Certification Report

Version 1.0

01 February 2021

CSA_CC_19002

for

DiskCrypt M10 (Enterprise)
Version: M321P32J1E1

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	01 February 2021	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 DiskCrypt M10 (Enterprise) Version: M321P32J1E1. The TOE has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Hardware

- Hardware enclosure (mechanical housing) and internal circuitry with the embedded application

TOE preparative and operative guidance (in PDF format)

- DiskCrypt M10 User Manual (via download)
- DiskCrypt M10 Administrator Guide (via enclosed CD)

The TOE is defined as a portable USB storage enclosure which provides a full disk encryption/decryption function for user data in the M.2 SATA III Solid State Drive within the TOE. It works with an authorized paired smartcard which stores the Smartcard Keying Material (SKM) to the key derivation function for the Data Encryption Key (DEK).

The evaluation of the TOE has been carried out by An Security Pte Ltd, a provisionally approved CC test laboratory, at the Evaluation Assurance Level 2 (EAL2) and completed on 17 November 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 Evaluation Assurance Level (EAL) 2.

The Security Functional Requirements (SFRs) relevant for the TOE are outlined in Chapter 6.2 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	
Identification and Authentication	Identification Each smartcard is paired to a TOE by a “MatchID”. When inserted, the MatchID of the smartcard is verified against the MatchID stored in the TOE. The correct MatchID is required for Users and Administrators to access decryption/encryption functions.

	Access to decryption/encryption function is allowed only if the paired smartcard is detected. <u>Authentication</u> Administrators are required to insert a paired smartcard and authenticate successfully, via an 8-digit PIN, to the TOE to invoke all Admin functions within the TOE. An unpaired smartcard can only be initialised by an administrator. Until the smartcard is initialised and paired, no other functions are accessible. The TOE is also designed with a “lockout mode” feature. Lockout mode is enabled by default. In this mode, the TOE automatically enters into an unauthenticated state whenever the smartcard is removed. This would require users to re-perform the authentication process to gain user access. It is possible for an authorised administrator to disable the Lockout mode.
Cryptographic Support	The TOE provides cryptographic functions such as symmetric data encryption/decryption and integrity verification using secure hashing. The TOE’s cryptographic module utilizes the DEK to perform real time data encryption when data is transferred from host machine to M.2 SSD and vice versa. Encryption and decryption of user data is performed in accordance to the cryptographic algorithm AES-256 XTS mode.
Security Management	The TOE provides the following administrative functions to the Administrator: 1) Pairing of legitimate smartcard to TOE 2) Enable/disable the smartcard lockout mode. 3) Change of Admin PIN. 4) DKM injection (device setup) The TOE enters into a “halt” state upon the successful invocation of each of the four administrative functions. The Administrator is required to authenticate again should they want to invoke any of the administrative function again.
Protection of the TSF	The TOE is designed with protection and detection mechanisms to prevent and detect possible malfunction or compromised TSF/TSF data. The DEK and Admin PIN are zeroised in the MCU’s memory after use.

	If lockout mode is enabled, the TOE automatically enters into an unauthenticated state whenever the smartcard is removed from the TOE, upon which data encryption keys stored in the internal RAM of the cryptographic chip will be zeroized. The TOE performs a Power-Up Self-Test (POST) upon every power up to perform integrity checks on the MCU, a critical subsystem of the TOE. POST includes the following tests: 1) LED Display Test 2) Memory Read/Write Test (includes MCU's internal RAM) 3) ROM (EEPROM) Integrity Check 4) SHA-1 Hash Check The cryptographic module conducts a Known Answer Test whenever it is enabled. The TOE performs zeroization of all parameters (e.g. DEK) upon failure of the KAT. In the event of failure of any of the above self-tests, the TOE enters into a "halt" and secure state, and the "ERROR" LED will be lighted up. In this state, the TOE is non-operational. The TSF shall resist physical manipulation and probing of critical components such as encryption chip and MCU chip as they are protected with stycast epoxy. Any tampering can be detected through visual inspection.

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 fully covered under 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 **31 January 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: DiskCrypt M10 (Enterprise) Version M321P32J1E1

The following table identifies the TOE deliverables.

Type	Name	Version	Form of Delivery
HW	DiskCrypt M10	Version M321P32J1E1	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
DOC	DiskCrypt M10 User Manual – Softcopy Document	Version 1.0	PDF format downloadable from website
DOC	DiskCrypt M10 Administrator's Guide	Version 1.0	PDF format stored within CD delivered together with TOE.

Table 2: Deliverables of the TOE

The following Non-TOE components are delivered together with the TOE:

Type	Name	Version	Form of Delivery
HW	DC Smartcards (User and Admin)	-	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
HW	USB 3.1 cable	-	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
HW	M.2 SATA III SSD	-	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery

SW	DMS Software	Version 1.0.0	Stored within CD delivered together with the TOE.
SW	AWP Manager Software	Version 1.0.0	Stored within CD delivered together with the TOE.
DOC	DiskCrypt Key Management Software (DMS) Guide	Version 1.0.0	PDF format stored within CD delivered together with the TOE.
DOC	AWP Manager Guide	Version 1.0.0	PDF format stored within CD to be delivered together with TOE.

Table 3: Non-TOE components deliverables together with the TOE

The guide for receipt and acceptance of the above mentioned TOE are described in chapter 3 of the Administrative Guidance [9].

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	DiskCrypt M10 (Enterprise) Version M321P32J1E1
Security Target	ST Engineering DiskCrypt M10 (Enterprise) Security Target, version 1.0
CC Scheme	Singapore Common Criteria Scheme (SCCS)
Methodology	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Assurance Level/cPP	EAL 2
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_19002
Certificate Validity	**01 February 2021** till **31 January 2026**

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 the following security functional classes:

- Identification and Authentication
- Cryptographic Support
- Security Management
- Protection of the TSF

Specific details concerning the abovementioned security policies can be found in chapter 6 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.TRUSTED_USER	The TOE users must operate the TOE in accordance to the user guidance documentation.
OE.ADMIN	Administrator of the TOE must administer the TOE in accordance to the admin guidance documentation.

Table 5: Usage Assumptions

Environmental Assumptions	Description
OE.SMARTCARD	The cryptographic smartcard used together with the TOE must conform to the following: • Secure Signature Creation Device Protection Profile Type 2 v1.04, EAL 4+ • Secure Signature Creation Device Protection Profile Type 3 v1.05, EAL 4+

Table 6: 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 the claims made in the Security Target [1].

5.3 Evaluated Configuration

The only evaluated configuration, as stated the Security Target [1], is shown in Figure 2. The TOE has a built-in keypad and smartcard reader. It is powered via its USB interface (USB 3.1) by connecting it to a host machine (USB 3.1/3.0/2.0 are supported). The TOE requires users to insert their authorized user smartcard and input his/her smartcard PIN via the integrated keypad of the TOE to authenticate to the smartcard. Upon successful user authentication to the smartcard, access to the user data is granted. TOE security management is also performed via the built-in keypad.

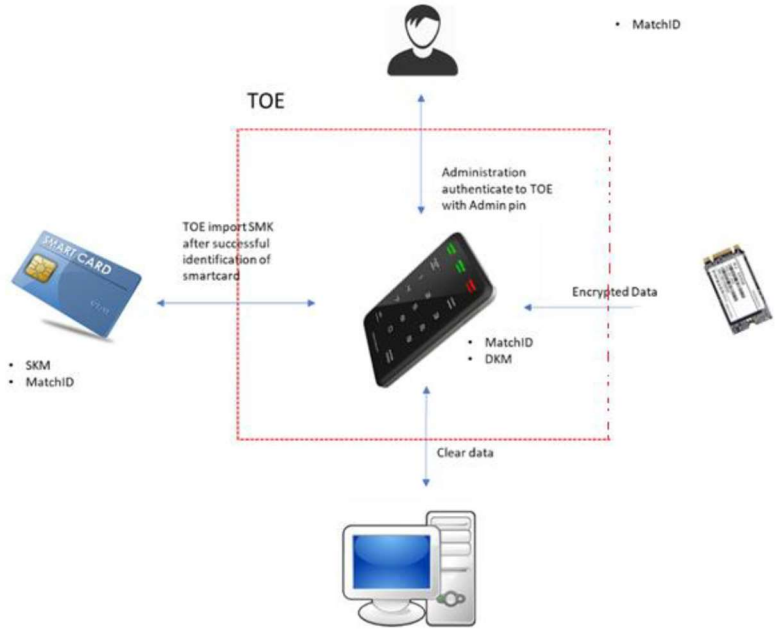

Figure 1: TOE Evaluated Configuration

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 requires additional components (i.e. hardware/software/firmware) for its operation. These non-TOE components include:

- DiskCrypt (DC) Smartcard
- DiskCrypt Key Management Software (DMS)
- AWP Manager Software
- Host Workstation
- KeyCrypt Token

More information is available in section 1.3.2 of the Security Target [1].

6 Architecture Design Information

The TOE has been apportioned broadly into 4 major subsystems, based on their functional roles, described as follows:

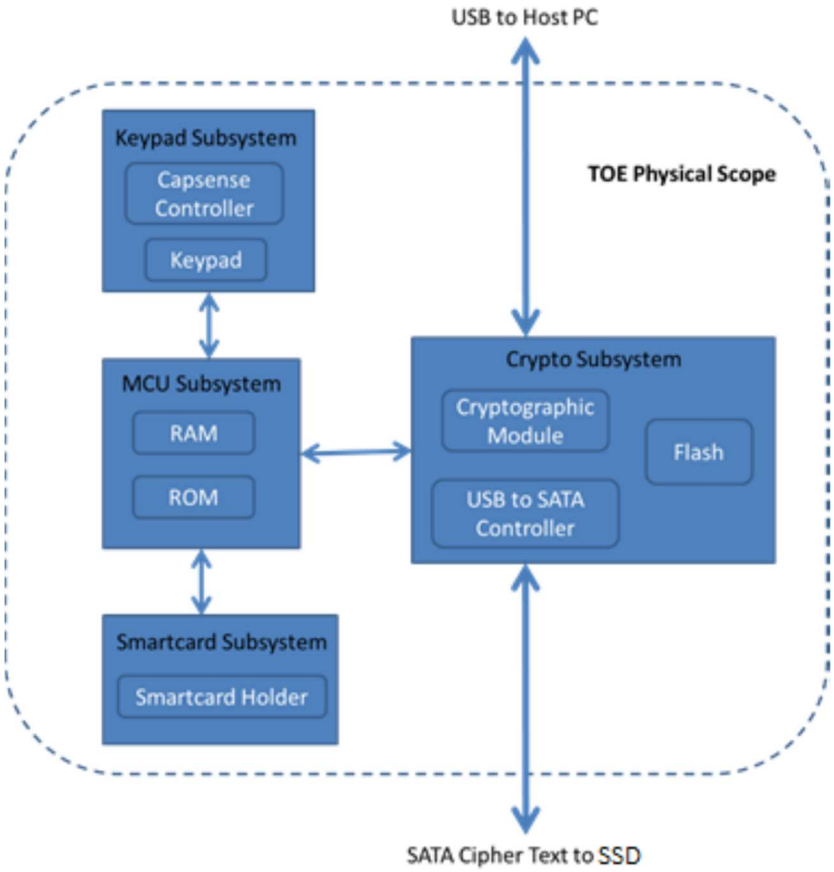

Figure 2: TOE Subsystems

Subsystem	Description
Keypad	The Keypad subsystem comprises of the keypad and CapSense controller modules which provide users the interface for input and status update of the TOE. The keypad subsystem essentially provides the means for users to authenticate the smartcard inserted by capturing the user input PIN and transferring it to the smartcard via the MCU subsystem. Administrators also invoke administrative functions and authenticate to the TOE via the keypad subsystem. (**SFR-supporting subsystem**)
MCU	The MCU Subsystem receives inputs from the Keypad Subsystem and provides output (status) through the Keypad. The MCU subsystem would receive and present the user input PIN to the smartcard to be verified. Upon successful user login, the SKM is fetched from the smartcard and stored on the MCU's RAM module before being transferred to the cryptographic module. **(SFR-Enforcing subsystem)**

Smartcard	The Smartcard subsystem operates with a smartcard which stores the SKM and MatchID. This subsystem consists of the smartcard holder module for both users and administrators to insert their smartcard into the TOE for login. The smartcard holder is the interface through which TSF data (SKM, matchID) is fetched from the inserted (tagged) smartcard. The fetched TSF data is sent to the MCU subsystem for processing. During user login, the MCU retrieves the user PIN from the keypad subsystem and sends it to the smartcard via the smartcard holder interface. The MCU communicates with the smartcard via APDU commands. (**SFR-Supporting subsystem**)
Crypto	The Cryptographic subsystem consists of the cryptographic module, a flash module and the USB to SATA controller module. Upon successful user login, the crypto subsystem is enabled, and the cryptographic module will perform a Known Answer Test (KAT) to ensure correct functionality. After successful KAT, the cryptographic module may proceed to perform real time, on demand data encryption and decryption operations using AES XTS algorithm. The DEK is stored in the internal RAM of the cryptographic module. It also contains the USB to SATA controller (Bridge) module that is inbuilt within the crypto Module. It provides the connection between the Host PC to the Solid State Drive (M.2 SATA III) via the cryptographic module. This module provides a communication link. (**SFR-Enforcing subsystem**)

Table 7: TOE Subsystems and Modules

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 delivered from the developer to the customer via website download or within CD together with TOE.

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. The tests consist of:

- Testing at all TSFI
    - All SFRs that are invoked at all TSFI are tested

According to the nature of the tests, the tests are conducted using the evaluated configuration as stated in the Administrator and user guidance.

8.1.2 Test Configuration

Figure 3 describes the base setup used for both developer's and evaluator's testing.

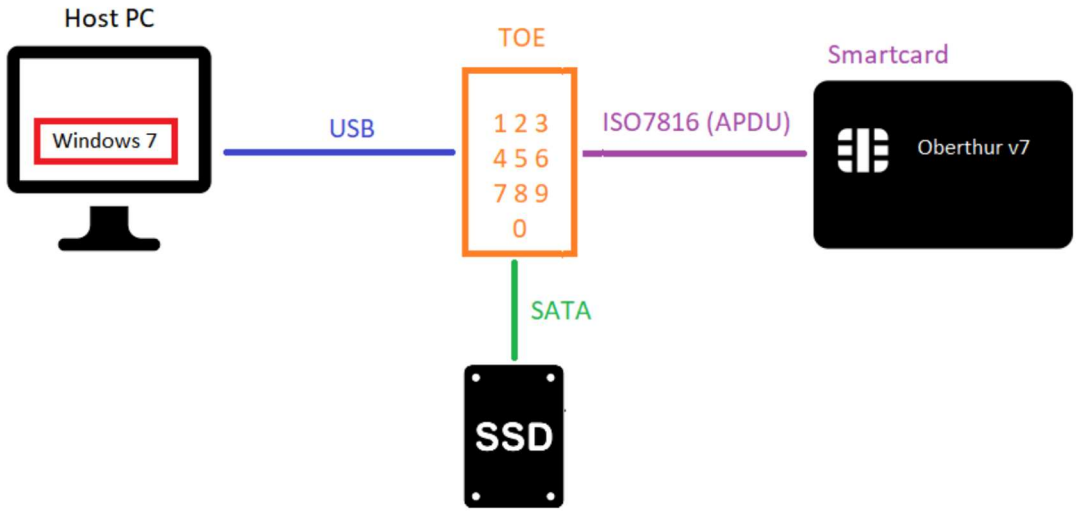

Figure 3: Developer's Base Test Setup

The TOE used for testing is configured according to the TOE guidance document [10]. For verification of cryptographic implementation, the ciphertext from the TOE is extracted and compared to the output from a reference implementation of the algorithm.

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

The evaluator first decided to repeat and performed all the test cases of the developer in their test plan. The reasons for the conduct of all developer tests are:

- There are only 17 test cases which is easily repeatable by the evaluator
- All the TSFI are covered through the evaluator testing. They include:
  - Keypad TSFI
  - USB TSFI
  - SmartCard TSFI
  - Hardware Casing

With an understanding of the expected behaviour of the TSF from the Security Target [1] and other developer documentation, the evaluator found that USB TSFI and FCS_COP.1.1/AES are not sufficiently tested as analysed in ATE_COV.1-1. Thus, IND1 and IND2 were developed to complement the Test Plan.

Test ID	Description
IND1	To validate that the TOE's USB interface can handle erroneous inputs in user authenticated state. Fuzzing of the TOE's USB interface is done after the User has successfully authenticated to the User smartcard.
IND2	To provide assurance that AES256-XTS encryption is correctly implemented. The evaluator shall repeat developer's cryptographic algorithm tests for AES-XTS with a new set of test vectors.

8.2.2 Test Configuration

Figure 3 describes the setup used by the evaluator for IND1.

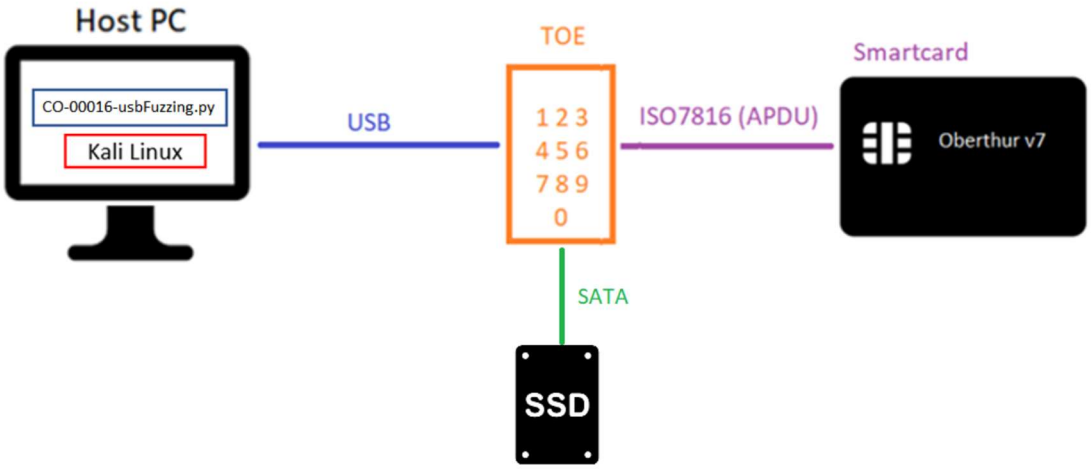

Figure 5: Evaluator's Setup for fuzzing the TOE

The test configuration for IND2 is the same as the developer's setup for verification of cryptographic algorithm.

8.2.3 Test Results

The evaluator verified that for all the developer's tests, the actual results matched the expected results from the test plan.

The evaluator's additional test case (IND1) verified that Erroneous inputs at the USB TSFI are not allowed and will not be processed.

The evaluator's additional test case (IND2) confirmed that AES256-XTS is correctly implemented by comparing the results from the TOE operations with a known implementation (OpenSSL FOM v1.1.1).

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 USB encrypted storage or Full Disk Encryption).
- 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.2) treating the resistance of the TOE to an attack with the BASIC attack potential. Amongst others, the evaluator used sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator analyzed 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 Basic or near to Basic, the evaluator conducted penetration tests for such attack scenarios. He analyzed then the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential BASIC was successful.

Test ID	Description
VA1	Fuzz USB interface when user smartcard is removed from the TOE after successful user authentication. The User inserts the User smartcard into the TOE first and perform user authentication. After successful user authentication, the User smartcard is removed from the TOE and fuzzing is performed on the USB interface.
VA2	Fuzz USB interface when TOE is in unauthenticated state. Fuzzing is performed on the TOE's USB interface to verify that the interface does not accept USB command when the TOE is in unauthenticated state.
VA3	Attempt to remove the epoxy applied over the PCBA of the TOE with heat and scalpel. After the epoxy removal, the evaluator performs a functional test to ensure that the TOE remains functional. The evaluators have added this test to perform a more rigorous testing of the TOE physical protection.

8.3.2 Test Configuration

The test configuration for VA1 and VA2 is the same as the evaluator's setup for independent testing in Figure 5. The test configuration for VA3 is the same as the developer's base setup in Figure 4.

8.3.3 Test Results

At EAL2, 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 EAL 2 assurance package

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

10 Evaluators' comments

There are no additional comments from the evaluators.

11 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.

The potential user is reminded that the administrative features will be blocked perpetually in the event there is 8 consecutive failed administrative login attempts. This access cannot be restored once blocked.

12 Acronyms

AES	Advanced Encryption Standard
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

13 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 ----------