National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Seagate® Secure NVMe Self-Encrypting Drives

Report Number: CCEVS-VR-VID11416-2024
Dated: April 25, 2024
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

Seada Mohammed

Jerome Myers

Marybeth Panock

The Aerospace Corporation

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 NVMe 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 on April 25, 2024. 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 Conformant and meets the assurance requirements of the following document:

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

The TOE is Seagate® Secure NVMe Self-Encrypting Drives.

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

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Seagate® Secure NVMe Self-Encrypting Drives
Security Target	*Seagate® Secure NVMe Self-Encrypting Drives Security Target*, Version 0.24, 07 March 7, 2024.
Sponsor	Seagate Technology, LLC 47488 Kato Road Fremont, CA 94538
Developer	Phison Electronics Corporation No.1, Qun-Yi Road, Jhunan, Miaoli County, Taiwan 350, R.O.C.
Completion Date	April 25, 2024
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, 1 February 2019
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Anthony Apted Pascal Patin
Validation Personnel	Seada Mohammed Jerome Myers Marybeth Panock

3 TOE Architecture

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

The TOE comprises the following Seagate® Secure NVMe Self-Encrypting Drives (SEDs) provided by Seagate Technology, LLC and developed by Phison Electronics Corporation:

Product Name	Model #	Firmware
Nytro 5550H 15mm U.2/U.3 Mixed Use	XP800LE70025 XP1600LE70025 XP3200LE70025 XP6400LE70025 XP12800LE70025	SE4SA530 SGEBHG02
Nytro 5350H 15mm U.2/U.3 Read Intensive	XP1920SE70025 XP3840SE70025 XP7680SE70025 XP15360SE70025	SE4SA530 SGEBHG02
Nytro 5550M 15mm U.2/U.3 Mixed Use	XP800LE70055 XP1600LE70055 XP3200LE70055 XP6400LE70055 XP12800LE70055	SE4SA530 SGEBHG02
Nytro 5350M 15mm U.2/U.3 Read Intensive	XP1920SE70055 XP3840SE70055 XP7680SE70055 XP15360SE70055	SE4SA530 SGEBHG02
Nytro 5550M 7mm U.2/U.3 Mixed Use	XP800LE10025 XP1600LE10025 XP3200LE10025 XP6400LE10025	SE4SA530 SGEBHG02
Nytro 5350M 7mm U.2/U.3 Read Intensive	XP1920SE10025 XP3840SE10025 XP7680SE10025	SE4SA530 SGEBHG02

The SEDs communicate with a host system using a standard protocol defined by the Trusted Computing Group (TCG), an organization sponsored and operated by companies in the computer, storage, and digital communications industry. The Storage Work Group of the TCG defines Opal storage Security Subsystem Classes (SSC).

The Opal SSC supports NVMe (PCIe). While the physical form factor and firmware of the drives differ, all models included in the TOE support the requirements specified in *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*.

The SEDs are passive devices that respond to commands but do not initiate actions. A SED does not support remote or out-of-band management (although a host platform may have such capabilities that invoke SED commands).

Each SED encrypts stored data in the out-of-the-box (default) configuration. Access to data is not restricted until a user takes ownership via a TCG controller. After a user takes ownership, an authentication key is needed to unlock the drive.

The SEDs use logical block addressing (LBA) to manage the user-addressable non-volatile memory space. The SEDs accept NVMe commands to read or write user data in this memory space. All user data in the user-addressable non-volatile memory space is encrypted.

Each SED also supports a non-volatile memory space termed the system area, which is available only to the SED. There is no logical or physical access to the system area from outside of the SED. The SED stores keys and key material in the system area and accepts TCG commands to indirectly access or modify values in the system area.

Additionally, the SED supports a non-volatile memory space known as the TCG Data Store Tables. This area is not available to the user but can be accessed by an administrator using access-controlled TCG commands. The SED does not encrypt data stored in the TCG Data Store Tables and does not place any restrictions on what data is stored. Guidance documentation instructs administrators not to store protected data in the tables.

The SEDs support subdividing user storage into areas called locking ranges. Each locking range is secured with its own key chain. A key chain commences with a password-based key and concludes with the Data Encryption Key. The SED derives the 256-bit password-based key from a 32-byte (256-bit) authentication PIN received from the host Authorization Acquisition component, using the Password Based Key Derivation Function v2 as specified in NIST SP 800-132.

The SED uses its approved HMAC_DRBG function to generate the following keys in the key chain: Transfer Encryption Key (TEK); Key Encryption Key (KEK); and Data Encryption Key (DEK). The SED uses the password-based key to wrap and unwrap the 256-bit TEK using AES key wrapping (AES-KW). The SED then uses the TEK to wrap and unwrap the 256-bit KEK using AES-KW. Finally, the SED uses the KEK to wrap and unwrap the 256-bit DEK using AES-KW. The SED uses the DEK in AES-XTS mode to encrypt data as it is written to non-volatile memory and to decrypt data as it is read from non-volatile memory. The SED only ever stores wrapped keys in non-volatile memory, unwrapping keys and storing them in volatile memory as needed, and erasing unwrapped keys in volatile memory when no longer required.

The SEDs ship with a set of default PIN values that allow for open access to the SED until an administrator takes ownership and establishes new PINs and locking settings. In accordance with the TCG Opal specification, the SEDs support the following authentication PIN types that control access to the SED's operational resources: User's Security Identifier (SID); Physical Security Identifier (PSID); Admin SP Admins; Locking SP Admins; and Users.

Each SED has two security providers (SPs), termed the "Admin SP" and the "Locking SP". These act as gatekeepers to the SED's security services. Security-related commands will not be accepted without the correct credentials to prove the requester is authorized to perform the command.

The following authentication PINs provide access to encrypted user data: Locking SP Admin (the SEDs support from 1 to 4 Locking SP Admins); and User (the SEDs support from 1 to 9 Users). The following authentication PINs provide access to SED management functions: SID; PSID; and Admin SP Admin (the SEDs support from 1 to 4 Admin SP Admins).

The SEDs never directly store PINs, either in volatile or non-volatile memory. Instead, the SED verifies the PIN by deriving the password-based key from the PIN value and attempting to unwrap the TEK. If the SED successfully unwraps the TEK, then the entered PIN value is valid.

All drives include the PS5020-E20 Module V1.00 cryptomodule. The cryptomodule is implemented on an Arm Cortex-R5 processor, which is based upon the ARMv7-R architecture. Each SED includes either firmware version SE4SA530 or SGEBHG02, depending on the intended market for the SED (retail or OEM). The try limit value settings differ between the two versions, but the cryptographic algorithm designs are the same.

The TOE requires a host system using the standard protocol defined by the TCG in its operational environment.

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 implements NIST-validated cryptographic algorithms supporting cryptographic functions. The TOE provides Key Wrapping, Key Derivation, and Border Encryption Value (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 AES in XTS mode with 256-bit encryption keys.

4.3 Security Management

The TOE supports management functions for changing and erasing the DEK, initiating TOE firmware updates, and configuring a password for firmware updates.

4.4 Protection of the TSF

The TOE: provides trusted firmware update and update access control functions; protects Key and Key Material; and supports power saving states. The TOE runs a suite of self-tests during initial start-up (on power on).

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references *collaborative Protection Profile for Full Drive Encryption – Encryption Engine* for the assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows[1]:

- Communication among and between product components (e.g., AA and EE) 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. 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.

[1] The TOE implements all cryptographic functionality and does not rely on any cryptographic functions in its Operational Environment. As such, assumption A.STRONG_CRYPTO is not relevant to the TOE.

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, 1 February 2019 ([5])
- This evaluation covers only the specific product models and versions identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Seagate® Secure NVMe Self-Encrypting Drives Security Target, Version 1.0, 07 March 2024 . 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® NVMe Self-Encrypting Drives Common Criteria Configuration Guide, Version 1.2, March 7, 2024

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 NVMe Self-Encrypting Drives Common Criteria Test Report and Procedures, Version 1.1, 25 April 2024 [9].

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

- *Assurance Activities Report for Seagate® Secure NVMe Self-Encrypting Drives*, Version 1.0, 25 April 2024 ([8]).

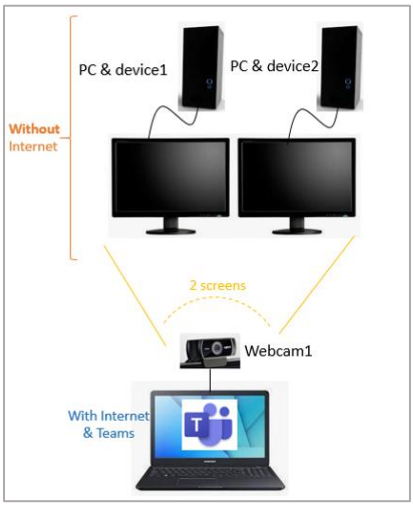
The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specification:

- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0+Errata 20190201, 1 February 2019.

The evaluation team devised a test plan based on the test activities specified in the above specifications. 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.

The TOE was tested remotely with the TOE being located at Phison's facility in Taiwan. The procedures and results of this testing are available in the test report referenced above.

The following figure depicts the test configuration used by the evaluation team to test the TOE on each of its supported platforms.



Both TOE instances were connected to computer running Ubuntu Linux running Phison's proprietary test tool. In order to maintain the integrity of the evaluation the test systems connected to the TOE were airgapped and did not have any network connectivity. Testing was observed using a webcam on a separate, internet-connected computer.

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 TOE comprises the following Seagate® Secure NVMe Self-Encrypting Drives (SEDs) provided by Seagate Technology, LLC and developed by Phison Electronics Corporation:

Product Name	Model #	Drive Writes per Day
Nytro 5550H 15mm U.2/U.3 Mixed Use	XP800LE70025 XP1600LE70025 XP3200LE70025 XP6400LE70025 XP12800LE70025	3
Nytro 5350H 15mm U.2/U.3 Read Intensive	XP1920SE70025 XP3840SE70025 XP7680SE70025 XP15360SE70025	1
Nytro 5550M 15mm U.2/U.3 Mixed Use	XP800LE70055 XP1600LE70055 XP3200LE70055 XP6400LE70055 XP12800LE70055	3
Nytro 5350M 15mm U.2/U.3 Read Intensive	XP1920SE70055 XP3840SE70055 XP7680SE70055 XP15360SE70055	1
Nytro 5550M 7mm U.2/U.3 Mixed Use	XP800LE10025 XP1600LE10025 XP3200LE10025 XP6400LE10025	3
Nytro 5350M 7mm U.2/U.3 Read Intensive	XP1920SE10025 XP3840SE10025 XP7680SE10025	1

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 NVMe Self-Encrypting Drives ([7]). 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, 1 February 2019 ([5])

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

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.

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

The evaluation team performed each test activity and applied each ATE_IND.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/).

The evaluation team performed NVD searches on the TOE using the following search terms:

- Vendor/developer/product names:
  - “Seagate”
  - “Phison”
  - “Nytro”
- Underlying components as required by [SD] for EE SED products:
  - “PS5020-E20”
  - “Arm Cortex-R5”
  - “ARMv7-R”
  - “self encrypting drive”
  - “opal”
- Search terms specified in [SD] for general FDE technology and for EE products specifically:
  - “drive encryption”
  - “disk encryption”
  - “key destruction”
  - “key sanitization”

The evaluation team also searched the vendor security advisories page (https://www.seagate.com/support/security/). These searches were conducted most recently on April 4, 2024.

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. In addition, the evaluation team’s testing 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

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Security Target

The ST for this product's evaluation is *Seagate® Secure NVMe Self-Encrypting Drives Security Target*, Version 0.24, 07 March 7, 2024.

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AES	Advanced Encryption Standard
BEV	Border Encryption Value
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
ETR	Evaluation Technical Report
HMAC	Hashed Message Authentication Code
IT	Information Technology
KEK	Key Encryption Key
NVMe	Nonvolatile Memory express
OEM	Original Equipment Manufacturer
PBKDF2	Password-Based Key Derivation Function version 2
PCL	Product Compliant List
PIN	Personal Identification Number
PP	Protection Profile
PSID	Physical Security Identification
SAR	Security Assurance Requirement
SED	Self-Encrypting Drive
SFR	Security Functional Requirement
SID	Security Identification
SSC	Security Subsystem Class
ST	Security Target
TCG	Trusted Computing Group
TEK	Transfer Encryption Key
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report
XEX	XOR-encrypt-XOR (a tweakable encryption mode used for disk encryption)
XTS	XEX-based tweaked-codebook mode with ciphertext stealing (a mode of AES used for disk encryption)

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, 1 February 2019.

[6] Seagate® Secure NVMe Self-Encrypting Drives Security Target, Version 0.24, 07 March 2024.

[7] Evaluation Technical Report for Seagate® Secure NVMe Self-Encrypting Drives, Version 1.0, 25 April 2024.

[8] Assurance Activities Report for Seagate® Secure NVMe Self-Encrypting Drives, Version 1.0, 25 April 2024.

[9] Seagate® Secure NVMe Self-Encrypting Drives Common Criteria Test Report and Procedures, Version 1.1, 25 April 2024.