National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Seagate Secure® TCG SSC Self-Encrypting Drives

Report Number:	**CCEVS-VR-10857-2018**
Dated:	**April 11, 2018**
Version:	**1.0**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Marybeth Panock, Aerospace Corporation
Jerome Myers, Aerospace Corporation

Common Criteria Testing Laboratory

Leidos
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user to determine the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST) [6][1], (which is where specific security claims are made) as well as this Validation Report (VR) (which describes how those security claims were evaluated, tested, and any restrictions that may be imposed upon the evaluated configuration) to help in that determination. Prospective users should carefully read the Assumptions and Clarification of Scope in section 4 and the Validator Comments in section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Seagate Secure® TCG[2] SSC[3] Self-Encrypting Drives. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Seagate Secure TCG SSC Self-Encrypting Drives was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in April 2018. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 [4] and the assurance activities specified in the *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 [10] and [11]. Leidos performed an analysis of the NIAP Technical Decisions (https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm). Leidos determined Technical Decision TD0233 applied to this evaluation. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the Seagate Secure TCG SSC Self-Encrypting drives are conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfied all of the security functional requirements stated in the ST. The information in this VR is largely derived from the publicly available Assurance Activities Report (AAR) [7] and the associated proprietary test report [8] produced by the Leidos evaluation team.

The TOE comprises the Seagate Secure TCG Enterprise SSC and TCG Opal SSC Self-Encrypting Drives by Seagate Technology, LLC. TOE model numbers and firmware versions are identified in

[1] See section 14 Bibliography.

[2] Trusted Computing Group

[3] Security Subsystem Class

the table below. Some Enterprise and Opal drives also support ATA Security as indicated in the table.

The TOE provides Encryption Engine functionality for Full-Drive Encryption as defined by *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine* [10] and [11]. 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 and other intermediate keys under its control.

Table 1 Seagate Secure TCG SSC Self-Encrypting Drives TOE Models

Product Name	Model #	Capacity	TCG Standard	Firmware
Nytro 3000 SSD, 7mm, SAS Interface	XS1600ME10023	1600	Enterprise SSC	7539
	XS800ME10023	800		
	XS400ME10023	400		
	XS6400LE70023	6400		
	XS1600LE10023	1600		
	XS1920SE10123	1920		
	XS3840TE10023	3840		
Nytro 3000 SSD 15mm, SAS Interface	XS3200ME70023	3200	Enterprise SSC	7539
	XS15360SE70123	15360		
	XS15360TE70023	15360		
	XS7680TE70023	7680		
Exos 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0166	900	Enterprise SSC	CK10
	ST600MP0156	600		
Exos 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0126	900	Enterprise SSC	CKF1
	ST600MP0026	600		
FireCuda 2.5", SATA Interface (Hybrid)	ST2000LX003	2000	Opal SSC ATA Security	SSM1
	ST1000LX017	1000		
BarraCuda 2.5", SATA Interface	ST2000LM010	2000	Opal SSC ATA Security	SDM2 RSE3 (1D) RDE3 (2D)
	ST1000LM038	1000		
	ST500LM033	500		
BarraCuda Pro 2.5", SATA Interface	ST1000LM050	1000	Opal SSC ATA Security	SDM2 RXE2
	ST500LM035	500		
Exos 10E2400, 2.5-Inch, 10K-RPM	ST1200MM0069	1200	Enterprise SSC	CSF2

Product Name	Model #	Capacity	TCG Standard	Firmware
Exos 10E2400, 2.5-Inch, 10K-RPM	ST2400MM0149	2400	Enterprise SSC	CS10
	ST1800MM0149	1800		
	ST1200MM0149	1200		
Exos X10, 3.5-inch, 7K-RPM, SAS Interface	ST10000NM0246	10000	Enterprise SSC	CT10
Exos X10, 3.5-inch, 7K-RPM, SAS Interface	ST10000NM0236	10000	Enterprise SSC	CT12
Exos X10, 3.5-inch, 7K-RPM, SATA Interface	ST10000NM0186	10000	Enterprise SSC ATA Security	CT14
Exos X10, 3.5-inch, 7K-RPM, SATA Interface	ST10000NM0176	10000	Enterprise SSC ATA Security	CTF1
BarraCuda 3.5", SATA Interface	ST2000DM011	2000	Opal SSC ATA Security	0001

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PP had been completed successfully and that the product satisfied all of the security functional and assurance requirements as stated in the ST.

Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Seagate Secure TCG SSC Self-Encrypting Drives Security Target.

Table 2 Evaluation Details

Item	Identifier
Evaluated Product	Seagate Secure TCG SSC Self-Encrypting Drives identified in Table 1
Sponsor & Developer	Seagate Technology, LLC 389 Disc Drive Longmont, Colorado 80503
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046

Item	Identifier
Completion Date	April 2018
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 Supporting Document, Mandatory Technical Document – Full Drive Encryption: Encryption Engine, CCDB-2016, Version 2.0
Disclaimer	The information contained in this Validation Report is not an endorsement of the Seagate Secure TCG SSC Self-Encrypting Drives by any agency of the U.S. Government and no warranty of the Seagate Secure TCG SSC Self-Encrypting Drives is either expressed or implied.
Evaluation Personnel	Gary Grainger Kevin Steiner
Validation Personnel	Marybeth Panock, Lead Validator Jerome Myers, Senior Validator

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) 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 information technology 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) (https://www.niap-ccevs.org/Product/).

The following table identifies the evaluated Security Target and TOE.

Name	Description
ST Title	Seagate Secure TCG SSC Self-Encrypting Drives Security Target
ST Version	1.0
Publication Date	April 4, 2018
Vendor and ST Author	Seagate Technology, LLC
TOE Reference	Seagate Secure TCG SSC Self-Encrypting Drives identified in Table 1
TOE Software Version	Firmware versions identified in Table 1
Keywords	Self-Encrypting Drive, SED, TCG Enterprise Security Subsystem Class (SSC), TCG Opal

2.1 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter.

- The cPP[4] addresses the primary threat of unauthorized disclosure of protected data stored on a storage device. If an adversary obtains a lost or stolen storage device (e.g., a storage device contained in a laptop or a portable external storage device), they may attempt to connect a targeted storage device to a host of which they have complete control and have raw access to the storage device (e.g., to specified disk sectors, to specified blocks).
- Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of keying

[4] Collaborative Protection Profile

material of equal importance to the data itself. Threat agents may look for keying material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash, or TPMs.

- Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release DEKs or otherwise put it in a state in which it discloses protected data to unauthorized users.
- Threat agents may perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms and/or parameters allow attackers to exhaust the key space through brute force and give them unauthorized access to the data.
- Threat agents know plaintext in regions of storage devices, especially in uninitialized regions (all zeroes) as well as regions that contain well known software such as operating systems. A poor choice of encryption algorithms, encryption modes, and initialization vectors along with known plaintext could allow an attacker to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
- Threat agents may trick authorized users into storing chosen plaintext on the encrypted storage device in the form of an image, document, or some other file. A poor choice of encryption algorithms, encryption modes, and initialization vectors along with the chosen plaintext could allow attackers to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
- Threat agents may attempt to perform an update of the product which compromises the security features of the TOE. Poorly chosen update protocols, signature generation and verification algorithms, and parameters may allow attackers to install software that bypasses the intended security features and provides them unauthorized access to data.
- An attacker attempts to replace the firmware on the SED via a command from the AA or from the host platform with a malicious firmware update that may compromise the security features of the TOE.
- An attacker attempts to modify the firmware in the SED via a command from the AA or from the host platform that may compromise the security features of the TOE.

2.2 Organizational Security Policies

There are no Organizational Security Policies for the *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine* [10].

3 Architectural Information

The TOE model series includes SSC Opal and SSC Enterprise drives. The Opal SSC series supports Serial AT Attached (SATA) interfaces. The Enterprise SSC series supports both SATA and Serial Attached SCSI (SAS) interfaces. Seagate Secure SEDs include hard-disk drives (HDD) and solid-state drives (SSD). All models are HDD except the Nytro 3000 models (SSD) and the FireCuda SATA models which are hybrid models (see Table 1). A hybrid model provides both HDD and SSD storage but with performance like an SSD. All SEDs meet the requirements set forth in the security target [6]. The devices behave the same except regarding the following functions:

- Destruction of cryptographic keys (See security target [6] section 6.2.2)
- Random number generation (See security target [6] section 6.2.6)
- Validation of BEV (See security target [6] section 6.2.8)

The TOE models and firmware all provide the same basic set of security functionality, differing mainly in capacity and hardware as identified in Table 1.

A host system using the standard protocol defined by the Trusted Computing Group (TCG) is required in the operational environment.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- 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 un-partitioned 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.

4.1 Clarification of Scope

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

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific hardware products, and firmware versions identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation. Any additional non-security related functional capabilities of the product, even those described in the ST, were not covered by this evaluation.
4. 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 [4] defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

5 Security Policy

Seagate Secure TCG SSC Self-Encrypting Drives enforce the following TOE security functional policies as specified in the ST.

5.1 Cryptographic Support

The TOE includes NIST-validated cryptographic algorithms supporting cryptographic functions. The TOE provides Key Wrapping, Key Derivation, and Border Encryption Value Validation.

5.2 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.

5.3 Security Management

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

5.4 Protection of the TSF

The TOE:

- Provides trusted firmware update and access control functions,
- Protects keys and key material, and
- Supports power saving states.

The TOE runs a suite of self-tests during initial start-up (on power on), before the function is first invoked.

6 Documentation

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- *Seagate Secure TCG Enterprise and TCG Opal SSC Self-Encrypting Drive Common Criteria Configuration Guide,* Version 1.0, February 14, 2018

The above document is considered to be part of the evaluated TOE. The document is available by download from the NIAP web site. It is also available by download from www.seagate.com but the configuration management of that site was not included within the scope of the evaluation

Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

7 Independent Testing

7.1 Evaluation team independent 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 1.2, April 4, 2018 [8]

A non-proprietary summary of the test configuration, test tools, and tests performed may be found in:

- *Seagate Secure TCG SSC Self-Encrypting Drives Common Criteria Assurance Activities Report*, Version 1.2, April 4, 2018 [7]

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 claiming conformance to *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine* [10] and [11].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine* [10] and [11]. 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 the Seagate facility in Longmont, Colorado from January 29, 2018 to February 2, 2018.

The evaluators received the TOE in the form that normal 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* [10] and [11] were fulfilled.

7.2 Vulnerability Survey

A search of public domain sources for potential vulnerabilities in the TOE did not reveal any known vulnerabilities.

The evaluator conducted penetration testing, based on the potential vulnerabilities identified in the general full-drive encryption technologies. The testing did not exploit any vulnerability. The details of the vulnerability survey can be found in the *Seagate Secure TCG SSC Self-Encrypting Drives Common Criteria Assurance Activities Report*, Version 1.2, April 4, 2018 [7], Section 3.6.2 Supporting Document Assurance Activities.

8 Evaluated Configuration

The evaluated version of the TOE consists of the Seagate Secure TCG SSC Self-Encrypting drives identified in Table 1.

The TOE must be deployed as described in section 4 Assumptions of this document and be configured in accordance with the documentation identified in Section 6.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine* [10] and [11] in conjunction with version 3.1 revision 4 of the CC and the CEM ([1], [2], [3], and [4]). A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that the evidence demonstrates the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR) [9], which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic function specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software, firmware, or hardware that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Table 4 Security Target Identification

Name	Description
ST Title	Seagate Secure TCG SSC Self-Encrypting Drives Security Target Security Target
ST Version	1.0
Publication Date	April 4, 2018

13 Abbreviations and Acronyms

AA	Authorization Acquisition
AAR	Assurance Activity Report
ATA	AT Attachment
BIOS	Basic Input/Output System
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Test Lab
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
DEK	Data encryption key
EE	Encryption Engine
ETR	Evaluation Technical Report
FDE	Full-drive encryption or full-disk encryption
HDD	Hard-disk drive
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PC	Personal Computer
PCL	Product Compliant List
PIN	Personal identification number
PP	Protection Profile
SAS	Serial Attached SCSI
SATA	Serial ATA
SCSI	Small Computer System Interface
SED	Self-encrypting drive
SSC	Security Subsystem Class
SSD	Solid-state drive

ST	Security Target
TCG	Trusted Computing Group
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSF	TOE Security Functions
VR	Validation Report

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluation Part 1: Introduction*, Version 3.1, Revision 4, September 2012.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements*, Version 3.1 Revision 4, September 2012.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components*, Version 3.1 Revision 4, September 2012.

[4] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, Version 3.1, Revision 4, September 2012.

[5] *Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories*, Version 2.0, 8 Sep 2008.

[6] *Seagate Secure TCG SSC Self-Encrypting Drives Security Target*, version 1.0, April 4, 2018

[7] *Seagate Secure TCG SSC Self-Encrypting Drives Common Criteria Assurance Activities Report*, Version 1.2, April 4, 2018

[8] *Seagate Secure TCG SSC Self-Encrypting Drives Common Criteria Test Report and Procedures*, Version 1.2, April 4, 2018

[9] *Evaluation Technical Report for Seagate Secure® TCG SSC Self-Encrypting Drives*, Version 1.0, February 15, 2018

[10] *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0, September 9, 2016

[11] *Supporting Document, Mandatory Technical Document – Full Drive Encryption: Encryption Engine*, CCDB-2016, Version 2.0, September 2016