National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Seagate Secure®

TCG Opal and Enterprise SSC Self-Encrypting Drives

Report Number: CCEVS-VR-VID11248-2022
Dated: 07 April 2022
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Meredith Hennan
Alex Korobchuk
Seada Mohammed
Jerome Myers
The Aerospace Corporation

Farid Ahmed
Richard (Rip) Toren
Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in April 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the following documents:

- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine,* Version 2.0 + Errata 20190201, February 1, 2019 ([5])

The TOE is Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives consisting of Seagate Secure® TCG Opal SSC Self-Encrypting Drive Series and Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive Series with the following specific product identifiers and models:

Product Name	Model #	Standard	Firmware
Exos X18 3.5” SAS HDD	ST18000NM007J ST16000NM007J ST14000NM007J ST12000NM007J ST10000NM016G	Enterprise SSC	EF02
Exos X18 3.5” SATA HDD	ST18000NM025J	Opal SSC ATA Security	MF01
Exos X18 3.5” SAS HDD	ST18000NM026J	Opal SSC	KF01
Exos 7E10 3.5” SAS HDD	ST10000NM022B ST10000NM011B ST8000NM022B ST8000NM011B ST6000NM024B ST6000NM013B ST4000NM013B	Enterprise SSC	EF01 KF01 NF01

Product Name	Model #	Standard	Firmware
	ST4000NM029B ST4000NM017B		
Exos 7E10 3.5” SATA HDD	ST10000NM021B ST8000NM021B ST6000NM023B ST4000NM012B ST4000NM028B	Enterprise SSC ATA Security	SF01 TF01

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([6]).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

<table>
<tr><th>Item</th><th>Identifier</th></tr>
<tr><td>Evaluation Scheme</td><td>United States NIAP Common Criteria Evaluation and Validation Scheme</td></tr>
<tr><td>TOE</td><td>Seagate Secure® TCG Opal SSC Self-Encrypting Drive Series
Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive Series

The specific TOE products and models include:
<table>
<tr><th>Product Name</th><th>Model #</th><th>Standard</th><th>Firmware</th></tr>
<tr><td>Exos X18 3.5” SAS HDD</td><td>ST18000NM007J
ST16000NM007J
ST14000NM007J
ST12000NM007J
ST10000NM016G</td><td>Enterprise SSC</td><td>EF02</td></tr>
<tr><td>Exos X18 3.5” SATA HDD</td><td>ST18000NM025J</td><td>Opal SSC
ATA Security</td><td>MF01</td></tr>
<tr><td>Exos X18 3.5” SAS HDD</td><td>ST18000NM026J</td><td>Opal SSC</td><td>KF01</td></tr>
<tr><td>Exos 7E10 3.5” SAS HDD</td><td>ST10000NM022B
ST10000NM011B
ST8000NM022B</td><td>Enterprise SSC</td><td>EF01
KF01
NF01</td></tr>
</table></td></tr>
</table>

Item	Identifier			
		ST8000NM011B ST6000NM024B ST6000NM013B ST4000NM013B ST4000NM029B ST4000NM017B		
	Exos 7E10 3.5" SATA HDD	ST10000NM021B ST8000NM021B ST6000NM023B ST4000NM012B ST4000NM028B	Enterprise SSC ATA Security	SF01 TF01
Security Target	Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives Security Target, v1.0, 10 March 2022 ([6])			
Sponsor & Developer	Seagate Technology, LLC 389 Disc Drive Longmont, Colorado 80503			
Completion Date	April 2022			
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017			
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017			
PP	*collaborative Protection Profile for Full Drive Encryption – Encryption Engine,* Version 2.0 + Errata 20190201, February 1, 2019 ([5])			
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant			
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046			
Evaluation Personnel	Dawn Campbell Pascal Patin Furukh Siddique			
Validation Personnel	Meredith Hennan Farid Ahmed Alex Korobchuk Seada Mohammed Jerome Myers Richard (Rip) Toren			

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE comprises Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives (SEDs) provided by Seagate Technology, LLC. The TOE model numbers and firmware versions are identified in Table 1.

The Seagate SEDs implement FIPS-approved and NIST-recommended cryptographic algorithms. All algorithms implementing cryptographic security functional requirements have applicable NIST Cryptographic Algorithm Validation Program (CAVP) certificates. The SEDs provide an Instant Secure Erase (ISE) function and full protection of customer data-at-rest with self-encrypting drive locking. The Seagate Secure Drives are designed in accordance with Trusted Computing Group (TCG) specifications.

The TOE provides the Full Disk Encryption (FDE) Encryption Engine functionality as defined by [CPPFDE_EE]. In particular, the TOE provides data encryption, policy enforcement, and key management functions. The TOE provides for the generation, update, protection, and destruction of the data encryption key (DEK) and other intermediate keys under its control. Seagate terminology refers to the DEK as the Media Encryption Key (MEK).

The TOE model series includes SSC Opal and SSC Enterprise and support either SATA or SAS interfaces. SEDs can be a hard-disk drive (HDD) or a solid-state drive (SSD). All models in the TOE are HDD. All SEDs meet the requirements set forth in this document and behave the same except for handling failed authentication attempts as part of the process of validating the BEV.

Table 1 identifies the products included in the TOE, along with their firmware releases and supported standard, and specifies each TOE model, including its capacity. All TOE models incorporate an ARM Cortex-M0 processor (ARMv6-M microarchitecture) and include the Janus Application-Specific Integrated Circuit (ASIC). All SATA drives additionally support ATA Security mode.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Cryptographic Support

The TOE includes CAVP-certified cryptographic algorithms supporting cryptographic functions. The TOE provides Key Wrapping, Key Derivation, and BEV Validation.

4.2 User Data Protection

The TOE performs Full Drive Encryption such that the drive contains no plaintext user data. The TOE performs user data encryption by default in the out-of-the-box configuration using XTS-AES-256 mode.

4.3 Security Management

The TOE supports management functions for changing and erasing the DEK, for initiating the TOE firmware updates, and for configuring the number of failed validation attempts required to trigger corrective action.

4.4 Protection of the TSF

The TOE provides trusted firmware update and access control functions; protects Key and Key Material; and supports a compliant power saving state. The TOE runs a suite of self-tests during initial start-up (on power on), before the function is first invoked.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- Communication among and between product components (e.g., Authorization Acquisition (AA) and Encryption Engine (EE) components) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
- Users enable Full Drive Encryption on a newly provisioned storage device free of protected data in areas not targeted for encryption. It is also assumed that data intended for protection should not be on the targeted storage media until after provisioning. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible - for example, data contained in “bad” sectors. While inadvertent exposure to data contained in bad sectors or unpartitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, un-partitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE pre-authentication software) contain no protected data.
- Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system.
- The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
- The user does not leave the platform and/or storage device unattended until the device is in a compliant power saving state or has fully powered off. This properly clears memories and locks down the device. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen or sleep state). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.
- The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform’s correct operation.

5.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following document:
    - *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201, February 1, 2019* ([5])
- This evaluation covers only the specific hardware and firmware identified in this document, and not any earlier or later versions released or in process.
- The TOE use case explicitly excludes the case when TOE is in powered state.
- The evaluation of security functionality of the product was limited to the functionality specified in Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives Security Target, Version 1.0, 10 March 2022 ([6]). Any additional security related functional capabilities included in the product were not covered by this evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Seagate Secure® TCG Enterprise and TCG Opal SSC Self-Encrypting Drive Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, 9 March 2022 ([7])

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Seagate Secure® TCG SSC Self-Encrypting Drives Common Criteria Test Report and Procedures*, Version 1.1, 04 April 2022 ([8])

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives Assurance Activity Report*, Version 1.0, 10 March 2022 ([9])

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specifications:

- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201, February 1, 2019* ([5])

The evaluation team devised a test plan based on the test activities specified in these documents. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from July 1, 2021 to January 30, 2022. The tested platforms covered instances of the TOE to cover a variety of firmware, native interfaces, standards and media types. Evaluators configured default environment configurations for the products as described in the guidance. In addition to using vendor proprietary tools, they used Python interpreter, 010 Hex editor, and Dell Optiplex 790 for the test.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the team test plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Full Drive Encryption – Encryption Engine* were fulfilled.

8 TOE Evaluated Configuration

The evaluated version of the TOE consists of the Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives identified in Table 1.

The TOE must be deployed as described in Section 5 Assumptions of this document and be configured in accordance with the documentation identified in Section 6.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report For Seagate Secure® TCG SSC Self-Encrypting Drives ([10]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in:

- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201, February 1, 2019* ([5])

The evaluation determined the TOE satisfies the conformance claims made in the Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives Security Target, of Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in the PP.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the National Vulnerability Database (https://nvd.nist.gov/), MITRE CVE, US-CERT, and Seagate Security Advisory website.

The evaluation team performed searches on 7 April 2022, using the following search terms:

- Seagate
- Seagate Secure TCG Opal SSC
- Seagate Secure TCG Enterprise SSC
- ARMv6-M
- Cortex-M0
- ARM Processor
- 800-90A DRBG in Hardware
- ARMv6 AES in Firmware
- ARMv6 AES Key Wrap in Firmware
- ARMv6 GCM in Firmware
- ARMv6 HMAC in Firmware
- ARMv6 RSA in Firmware
- ARMv6 SHS in Firmware
- Janus
- drive encryption
- disk encryption
- key destruction
- key sanitization
- self encrypting drive (sed)
- opal

- opal ssc ata security
- enterprise ssc
- Enterprise SSC ATA Security
- tcg ssc
- Exos X18
- Exos 7E10

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

All of the validators concerns are adequately captured in Section 5, Assumptions and Clarification of Scope.

11 Security Target

The ST for this product's evaluation is *Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives* Security *Target*, Version 1.0, 10 March 2022 ([6]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AES	Advanced Encryption Standard
ASIC	Application-Specific Integrated Circuit
ATA	Advanced Technology Attachment
BEV	Border Encryption Value
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CLI	Command Line Interface
CPP	Collaborative Protection Profile
CPPFDE_EE	Collaborative Protection Profile for Full Drive Encryption – Encryption Engine
CPPFDE_AA	Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition
CSPSK	Critical Security Parameter Sanitization Key
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
EE	Encryption Engine
FDE	Full Drive Encryption
FIPS	Federal Information Processing Standard
FW	Firmware
GCM	Galois Counter Mode
HDD	Hard Disk Drive
HMAC	Hashed Message Authentication Code
ISE	Instant Secure Erase
IT	Information Technology
IV	Initialization Vector
KEK	Key Encryption Key
KMD	Key Management Description
LBA	Logical Block Addressing
MEK	Media Encryption Key
MEKEK	Media Encryption Key Encryption Key
MK	Master Key
PP	Protection Profile
PSID	Physical SID (public drive-unique value)
RBG	Random Bit Generator
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
RTU	Root of Trust for Update
SAR	Security Assurance Requirement
SAS	Serial Attached SCSI
SATA	Serial ATA (Serial AT Attachment)
SCSI	Small Computer Systems Interface
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SID	Security Identifier, (aka Drive Owner PIN)
SFR	Security Functional Requirement
SPD	Security Problem Definition
SPI	Serial Peripheral Interface
SSC	Security Subsystem Class
SSD	Solid State Drive
ST	Security Target

TCG	Trusted Computer Group
TOE	Target of Evaluation
TSF	TOE Security Functions
XOR	Exclusive or
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201, February 1, 2019.

[6] Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives Security Target, v1.0, 10 March 2022

[7] Seagate Secure® TCG Enterprise and TCG Opal SSC Self-Encrypting Drive Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, 9 March 2022

[8] Seagate Secure® TCG SSC Self-Encrypting Drives Common Criteria Test Report and Procedures, Version 1.0, 10 March 2022

[9] Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives Assurance Activity Report, Version 1.0, 9 March 2022

[10] Evaluation Technical Report For Seagate Secure® TCG SSC Self-Encrypting Drives, Version 1.0, 25 February 2022.