National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Seagate Secure® TCG SSC Self-Encrypting Drives

Report Number: **CCEVS-VR-VID11209-2021**

Dated: **December 2, 2021**

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

Jerome Myers
Meredith Hennan
Seada Mohammed
Alex Korobchuk
The 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 5 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 December 2021. 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 5 [4] and the assurance activities specified in the *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201 (CPPFDE_EE20e) [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* [CPPFDE_EE20e] [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 #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
Nytro® 3730 SSD, 7mm, SAS Interface	XS1600ME10023 XS800ME10023 XS400ME10023	Balto	Enterprise SSC	1600, 800, 400	7539 0004 0005	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3530 SSD, 7mm, SAS Interface	XS6400LE70023 XS1600LE10023	Balto	Enterprise SSC	6400, 1600	7539 0004 0005	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3330 SSD, 7mm, SAS Interface	XS1920SE10123	Balto	Enterprise SSC	1920	7539 0004 0005	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3130 SSD, 7mm, SAS Interface	XS3840TE10023	Balto	Enterprise SSC	3840	7539 0004 0005	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3730 SSD, 15mm, SAS Interface	XS3200ME70023	Balto	Enterprise SSC	3200	7539 0004 0005	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3330 SSD, 15mm, SAS Interface	XS15360SE70123	Balto	Enterprise SSC	15360	7539 0004 0005	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware)

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3130 SSD, 15mm, SAS Interface	XS15360TE70023 XS7680TE70023	Balto	Enterprise SSC	15360, 7680	7539 0004 0005	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3031 SSD, 15mm, SAS Interface	XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024	Balto	Enterprise SSC	6400, 400, 800, 3840, 7680	0001 0003 0004 0005 A003	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3031 SSD, 15mm, SAS Interface	XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024	Balto	Enterprise SSC	800, 960, 1600, 1920, 3200, 3840, 7680, 15360	0001 0002 0003 0004 0005 A001 A003	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
	XS3840SE70024 XS7680SE70024 XS15360TE70024					ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 2032 SSD, 15mm SAS Interface	XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	Balto	Enterprise SSC	960, 1920, 3840, 7680	0001 0002	Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Nytro® 3032 SSD, 15mm SAS Interface	XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104	Balto	Enterprise SSC	400, 800, 1600, 3200, 800, 1600, 3200, 6400, 960, 1920, 3840, 7680, 15360, 3840, 680	0001 0002	Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Exos™ 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0166 ST600MP0156	Myna	Enterprise SSC	900, 600	CK10 CF04	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						ARMv7 AES in Firmware 3.0 (Firmware)
Exos™ 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0126 ST600MP0026	Myna	Enterprise SSC	900, 600	CKF1 NF04	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
FireCuda™ 2.5", SATA Interface (Hybrid)	ST2000LX003 ST1000LX017	Cheops	Opal SSC ATA Security	2000, 1000	SSM1	ARMv7 GCM in Firmware 1.0 ARMv7 SHS in Firmware 3.0 ARMv7 RSA in Firmware 5.0 800-90 DRBG 1.0 (Firmware) ARMv7 HMAC in Firmware 4.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
BarraCuda 2.5", SATA Interface	ST2000LM010 ST1000LM038 ST500LM033	Cheops	Opal SSC ATA Security	2000, 1000, 500	SDM2 RSE3 (1D) RDE3 (2D) RTE2 REE2	ARMv7 GCM in Firmware 1.0 ARMv7 SHS in Firmware 3.0 ARMv7 RSA in Firmware 5.0 800-90 DRBG 1.0 (Firmware) ARMv7 HMAC in Firmware 4.0

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
BarraCuda Pro 2.5", SATA Interface	ST1000LM050 ST500LM035	Cheops	Opal SSC ATA Security	100, 500	SDM2 RXE2 RXE3 LXM7 RPE2 0001	ARMv7 GCM in Firmware 1.0 ARMv7 SHS in Firmware 3.0 ARMv7 RSA in Firmware 5.0 800-90 DRBG 1.0 (Firmware) ARMv7 HMAC in Firmware 4.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Exos® 10E2400, 2.5-Inch, 10K-RPM SAS Interface	ST1200MM0069	Myna	Enterprise SSC	1200	CSF2 NF04	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Exos® 10E2400, 2.5-Inch, 10K-RPM SAS Interface	ST2400MM0149 ST1800MM0149 ST1200MM0149	Myna	Enterprise SSC	2400, 1800, 1200	CS10 CF04	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Exos® X10, 3.5-inch, 7K-RPM, SAS Interface	ST10000NM0246	Myna	Enterprise SSC	10000	CT10	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Exos® X10, 3.5-inch, 7K-RPM, SAS Interface	ST10000NM0236	Myna	Enterprise SSC	10000	CT12	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
ExosTM 7E8, SAS Interface	ST4000NM014A ST8000NM010A ST6000NM033A	Myna	Enterprise SSC	8000 6000	EF01 EFA2	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
ExosTM 7E8, SAS Interface	ST4000NM015A ST3000NM005A	Myna	Enterprise SSC	4000 3000	NF01 NFA2	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
ExosTM 7E8, SATA Interface	ST4000NM012A ST8000NM008A ST6000NM025A	Myna	Enterprise SSC	8000 6000	SF01 SFA2	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
ExosTM 7E8, SATA Interface	ST3000NM004A ST4000NM013A	Myna	Enterprise SSC	3000	TF01 TFA2	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
ExosTM 16, SAS Interface	ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	Myna	Enterprise SSC	10000 12000 14000 16000	EF01 EF02 EF03	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Exos® X10, 3.5-inch, 7K-RPM, SAS Interface	ST10000NM0186	Cheops	Enterprise SSC ATA Security	10000	CT14	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Exos® X10, 3.5-inch, 7K-RPM, SAS Interface	ST10000NM0176	Cheops	Enterprise SSC ATA Security	10000	CTF1	ARMv7 GCM in Firmware 2.0 ARMv7 SHS in Firmware 5.0 ARMv7 RSA in Firmware 5.1 Hash_Based DRBG 2.0 (Firmware)

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						ARMv7 HMAC in Firmware 5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
BarraCuda 3.5", SATA Interface	ST2000DM011	Cheops	Opal SSC ATA Security	2000	0001	ARMv7 GCM in Firmware 1.0 ARMv7 SHS in Firmware 3.0 ARMv7 RSA in Firmware 5.0 800-90 DRBG 1.0 (Firmware) ARMv7 HMAC in Firmware 4.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)

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

Item	Identifier
Sponsor & Developer	Seagate Technology, LLC 389 Disc Drive Longmont, Colorado 80503
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	December 2021
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017
PP	Collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 Supporting Document, Mandatory Technical Document – Full Drive Encryption: Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019
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	Pascal Patin Furukh Siddique Greg Beaver *Leidos*
Validation Personnel	Meredith Hennan Alex Korobchuk Seada Mohammed Jerome Myers *The Aerospace Corporation*

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.

Table 3 TOE Identification

Name	Description
ST Title	Seagate Secure TCG SSC Self-Encrypting Drives Security Target
ST Version	V 1.0
Publication Date	November 9, 2021
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

[4] Collaborative Protection Profile

an unauthorized user to defeat the encryption. The cPP considers possession of keying 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

3.1 TOE Description

The TOE comprises the 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. The Cryptographic Algorithm Validation Program (CAVP) certificates are identified in Section 6.2 of the security target. 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 the *collaborative Protection Profile for Full Drive Encryption - Encryption Engine, version 2.0 + Errata 20190201, 1 February 2019* [CPPFDE_EE20e]. 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).

3.2 TOE 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 5.1 Assumptions of this document and be configured in accordance with the documentation identified in Section 6.

3.3 Physical Scope of the TOE

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 models (SSD) and some of the 2.5" SATA models which are hybrid models (see Table 2). Hybrid models provide both HDD and SSD; and behave like a 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 Security Policy

This section summarizes the security functions provided by the Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives:

- Cryptographic support
- User Data Protection
- Security Management
- Protection of the TSF.

4.1.1 Cryptographic Support

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

4.1.2 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.

4.1.3 Security Management

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

4.1.4 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 security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) from the *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201, 1 February 2019, [CPPFDE_EE20e]* excluding A.STRONG_CRYPTO. This information has not been reproduced here and the CPPFDE_EE20e should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the CPPFDE_EE20e as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

5.2 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 CPPFDE_EE20e 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. 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.
4. The evaluation of security functionality of the product was limited to the functionality specified in the CPPFDE_EE20e and applicable Technical Decisions. 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.

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* [12].

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 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 1.0, November 12, 2021* [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 Activity Report, Version 1.0, November 14, 2021*[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 Leidos facility in Columbia Maryland from March 1, 2021 to November 12, 2021.

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.

A description of the Test Tools and Test Configurations used in the evaluation may be found in Section 3.5.1 of the Assurance Activity Report.

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.

7.3 Vulnerability Survey

A search of public domain sources for potential vulnerabilities in the TOE did not reveal any known vulnerabilities. The vulnerability searches of the following public vulnerability databases were performed on 11/11/2021:

- National Vulnerability Database (NVD, https://nvd.nist.gov/)
- MITRE Common Vulnerabilities and Exposures (CVE, http://cve.mitre.org/cve/)
- Seagate Security Advisories Web Page (https://www.seagate.com/support/security/)

Search terms investigated:

Table 4 Vulnerability Search Terms

Search Terms	Term Type
Seagate	Vendor
Seagate Secure TCG Opal SSC	Product Name
Seagate Secure TCG Enterprise SSC	Product Name
ARMv7	Component
ARM Cortex-R	Component
ARM Processor	Component
800-90 DRBG 1.0 Firmware	Component
ARMv7 AES in Firmware	Component
ARMv7 AES Key Wrap in Firmware	Component
ARMv7 GCM in Firmware	Component
ARMv7 HMAC in Firmware	Component
ARMv7 RSA in Firmware	Component
ARMv7 SHS in Firmware	Component
Hash_Based DRBG 2.0 Firmware	Component
Balto	Component
Cheops	Component
Myna	Component
drive encryption	iTC mandated
disk encryption	iTC mandated
key destruction	iTC mandated
key sanitization	iTC mandated
self-encrypting drive	iTC mandated
self encrypting drive	iTC mandated
sed	iTC mandated
opal	iTC mandated
enterprise ssc	iTC synonym
tcg ssc	iTC synonym

The evaluation team conducted penetration testing, based on the potential vulnerabilities identified in the general full-drive encryption technologies.   The testing did not exploit any vulnerability.

8 Evaluated Configuration

Detail regarding the evaluated configuration is provided in Section 3.2 above.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary Detailed Test Report (DTR) and Evaluation Technical Report (ETR). The reader of this document can assume that all assurance activities and work units received a passing verdict.

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 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Seagate Secure TCG SSC Self-Encrypting Drives TOE to be Part 2 extended, and to meet the SARs contained in the CPPFDE_EE20e. Additionally, the evaluation team performed the Assurance Activities specified in the CPPFDE_EE20e.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Seagate Secure TCG SSC Self-Encrypting Drive products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally, the evaluation team performed the assurance activities specified in the CPPFDE_EE20e related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the CPPFDE_EE20e and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

Please see Section 7.3 for details on the vulnerability analysis performed by the evaluation team.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. 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 validator comments are covered in Section 5, Assumptions and Clarification of Scope.

11 Annexes

Not applicable.

12 Security Target

Table 5 Security Target Identification

Name	Description
ST Title	Seagate Secure TCG SSC Self-Encrypting Drives Security Target Security Target
ST Version	V 1.0
Publication Date	November 9, 2021

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 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements*, Version 3.1 Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components,* Version 3.1 Revision 5, April 2017.

[4] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology,* Version 3.1, Revision 5, April 2017.

[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, November 9, 2021

[7] *Seagate Secure TCG SSC Self-Encrypting Drives Common Criteria Assurance Activity Report,* Version 1.0, November 14, 2021

[8] *Seagate Secure TCG SSC Self-Encrypting Drives Common Criteria Test Report and Procedures,* Version 1.0, November 12, 2021

[9] *Evaluation Technical Report for Seagate Secure® TCG SSC Self-Encrypting Drives,* Version 1.0, November 12, 2021 (Proprietary)

[10] *Collaborative Protection Profile for Full Drive Encryption - Encryption Engine,* Version 2.0 + Errata 20190201, February 1, 2019

[11] *Supporting Document, Mandatory Technical Document – Full Drive Encryption: Encryption Engine,* Version 2.0 + Errata 20190201, February 1, 2019

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