
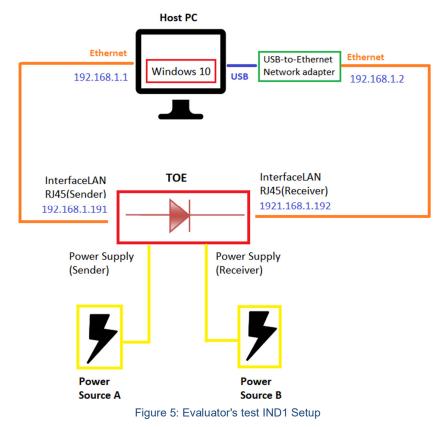
The evaluator repeated all of the developer tests at the developer's premise on model 3283 of the TOE and verified the accuracy of the developer's test results.

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 test configuration is as described below.

Figure 5: Evaluator's test IND1 Setup

8.2.3 Test Results

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

The evaluator's additional test case (IND1) verified that both power sources each powering motherboards (Sender Motherboard and Receiver Motherboard) must be available before data is allowed to flow through the TOE.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the TOE and to demonstrate that the vulnerabilities were not exploitable in the intended environment of the TOE.

The general approach for the vulnerability analysis is based on the following:

- Public domain vulnerability analysis of the TOE specific vulnerability (both hardware and software);
- Public domain vulnerability analysis of the TOE-type vulnerabilities (i.e. vulnerabilities that are generic for data diode)
- Analysis of the TOE deliverables (ARC, TDS, FSP, AGD etc.).

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.5) treating the resistance of the TOE to an attack with the High attack potential.

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 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 EAL4+AVA_VAN.5 assurance package

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

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 2 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.

11 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
SFP+	Enhanced Small Form-factor Pluggable
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] ST Electronics (Info-Security), "ST Engineering Data Diode model 328X Security Target v2.0," 2020.

[2] 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.

[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 1: Introduction and general model [Document Number CCMB-2017-04-001]. 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] ST Electronics (Info-Security), "Data Diode Model 3282 version 2.2 Setup Guide v2.3," 2018.

[10] ST Electronics (Info-Security), "Data Diode Model 3283 version 2.2 Setup Guide v2.3," 2018.

[11] ST Electronics (Info-Security), "Data Diode Model 3284 version 2.2 Setup Guide v2.3," 2018.

[12] ST Electronics (Info-Security), "Data Diode Model 328X Acceptance Test v2.0," 2018.

[13] ST Electronics (Info-Security), "Data Diode Model 328X Management Portal User Guide v2.3," 2018.

--End of Report ---