Certification Report

Version 2.0

1 February 2019

CSA_CC_17002

for

DiskCrypt M100 (Enterprise)
ID: 9910-8000-1239
Version: M253P15AO206

From

ST Electronics (Info-Security) Pte Ltd

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 to provide a cost effective regime 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	23 July 2018	Released
2.0	1 February 2019	Covered under CCRA

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 M100 (Enterprise) ID: 9910-8000-1239, Version: M253P15AO206. It is a portable USB encrypted storage device and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises the following components:

- DiskCrypt M100 (Enterprise)
- DiskCrypt M100 Administrator's Guide, Version 1.0.0 (provided in PDF format in CD delivered with TOE)
- DiskCrypt M100 User Manual, Issue A (provided in hardcopy delivered with TOE)
- 2.5 inch SATA hard disk

The TOE is a portable USB encrypted storage device that provides a full disk encryption/decryption function for user data residing in the 2.5" SATA hard disk within the TOE. The TOE interoperates with an authorised paired smartcard (that stores the input keying material to the key derivation function for the Data Encryption Key – DEK). User must provide the paired smartcard and the pin to the smartcard before access to the user data is granted.

The evaluation of the TOE has been carried out by An Security Pte Ltd, a provisionally approved CC test laboratory, at the assurance level CC EAL2 and completed on 23 July 2018. 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 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	<u>Identification</u> Each smartcard is paired to a TOE by a "MatchID". The MatchID is required for both User and Administrator access. The MatchID of the smartcard is verified against the MatchID stored in the TOE.

	Users are first required to insert a paired smartcard containing the correct SKM. Upon successful identification of the smartcard (MatchID), the SKM will be allowed to be imported by the TOE allowing decryption of the data (Master Boot Record, file allocation table, etc) to enable access to the user data in the encrypted hard disk. In the event that an unpaired smartcard is inserted, no access to the decryption/encryption function is allowed. <u>Authentication</u> Administrator, similarly, is required to insert a paired smartcard and authenticate successfully to the TOE to successfully invoke any Admin function (modification of: Admin PIN, lockout mode, DKM, MatchID) of the TOE. The administrator is required to enter a 8-digit PIN to authenticate to the TOE. The TOE maintains a counter of the number of failed consecutive Admin authentication attempts. All access to administrative functions will be blocked after 8 consecutive wrong PIN entries. In the event, that an unpaired smartcard is inserted, only access to the Admin functions: initialize smartcard shall be allowed upon successful authentication. The TOE is also designed with a “lockout mode” feature. If lockout mode is enabled, 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. This is enabled by default.
Cryptographic Support	The TOE provides cryptographic function such as symmetric data encryption/decryption and integrity verification using hash functions. The SKM retrieved from the inserted smartcard and the DKM that is stored in the TOE are used as inputs to a key derivation function to generate the DEK. The DEK is then loaded into the cryptographic module of

	the TOE where the MBR or file allocation table will be decrypted and sent to the host PC; thereafter user may access the encrypted hard disk of the TOE. The TOE's cryptographic module utilizes the DEK to perform real time data encryption and decryption when data is transferred from host machine to encrypted hard disk 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) Option 1 enables the Administrator to pair a smartcard with a TOE using the smartcard's MatchID attribute. The smartcard's MatchID is stored in the TOE. Option 2 enables the Administrator to enable/disable the lockout mode (enabled by default). When lockout mode is enabled, the TOE will enter into an unauthenticated state whenever the smartcard is removed from the TOE. Option 3 enables the Administrator to change the Admin PIN. The Admin PIN must be 8 digits in length and will be stored as a hash (SHA1) within the TOE. Option 4 enables the Administrator to inject the DKM (from the Administrator smartcard) into the TOE during 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 performs a POST upon every power up to perform integrity checks on the MCU, a critical subsystem of the TOE. In the event of any POST failure, the TOE will enter a “halt” state. 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 performs a Known Answer Test (KAT) whenever it is enabled. The TOE performs zeroisation 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 TOE is also housed in a tamper evident casing where any physical tampering to the TOE can be visually detected.

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 the 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.

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.

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 (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 **22 July 2023**[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 M100 (Enterprise), ID: 9910-8000-1239, Version: M253P15AO206.

The following table identifies the TOE deliverables:

Type	Name	Version	Form of Delivery
HW	DiskCrypt M100	ID: 9910-8000-1239 Version: M253P15AO206	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
DOC	DiskCrypt M100 User Manual – Hardcopy Document	Issue A, Version 2.0	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
HW	2.5 inch SATA hard disk	-	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
DOC	DiskCrypt M100 Administrator's Guide	Version 1.0.0	PDF format stored within CD to be 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	USB 3.0 cable	-	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery

SW	DMS Software	Version 2.4	Burnt into a CD and delivered together with the TOE.
SW	AWP Manager Software	Version 4.6	Burnt into a CD and delivered together with the TOE.
DOC	DiskCrypt Key Management Software Guide	Version 1.0.0	PDF format stored within CD to be delivered together with 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].

Additional identification information relevant to this Certification procedure as follows:

TOE	DiskCrypt M100 (Enterprise) ID: 9910-8000-1239 Version: M253P15AO206
Security Target	DiskCrypt M100 (Enterprise) Security Target V2.0, 6 July 2018
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_17002
Certificate Validity	**23 July 2018** till **22 July 2023**

Table 4: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the selected set of SFRs 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 above mentioned 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. ADMIN	The TOE users must operate the TOE in accordance to the user guidance documentation.
OE.TRUSTED_USER	The TOE users must operate the TOE in accordance to the user 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 those claims made in the Security Target [1].

5.3 Evaluated Configuration

The evaluated configuration is a portable USB encrypted storage device that provides full disk encryption/decryption function on user data residing in the 2.5" SATA hard disk within the TOE. The TOE interoperates with an authorised paired external smartcard that stores the input keying material to the key derivation function for the Data Encryption Key (DEK). Although the SATA hard disk is considered part of the TOE, by itself, it does not implement any security functions. Smartcard lockout mode is enabled by default.

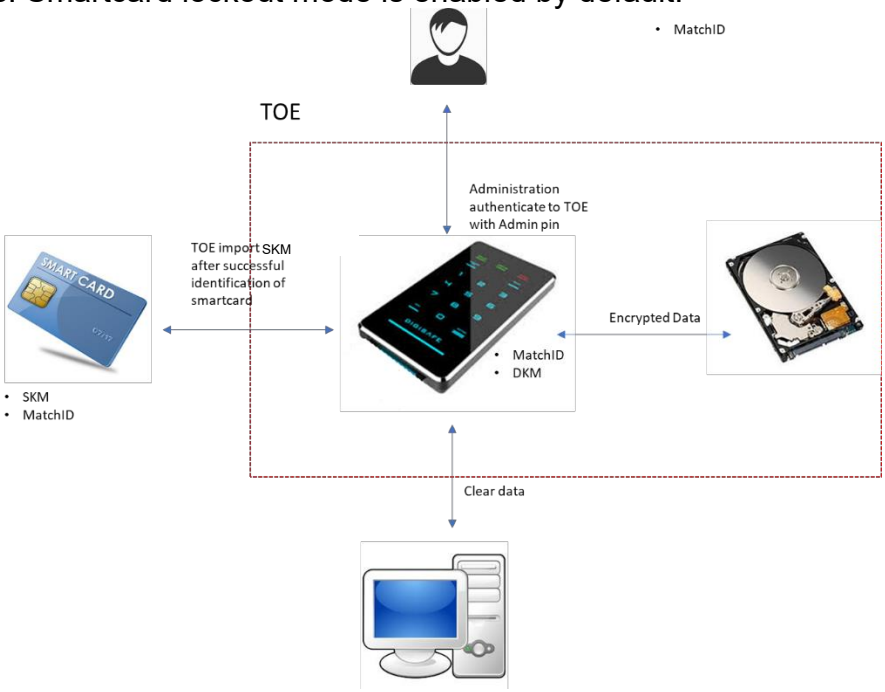

Figure 1: Evaluated configuration

5.4 Non-Evaluated Functionalities

Potential users of the TOE are advised that some functional and services have not been evaluated as part of the evaluation. Potential users of the TOE shall carefully consider their requirements for using functions and services outside of the evaluated configuration.

These non-evaluated functionalities include:

- A layer of epoxy is applied over the entire PCB. While it was tested that basic tampering methods such as scrapping would result in causing

visible marks to the epoxy, no assurance claims were made. This feature is not mapped to the FPT_PHP.1 defined in the Security Target [1].

5.5 Non-TOE components

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

- DCM Smartcard
- DiskCrypt Key Management Software
- AWP Manager Software
- Host Workstation

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

6 Architecture Design Information

The general architecture consists of 4 subsystems.

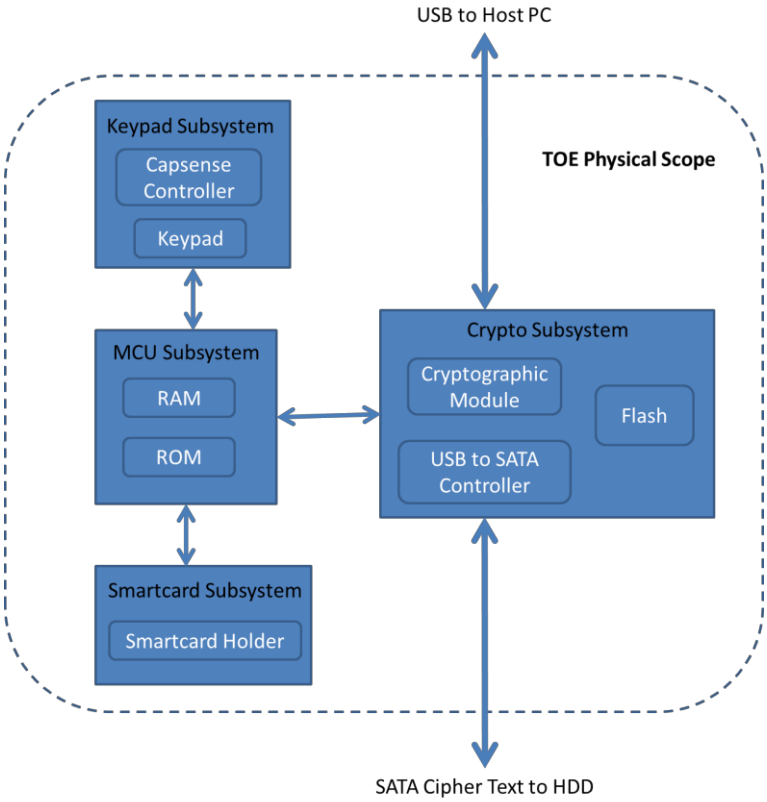

Figure 2: Subsystems of TOE

Subsystem	Description
Keypad	The Keypad subsystem comprises the keypad and CapSense controller modules that 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 DEK is fetched from the smartcard and stored on the MCU's RAM module before being transferred to the cryptographic module. The MCU Subsystem implements the

	Identification and authentication of users, cryptographic functions such as hashing, self-test and all of the administrative functions. (SFR-Enforcing subsystem)
Smartcard	The Smartcard subsystem operates with a smartcard that stores the DEK 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 (DEK, 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 on-the-fly 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 in-built within the crypto Module. It provides the connection between the Host PC to the hard disk drive (SATA II) via the cryptographic module. This module provides a communication link. (SFR-Enforcing subsystem)

Table 7: Subsystems of TOE

7 Documentation

The evaluated documentation are listed in Table 2: Deliverables of the TOE and 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 shipped securely together with the TOE.

8 IT Product Testing

8.1 Developer Testing

8.1.1 Test Approach, coverage and depth

The developer performed testing on all SFRs based on the evaluated configuration. For specific functionalities without TSFI, the developers used a version of the TOE without the epoxy and connect directly to the cryptographic subsystem. By leveraging on the Mircochip IDE and debugger, the developer is able to step through the live execution of the codes. This approach allowed the developer to verify the correctness of implementation for several functionalities such as zeroisation of pin and keys and entering of halt state when self-tests have failed.

The functional specification has identified the following interfaces – keypad, USB (USB Mass Storage Class Bulk-Only Transport) and smartcard (ISO/IEC 7816). The test mapping provided by the developer shows that the tests cover all individual TSFI identified for the TOE. An extension to this mapping by the evaluator also shows that the TSFI have been covered with the developer's test suite.

8.1.2 Test Configuration

The base setup was used by both developer and evaluator for the testing is

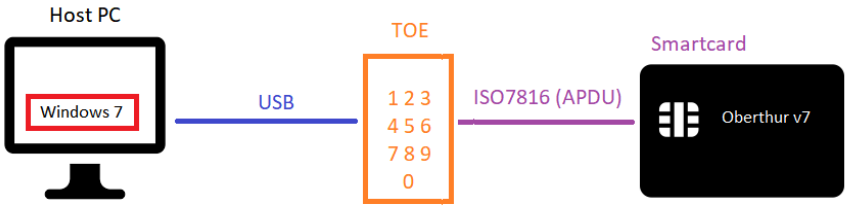

Figure 3: Basic test configuration

As mentioned in the approach above, testing of certain functionalities without any externally visible interfaces were performed using other setups.

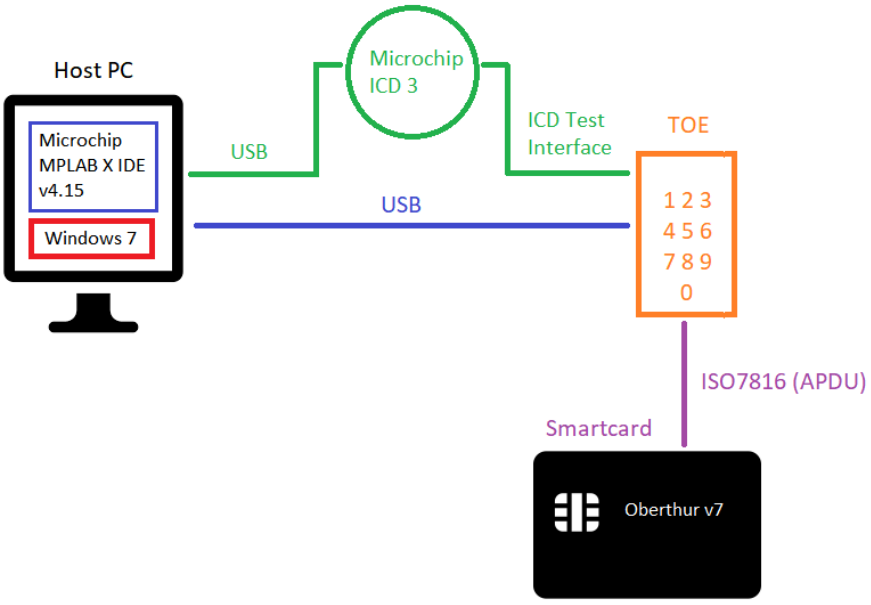

Figure 4: Test configuration to test functionalities without externally visible interfaces

The TOE used for testing is configured according to the DiskCrypt M100 Administrator's Guide Chapter 4 & 5 [9].

8.1.3 Test Results

The evaluator was able to follow and fully understand the developer testing approach by using the information provided by the developer.

The evaluator analysed the developer testing coverage and the depth of the testing by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification as well as the subsystem interfaces identified in the design documentation. 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 and verified the accuracy of the developer's test results.

The evaluator further devised additional tests cases for the TOE:

- Verification of visible signs of tampering when an attempt is made to remove the epoxy applied over the PCBA of the TOE using heat and scalpel.
- Verification of visible signs of tampering when an attempt is made to remove the epoxy applied over the PCBA of the TOE using acetone and

scalpel.

- Verification of visible signs of tampering when an attempt is made to remove the acrylic front panel from the metal part of the enclosure.
- Verification of visible signs of tampering when an attempt is made to remove the plastic recess (for holding internal HDD) within the TOE enclosure to expose the internal PCBA.
- Verification of the correct implementation of AES-XTS

8.2.2 Test Configuration

The same test configuration as described in section 8.1.2.

8.2.3 Test Results

The tests were performed primarily at evaluator's site. Nonetheless, for a subset of test cases which require access to source code, these were performed at developer's site. All of the developer's test were verified by the evaluator to conform to the expected results from the test plan.

8.3 Penetration Testing (AVA_VAN)

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.

The evaluator then devised attack scenarios where 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. Thereafter the evaluator analysed the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential Basic was actually successful.

At EAL2, the evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration.

The following could be possible at higher attack potential:

- Tampering the TOE and/or TOE's executing platform in the absence of TOE user.

- Substitution of legit TOE with a malicious one.

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 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 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. This is especially so as the firmware of the TOE could not be updated.

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.

In addition, the potential user should note the functionalities listed in section 5.4 that are not evaluated and determine that these exclusions are acceptable for his/her usage.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Testing 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
IKE	Internet Key Exchange
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] ST Electronics (Info-Security), “DiskCrypt M100 (Enterprise) Security Target, Version 2.0,” 2018.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2017-04-003], 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 Numnber 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 Criteria 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), "DiskCrypt M100 Administrator's Guide, Version 1.0.0," 2018.

[10] Common Criteria Recognition Arrangement Management Committee, "Operating Procedures - Conducting Shadow Certifications [Document number 2004-07-01]," 2017.

[11] ST Electronics (Info-Security), "DiskCrypt M100 User Manual, Issue A, Version 2.0," 2018.

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