Certificate Report

Version 1.0

2 July 2025

CSA_CC_22005

For

DiskCrypt Family Series
Version: M331P10J1E1

From

ST Engineering 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	2 July 2025	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 DiskCrypt Family Series, version M331P10J1E1 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Identifier	Version
Hardware	DiskCrypt M20 1TB, part number 9910-2401-099G DiskCrypt M20 2TB, part number 9910-2401-100G DiskCrypt M200, part number 9910-2401-098G In-house delivery – for Singapore Delivery Trusted Courier – for Overseas Delivery

Table 1 - TOE components identifier

The list of guidance documents to use with the product in its certified configuration is as follows.

Name	Version	Method of Delivery
DiskCrypt User Manual	1.0.2	Soft Copy (available on the website)
DiskCrypt Administrator Guide	1.0.2	Soft Copy (available on CD) In-house delivery – for Singapore Delivery Trusted Courier – for Overseas Delivery

Table 2 - List of guidance documents

The TOE, namely, DiskCrypt Family Series, is a USB data storage encryptor using the AES-256 XTS algorithm to provide hardware-based real time full disk encryption (FDE) for user data stored within its internal storage. The internal storage is out of the TOE scope.

The TOE consists of the following logical scope:

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

The evaluation of the TOE has been carried out by Setsco-An Security Pte Ltd, an approved CC Test Laboratory, at the assurance level CC EAL 2 and completed on 30 June 2025.

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

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

TOE Security Functionality
Identification 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 that is encrypted in the internal storage. If an unpaired smartcard is inserted, no access to the decryption/encryption function is allowed
Authentication The TOE requires the Administrator to be authenticated before they are allowed to administer the TOE using the administrative functions available in the TOE. Administrators shall present the paired smart card and input the correct Admin PIN via the integrated keypad, authenticating to the TOE. During Administrator authentication, a hash of the input Admin PIN is computed and compared with the stored hash value. Upon successful authentication, the administrative function selected will be successfully invoked. The Admin PIN is zeroized upon completion of usage.
Cryptographic Support User data sent from the host machine via the USB interface will be encrypted and stored in the internal storage. Similarly, all data retrieved from the encrypted storage will be decrypted and sent to the host machine. Data encryption is performed using the DEK (AES-256 XTS algorithm) to provide user data confidentiality. The DEK is derived from 2 separate keying materials. The first keying material (SKM – Smart card Keying Material) is retrieved from the user’s smart card. The second keying material (DKM – Device Keying Material) is injected into the TOE during device setup by the administrator. 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 data stored in the internal storage of the TOE. The TOE’s cryptographic module utilizes the DEK to perform real-time data encryption when data is transferred from the host machine to internal storage and vice versa.

The TOE performs Hashing to verify the integrity of TSF data (TOE application, configuration data, DKM and Admin PIN) during POST. The Admin PIN is stored as a hash within the TOE during device setup.

The TOE performs zeroization of SKM and DEK when no longer required.

Security Management

The TOE shall provide the following administrative functions:

1) Pairing of the legitimate smartcard to TOE
2) Enable/disable the smartcard lockout mode.
3) Change Admin PIN.
4) DKM injection (device setup) / Admin Smart Card Initialization

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 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 (SHA-256) 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 a "halt" state upon the successful invocation of each of the four administrative functions. The Administrator is required to power cycle the TOE and authenticate again should they want to invoke any of the administrative functions again.

Protection of TSF

The TOE is designed with protection and detection mechanisms to prevent and detect possible malfunction or compromised TSF/TSF data.

After the DEK is derived from the SKM and DKM, the TOE transfers the DEK to the cryptographic module and performs the zeroization of the SKM and the DEK from the MCU's memory.

The TOE performs zeroization of the Admin PIN upon completion of usage.

The "lockout mode" feature forces the TOE to automatically enter an unauthenticated state whenever the smartcard is removed from the TOE.

When the TOE enters an unauthenticated state, the DEK stored in the internal RAM of the cryptographic chip will be zeroized.

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-256 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 a “halt” and secure state, and the “ERROR” LED will be lighted up. In this state, the TOE is non-operational.

Table 3: 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 4 of the Security Target [1]

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

The certification results only apply to the version of the product indicated in the certificate and on the condition that 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 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

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

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

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **2 July 2030**[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 (https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/singapore-common-criteria-scheme/product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: DiskCrypt M20 1TB, DiskCrypt M20 2TB & DiskCrypt M200.

The following table identifies the TOE deliverables.

Identifier	Version
Hardware	DiskCrypt M20 1TB, part number 9910-2401-099G DiskCrypt M20 2TB, part number 9910-2401-100G DiskCrypt M200, part number 9910-2401-098G

Table 4 - TOE Deliverables

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

Name	Version	Method of Delivery
DiskCrypt User Manual	1.0.2	Download from developer's website
DiskCrypt Administrator Guide	1.0.2	In-house delivery or trusted courier

Table 5 - Guidance Document (part of TOE deliverables)

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

Name	Format	Method of Delivery
Smart cards (User and Admin)	Hardware	In-house delivery or trusted courier
USB cable	Hardware	
KeyCrypt	Hardware	
Internal Storage Device[2]	Hardware	
DiskCrypt Key Management Software (DMS)	MSI stored in CD	
AWP Manager Software	MSI stored in CD	
DMS Guide Version 2.4	PDF stored in CD	
AWP Manager Guide Version 1.5	PDF stored in CD	

Table 6 – Non-TOE components

[2] DiskCrypt M20 comes delivered with internal storage device. DiskCrypt M200 comes delivered without internal storage device.

Additional identification information relevant to this Certification procedure as follows:

TOE	DiskCrypt M20 1TB, DiskCrypt M20 2TB & DiskCrypt M200
Security Target	DiskCrypt Series Security Target Version 0.4
Developer	ST Engineering
Sponsor	ST Engineering
Evaluation Facility	Setsco-An Security Pte Ltd
Completion Date of Evaluation	30 June 2025
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_22005
Certificate Validity	5 years from date of issuance

Table 7: 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
- Authentication
- Cryptographic Support
- Security Management
- Protection of TSF

Specific details concerning the above-mentioned security policy can be found in Chapter 2 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:

Environmental Assumptions	Description
A.TRUSTED_USER	Users of the TOE are able to operate the TOE in a secure manner in accordance to the user guidance documentation.
A.ADMIN	Administrator of the TOE is trusted, well-trained and adheres to all guidance documentation provided.
A.SMARTCARD	The 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 8: Assumptions

Details can be found in section 4.4 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].

Users are reminded to set up the TOE as per guidance. Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

5.3 Evaluated Configuration

This TOE is a USB data storage encryptor which provides real-time full disk encryption (FDE) for user data stored within its internal storage. The internal storage is out of the TOE scope.

The TOE operates with a paired smart card which stores a smart card keying material (SKM). At the same time, a device keying material (DKM) is stored within the TOE. To access the user data stored within the internal storage, a user must authenticate itself to the smart card using a smart card PIN. After the smart card has successfully authenticated the user, the smart card releases the SKM to the TOE. The SKM and DKM are inputs to the TOE's key derivation function that derives a Data Encryption Key (DEK). The DEK shall then be used for disk encryption/decryption, in turn, the user gains read/write access to the user data stored within the internal storage.

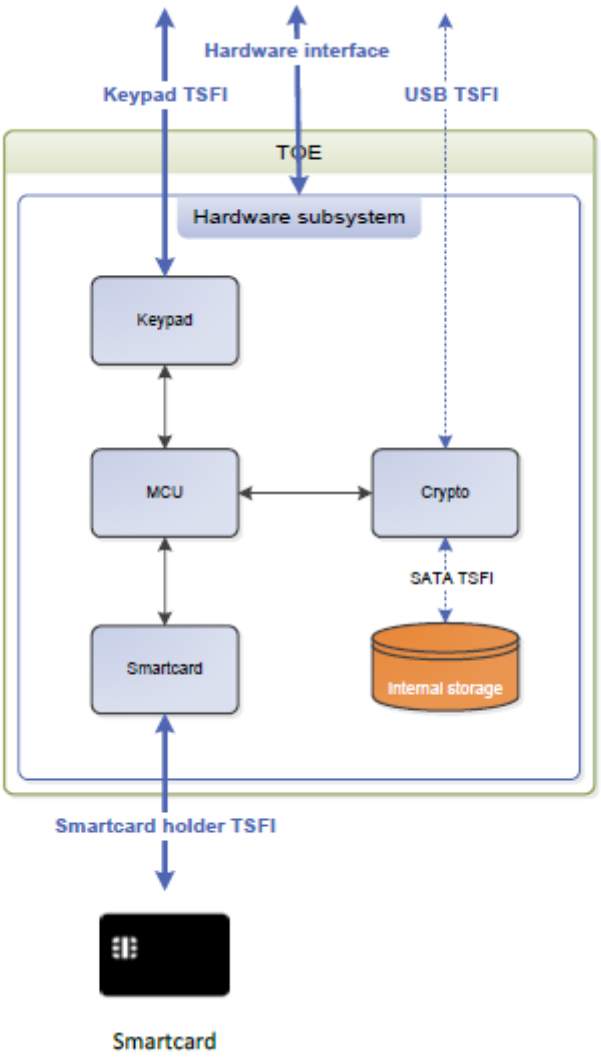

Figure 1 - Evaluated Configuration

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 for its operation. These non-TOE components include:

1. **DiskCrypt (DC) Smart Card** – Two types of PKCS #11 compliant smart cards are provided: **Admin Smart Card** and **User Smart Card**. The Admin Smart Card stores the DKM, and the User Smart Card stores the SKM. The Admin Smart Card is used to inject the DKM into the TOE during TOE preparation. DKM and SKM are input to the key derivation function for the DEK. The Smart Cards are also used for identification.
2. **DiskCrypt Key Management Software (DMS)** - The smart cards issued along with the DiskCrypt are provisioned by the Administrator using the DiskCrypt Key Management software (DMS). The DMS is an external software application for enterprises to manage their smart cards and SKM for usage with DiskCrypt. Administrators may refer to the DMS Guide for installation and operation guidance.
3. **AWP Manager Software Version** – AWP Manager is a software application used for performing cryptographic modification of smart cards issued with DiskCrypt. It communicates with the smart cards through a PKCS #11 module.
4. **Host Workstation** – The TOE requires a host system that provides a USB interface (USB 3.1/3.0) supporting the USB mass storage device class.
5. **KeyCrypt Token** – Used for 2FA login to the DMS software application
6. **Internal Storage Device** – 2.5inch SSD (use in DiskCrypt M200 Type C) and M.2 SSD with 2280 form factor (used in DiskCrypt M20).

6 Architecture Design Information

As described in the Security Target *[1]*, the high-level logical architecture of the TOE can be depicted as follows:

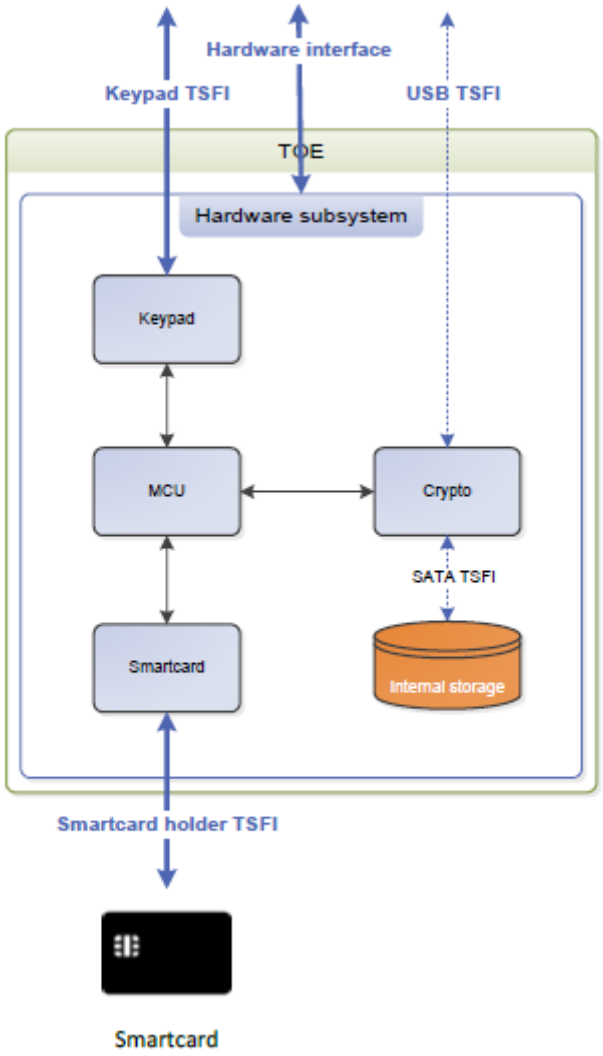

Figure 2 - Logical Architecture of the TOE

Subsytem	**Description**
Keypad	Provides an interface for the MCU subsystem to interact with the TOE user's key presses.
MCU	The main processing unit that enforces the following TSF • Identification • Authentication • Security management • Self-test
Smartcard	Provides an interface for the MCU subsystem to interact with the external smartcard.
Crypto	Provides real-time encryption/decryption of user data in the internal storage.
Hardware	Provides physical tamper-evidence protection.

Table 9 – Subsystem description

7 Documentation

The evaluated documentation as listed in Table 5 - Guidance Document (part of TOE deliverables) is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The evaluator sampled and repeated the developer's testing to validate the correctness of the TSF at the TSFI and the subsystem level.

8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance documents [9] [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

Based on Figure 2, the evaluator has identified 4 TSFIs

- Keypad
- USB
- Smartcard Holder
- SATA

These TSFIs are exposed to threats from threat agents; other interfaces are made inaccessible by OE.TRUSTED_USER, OE.ADMIN, OE.SMARTCARD.

The evaluator sampled and repeated developer's test cases that are related to the correctness of these TSFIs.

During ATE, the evaluator devised test subsets to augment and supplement the developer's test cases to further gain assurance of the correctness of the TSFIs.

The evaluator's strategy for devising independent tests was based on the following:

- Analysis of ADV_FSP

- Analysis of ADV_TDS
- Analysis of AGD_OPE

8.2.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance documents [9] [10].

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 evaluator conducted a vulnerability search using public sources of information like the Common Vulnerabilities and Exposures (CVE). The following keywords were used during the search:

- DigiSAFE. This is the developer's name.
- diskcrypt. This is the TOE product name.
- FDE. This is one of the TSFIs name.
- Full disk encryption

With no useful CVE information discovered, the evaluator used the Google search engine. The following were found during the search

- Encryption Bypass Vulnerability Impacts Half of Android Devices
- TPM vulnerability: Bitlocker Full Disk Encryption Impacted

However, these vulnerabilities are not applicable to the TOE

Combined with the analysis of the TOE, the evaluator then identified potential vulnerabilities applicable to the TOE in its operational environment. Attack scenarios were then devised and a theoretical analysis of the attack potentials for the scenarios were performed. Penetration tests were conducted for scenarios where the attack potentials were Basic.

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.

Penetration Test	Description

VA1	Perform the removal of the epoxy coating applied over the PCBA of the TOE using heat, scalpel, and dichloromethane to grant physical access to PCB components and the underlying subsystems.

Table 10 - Penetration Test Case

No exploitable vulnerabilities were found 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 and AVA_VAN.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 - List of guidance documents* 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.

Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

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
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] ST Engineering, “DiskCrypt Series Security Target Version 0.4,” 23 June 2025.

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

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

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

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

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 7.1,” 2024.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 7.1,” 2024.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 7.1,” 2024.

[9] ST Engineering, “DISKSCRYPT Administrator's Guide v1.0.2,” January 2025.

[10] ST Engineering, “DISKCRYPT M20 & M200 User Manual v1.0.2,” January 2025.

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