Seagate Secure®
TCG SSC Self-Encrypting Drives
Assurance Activity Report

Version 1.0

November 14, 2021

Prepared by:

Leidos Inc.

https://www.leidos.com/CC-FIPS140
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

Prepared for:

National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:

Seagate Technology, LLC

389 Disc Drive
Longmont, CO 80503

The TOE Evaluation was Sponsored by:

Seagate Technology, LLC

389 Disc Drive

Longmont, CO 80503

Evaluation Personnel:

Greg Beaver

Furukh Siddique

Common Criteria Versions

- *Common Criteria for Information Technology Security Evaluation Part 1: Introduction,* Version 3.1, Revision 5, April 2017
- *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components,* Revision 5, April 2017
- *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components,* Revision 5, April 2017

Common Evaluation Methodology Versions

- *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology,* Version 3.1, Revision 5, April 2017

Protection Profiles

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

Table of Contents

1 INTRODUCTION

This document presents assurance activity evaluation results of the Seagate Technology Seagate Secure TCG SSC Self-Encrypting Drives evaluation. There are three types of assurance activities and the following is provided for each:

1. TOE Summary Specification (TSS)—an indication that the required information is in the TSS section of the Security Target
2. Guidance—a specific reference to the location in the guidance is provided for the required information
3. Test—a summary of the test procedure and result is provided for each required test activity.

This Assurance Activities Report contains sections for each functional class and family and sub-sections addressing each of the SFRs specified in the Security Target.

1.1 Evidence

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

[KMD] *Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive and TCG Opal SSC Self-Encrypting Drive Common Criteria Full Drive Encryption – Encryption Engine Key Management Description,* Version 0.3, Dated: November 11, 2021 (Seagate Proprietary)

[ST] *Seagate Secure® TCG SSC Self-Encrypting Drives Security Target,* Version 1.0, November 9, 2021 (Non-Proprietary)

1.2 Protection Profile

[CPP FDE EE] *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201,* February 1, 2019, [CPPFDE_EE]

[CPP FDE EE SD] *Supporting Document, Mandatory Technical Document – Full Drive Encryption: Encryption Engine+ Errata 20190201,* February 1, 2019

1.3 TCG Storage and ATA Security Specifications

[ATA-8 ACS2] Information technology - ATA/ATAPI Command Set - 2 (ACS-2), INCITS 482-2012, May 30, 2012[1]

[TCG Core] *TCG Storage Architecture Core Specification,* Specification Version 2.00, Revision 2.00, November 4, 2011

[TCG Ent] *TCG Storage Security Subsystem Class: Enterprise,* Specification Version 1.00 Final, Revision 3.00, January 10, 2011

[1] The evaluation team relied upon public draft: Information technology - ATA/ATAPI Command Set - 2 (ACS-2), Working Draft Project American National Standard, Revision 7, June 22, 2011

[TCG Opal] *TCG Storage Security Subsystem Class: Opal*, Specification Version 2.00, Revision 1.00, February 24, 2012

[TCG SIIS] *TCG Storage Interface Interactions Specification*, Specification Version 1.0, January 27, 2009

[TCG SUDR] TCG Storage Opal SSC Feature Set: Single User Mode, Specification Version 1.00, Revision 1.00, February 24, 2012

1.4 Evaluation Reports

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

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

[VS] *Seagate Secure TCG SSC Self-Encrypting Drives Vulnerability Survey*, Version 1.0, November 11, 2021

1.5 NIAP Technical Decisions

The following NIAP Technical Decisions were considered during the evaluation and are either satisfied or not applicable as indicated.

- **TD0464:** FIT Technical Decision for FPT_PWR_EXT.1 compliant power saving states
  The Technical Decision is applicable to the evaluation. The ST contains FPT_PWR_EXT.1.
- **TD0460:** FIT Technical Decision for FPT_PWR_EXT.1 non-compliant power saving states
  The Technical Decision is applicable to the evaluation. The ST contains FPT_PWR_EXT.1.
- **TD0458:** FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities
  The Technical Decision is applicable to the evaluation. The ST contains FPT_KYP_EXT.1.

2 Security Functional Requirement Assurance Activities

2.1 Cryptographic Support (FCS)

2.1.1 FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)

FCS_CKM.1(b) is a selection-based requirement.

2.1.1.1 Application Notes

The symmetric key generation function may be used to generate keys along the key chain or a DEK. It may also be used to provide inputs for key combining, key encryption, or key wrapping. Therefore, the

ST author should select FCS_CKM.1(b), if Symmetric key generation is used. FCS_CKM.4(b) Cryptographic Key Destruction (TOE-Controlled Hardware).

2.1.1.2 TSS Assurance Activities

The evaluator shall review the TSS to determine that a symmetric key is supported by the product, that the TSS includes a description of the protection provided by the product for this key.

[ST] section 6.1 "Overview of TOE Operations" summarizes how Seagate self-encrypting drives (SEDs) encrypt all user data. In particular, "Seagate SEDs support subdividing user storage. The storage ranges are called bands. Each band is secured with its own authentication key and media encryption key Section 6.1 and section 6.2.5 "Key Chaining (Recipient) (FCS_KYC_EXT.2)" summarize key chain protections (search for "Each Band has its own key chain" and "maintaining a chain of intermediary keys originating from the BEV to the DEK" respectively). Table 1 lists the keys that make up a band's key chain.

Table 1 Per-band Key Chain

ST Key Name(s)	PP Key Name	Purpose
Media Encryption Key (MEK)	Data Encryption Key (DEK)	Encrypt/decrypt user data on disk
Intermediate keys	Intermediate keys	Validate Authentication Key, protect MEK for per-user access, and support Instant Secure Erase (ISE) function
Authentication Key Drive Lock PIN TCG PIN	Border Encryption Value (BEV)	User authorization factor used to derive initial intermediate key

[ST] section 6.2.1 "Cryptographic Key Generation (FCS_CKM.1(b), FCS_CKM.1(c))" identifies symmetric keys used for data encryption and key validation (search for "The TOE generates symmetric cryptographic keys using a Random Bit Generator"). These keys are the per-band MEK (for AES-XTS) and intermediate keys.

Section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" covers the lifetime of plain text keys including their destruction.

The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE.

[ST] section 6.2.1 "Cryptographic Key Generation (FCS_CKM.1(b), FCS_CKM.1(c))" states the size of an MEK is 512 bits (for AES-XTS-256) and the size of all other symmetric keys (that is, intermediate keys) is 256 bits.

2.1.1.3 Guidance Assurance Activities

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key size(s) for all uses specified by the AGD documentation and defined in

this cPP.

[Guide] section “Cryptographic Symmetric Key Sizes and Key Generation” states, “The size of the AES keys is not configurable.”

2.1.1.4 KMD Assurance Activities

If the TOE uses a symmetric key as part of the key chain, the KMD should detail how the symmetric key is used as part of the key chain.

[KMD] describes the generation and use of intermediate keys and MEK keys.

2.1.1.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.2 FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key)

FCS_CKM.1(c) is an unconditional requirement.

2.1.2.1 Application Notes

This SFR is iterated because additional iterations are defined as optional requirements in Appendix A. Iteration (c) was chosen specifically to ensure consistency between the FDE cPPs.

The purpose of this requirement is to explain DEK generation during provisioning.

If the TOE can be configured to obtain a DEK through more than one method, the ST author chooses the applicable options within the selection. For example, the TOE may generate random numbers with an approved RBG to create a DEK, as well as provide an interface to accept a DEK from the environment.

If the ST author chooses the first and/or third option in the selection, the corresponding requirement is pulled from Appendix A and included in the body of the ST.

2.1.2.2 TSS Assurance Activities

The evaluator shall examine the TSS to determine that it describes how the TOE obtains a DEK (either generating the DEK or receiving from the environment).

[ST] section 6.2.1 “Cryptographic Key Generation (FCS_CKM.1(b), FCS_CKM.1(c))” states “The TOE generates symmetric cryptographic keys using a Random Bit Generator (Hash_DRBG (any))”. Section 6.2.1 covers the Media Encryption Key for each band, which are the AES-XTS DEKs used by the TOE.

If the TOE generates a DEK, the evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked. If the DEK is generated outside of the TOE, the evaluator checks to ensure that for each platform identified in the TOE Description, the TSS describes the interface used by the TOE to invoke this functionality. The evaluator uses the description of the interface between the RBG and the TOE to determine that it requests a key greater

than or equal to the required key sizes.

[ST] section 6.2.1 “Cryptographic Key Generation (FCS_CKM.1(b), FCS_CKM.1(c))” states the TOE invokes the drive’s Hash_DRBG(any) random bit generator to obtain 512 bits for AES-XTS-256 keys.

If the TOE received the DEK from outside the host platform, then the evaluator shall examine the TSS to determine that the DEK is sent wrapped using the appropriate encryption algorithm.

The TOE generates all DEKs. Thus, this assurance activity is not applicable.

2.1.2.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR

2.1.2.4 KMD Assurance Activities

If the TOE received the DEK from outside the host platform, then the evaluator shall verify that the KMD describes how the TOE unwraps the DEK.

The TOE generates all DEKs. Thus, this assurance activity is not applicable.

2.1.2.5 Test Assurance Activities

The evaluator shall perform the following tests:

Test 1: *The evaluator shall configure the TOE to ensure the functionality of all selections.*

The evaluator queried the DRBG for random 256 bit data three times. The evaluator confirmed that each output was 256 bits and unique.

2.1.3 FCS_CKM.4(a) Cryptographic Key Destruction (Power Management)

FCS_CKM.4(a) is an unconditional requirement.

2.1.3.1 Application Notes

In some cases, erasure of keys from volatile memory is only supported by the Operational Environment, in which case the Operational Environment must expose a well-documented mechanism or interface to invoke the memory clearing operation.

Self-encrypting drives do not store keys in the Operational Environment and cannot instruct the Operational Environment to perform functionality so they are not expected to select “instruct the Operational Environment to clear”.

2.1.3.2 TSS Assurance Activities

The evaluator shall verify the TSS provides a high level description of how keys stored in volatile memory are destroyed. The evaluator to verify that TSS outlines:

- *if and when the TSF or the Operational Environment is used to destroy keys from volatile memory;*

[ST] FCS_CKM.4(a) selects option "erase" and so this assurance activity is not applicable.

The evaluator to verify that TSS outlines:
- *if and how memory locations for (temporary) keys are tracked;*

[ST] section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" identifies The TOE destroys all key material, BEV, and authentication factors stored in plaintext when transitioning to a Compliant power saving state. The TOE supports device full off and D3. When power is removed from the drive, the device goes off and keys are removed. (FCS_CKM_EXT.4(b)).

This behavior is consistent with FCS_CKM.4(b) (see section 2.1.4 below), which is one of the options selected in FCS_CKM_EXT.6 (see section 2.1.9 below). Section 6.2.2 describes temporary storage of keys (search for "volatile memory in DRAM on the stack").

The evaluator to verify that TSS outlines:
- *details of the interface used for key erasure when relying on the OE for memory clearing.*

[ST] FCS_CKM.4(a) selects option "erase" and so this assurance activity is not applicable.

2.1.3.3 Guidance Assurance Activities

The evaluator shall check the guidance documentation if the TOE depends on the Operational Environment for memory clearing and how that is achieved.

[ST] FCS_CKM.4(a) selects option "erase" and so this assurance activity is not applicable.

2.1.3.4 KMD Assurance Activities

The evaluator shall check to ensure the KMD lists each type of key, its origin, possible memory locations in volatile memory.

[KMD] section 2 is "Keys and Key Hierarchy." Section 2 describes the Authentication Key, intermediate keys, and MEK that make up the key hierarchy for each band. The proprietary version of this AAR summarizes the type of each key, its origins, and possible locations in volatile memory as well as identifying [KMD] sections containing this information.

2.1.3.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.4 FCS_CKM.4(b) Cryptographic Key Destruction (TOE-Controlled Hardware)

FCS_CKM.4(b) is a selection-based requirement.

2.1.4.1 Application Notes

In the first selection, the ST Author is presented options for destroying a key based on the memory or storage technology where keys are stored within the TOE.

If non-volatile memory is used to store keys, the ST Author selects whether the memory storage algorithm uses wear-leveling or not. Storage technologies or memory types that use wear-leveling are not required to perform a read verify. The selection for destruction includes block erase as an option, and this option applies only to flash memory. A block erase does not require a read verify, since the mappings of logical addresses to the erased memory locations are erased as well as the data itself.

Within the selections is the option to overwrite a disused key with a new value of a key. The intent is that a new value of a key (as specified in another SFR within the PP) can be used to "replace" an existing key.

If a selection for read verify is chosen, it should generate an audit record upon failures.

Several selections allow assignment of a 'value that does not contain any CSP'. This means that the TOE uses some other specified data not drawn from an RBG meeting FCS_RBG_EXT requirements, and not being any of the particular values listed as other selection options. The point of the phrase 'does not contain any CSP' is to ensure that the overwritten data is carefully selected, and not taken from a general 'pool' that might contain current or residual data that itself requires confidentiality protection.

Key destruction does not apply to the public component of asymmetric key pairs.

2.1.4.2 TSS Assurance Activities

Key Management Description may be used if necessary details describe proprietary information

The evaluator examines the TSS to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how they are overwritten.

[ST] section 6.1 "Overview of TOE Operations" and section 6.2.5 "Key Chaining (Recipient) (FCS_KYC_EXT.2)" summarize key chain protections (search for "Each Band has its own key chain" and "maintaining a chain of intermediary keys originating from the BEV to the DEK" respectively). The sections describe how each key is introduced into volatile memory, as summarized in Table 2 below.

Table 2 Per-band Key Storage in Volatile Memory

ST Key Name(s)	Introduction
MEK	Decrypt using intermediate key
Intermediate keys	Derived from Authentication Key, loaded from non-volatile memory, decrypted using intermediate key
Authentication Key	Transferred from Authorization Acquisition

[KMD] describes Seagate SED functions that use a drive's key chains. [ST] section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" states "When the SED generates a new key to erase a band, the existing key is overwritten with a new value of a key" and "The keys are removed immediately after they are used or when they are no longer needed, using a single overwrite of zeroes."

The evaluator shall check to ensure the TSS lists each type of key that is stored, and identifies the memory type where key material is stored. When listing the type of memory employed, the TSS will list each type of memory selected in the FCS_CKM.4.1 SFR, as well as any memory types that employ a different memory controller or storage algorithm. For example, if a TOE uses NOR flash and NAND flash, both types are to be listed.

[ST] FCS_CKM.4(b) applies to volatile memory only. Table 2 Per-band Key Storage in Volatile Memory summarizes the keys stored in volatile memory. [ST] section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" describes the types of volatile memory along with type of memory controller used to access volatile memory (search for "The TOE contains two types of volatile memory").

The evaluator shall examine the TSS to ensure it describes the method that is used by the memory controller to write and read memory from each type of memory listed. The purpose here is to provide a description of how the memory controller works so one can determine exactly how keys are written to memory. The description would include how the data is written to and read from memory (e.g., block level, cell level), mechanisms for copies of the key that could potentially exist (e.g., a copy with parity bits, a copy without parity bits, any mechanisms that are used for redundancy).

[ST] FCS_CKM.4(b) applies to volatile memory only. [ST] section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" describes memory controller access to volatile memory (search for "volatile memory is accessed using standard micro-controller memory interface controllers and addressing schemes").

The evaluator shall examine the TSS to ensure it describes the destruction procedure for each key that has been identified. If different types of memory are used to store the key(s), the evaluator shall check to ensure that the TSS identifies the destruction procedure for each memory type where keys are stored (e.g., key X stored in flash memory is destroyed by overwriting once with zeros, key X' stored in EEPROM is destroyed by a overwrite consisting of a pseudo random pattern – the EEPROM used in the TOE uses a wear-leveling scheme as described).

[ST] FCS_CKM.4(b) applies to volatile memory only. [ST] Section 6.2.2 summarizes volatile memory key destruction during drive operation as described below:

"For the volatile memory scenario, a SED will destroy keys when power is removed, the drive is locked, or the SED generates a new key to erase a band. The TOE contains two types of volatile memory: static RAM and dynamic RAM. In both cases the volatile memory is accessed using standard micro-controller memory interface controllers and addressing schemes. The volatile memory is 8, 16 or 32 bit

addressable. There is no built in redundancy for volatile memory in the TOE. When the SEDs are powered off: all keys are destroyed. When the device is Locked all keys are overwritten with zeros. When the SED generates a new key to erase a band, the existing key is overwritten with a new value of a key. Unlocked band keys are stored in plaintext form for use by the FDE engine as needed. All other plaintext keys are temporarily stored in volatile memory in DRAM on the stack for a short time after being generated and during the operations "Take Ownership Function" and "Verify PIN Function". The keys are removed immediately after they are used or when they are no longer needed, using a single overwrite of zeroes."

Please see section 2.1.3 above for key destruction by removal of power to memory.

If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify that the pattern does not contain any CSPs.

[ST] FCS_CKM.4(b) does not make use of the open assignment for fill value. This assurance activity does not apply.

The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.

The evaluator checked [ST] section 6 "TOE Summary Specification." The evaluator found no configurations or circumstances that did not conform strictly to key destruction requirement FCS_CKM.4(b).

Upon completion of the TSS examination, the evaluator understands how all the keys (and potential copies) are destroyed.

See findings in section 2.1.4.2 TSS Assurance Activities.

2.1.4.3 Guidance Assurance Activities

There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information. The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.

For example, when the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-leveling and garbage collection. This may create additional copies of the key that are logically inaccessible but persist physically. In this case, it is assumed the drive supports the TRIM command and implements garbage collection to destroy these persistent copies when not actively engaged in other tasks.

FCS_CKM.4.1(b) only applies to volatile memory based on the selections in [ST]. Overwriting volatile memory immediately destroys a key.

Drive vendors implement garbage collection in a variety of different ways, as such there is a variable amount of time until data is truly removed from these solutions. There is a risk that data may persist for a longer amount of time if it is contained in a block with other data not ready for erasure. It is assumed the operating system and file system of the OE support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion.

As described above, overwriting volatile memory immediately destroys a key.

It is assumed that if a RAID array is being used, only set-ups that support TRIM are utilized. It is assumed if the drive is connected via PCI-Express, the operating system supports TRIM over that channel. It is assumed the drive is healthy and contains minimal corrupted data and will be end of life before a significant amount of damage to drive health occurs, it is assumed there is a risk small amounts of potentially recoverable data may remain in damaged areas of the drive.

Each Seagate device is a single drive. Hence, this assurance activity is not applicable.

Finally, it is assumed the keys are not stored using a method that would be inaccessible to TRIM, such as being contained in a file less than 982 bytes which would be completely contained in the master file table.

As described above, overwriting volatile memory immediately destroys a key.

For destruction on wear-leveled memory, if a time period is required before is processed destruction the ST author shall provide an estimated range.

[ST] Section 6.2.2 states that for the volatile memory scenario, a SED will destroy keys when the following occurs:

- when power is removed
- the drive is locked, or
- the SED generates a new key to erase a band.

When the SEDs are powered off: all keys are destroyed. When the device is Locked all keys are overwritten with zeros. When the SED generates a new key to erase a band, the existing key is overwritten with a new value of a key.

Unlocked band keys are stored in plaintext form for use by the FDE engine as needed. All other plaintext keys are temporarily stored in volatile memory in DRAM on the stack for a short time after being generated and during the operations (Take Ownership Function, Verify PIN Function).

The keys are removed immediately after they are used or when they are no longer needed, using a single overwrite of zeroes.

2.1.4.4 KMD Assurance Activities

See security target assurance activities above.

The evaluator checked [KMD], which confirms the [ST] information cited above.

2.1.4.5 Test Assurance Activities

There is no test evaluation activity for this SFR.

For these tests the evaluator shall utilize appropriate development environment (e.g. a Virtual Machine) and development tools (debuggers, simulators, etc.) to test that keys are cleared, including all copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

For destruction on wear-leveled memory, if a time period is required before is evaluator shall wait that amount of time after clearing the key in tests 2 and 3.

***Test 1:** Applied to each key held as plaintext in volatile memory and subject to destruction by overwrite by the TOE (whether or not the plaintext value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator shall:*

1. *Record the value of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Cause the TOE to stop the execution but not exit.*
5. *Cause the TOE to dump the entire memory of the TOE into a binary file.*
6. *Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.*
7. *Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece.*

Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.

Step 7 ensures that partial key fragments do not remain in memory. If a fragment is found, there is a miniscule chance that it is not within the context of a key (e.g., some random bits that happen to match). If this is the case the test should be repeated with a different key in Step #1. If a fragment is found the test fails.

This test has been performed in conjunction with FCS_CKM.4(c).

***Test 2:** Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:*

1. *Record the value of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Search the non-volatile memory the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.*
5. *Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece. If a fragment is found then the test is repeated (as described for test 1 above), and if a*

fragment is found in the repeated test then the test fails.

This test has been performed in conjunction with FCS_CKM.4(c).

Test 3: *Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:*

1. *Record the storage location of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Read the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.*

The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.

This test has been performed in conjunction with FCS_CKM.4(c).

2.1.5 FCS_CKM.4(c) Cryptographic Key Destruction (General Hardware)

FCS_CKM.4(c) is a selection-based requirement. [ST] iterates FCS_CKM.4(c) as FCS_CKM.4(1)(c) HDD and FCS_CKM.4(2)(c) SDD and Hybrid. This section covers both iterations of the requirement.

2.1.5.1 Application Notes

In the first selection, the ST Author is presented options for destroying disused cryptographic keys based on whether they are in volatile memory or non-volatile storage within the TOE. The selection of block erase for non-volatile storage applies only to flash memory. A block erase does not require a read-verify, since the reference to the memory location is erased as well as the data itself.

Within the selections is the option to overwrite the memory location with a new value of a key. The intent is that a new value of a key (as specified in another SFR within the PP) can be used to "replace" an existing key.

Several selections allow assignment of a 'value that does not contain any CSP'. This means that the TOE uses some other specified data not drawn from an RBG meeting FCS_RBG_EXT requirements, and not being any of the particular values listed as other selection options. The point of the phrase 'does not contain any CSP' is to ensure that the overwritten data is carefully selected, and not taken from a general 'pool' that might contain current or residual data that itself requires confidentiality protection.

Key destruction does not apply to the public component of asymmetric key pairs.

2.1.5.2 TSS Assurance Activities

Key Management Description may be used if necessary details describe proprietary information

The evaluator examines the TSS to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how

they are overwritten.

[ST] FCS_CKM.4(c)(1) and FCS_CKM.4(c)(2) apply to non-volatile memory only. Please see section 2.1.4 above for volatile memory key destruction.

The evaluator shall check to ensure the TSS lists each type of key that is stored, and identifies the memory type (volatile or non-volatile) where key material is stored.

Table 1 Per-band Key Chain in section 2.1.1 above lists keys used by Seagate SEDs. Please see section 2.1.4 above for volatile memory key storage. [ST] section 6.1 "Overview of TOE Operations" indicates a Seagate SED never stores an Authentication Key in non-volatile memory (search for "PIN values are never stored directly on the SED.") [ST] section 6.1 "Overview of TOE Operations" and section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" indicate each initial intermediate key is derived not stored in non-volatile memory (search for "The drive lock PIN is used as an input to the PBKDF function to generate an intermediate key" and "All keys and key material are stored in the system area on the media", respectively).

The TSS identifies and describes the interface(s) that is used to service commands to read/write memory. The evaluator examines the interface description for each different media type to ensure that the interface supports the selection(s) made by the ST Author.

[ST] section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" describes key destruction for the three types of TOE devices: hard-disk drive (HDD), solid-state drive (SDD), and hybrid devices.

For HDD devices, the device stores keys in the system area of drive media (search for "For the non-volatile memory key destruction on HDD scenario"). An HDD device invokes the HDD sequence to write data blocks to drive media (search for "If the TOE commands the HDD sequencer"). Block writes support writing new key values as specified in FCS_CKM.4(c)(1).

For SDD and hybrid devices, the device stores keys in the system data, which is NOR and NAND flash (search for "For the non-volatile memory key destruction on solid state flash drives and hybrid drives scenario"). A SDD or hybrid device invokes a serial flash controller. For both types of flash memory, an SDD/hybrid device overwrites a key with a new key value. For NOR flash, the device performs a block erase before the write. For NAND flash, the flash system performs erase or wear leveling as necessary.

If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify that the pattern does not contain any CSPs.

[ST] FCS_CKM.4(c)(1) and FCS_CKM.4(c)(2) do not make use of the open assignment for fill value. This assurance activity does not apply.

The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.

The evaluator checked [ST] section 6 “TOE Summary Specification.” The evaluator found no configurations or circumstances that did not conform strictly to key destruction requirements FCS_CKM.4(c)(1) and FCS_CKM.4(c)(2).

2.1.5.3 Guidance Assurance Activities

There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information. The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.

For example, when the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-leveling and garbage collection. This may create additional copies of the key that are logically inaccessible but persist physically. In this case, it is assumed the drive supports the TRIM command and implements garbage collection to destroy these persistent copies when not actively engaged in other tasks.

FCS_CKM.4.1(c)(1) and FCS_CKM.4.1(c)(2) only apply to non-volatile memory based on the selections in [ST].

[Guide] section “Cryptographic Key Destruction” describes wear leveling implemented in Seagate TCG Enterprise SSD and TCG Opal Hybrid HDD SED drives implement a NAND flash wear-leveling algorithm. A side effect of this algorithm is that when a key value is over written in the NAND system area the original block is unmapped. At this point, the old key value is logically inaccessible but does persist physically in the unmapped block. The wear levelling algorithm will eventually recycle and remap the original block. During this process, the contents of the original block will be erased to 0xFF and the original block will be mapped to a different logical address.

In addition to the wear leveling algorithm Seagate SSD and Hybrid HDD drives also support a read/write encoding scheme such that a read to a unmapped physical block produces random results. With this method, the old key material is unavailable immediately after the block is unmapped.

Drive vendors implement garbage collection in a variety of different ways, as such there is a variable amount of time until data is truly removed from these solutions. There is a risk that data may persist for a longer amount of time if it is contained in a block with other data not ready for erasure. It is assumed the operating system and file system of the OE support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion.

As described above, key destruction is effectively immediate on Seagate solid-state and hybrid devices. Key destruction (overwriting) is immediate on hard-disk devices.

It is assumed that if a RAID array is being used, only set-ups that support TRIM are utilized. It is assumed if the drive is connected via PCI-Express, the operating system supports TRIM over that channel. It is assumed the drive is healthy and contains minimal corrupted data and will be end of life before a significant amount of damage to drive health occurs, it is assumed there is a risk small amounts of potentially recoverable data may remain in damaged areas of the drive.

Each Seagate device is a single drive. Hence, this assurance activity is not applicable.

Finally, it is assumed the keys are not stored using a method that would be inaccessible to TRIM, such as being contained in a file less than 982 bytes which would be completely contained in the master file table.

As described above, key destruction is effectively immediate on Seagate solid-state and hybrid devices. Key destruction (overwriting) is immediate on hard-disk devices.

2.1.5.4 KMD Assurance Activities

See security target assurance activities above.

The evaluator checked [KMD], which confirms the [ST] information cited above.

2.1.5.5 Test Assurance Activities

For these tests the evaluator shall utilize appropriate development environment (e.g. a Virtual Machine) and development tools (debuggers, simulators, etc.) to test that keys are cleared, including all copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

***Test 1:** Applied to each key held as plaintext in volatile memory and subject to destruction by overwrite by the TOE (whether or not the plaintext value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator shall:*

1. *Record the value of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Cause the TOE to stop the execution but not exit.*
5. *Cause the TOE to dump the entire memory of the TOE into a binary file.*
6. *Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.*
7. *Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece.*
8. *Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.*

Step 7 ensures that partial key fragments do not remain in memory. If a fragment is found, there is a miniscule chance that it is not within the context of a key (e.g., some random bits that happen to match). If this is the case the test should be repeated with a different key in Step #1. If a fragment is found the test fails.

Combined with Test 3.

Test 2: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary,

to view the key storage location:

1. *Record the value of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Search the non-volatile memory the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.*
5. *Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece. If a fragment is found then the test is repeated (as described for test 1 above), and if a fragment is found in the repeated test then the test fails.*

Combined with Test 3

Test 3: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

1. *Record the storage location of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Search the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.*

The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.

Tests 1-3 above have been combined in a test suite in which the evaluator performed all tests in conjunction. The test suite comprised of 17 tests; designed to test three main components: key (PIN, intermediate keys, MEK LOCK/UNLOCK, MEK ERASE BAND, AUTHENTICATE PASSWORD, and ERASE UNIT), type of memory (Volatile and Non-Volatile), and Standard (TCG and ATA). Each test recorded the value of the key material, destroyed the key, and verified the key was destroyed by searching memory that no traces of the key remained. For the situation where the key was not stored in plaintext the evaluator recorded the value of the key, confirmed that a search for the key returned the key not found, destroyed the key, confirmed that a search for the key still yielded it not being found then finally performing a binary compare of memory both before and after the key destruction to confirm no data segments of memory remained the same.

2.1.6 FCS_CKM.4(e) Cryptographic Key Destruction (Key Cryptographic Erase)

FCS_CKM.4(e) is an optional requirement.

2.1.6.1 Application Notes

A key can be considered destroyed by destroying the key that protects the key. If a key is wrapped or encrypted it is not necessary to “overwrite” that key, overwriting the key that is used to wrap or encrypt the key used to encrypt/decrypt data, using the appropriate method for the memory type involved, will suffice. For example, if a product uses a Key Encryption Key (KEK) to encrypt a Data Encryption Key (DEK), destroying the KEK using one of the methods in FCS_CKM.EXT.6.1 is sufficient, since the DEK would no longer be usable (of course, presumes the DEK is still encrypted.

2.1.6.2 TSS Assurance Activities

There is no TSS evaluation activity for this SFR.

2.1.6.3 Guidance Assurance Activities

There are no AGD evaluation activity for this SFR.

2.1.6.4 KMD Assurance Activities

The evaluator shall examine the TOE's keychain in the TSS/KMD and identify each instance a key is destroyed by this method. In each instance the evaluator shall verify all keys capable of decrypting the target key are destroyed in accordance with a specified key destruction method.

[KMD] identifies the Seagate SED functions that use cryptographic erase. In each function, the Seagate SED destroys all the keys capable of decrypting the target key.

2.1.6.5 Test Assurance Activities

There is no test evaluation activity for this SFR.

2.1.7 FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)

FCS_CKM_EXT.4(a) is an unconditional requirement.

2.1.7.1 Application Notes

Keys, including intermediate keys and key material that are no longer needed are destroyed by using an approved method, FCS_CKM_EXT.6. Examples of keys are intermediate keys, submasks, and BEV. There may be instances where keys or key material that are contained in persistent storage are no longer needed and require destruction. Based on their implementation, vendors will explain when certain keys are no longer needed. There are multiple situations in which key material is no longer necessary, for example, a wrapped key may need to be destroyed when a password is changed. However, there are instances when keys are allowed to remain in memory, for example, a device identification key.

2.1.7.2 TSS Assurance Activities

The evaluator shall verify the TSS provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.

[ST] section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" states "The keys are removed immediately after they are used or when they are no longer needed". Section 6.2.2 explains "Unlocked band keys are stored in

plaintext form for use by the FDE engine as needed." However, Seagate SED destroys a MEK in volatile memory when the drive locks the band (search for "When the device is Locked").

2.1.7.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.1.7.4 KMD Assurance Activities

The evaluator shall verify the KMD includes a description of the areas where keys and key material reside and ...

Please see sections 2.1.4 and 2.1.5 above for a summary of keys in volatile and non-volatile memory. [KMD] includes additional detail regarding key material.

The evaluator shall verify the KMD includes a description of ... and when the keys and key material are no longer needed.

Please see sections 2.1.4 and 2.1.5 above for a summary of keys in volatile and non-volatile memory. [KMD] includes additional detail regarding key material.

The evaluator shall verify the KMD includes a key lifecycle, that includes

1. *a description where key material reside,*
2. *how the key material is used,*
3. *how it is determined that keys and key material are no longer needed, and*
4. *how the material is destroyed once it is not needed*

and that the documentation in the KMD follows FCS_CKM.4(a) for the destruction.

[KMD] describes Seagate SED functions that use a drive's key chains.

Each function description in [KMD] provides a detailed description of how the function uses each key and associated key material.

2.1.7.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.8 FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)

FCS_CKM_EXT.4(b) is an unconditional requirement.

2.1.8.1 Application Notes

The TOE may end up in a non-Compliant power saving state indistinguishable from a Compliant power state (e.g. as result of sudden and/or unexpected power loss). Guidance documentation must state what

conditions may result in clear text keys or key materials to stay in volatile memory and identify mitigation measures that result in clearing of volatile memory.

2.1.8.2 TSS Assurance Activities

The evaluator shall verify the TSS provides a description of what keys and key material are destroyed when entering any Compliant power saving state.

[ST] section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" identifies device full off (D3) as the only compliant power saving state. Section 6.2.2 claims the TOE destroys all key material, BEV, and authentication factors stored in plaintext when transitioning to a compliant power saving state (search for "When power is removed from the drive, the device goes off and keys are removed.").

2.1.8.3 Guidance Assurance Activities

The evaluator shall validate that guidance documentation contains clear warnings and information on conditions in which the TOE may end up in a non-Compliant power saving state indistinguishable from a Compliant power saving state.

[Guide] section "Cryptographic Key and Key Material Destruction (Power Management)" states "It is not possible for a Seagate Self Encrypting Drive to end up in a non-compliant power saving state."

In that case it must contain mitigation instructions on what to do in such scenarios.

Seagate SEDs support only one power-saving state. Hence, this assurance activity is not applicable.

2.1.8.4 KMD Assurance Activities

The evaluator shall verify the KMD includes a description of the areas where keys and key material reside.

This assurance activity duplicates a KMD assurance activity in section 2.1.7 above. Please see the results in that section.

The evaluator shall verify the KMD includes a key lifecycle that includes0

1. *a description where key material reside,*
2. *how the key material is used,*
3. *and how the material is destroyed once it is not needed*

and that the documentation in the KMD follows FCS_CKM.4(b) for the destruction.

This assurance activity duplicates a KDM assurance activity in section 2.1.7 above. Please see the results in that section.

2.1.8.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.9 FCS_CKM_EXT.6 Cryptographic Key Destruction Types

FCS_CKM_EXT.6 is an unconditional requirement.

2.1.9.1 Application Notes

If multiple selections are made, the TSS shall identify which keys are destroyed according to which selections.

2.1.9.2 TSS Assurance Activities

Key Management Description may be used if necessary details describe proprietary information)

The evaluator shall examine the TOE's keychain in the TSS/KMD and verify all keys subject to destruction are destroyed according to one of the specified methods.

Please see sections 2.1.4 and 2.1.5 above.

2.1.9.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.1.9.4 KMD Assurance Activities

See security target assurance activities above.

The evaluator checked [KMD], which confirms the [ST] information cited above.

2.1.9.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.10 FCS_COP.1(a) Cryptographic Operation (Signature Verification)

FCS_COP.1(a) is a selection-based requirement.

2.1.10.1 Application Notes

The selection should be consistent with the overall strength of the algorithm used for FCS_COP.1(a) and quantum resistant recommendations. For example, SHA-256 should be chosen for 2048-bit RSA or ECC with P-256, SHA-384 should be chosen for 3072-bit RSA, 4096-bit RSA, or ECC with P-384, and SHA-512 should be chosen for ECC with P-521. The selection of the standard is made based on the algorithms selected.

2.1.10.2 TSS Assurance Activities

The evaluator shall check the TSS to ensure that it describes the overall flow of the signature verification. This should at least include

1. *identification of the format and general location (e.g., "firmware on the hard drive device" rather than "memory location 0x00007A4B") of the data to be used in verifying the digital signature;*
2. *how the data received from the operational environment are brought on to the device; and*
3. *any processing that is performed that is not part of the digital signature algorithm (for instance, checking of certificate revocation lists).*

[ST] section 6.2.3 "Cryptographic Operation (FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(f))" describes signature verification (search for "The TOE supports both secure FW download and a secure boot procedure.") Seagate SEDs verify RSA signatures for firmware download and secure boot. A drive stores the Seagate RSA public key in ROM. For secure firmware download, the TOE receives a signed firmware update package from the host and stores it in DRAM. For the secure boot process, the TOE loads the firmware from flash into DRAM using routines in ROM. The description covers behavior when signature verification fails.

2.1.10.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.1.10.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.1.10.5 Test Assurance Activities

Each section below contains the tests the evaluators must perform for each type of digital signature scheme. Based on the assignments and selections in the requirement, the evaluators choose the specific activities that correspond to those selections.

It should be noted that for the schemes given below, there are no key generation/domain parameter generation testing requirements. This is because it is not anticipated that this functionality would be needed in the end device, since the functionality is limited to checking digital signatures in delivered updates. This means that the domain parameters should have already been generated and encapsulated in the hard drive firmware or on-board non-volatile storage. If key generation/domain parameter generation is required, the evaluation and validation scheme must be consulted to ensure the correct specification of the required evaluation activities and any additional components.

The following tests are conditional based upon the selections made within the SFR.

The following tests may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

Seagate Secure TCG SSC Self-Encrypting Drives use algorithm implementations validated under the CAVP (http://csrc.nist.gov/groups/STM/cavp/index.html). NIAP Policy Letter #5 defines the

applicability and relationship of NIST CAVP and CMVP testing to assurance activities associated with cryptography requirements in NIAP-approved protection profiles (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf). This section along with section 3.5.2 Cryptographic Algorithm Validation Programming Testing confirm CAVP certificates cited in [ST] contain the information required by NIAP Policy Letter #5.

ECDSA Algorithm Tests

ECDSA FIPS 186-4 Signature Verification Test

For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator shall obtain in response a set of 10 PASS/FAIL values.

[ST] does not select the ECDSA option in FCS_COP.1(a). Thus, this assurance activity is not applicable.

RSA Signature Algorithm Tests

Signature Verification Test

The evaluator shall perform the Signature Verification test to verify the ability of the TOE to recognize another party's authentic and unauthentic signatures. The evaluator shall inject errors into the test vectors produced during the Signature Verification Test by introducing errors in some of the public keys e, messages, IR format, and/or signatures. The TOE attempts to verify the signatures and returns success or failure.

The evaluator shall use these test vectors to emulate the signature verification test using the corresponding parameters and verify that the TOE detects these errors.

[ST] Table 2 TOE Hardware and Firmware and Table 6 Cryptographic Functions provide information on cryptographic implementations and CAVP certificates for each TOE device. In section 3.5.2 below, Table 19, Table 20, and Table 21 verify the correspondence between each TOE device, its cryptographic implementations (hardware and firmware), and CAVP certificates. The tables confirm information required by NIAP Policy #5 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf) for each TOE device. Table 3 lists certificates and implementations applicable to FCS_COP.1(a).

Table 3 Seagate Secure TCG SSC Self-Encrypting Drives CAVP RSA Certificates

Cert	Implementation
#2662	Balto RSA in Hardware
#1933	Cheops RSA in Hardware
#2013	Myna RSA in Hardware
#1934	ARMv7 RSA in Firmware 5.0 (Firmware)
#2056	ARMv7 RSA in Firmware 5.1 (Firmware)

2.1.11 FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)

FCS_COP.1(b) is a selection-based requirement.

2.1.11.1 Application Notes

The selection should be consistent with the overall strength of the algorithm used for FCS_COP.1(a) and quantum resistant recommendations. For example, SHA-256 should be chosen for 2048-bit RSA or ECC with P-256, SHA-384 should be chosen for 3072-bit RSA, 4096-bit RSA, or ECC with P-384, and SHA-512 should be chosen for ECC with P-521. The selection of the standard is made based on the algorithms selected.

2.1.11.2 TSS Assurance Activities

The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

[ST] section 6.2.3 "Cryptographic Operation (FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(f))" indicates the hash function is used with HMAC-SHA-256 message authentication, Hash_DRBG(any), and RSA signature verification (search for "The TOE performs SHA-256 cryptographic hashing services").

2.1.11.3 Guidance Assurance Activities

The evaluator checks the operational guidance documents to determine that any system configuration necessary to enable required hash size functionality is provided.

[Guide] section "Cryptographic Operation (Hash Algorithm)" states the hash algorithm is not configurable in Seagate SEDs.

2.1.11.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.1.11.5 Test Assurance Activities

The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this cPP.

Seagate Secure TCG SSC Self-Encrypting Drives use algorithm implementations validated under the CAVP (http://csrc.nist.gov/groups/STM/cavp/index.html). NIAP Policy Letter #5 defines the applicability and relationship of NIST CAVP and CMVP testing to assurance activities associated with cryptography requirements in NIAP-approved protection profiles (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf). This section along with section 3.5.2 Cryptographic Algorithm Validation Programming Testing confirm CAVP certificates cited in [ST] contain the information required by NIAP Policy Letter #5.

Short Messages Test – Bit-oriented Mode

The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Short Messages - Test Byte-oriented Mode

The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages - Test Bit-oriented Mode

*The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.*

Selected Long Messages - Test Byte-oriented Mode

*The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.*

Pseudo-randomly Generated Messages Test

This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

[ST] Table 2 TOE Hardware and Firmware and Table 6 Cryptographic Functions provide information on cryptographic implementations and CAVP certificates for each TOE device. In section 3.5.2 below, Table 19, Table 20, and Table 21 verify the correspondence between each TOE device, its cryptographic

implementations (hardware and firmware), and CAVP certificates. The tables confirm information required by NIAP Policy #5 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf) for each TOE device. Table 4 lists certificates and implementations applicable to FCS_COP.1(b).

Table 4 Seagate Secure TCG SSC Self-Encrypting Drives CAVP SHS Certificates

Cert	Implementation
#3984	Balto SHA in Hardware
#3515	Cheops SHA in Hardware
#3128	Cheops SHA in Hardware
#3250	Myna SHA in Hardware
#1225	ARMv7 SHS in Firmware 3.0 (Firmware)
#3304	ARMv7 SHS in Firmware 5.0 (Firmware)

2.1.12 FCS_COP.1(c) Cryptographic Operation (Message Authentication)

FCS_COP.1(c) is a selection-based requirement.

2.1.12.1 Application Notes

If one or more HMAC algorithms are selected, the ST author selects "HMAC" in the second selection and "ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'" in the third selection. For the assignment, the key size [k] falls into a range between L1 and L2 (defined in ISO/IEC 10118 for the appropriate hash function). For example, for SHA-256, L1 = 512 and L2 = 256 where $L2 \leq k \leq L1$.

If one or more CMAC algorithms are selected, the ST author selects "AES" in the second selection and "NIST SP 800-38B" in the third selection. For the assignment, the key size will fall into a range between 128 and 256.

2.1.12.2 TSS Assurance Activities

If HMAC was selected:

The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

[ST] section 6.2.3 "Cryptographic Operation (FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(f))" identifies the HMAC key length, hash function used, block size, and output MAC length used as, respectively, 256 bits, SHA-256, block size is 64 bytes, and the output MAC length size is 32 bytes.

If CMAC was selected:

The evaluator shall examine the TSS to ensure that it specifies the following values used by the CMAC function: key length, block cipher used, block size (of the cipher), and output MAC length used.

[ST] does not select the CMAC option in FCS_COP.1(c). Thus, this assurance activity is not applicable.

2.1.12.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.1.12.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.1.12.5 Test Assurance Activities

Seagate Secure TCG SSC Self-Encrypting Drives use algorithm implementations validated under the CAVP (http://csrc.nist.gov/groups/STM/cavp/index.html). NIAP Policy Letter #5 defines the applicability and relationship of NIST CAVP and CMVP testing to assurance activities associated with cryptography requirements in NIAP-approved protection profiles (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf). This section along with section 3.5.2 Cryptographic Algorithm Validation Programming Testing confirm CAVP certificates cited in [ST] contain the information required by NIAP Policy Letter #5.

If HMAC was selected:

For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key using a known good implementation.

[ST] Table 2 TOE Hardware and Firmware and Table 6 Cryptographic Functions provide information on cryptographic implementations and CAVP certificates for each TOE device. In section 3.5.2 below, Table 19, Table 20, and Table 21 verify the correspondence between each TOE device, its cryptographic implementations (hardware and firmware), and CAVP certificates. The tables confirm information required by NIAP Policy #5 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf) for each TOE device. Table 5 lists certificates and implementations applicable to FCS_COP.1(c).

Table 5 Seagate Secure TCG SSC Self-Encrypting Drives CAVP HMAC Certificates

Cert	Implementation
#3243	Balto HMAC in Hardware
#2815	Cheops HMAC in Hardware
#2460	Cheops HMAC in Hardware
#2565	Myna HMAC in Hardware
#1597	ARMv7 HMAC in Firmware 4.0 (Firmware)
#2613	ARMv7 HMAC in Firmware 5.0 (Firmware)

If CMAC was selected:

For each of the supported parameter sets, the evaluator shall compose at least 15 sets of test data.

Each set shall consist of a key and message data. The test data shall include messages of different lengths, some with partial blocks as the last block and some with full blocks as the last block. The test data keys shall include cases for which subey K1 is generated both with and without using the irreducible polynomial R_b, as well as cases for which subkey K2 is generated from K1 both with and without using the irreducible polynomial R_b. (The subkey generation and polynomial R_b are as defined in SP800-38E.) The evaluator shall have the TSF generate CMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating CMAC tags with the same key using a known good implementation.

[ST] does not select the CMAC option in FCS_COP.1(c). Thus, this assurance activity is not applicable.

2.1.13 FCS_COP.1(d) Cryptographic Operation (Key Wrapping)

FCS_COP.1(d) is a selection-based requirement.

2.1.13.1 Application Notes

This requirement is used in the body of the ST if the ST author chooses to use key wrapping in the key chaining approach that is specified in FCS_KYC_EXT.2.

2.1.13.2 TSS Assurance Activities

The evaluator shall verify the TSS includes a description of the key wrap function(s) and shall verify the key wrap uses an approved key wrap algorithm according to the appropriate specification.

[ST] section 6.1 “Overview of TOE Operations” and section 6.2.3 “Cryptographic Operation (FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(f))” describe the key wrap functions (search for “This intermediate key is used as an input to the AES GCM mode function to generate an intermediate wrap key” and “This wrap key and a second plain text intermediate wrap key are used as inputs in a two step AES KW function process to wrap the media encryption key (MEK)”, respectively).

2.1.13.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.1.13.4 KMD Assurance Activities

The evaluator shall review the KMD to ensure that all keys are wrapped using the approved method and a description of when the key wrapping occurs.

The description of key wrapping in [KMD] is consistent with the summary in [ST] sections 6.1 and 6.2.3 identified above. [KMD] describes Seagate SED functions that use a drive’s key chains. The description for each function identifies each instance when a Seagate SED uses AES-GCM or AES-KW key wrap.

2.1.13.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.14 FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1(f) is a selection-based requirement.

2.1.14.1 Application Notes

This cPP allows for software encryption or hardware encryption. In software encryption, the TOE can provide the data encryption/decryption or the host platform could provide the encryption/decryption. Conversely, for hardware encryption, the encryption/decryption could be provided by a variety of mechanisms - dedicated hardware within a general purpose controller, the storage device's SOC, or a dedicated (co-)processor.

If XTS Mode is selected, a cryptographic key of 256-bit or of 512-bit is allowed as specified in IEEE 1619. XTS-AES key is divided into two AES keys of equal size - for example, AES-128 is used as the underlying algorithm, when 256-bit key and XTS mode are selected. AES-256 is used when a 512-bit key and XTS mode are selected.

The intent of this requirement is to specify the approved AES modes that the ST author may select for AES encryption of the appropriate information on the hard disk. For the first selection, the ST author should indicate the mode or modes supported by the TOE implementation. The second selection indicates the key size to be used, which is identical to that specified for FCS_CKM.1(1). The third selection must agree with the mode or modes chosen in the first selection. If multiple modes are supported, it may be clearer in the ST if this component was iterated.

2.1.14.2 TSS Assurance Activities

The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for encryption.

[ST] section 6.2.3 "Cryptographic Operation (FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(f))" describes Seagate SED use of AES-GCM and XTS-AES-256 for encrypting intermediate keys and user data, respectively (search for "The TOE performs AES GCM mode encryption and decryption using cryptographic key size 256 bits", and "programmed into the FDE hardware as the XTS-AES-256 mode encryption key for data encryption/decryption").

2.1.14.3 Guidance Assurance Activities

If multiple encryption modes are supported, the evaluator examines the guidance documentation to determine that the method of choosing a specific mode/key size by the end user is described.

[Guide] section "Cryptographic Operation (AES Data Encryption/Decryption)" states, "For each function the specific AES encryption/decryption mode is fixed and not configurable."

2.1.14.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.1.14.5 Test Assurance Activities

Seagate Secure TCG SSC Self-Encrypting Drives use algorithm implementations validated under the CAVP (http://csrc.nist.gov/groups/STM/cavp/index.html). NIAP Policy Letter #5 defines the applicability and relationship of NIST CAVP and CMVP testing to assurance activities associated with cryptography requirements in NIAP-approved protection profiles (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf). This section along with section 3.5.2 Cryptographic Algorithm Validation Programming Testing confirm CAVP certificates cited in [ST] contain the information required by NIAP Policy Letter #5.

The following tests are conditional based upon the selections made in the SFR.

For the AES-CBC tests described below, the plaintext, ciphertext, and IV values shall consist of 128-bit blocks. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known-good implementation.

AES-CBC Tests

For the AES-CBC tests described below, the plaintext, ciphertext, and IV values shall consist of 128-bit blocks. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known-good implementation.

These tests are intended to be equivalent to those described in NIST's AES Algorithm Validation Suite (AESAVS) (http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf). Known answer values tailored to exercise the AES-CBC implementation can be obtained using NIST's CAVS Algorithm Validation Tool or from NIST's ACPV service for automated algorithm tests (acvp.nist.gov), when available. It is not recommended that evaluators use values obtained from static sources such as the example NIST's AES Known Answer Test Values from the AESAVS document, or use values not generated expressly to exercise the AES-CBC implementation.

AES-CBC Known Answer Tests

KAT-1 (GFSBox):

To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of five different plaintext values for each selected key size and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros.

To test the decrypt functionality of AES-CBC, the evaluator shall supply a set of five different ciphertext values for each selected key size and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using a key value of all zeros and an IV of all zeros.

KAT-2 (KeySBox):

To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of five different key values for each selected key size and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros.

To test the decrypt functionality of AES-CBC, the evaluator shall supply a set of five different key

values for each selected key size and obtain the plaintext that results from AES-CBC decryption of an all-zeros ciphertext using the given key and an IV of all zeros.

KAT-3 (Variable Key):

To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of keys for each selected key size (as described below) and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using each key and an IV of all zeros.

Key i in each set shall have the leftmost i bits set to ones and the remaining bits to zeros, for values of i from 1 to the key size. The keys and corresponding ciphertext are listed in AESAVS, Appendix E.

To test the decrypt functionality of AES-CBC, the evaluator shall use the same keys as above to decrypt the ciphertext results from above. Each decryption should result in an all-zeros plaintext.

KAT-4 (Variable Text):

To test the encrypt functionality of AES-CBC, for each selected key size, the evaluator shall supply a set of 128-bit plaintext values (as described below) and obtain the ciphertext values that result from AES-CBC encryption of each plaintext value using a key of each size and IV consisting of all zeros.

Plaintext value i shall have the leftmost i bits set to ones and the remaining bits set to zeros, for values of i from 1 to 128. The plaintext values are listed in AESAVS, Appendix D.

To test the decrypt functionality of AES-CBC, for each selected key size, use the plaintext values from above as ciphertext input, and AES-CBC decrypt each ciphertext value using key of each size consisting of all zeros and an IV of all zeros.

AES-CBC Multi-Block Message Test

The evaluator shall test the encrypt functionality by encrypting nine i-block messages for each selected key size, for $2 \leq i \leq 10$. For each test, the evaluator shall supply a key, an IV, and a plaintext message of length i blocks, and encrypt the message using AES-CBC. The resulting ciphertext values shall be compared to the results of encrypting the plaintext messages using a known good implementation.

The evaluator shall test the decrypt functionality by decrypting nine i-block messages for each selected key size, for $2 \leq i \leq 10$. For each test, the evaluator shall supply a key, an IV, and a ciphertext message of length i blocks, and decrypt the message using AES-CBC. The resulting plaintext values shall be compared to the results of decrypting the ciphertext messages using a known good implementation.

AES-CBC Monte Carlo Tests

The evaluator shall test the encrypt functionality for each selected key size using 100 3-tuples of pseudo-random values for plaintext, IVs, and keys.

The evaluator shall supply a single 3-tuple of pseudo-random values for each selected key size. This 3-tuple of plaintext, IV, and key is provided as input to the below algorithm to generate the remaining 99 3-tuples, and to run each 3-tuple through 1000 iterations of AES-CBC encryption.

 # Input: PT, IV, Key
Key[0] = Key
IV[0] = IV

PT[0] = PT

for i = 1 to 100 {
Output Key[i], IV[i], PT[0]
for j = 1 to 1000 {
if j == 1 {
CT[1] = AES-CBC-Encrypt(Key[i], IV[i], PT[1])
PT[2] = IV[i]
} else {
CT[j] = AES-CBC-Encrypt(Key[i], PT[j])
PT[j+1] = CT[j-1]
}
}
Output CT[1000]

If KeySize == 128 { Key[i+1] = Key[i] xor CT[1000] }
If KeySize == 256 { Key[i+1] = Key[i] xor ((CT[999] << 128) | CT[1000]) }

IV[i+1] = CT[1000]
PT[0] = CT[999]
}

The ciphertext computed in the 1000th iteration (CT[1000]) is the result for each of the 100 3-tuples for each selected key size. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

The evaluator shall test the decrypt functionality using the same test as above, exchanging CT and PT, and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.

[ST] Table 2 TOE Hardware and Firmware and Table 6 Cryptographic Functions provide information on cryptographic implementations and CAVP certificates for each TOE device. In section 3.5.2 below, Table 19, Table 20, and Table 21 verify the correspondence between each TOE device, its cryptographic implementations (hardware and firmware), and CAVP certificates. The tables confirm information required by NIAP Policy #5 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf) for each TOE device. Table 6 lists certificates and implementations applicable to FCS_COP.1(c).

Table 6 Seagate Secure TCG SSC Self-Encrypting Drives CAVP AES-CBC Certificates

Cert	Implementation
#4843	Balto AES in Hardware
#4279	Cheops AES in Hardware
#3758	Cheops AES in Hardware
#3940	Myna AES in Hardware
#1343	ARMv7 AES in Firmware 3.0 (Firmware)

The following tests are conditional based upon the selections made in the SFR.

AES-GCM Test

The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:

128 bit and 256 bit keys

Two plaintext lengths. *One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.*

Three AAD lengths. *One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.*

Two IV lengths. *If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.*

The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.

The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

[ST] Table 2 TOE Hardware and Firmware and Table 6 Cryptographic Functions provide information on cryptographic implementations and CAVP certificates for each TOE device. In section 3.5.2 below, Table 19, Table 20, and Table 21 verify the correspondence between each TOE device, its cryptographic implementations (hardware and firmware), and CAVP certificates. The tables confirm information required by NIAP Policy #5 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf) for each TOE device. Table 7 lists certificates and implementations applicable to FCS_COP.1(c).

Table 7 Seagate Secure TCG SSC Self-Encrypting Drives CAVP AES-GCM and AES-KW Certificates

Cert	Implementation
#4843	Balto AES in Hardware
#2804	ARMv7 GCM in Firmware 1.0 (Firmware)
#2841	ARMv7 GCM in Firmware 2.0 (Firmware)

The following tests are conditional based upon the selections made in the SFR.

XTS-AES Test

The evaluator shall test the encrypt functionality of XTS-AES for each combination of the following input parameter lengths:

256 bit (for AES-128) and 512 bit (for AES-256) keys

Three data unit (i.e., plaintext) lengths. *One of the data unit lengths shall be a non-zero integer multiple of 128 bits, if supported. One of the data unit lengths shall be an integer multiple of 128 bits, if supported. The third data unit length shall be either the longest supported data unit length or 216 bits, whichever is smaller.*

using a set of 100 (key, plaintext and 128-bit random tweak value) 3-tuples and obtain the ciphertext that results from XTS-AES encrypt.

The evaluator may supply a data unit sequence number instead of the tweak value if the implementation supports it. The data unit sequence number is a base-10 number ranging between 0 and 255 that implementations convert to a tweak value internally.

The evaluator shall test the decrypt functionality of XTS-AES using the same test as for encrypt, replacing plaintext values with ciphertext values and XTS-AES encrypt with XTS-AES decrypt.

[ST] Table 2 TOE Hardware and Firmware and Table 6 Cryptographic Functions provide information on cryptographic implementations and CAVP certificates for each TOE device. In section 3.5.2 below, Table 19, Table 20, and Table 21 verify the correspondence between each TOE device, its cryptographic implementations (hardware and firmware), and CAVP certificates. The tables confirm information required by NIAP Policy #5 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf) for each TOE device. Table 8 lists certificates and implementations applicable to FCS_COP.1(c).

Table 8 Seagate Secure TCG SSC Self-Encrypting Drives CAVP XTS-AES Certificates

Cert	Implementation
#4843	Balto AES in Hardware
#4279	Cheops AES in Hardware
#3758	Cheops AES in Hardware
#3940	Myna AES in Hardware

2.1.15 FCS_KDF_EXT.1 Cryptographic Key Derivation

FCS_KDF_EXT.1 is a selection-based requirement.

2.1.15.1 Application Notes

This requirement is used in the body of the ST if the ST author chooses to use key derivation in the key chaining approach that is specified in FCS_KYC_EXT.2.

This requirement establishes acceptable methods for generating a new random key or an existing submask to create a new key along the key chain.

2.1.15.2 TSS Assurance Activities

The evaluator shall verify the TSS includes a description of the key derivation function and shall verify the key derivation uses an approved derivation mode and key expansion algorithm according to SP 800-108 and SP 800-132.

[ST] section 6.2.4 “Cryptographic Key Derivation (FCS_KDF_EXT.1)” describes how Seagate SEDs derive an intermediate key from an Authentication PIN in accordance with NIST SP 800-132.

2.1.15.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.1.15.4 KMD Assurance Activities

The evaluator shall examine the vendor’s KMD to ensure that all keys used are derived using an approved method and a description of how and when the keys are derived.

The description of key wrapping in [KMD] is consistent with the summary in [ST] section 6.2.4 identified above. [KMD] describes Seagate SED functions that use a drive’s key chains. The description for each function identifies each instance when a Seagate SED drives an intermediate key.

2.1.15.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.16 FCS_KYC_EXT.2 Key Chaining (Recipient)

FCS_KYC_EXT.2 is an unconditional requirement.

2.1.16.1 Application Notes

Key Chaining is the method of using multiple layers of encryption keys to ultimately secure the protected data encrypted on the drive. The number of intermediate keys will vary – from two (e.g., using the BEV as an intermediary key to wrap the DEK) to many. This applies to all keys that contribute to the ultimate wrapping or derivation of the DEK; including those in areas of protected storage (e.g. TPM stored keys, comparison values).

2.1.16.2 TSS Assurance Activities

There are no TSS evaluation activities for this SFR.

2.1.16.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.1.16.4 KMD Assurance Activities

The evaluator shall examine the KMD to ensure it describes a high level key hierarchy and details of the key chain. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap or key derivation methods that meet FCS_KDF_EXT.1, FCS_COP.1(d), FCS_COP.1(e), and/or FCS_COP.1(g).

Table 1 Per-band Key Chain in section 2.1.1 above summarize the key chain as presented in [ST]. Sections 2.1.15 "FCS_KDF_EXT.1 Cryptographic Key Derivation" and 2.1.13 "FCS_COP.1(d) Cryptographic Operation (Key Wrapping)" address key derivation and key wrap methods Seagate SEDs use to protect the key chain from BEV (Authentication PIN) to DEK (MEK).

The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or knowledge of the BEV and the effective strength of the DEK is maintained throughout the Key Chain.

Figure 1 Key Hierarchy Diagram in [KMD] provides an overview of the key chain and key processing. [KMD] describes each key together with supporting values (such as, salt and initialization vector values), [KMD] describes Seagate SED functions that use a drive's key chains. Each function description in [KMD] provides a detailed description of how the function uses each key and associated key material.

The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.

[KMD] demonstrates Seagate SEDs maintain key strength of 256 bits consistently throughout the key chain.

2.1.16.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.17 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1 is a selection-based requirement.

2.1.17.1 Application Notes

ISO/IEC 18031:2011 contains different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used and include the specific underlying cryptographic primitives used in the requirement. While any of the identified hash functions (SHA-256, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CTR_DRBG are allowed. Table C.2 in ISO/IEC

18031:2011 provides an identification of Security strengths, Entropy and Seed length requirements for the AES-128 and 256 Block Cipher.

The CTR_DRBG in ISO/IEC 18031:2011 requires using derivation function, whereas NIST SP 800-90A does not. Either model is acceptable. In the first selection in FCS_RBG_EXT.1.1, the ST author choses the standard to which the TSF is compliant.

In the first selection in FCS_RBG_EXT.1.2 the ST author fills in how many entropy sources are used for each type of entropy source they employ. It should be noted that a combination of hardware and software based noise sources is acceptable.

It should be noted that the entropy source is considered to be a part of the DRBG and if the DRBG is included in the TOE, the developer is required to provide the entropy description outlined in Appendix D. The documentation *and tests* required in the Evaluation Activity for this element necessarily cover each source indicated in FCS_RBG_EXT.1.2. Individual contributions to the entropy pool may be combined to provide the minimum amount of entropy as long as the Entropy Documentation demonstrates that entropy from each of these individual sources is generated independently.

2.1.17.2 TSS Assurance Activities

For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator shall verify that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG.

Seagate SEDs do not make use of third-party RBG services. This assurance activity does not apply.

If the ST specifies more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each DRBG mechanism.

Seagate SEDs use only one DRBG, which [ST] section 6.2.6 “Random Bit Generation (FCS_RBG_EXT.1)” describes.

2.1.17.3 Guidance Assurance Activities

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected DRBG mechanism(s), if necessary, and provides information regarding how to instantiate/call the DRBG for RBG services needed in this cPP.

[Guide] section “Cryptographic Operation (Random Bit Generation)” states, “Neither the DRBG or the entropy system are configurable.”

2.1.17.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.1.17.5 Test Assurance Activities

Seagate Secure TCG SSC Self-Encrypting Drives use algorithm implementations validated under the CAVP (http://csrc.nist.gov/groups/STM/cavp/index.html). NIAP Policy Letter #5 defines the applicability and relationship of NIST CAVP and CMVP testing to assurance activities associated with cryptography requirements in NIAP-approved protection profiles (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf). This section along with section 3.5.2 Cryptographic Algorithm Validation Programming Testing confirm CAVP certificates cited in [ST] contain the information required by NIAP Policy Letter #5.

The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable by the TOE, the evaluator shall perform 15 trials for each configuration. The evaluator shall verify that the instructions in the operational guidance for configuration of the RNG are valid.

If the RNG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP800-90A).

If the RNG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

***Entropy input:** the length of the entropy input value must equal the seed length.*

***Nonce:** If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.*

***Personalization string:** The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.*

***Additional input:** the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.*

[ST] Table 2 TOE Hardware and Firmware and Table 6 Cryptographic Functions provide information on cryptographic implementations and CAVP certificates for each TOE device. In section 3.5.2 below, Table 19, Table 20, and Table 21 verify the correspondence between each TOE device, its cryptographic

implementations (hardware and firmware), and CAVP certificates. The tables confirm information required by NIAP Policy #5 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf) for each TOE device. Table 9 lists certificates and implementations applicable to FCS_RBG_EXT.1.

Table 9 Seagate Secure TCG SSC Self-Encrypting Drives CAVP DRBG Certificates

Cert	Implementation
#62	800-90 DRBG 1.0 (Firmware)
#1146	Hash_Based DRBG 2.0 (Firmware)

2.1.18 FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

FCS_SNI_EXT.1 is an unconditional requirement.

2.1.18.1 Application Notes

This SFR does not prescribe when salts, nonces, and IVs must be used, only that when they are used they must be generated in a certain manner. The ST author is expected to document each claimed SFR that requires the use of salts, nonces, and/or IVs (such as symmetric key generation as defined by FCS_CKM.1(b) and AES encryption/decryption as defined by FCS_COP.1(f)). If the TSF does not use salts, nonces, or IVs for any function, then this SFR is considered to be vacuously satisfied.

This requirement covers several important factors – the salt must be random, but the nonces only have to be unique. FCS_SNI_EXT.1.3 specifies how the IV should be handled for each encryption mode. Assigned consecutively could mean using a one-up counter. Additionally, nonce is referred to as Starting Variable (SV) in ISO/IEC 19772.

Tweak values shall be non-negative numbers, starting at an arbitrary non-negative number, and all subsequent tweak values shall be incremented from the initial value.

2.1.18.2 TSS Assurance Activities

The evaluator shall ensure the TSS describes how salts are generated. The evaluator shall confirm that the salt is generating using an RBG described in FCS_RBG_EXT.1 or by the Operational Environment. If external function is used for this purpose, the TSS should include the specific API that is called with inputs.

[ST] section 6.2.7 “Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (FCS_SNI_EXT.1)” describes the 128-bit salt values associated with Authentication PINs, which Seagate SEDs use to derive intermediate keys. The Seagate SEDs generate random salt values.

The evaluator shall ensure the TSS describes how nonces are created uniquely and how IVs and tweaks are handled (based on the AES mode). The evaluator shall confirm that the nonces are unique and the IVs and tweaks meet the stated requirements.

[ST] FCS_SNI_EXT.1.2 selects option “no nonces”. [ST] section 6.2.7 “Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (FCS_SNI_EXT.1)” describes tweaks and IV consistent with FCS_SNI_EXT.1.3 (search for “The tweak values used for XTS are non-negative integers”)

2.1.18.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.1.18.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.1.18.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.1.19 FCS_VAL_EXT.1 Validation

FCS_VAL_EXT.1 is an unconditional requirement. [ST] iterates FCS_VAL_EXT.1 as FCS_VAL_EXT.1(a) and FCS_VAL_EXT.1(b).

2.1.19.1 Application Notes

“Validation” of the BEV can occur at any point in the key chain, including when the DEK is decrypted. For the purposes of this requirement, validating a key derived from the BEV equates to “validating” the BEV. The purpose of performing secure validation is to not expose any material that might compromise the submask(s).

The TOE validates the BEV prior to allowing the user access to the data stored on the drive. When the key wrap in FCS_COP.1(d) is used, the validation is performed inherently.

The delay must be enforced by the TOE, but this requirement is not intended to address attacks that bypass the product (e.g. attacker obtains hash value or “known” crypto value and mounts attacks outside of the TOE, such as a third party password cracker). The cryptographic functions (i.e., hash, decryption) performed are those specified in FCS_COP.1(b) and FCS_COP.1(f).

2.1.19.2 TSS Assurance Activities

The evaluator shall examine the TSS to determine which authorization factors support validation.

[ST] section 6.2.8 “Validation (FCS_VAL_EXT.1(a), FCS_VAL_EXT.1(b))” explains all Authentication PINs support validation (search for “the PIN is validated by”).

The evaluator shall examine the TSS to review a high-level description if multiple submasks are used within the TOE, how the submasks are validated (e.g., each submask validated before combining, once combined validation takes place).

The validation process described in [ST] section 6.2.8 “Validation (FCS_VAL_EXT.1(a), FCS_VAL_EXT.1(b))” does not use multiple submasks.

The evaluator shall also examine the TSS to determine that a subset or all of the authorization factors identified in the SFR can be used to exit from a Compliant power saving state.

[ST] Table 7 Try Limits Summary identifies Authentication PINs that can unlock a Seagate SED band. These Authentication PINs are labeled BEV in the Credential Name column of Table 7. [ST] section 6.2.8 “Validation (FCS_VAL_EXT.1(a), FCS_VAL_EXT.1(b))” states “The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a compliant power saving state.”

2.1.19.3 Guidance Assurance Activities

[conditional] If the validation functionality is configurable, the evaluator shall examine the operational guidance to ensure it describes how to configure the TOE to ensure the limits regarding validation attempts can be established.

[ST] FCS_VAL_EXT.1(b) specifies the validation function is not configurable for Seagate SEDs with SAS interface.

[ST] FCS_VAL_EXT.1(a) specifies validation function limits on failed validation attempts are configurable for Seagate SEDs with SATA interfaces. Seagate SED drives have a separate counter for each credential which keeps track of the number of unsuccessful authentication attempts for each credential. [Guide] section “Validation - Try Limits and Persistence Settings” identifies which validation failure limits an administrator may configure. [TCG Core] sections 5.3.4.1.1.2 and 5.3.2.12 and [TCG Opal] sections 4.2.1.8 and 4.3.1.9 cover Try Limit behavior and configuration.

[conditional] (conditional) If the validation functionality is specified by the ST author, the evaluator shall examine the operational guidance to ensure that it states the values that the TOE uses for limits regarding validation attempts.

[Guide] section “Validation - Try Limits and Persistence Settings” identifies which validation failure limits an administrator may configure. The section includes a table identifying the default value of each validation failure limit.

The evaluator shall verify that the guidance documentation states which authorization factors are allowed to exit a Compliant power saving state.

The table in [Guide] section “Validation - Try Limits and Persistence Settings” identifies which of the authorization factors are a BEV, which allow to management functions or encrypted user data after power is applied to a Seagate SED.

2.1.19.4 KMD Assurance Activities

The evaluator shall examine the KMD to verify that it described the method the TOE employs to limit the number of consecutively failed authorization attempts.

[ST] section 6.2.8 “Validation (FCS_VAL_EXT.1(a), FCS_VAL_EXT.1(b))” described the method the TOE employs to limit the number of consecutively failed authorization attempts. This description is consistent with a more detailed description in [KMD].

The evaluator shall examine the vendor’s KMD to ensure it describes how validation is performed. The description of the validation process in the KMD provides detailed information how the TOE validates the BEV.

[ST] section 6.2.8 “Validation (FCS_VAL_EXT.1(a), FCS_VAL_EXT.1(b))” summarizes the validation process (search for “Next call the AES GCM Key Unwrap function”). This summary is consistent with a more detailed description in [KMD].

The KMD describes how the process works, such that it does not expose any material that might compromise the submask(s).

[KMD] includes a step-by-step validation procedure. The procedure shows Seagate SEDs use approved algorithms as intended and handles keys as specified in [CPP FDE EE].

2.1.19.5 Test Assurance Activities

The evaluator shall perform the following tests:

Test 1: *The evaluator shall determine the limit on the average rate of the number of consecutive failed authorization attempts. The evaluator will test the TOE by entering that number of incorrect authorization factors in consecutive attempts to access the protected data. If the limit mechanism includes any “lockout” period, the time period tested should include at least one such period. Then the evaluator will verify that the TOE behaves as described in the TSS.*

Covered by FCS_VAL_EXT.1 Test 2.

Test 2: *The evaluator shall force the TOE to enter a Compliant power saving state, attempt to resume it from this state, and verify that only a valid authorization factor as defined by the guidance documentation is sufficient to allow the TOE to exit the Compliant power saving state.*

The evaluator attempted to authenticate to the TOE with incorrect credentials until the lockout limit was reached. Next, the evaluator power cycled the TOE. The evaluator confirmed that when the lockout was expected to be persistent the TOE was still locked out and for the non-persistent instances of the TOE it allowed successful authentication with correct credentials.

2.2 User Data Protection (FDP)

2.2.1 FDP_DSK_EXT.1 Protection of Data on Disk

FDP_DSK_EXT.1 is an unconditional requirement.

2.2.1.1 Application Notes

The intent of this requirement is to specify that encryption of any protected data will not depend on a user electing to protect that data. The drive encryption specified in FDP_DSK_EXT.1 occurs transparently to the user and the decision to protect the data is outside the discretion of the user, which is a characteristic that distinguishes it from file encryption. The definition of protected data can be found in the glossary.

The cryptographic functions that perform the encryption/decryption of the data may be provided by the Operational Environment. Note that if this is the case, it is assumed that the environmental implementation of AES is consistent with the behavior described in FCS_COP.1(f). If the TOE provides the cryptographic functions to encrypt/decrypt the data, the ST author includes FCS_COP.1(f) as defined in Appendix A in the main body of the ST.

2.2.1.2 TSS Assurance Activities

The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the disk and the point at which the encryption function is applied. The TSS must make the case that standard methods of accessing the disk drive via the host platforms operating system will pass through these functions.

[ST] section 6.4.1 “Protection of Data on Disk (FDP_DSK_EXT.1)” states “The TOE is encrypted by default without user intervention using AES:XTS”. Seagate Opal SEDs provide unencrypted storage for operating system use, which includes a shadow master boot record used for booting the host. Seagate SEDs use unencrypted system area (for example, to store keys wrapped in accordance with FCS_COP.1(d)). Section 6.4.1 explains there is no host access to the system area. The system area includes TCG Data Store tables, which can only be accessed by administrators through access-controlled TCG commands. The section warns administrators not to store protected data in the TCG Data Tables.

For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes, for each platform identified in the ST, the interface(s) used by the TOE to invoke this functionality.

Seagate SEDs provide their own cryptographic functions. Thus, this assurance activity is not applicable.

The evaluator shall verify the TSS in performing the evaluation activities for this requirement. The evaluator shall ensure the comprehensiveness of the description, confirms how the TOE writes the data to the disk drive, and the point at which it applies the encryption function.

As summarized above, Seagate SEDs encrypt all user data by default.

The evaluator shall verify that the TSS describes the initialization of the TOE and the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the TOE.

As summarized above, Seagate SEDs encrypt all user data by default. [ST] section 6.4.1 “Protection of Data on Disk (FDP_DSK_EXT.1)” describes taking ownership of a drive, which restricts data reads and writes to authenticated users. [ST] section 6.1 “Overview of TOE Operations” describes subdividing user storage into storage ranges called bands.

The evaluator shall verify the TSS describes areas of the disk that it does not encrypt (e.g., portions associated with the Master Boot Records (MBRs), boot loaders, partition tables, etc.).

Seagate Opal SEDs provide unencrypted storage for operating system use, which includes a shadow master boot record used for booting the host. Seagate SEDs use unencrypted system area (for example, to store keys wrapped in accordance with FCS_COP.1(d)). Section 6.4.1 explains there is no host access to the system area. The system area includes TCG Data Store tables, which can only be accessed by administrators through access-controlled TCG commands. The section warns administrators not to store protected data in the TCG Data Tables.

If the TOE supports multiple disk encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all storage devices on the platform.

Seagate SEDs do not support multiple disk encryptions. Thus, this assurance activity is not applicable.

2.2.1.3 Guidance Assurance Activities

The evaluator shall review the AGD guidance to determine that it describes the initial steps needed to enable the FDE function, including any necessary preparatory steps. The guidance shall provide instructions that are sufficient, on all platforms, to ensure that all hard drive devices will be encrypted when encryption is enabled.

[Guide] describes putting a Seagate SED into its evaluated configuration in the following three sections (depending on device type).

- TCG Enterprise Configuration & Operation
- TCG Opal Configuration & Operation
- ATA Mode Configuration & Operation

Each of these sections includes example commands for each configuration step. While examining the TOE security function interfaces, the evaluation team confirmed the steps and example commands would provide sufficient instructions to a host controller developer. Please see section 3.1.1 below for a description of the examination.

2.2.1.4 KMD Assurance Activities

The evaluator shall verify the KMD includes a description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the product, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions associated with the Master Boot Record (MBRs), partition tables, etc.)). The evaluator shall verify the KMD provides a functional (block) diagram showing the main components (such as memories and processors) and the data path between, for hardware, the device's host interface and the device's persistent media storing the data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the storage device entirely when a user or administrator first provisions the product. The hardware encryption diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the hardware

encryption diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine.

[KMD] provides a description of the Seagate SEDs. The description includes a block diagram of the data encryption engine, write and read data flows through the Seagate SED, and drive operation. The description covers access to the unencrypted shadow master boot record and TCG Data Store Tables of the drive. [KMD] describes the TCG Opal boot process as well as initial conditions required for each type of Seagate SED. [KMD] provides the information required by this assurance activity.

The evaluator shall verify the KMD provides sufficient instructions for all platforms to ensure that when the user enables encryption, the product encrypts all hard storage devices. The evaluator shall verify that the KMD describes the data flow from the device's host interface to the device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted Master Boot Record area).

[KMD] explains Seagate SEDs encrypt all user data by default. Seagate SEDs restricts user data reads and writes once a user takes ownership suing a TCG controller. [KMD] also explains exceptions for unencrypted access to Opal SED shadow master boot record and TCG Data Store Tables (search for "TCG Opal SEDs contain two other unencrypted areas"). The explanations include the data flow from a Seagate SED's host interface to the drives persistent media.

The evaluator shall verify that the KMD provides a description of the platform's boot initialization, the encryption initialization process, and at what moment the product enables the encryption. The evaluator shall validate that the product does not allow for the transfer of user data before it fully initializes the encryption.

The Seagate TOE consists of self-encrypting drivers. [KMD] states "Out of the box all Seagate SED drives are encrypted but not locked by default."

The evaluator shall ensure the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key.

Seagate has test tools with multiple functions to support drive examination.

2.2.1.5 Test Assurance Activities

The evaluator shall perform the following tests:

Test 1: *Write data to random locations, perform required actions and compare:*

a) Ensure TOE is initialized and, if hardware, encryption engine is ready;

b) Provision TOE to encrypt the storage device. For SW Encryption products, or hybrid products use a known key and the developer tools.

c) Determine a random character pattern of at least 64 KB;

d) Retrieve information on what the device TOE's lowest and highest logical address is for which

encryption is enabled.

Covered by Test 3

Test 2: Write pattern to storage device in multiple locations:

a) For HW Encryption, randomly select several logical address locations within the device's lowest to highest address range and write pattern to those addresses;

b) For SW Encryption, write the pattern using multiple files in multiple logical locations.

Covered by Test 3

Test 3: Verify data is encrypted:

For HW Encryption:

a) engage device's functionality for generating a new encryption key, thus performing an erase of the key per FCS_CKM.4(a);

b) Read from the same locations at which the data was written;

c) Compare the retrieved data to the written data and ensure they do not match

For SW Encryption, using developer tools;

a) Review the encrypted storage device for the plaintext pattern at each location where the file was written and confirm plaintext pattern cannot be found.

b) Using the known key, verify that each location where the file was written, the plaintext pattern can be correctly decrypted using the key.

c) If available in the developer tools, verify there are no plaintext files present in the encrypted range.

The evaluator determined the size of the drive and then configured the TOE to have 64 KB bands at the beginning and end of the drive. The evaluator wrote repeating instances of the string 'AB' to the beginning of the drive and repeating instances of the string 'CD' to the end of the drive. The evaluator then queried the drive to confirm the data had been written to the correct location. The evaluator then generated a new encryption key for each band. The evaluator queried each band and confirmed that the values of the data stored did not match the previous stored values.

2.3 Security Management (FMT)

2.3.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 is an unconditional requirement.

2.3.1.1 Application Notes

The intent of this requirement is to express the management capabilities that the TOE possesses. This means that the TOE must be able to perform the listed functions. Item (d) is used to specify functionality that may be included in the TOE, but is not required to conform to the cPP. "Configure cryptographic functionality" could include key management functions, for example, the BEV will be wrapped or encrypted, and the EE will need to unwrap or decrypt the BEV. In item (d), if no other management

functions are provided (or claimed), then “no other functions” should be selected. Default Authorization factors are the initial values that are used to manipulate the drive.

For the purposes of this document, key sanitization means to destroy the DEK, using one of the approved destruction methods. This applies to instances of the protected key that exist in non-volatile storage.

2.3.1.2 TSS Assurance Activities

Option A: The evaluator shall ensure the TSS describes how the TOE changes the DEK.

[ST] section 6.3.1 “Specification of Management Functions (FMT_SMF.1)” describes destroying and generating a new MEK when changing the MEK (search for “The TOE changes a DEK”). Seagate SEDs generate MEKs and do not support provisioning keys.

Option B: The evaluator shall ensure the TSS describes how the TOE cryptographically erases the DEK.

[ST] section 6.2.2 “Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)” covers key destruction. Please see above for assurance activity results regarding key destructions, particularly sections 2.1.4 and 2.1.5.

Option C: The evaluator shall ensure the TSS describes the process to initiate TOE firmware/software updates.

[ST] section 6.3.1 “Specification of Management Functions (FMT_SMF.1)” covers steps needed to initiate a firmware update: take ownership of the drive, change the SID, and issue download command (search for “Firmware updates are initiated using”). [ST] section 6.5.1 “Firmware Access Control and Update Authentication (FPT_FAC_EXT.1, FPT_FUA_EXT.1)” provides additional process details. Please see also sections 2.4.1 and 2.4.2 below.

Option D: If additional management functions are claimed in the ST, the evaluator shall verify that the TSS describes those functions.

FMT_SMF.1 in [ST] claims two additional functions: 1) configure a password for firmware update and 2) configure the number of failed validation attempts required to trigger corrective behavior (TCG Opal only). [ST] section 6.3.1 “Specification of Management Functions (FMT_SMF.1)” describes changing the SID as part of taking ownership of the drive. Section 6.3.1 also describes using Opal Try Limit command to configure the limit on failed validation attempts.

2.3.1.3 Guidance Assurance Activities

Option A: The evaluator shall review the AGD guidance and shall determine that the instructions for changing a DEK exist. The instructions must cover all environments on which the TOE is claiming conformance, and include any preconditions that must exist in order to successfully generate or re-generate the DEK.

Seagate terminology refers to the DEK as the Media Encryption Key (MEK).

Modifying the EraseMaster credential and executing the RevertSP command will change MEKs. The evaluator confirmed the [Guide] includes sufficient instructions to modify the EraseMaster credential and invoke the RevertSP command. Modifying the EraseMaster credential will erase user data in an LBA range by cryptographic means: changing the Media encryption key (MEK). BandMaster PIN is also reset. Executing the RevertSP command will cause the drive to enter an uninitialized state.

Option C: The evaluator shall examine the operational guidance to ensure that it describes how to initiate TOE firmware/software updates.

[Guide] section "Firmware Access Control and Firmware Trusted Update" provides instructions for initiating a TOE firmware update.

Option D: Default Authorization Factors: It may be the case that the TOE arrives with default authorization factors in place. If it does, then the selection in item D must be made so that there is a mechanism to change these authorization factors. The operational guidance shall describe the method by which the user changes these factors when they are taking ownership of the device. The TSS shall describe the default authorization factors that exist.

[Guide] describes putting a Seagate SED into its evaluated configuration in section "General Setup & Configuration." The configuration steps for each type of drive include changing PINs (that is, authorization factors) to take ownership of a drive. [ST] section 6.1 "Overview of TOE Operations" identifies applicable PINs (search for "For TCG Enterprise there are four authentication PINs needed in order to gain access to all" and "For TCG Opal there are five authentication PINs needed in order to gain access to all" and "In addition, for ATA security mode, there are also").

Disable Key Recovery: The guidance for disabling this capability shall be described in the AGD documentation.

Neither [ST] nor [Guide] identify a key recovery mechanism for Seagate SEDs. Thus, this assurance activity is not applicable.

2.3.1.4 KMD Assurance Activities

Option D: If the TOE offers the functionality to import an encrypted DEK, the evaluator shall ensure the KMD describes how the TOE imports a wrapped DEK and performs the decryption of the wrapped DEK.

Seagate SEDs do not offer functionality to import an encrypted DEK. Thus, this assurance activity is not applicable.

2.3.1.5 Test Assurance Activities

Option A and B: The evaluator shall verify that the TOE has the functionality to change and cryptographically erase the DEK (effectively removing the ability to retrieve previous user data).

This testing was performed in conjunction with FCS_CKM.4(c) and FDP_DSK_EXT.1.

Option C: The evaluator shall verify that the TOE has the functionality to initiate TOE firmware/software updates.

This testing was performed in conjunction with FPT_TUD_EXT.1.

Option D: If additional management functions are claimed, the evaluator shall verify that the additional features function as described.

The evaluator authenticated to the TOE, changed the authentication PIN and successfully toggled the firmware download port. The evaluator then attempted to toggle the firmware download port without authenticating, which was denied by the TOE. For TCG Opal, the evaluator authenticated and successfully configured the authentication try limit. For TCG Enterprise, the evaluator authenticated and attempted to configure the authentication try limit, which is not supported and denied by the TOE.

2.4 Protection of the TSF (FPT)

2.4.1 FPT_FAC_EXT.1 Firmware Access Control

FPT_FAC_EXT.1 is an optional requirement.

2.4.1.1 Application Notes

Before an update takes place, the drive owner will authorize the update by providing either a known unique value (for example, a serial number) that is printed on the drive, a password (which should be administratively configurable as defined in FMT_SMF.1) or perform the operation as a privileged user. It is assumed that physical presence to the drive is limited to authorized personnel. If the correct value is not provided, the update will not take place. The values are intended to be unique per drive so they cannot be easily exhausted.

The same requirements for cleaning up a password still apply.

2.4.1.2 TSS Assurance Activities

The evaluator shall examine the TSS to ensure that it describes information stating how the Access Control process takes place along with a description of the values that are used.

In the evaluated configuration, a Seagate SED's download port is locked. [ST] section 6.5.1 "Firmware Access Control and Update Authentication (FPT_FAC_EXT.1, FPT_FUA_EXT.1)" explains a drive requires an administrator to authenticate with the drive's SID in order to unlock firmware download (search for "requires the administrator to unlock the firmware download port").

2.4.1.3 Guidance Assurance Activities

The evaluator ensures that the Operational Guidance describes how the user will be expected to interact with the authorization process.

[Guide] section “Firmware Access Control and Firmware Trusted Update” describes the authorization process (search for “Authenticate with SID credential (password).”).

2.4.1.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.4.1.5 Test Assurance Activities

The evaluator shall perform the following test.

Test 1: *The evaluator shall try installing a firmware upgrade and verify that a prompt is required and the appropriate value is necessary for the update to continue.*

The evaluator authenticated to the TOE and confirmed that the firmware upgrade was rejected as the firmware download port is locked. The evaluator then unlocked the firmware download port and attempted to upgrade the TOE. The evaluator confirmed that this attempt was successful.

2.4.2 FPT_FUA_EXT.1 Firmware Update Authentication

FPT_FUA_EXT.1 is a selection-based requirement.

2.4.2.1 Application Notes

FPT_FUA_EXT.1.1 to 1.3

The firmware portion of TSF (e.g., RTU (key store and the signature verification algorithm)) shall be stored in a write protected area on the TOE. The firmware shall only be modifiable in a post-manufacturing state using the authenticated update mechanism described in FPT_FUA_EXT.1. The TSF is modifiable only by using the mechanisms specified in FPT_TUD_EXT.

FPT_FUA_EXT.1.4

These requirements are for a SED in an operational state – not a drive in manufacturing.

The authenticated firmware update mechanism employs digital signatures to ensure the authenticity of the firmware update image. The TSF provides a RTU that contains a signature verification algorithm and a key store that includes the public key needed to verify the signature on the update image. The key store in the RTU shall include a public key used to verify the signature on an update image or a hash of the public key if a copy of the public key is provided with the update image. In the latter case, the update mechanism shall hash the public key provided with the update image, and ensure that it matches a hash which appears in the key store before using the provided public key to verify the signature on the update image. If the hash of the public key is selected, the ST author may iterate the FCS_COP.1(b) requirement - to specify the hashing functions used.

The intent of this requirement is to specify that the authenticated update mechanism shall ensure that the new image has been digitally signed; and that the digital signature can be verified by using a public key before the update takes place. The requirement also specifies that the authenticated update mechanism only allows installation of updates when the digital signature has been successfully verified by the TSF.

2.4.2.2 TSS Assurance Activities

The evaluator shall examine the TSS to ensure that it describes how the TOE uses the RTU, what type of key or hash value, and where the value is stored on the RTU. The evaluator shall also verify that the TSS contains a description (storage location) of where the original firmware exists.

[ST] section 6.5.1 "Firmware Access Control and Update Authentication (FPT_FAC_EXT.1, FPT_FUA_EXT.1)" describes the firmware download and installation process. The description covers:

- Firmware validation in volatile memory (DRAM)
- Firmware validation using a 2048-bit public key for Seagate,
- Storage of the Seagate public key in ROM,
- Error exit if firmware validation fails,
- Storage of firmware in flash memory if validation succeeds, and
- Locking download port either by explicit command from administrator or by power-on reset.

[ST] section 6.2.3 "Cryptographic Operation (FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(f))" adds that Seagate SEDs store the signature validation firmware routines in ROM (search for "using FW routines and the public key in ROM").

2.4.2.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.4.2.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.4.2.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.4.3 FPT_KYP_EXT.1 Protection of Key and Key Material

FPT_KYP_EXT.1 is an unconditional requirement.

2.4.3.1 Application Notes

The plaintext key storage in non-volatile memory is allowed for several reasons. If the keys exist within protected memory that is not user accessible on the TOE or OE, the only methods that allow it to play a security relevant role for protecting the BEV or the DEK are if it is a key split or providing additional layers of wrapping or encryption on keys that have already been protected.

When stored in non-volatile memory (even in protected storage), the DEK is always encrypted (wrapped) and only exists in plaintext form in volatile memory, when it is being used to encrypt or decrypt data. Provisioning keys may exist in plaintext form in non-volatile memory before provisioning by the drive owner.

If the TOE does not store keys in non-volatile memory, a statement in the TSS stating that keys are never stored in non-volatile memory is all that is required and no evaluation activity needs to be performed.

This requirement is addressing the keys related to the encryption of user data – specifically keys from within the key chain.

2.4.3.2 TSS Assurance Activities

Modified by TD0458

The evaluator shall examine the TSS and verify it identifies the methods used to protect keys stored in non-volatile memory.

[ST] section 6.5.2 “Protection of Key and Key Material (FPT_KYP_EXT.1)” states “Intermediate keys are not generated using submask combining.” Rather Seagate SEDs store keys in non-volatile memory using AES-GCM and AES-KW key wrapping.

2.4.3.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.4.3.4 KMD Assurance Activities

Modified by TD0458

The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in non-volatile memory. The description of the key chain shall be reviewed to ensure the selected method is followed for the storage of wrapped or encrypted keys in non-volatile memory and plaintext keys in non-volatile memory meet one of the criteria for storage.

[ST] section 6.5.2 “Protection of Key and Key Material (FPT_KYP_EXT.1)” explains Seagate SEDs store keys in non-volatile memory using AES-GCM and AES-KW key wrapping. Please see section 2.1.13 above for assurance activity results regarding key wrapping.

2.4.3.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.4.4 FPT_PWR_EXT.1 Power Saving States

FPT_PWR_EXT.1 is an unconditional requirement.

2.4.4.1 Application Notes

Power saving states S3, S4, G2(S5), G3, D1, D2, D3 are defined by the Advanced Configuration and Power Interface (ACPI) standard.

2.4.4.2 TSS Assurance Activities

Modified per TD0464

The evaluator shall validate the TSS contains a list of Compliant power saving states.

[ST] section "6.5.3 Power Saving States and Timing (FPT_PWR_EXT.1, FPT_PWR_EXT.2)" states "The TOE supports a single Compliant power state of device full off (D3)".

2.4.4.3 Guidance Assurance Activities

Modified per TD0460

Modified per TD0464

The evaluator shall ensure that guidance documentation contains a list of Compliant power saving states.

[Guide] section "Power Saving States and Timing of Power Saving States" identifies that the TOE supports a single Compliant power state of device full off (D3). The TOE SEDs have two possible transitions: power off to on; and on to off. Only the transition from on to off applies to this requirement. The device changes to off when the system removes power to the drive. This can happen immediately or when the user initiates a system shutdown request. After power is removed, it takes approximately 2 seconds for DRAM volatile memory and about 30 mS for SRAM volatile memory to completely power down.

Modified per TD0460

Modified per TD0464

If additional power saving states are supported, then the evaluator shall validate that the guidance documentation states how the use of non-Compliant power saving states are disabled.

Seagate SEDs do not support any additional power saving states. Thus, this assurance activity is not applicable.

2.4.4.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.4.4.5 Test Assurance Activities

The evaluator shall confirm that for each listed Compliant state all key/key materials are removed from volatile memory by using the test defined in FCS_CKM.4(b).

N/A—The TOE does not support any Compliant power saving states. The TOE only supports 2 power states; *Fully On* and *Off*.

2.4.5 FPT_PWR_EXT.2 Timing of Power Saving States

FPT_PWR_EXT.2 is an unconditional requirement.

2.4.5.1 Application Notes

If volatile memory is not cleared as part of an unexpected power shutdown sequence then guidance documentation must define mitigation activities (e.g. how long users should wait after an unexpected power-down before volatile memory can be considered cleared).

2.4.5.2 TSS Assurance Activities

The evaluator shall validate that the TSS contains a list of conditions under which the TOE enters a Compliant power saving state.

[ST] section "6.5.3 Power Saving States and Timing (FPT_PWR_EXT.1, FPT_PWR_EXT.2)" states "The device changes to off when the system removes power to the drive."

2.4.5.3 Guidance Assurance Activities

The evaluator shall check that the guidance contains a list of conditions under which the TOE enters a Compliant power saving state.

[Guide] section "Power Saving States and Timing of Power Saving States" explains "The device changes to off when the system removes power to the drive."

Additionally, the evaluator shall verify that the guidance documentation provides information on how long it is expected to take for the TOE to fully transition into the Compliant power saving state (e.g. how many seconds for the volatile memory to be completely cleared).

[Guide] section "Power Saving States and Timing of Power Saving States" states, "After power is removed, it takes approximately 2 seconds for DRAM volatile memory and about 30 ms for SRAM volatile memory to completely power down."

2.4.5.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.4.5.5 Test Assurance Activities

The evaluator shall trigger each condition in the list of identified conditions and ensure the TOE ends up in a Complaint power saving state by running the test identified in FCS_CKM.4(b).

N/A—The TOE does not support any Compliant power saving states. The TOE only supports 2 power states; *Fully On* and *Off*.

2.4.6 FPT_RBP_EXT.1 Rollback Protection

FPT_RBP_EXT.1 is an optional requirement.

2.4.6.1 Application Notes

This requirement prevents an unauthorized rollback of the firmware to an earlier authentic version. This mitigates against unknowing installation of an earlier authentic firmware version that may have a security weakness. It is expected that vendors will increase security version numbers with each new update package.

For FPT_RBP_EXT.1.1 the purpose is to verify that the new package has a security version number equal to or larger than the security version number of currently installed firmware package.

The administrator guidance would include instructions for the administrator to configure the rollback prevention mechanism, if appropriate.

2.4.6.2 TSS Assurance Activities

The evaluator shall examine the TSS to ensure that it describes at a high level the process for verifying that security version checking is performed before an upgrade is installed.

[ST] section 6.5.4 “RollBack Protection (FPT_RBP_EXT.1)” describes in general terms an internal block point mechanism that Seagate SEDs use to prevent downgrading to a lower security version number.

The evaluator shall verify that a high level description of the types of error codes are provided and when an error would be triggered.

[ST] section 6.5.4 “RollBack Protection (FPT_RBP_EXT.1)” explains Seagate SEDs reject firmware with a lower security version number and return an error code. Section 6.5.4 includes error codes and messages.

2.4.6.3 Guidance Assurance Activities

The evaluator ensures that a description is provided on how the user should interpret the error codes.

[Guide] section “Firmware Rollback Protection” identifies the rollback error codes and provides messages explaining the errors.

2.4.6.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.4.6.5 Test Assurance Activities

The evaluator shall perform the following test:

Test 1: *The evaluator shall try installing a lower security version number upgrade (either by just*

modifying the version number or by using an upgrade provided by the vendor) and will verify that the lower version cannot be installed and an error is presented to the user.

The evaluator queried the current version of TOE firmware. The evaluator then attempted to upgrade the TOE to an earlier version of the firmware. The attempted was denied by the TOE and an error was presented. The evaluator then queried the firmware version of the TOE and confirmed it remained unchanged.

2.4.7 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1 is an unconditional requirement.

2.4.7.1 Application Notes

The tests regarding cryptographic functions implemented in the TOE can be deferred, as long as the tests are performed before the function is invoked.

If FCS_RBG_EXT.1 is implemented by the TOE and according to NIST SP 800-90, the evaluator shall verify that the TSS describes health tests that are consistent with section 11.3 of NIST SP 800-90.

If any FCS_COP functions are implemented by the TOE, the TSS shall describe the known-answer self-tests for those functions.

The evaluator is expected to verify that the TSS describes, for some set of non-cryptographic functions affecting the correct operation of the TSF, the method by which those functions are tested. The TSS will describe, for each of these functions, the method by which correct operation of the function/component is verified. The evaluator should determine that all of the identified functions/components are adequately tested on start-up.

2.4.7.2 TSS Assurance Activities

The evaluator shall verify that the TSS describes the known-answer self-tests for cryptographic functions.

[ST] section 6.5.5 “TST Testing (FPT_TST_EXT.1)” identifies the power-on and continuous self-test for Seagate SED cryptographic functions.

The evaluator shall verify that the TSS describes, for some set of non-cryptographic functions affecting the correct operation of the TOE and the method by which the TOE tests those functions. The evaluator shall verify that the TSS includes each of these functions, the method by which the TOE verifies the correct operation of the function.

[ST] section 6.5.5 “TST Testing (FPT_TST_EXT.1)” describes firmware load check and secure boot process, which validate drive firmware at download and at drive power-on, respectively. Please see sections 2.1.10 and 2.4.2 above for review of the firmware download and power-on function tests.

The evaluator shall verify that the TSF data are appropriate for TSF Testing. For example, more than blocks are tested for AES in CBC mode, output of AES in GCM mode is tested without truncation, or 512-bit key is used for testing HMAC-SHA-512.

The test assurance activities in the following sections of this report ensure the TSF data is suitable for testing.

- 2.1.10 FCS_COP.1(a) Cryptographic Operation (Signature Verification)
- 2.1.11 FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)
- 2.1.12 FCS_COP.1(c) Cryptographic Operation (Message Authentication)
- 2.1.13 FCS_COP.1(d) Cryptographic Operation (Key Wrapping)
- 2.1.14 FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)
- 2.1.17 FCS_RBG_EXT.1 Random Bit Generation

If FCS_RBG_EXT.1 is implemented by the TOE and according to NIST SP 800-90, the evaluator shall verify that the TSS describes health tests that are consistent with section 11.3 of NIST SP 800-90.

[ST] section 6.5.5 "TST Testing (FPT_TST_EXT.1)" describes tests Firmware 800-90 DRBG (CRNGT) and Firmware 800-90 DRBG Entropy (CRNGT) in addition to Firmware 800-90 DRBG KAT (search for "Health test as described above").

If any FCS_COP functions are implemented by the TOE, the TSS shall describe the known-answer self-tests for those functions.

[ST] section 6.5.5 "TST Testing (FPT_TST_EXT.1)" identifies the power-on and continuous self-test for Seagate SED cryptographic functions.

The evaluator shall verify that the TSS describes, for some set of non-cryptographic functions affecting the correct operation of the TSF, the method by which those functions are tested. The TSS will describe, for each of these functions, the method by which correct operation of the function/component is verified. The evaluator shall determine that all of the identified functions/components are adequately tested on start-up.

[ST] section 6.5.5 "TST Testing (FPT_TST_EXT.1)" describes firmware load check and secure boot process, which validate drive firmware at download and at drive power-on, respectively. Please see sections 2.1.10 and 2.4.2 above for review of the firmware download and power-on function tests.

2.4.7.3 Guidance Assurance Activities

There are no AGD evaluation activities for this SFR.

2.4.7.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.4.7.5 Test Assurance Activities

There are no test evaluation activities for this SFR.

2.4.8 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1 is an unconditional requirement.

2.4.8.1 Application Notes

“Authorized users” refers to an individual who has rightful physical possession of the device.

The digital signature mechanism referenced in the third element is the one specified in FCS_COP.1(a) in Appendix A. While this component requires the TOE to implement the update functionality itself, it is acceptable to perform the cryptographic checks using functionality available in the Operational Environment.

If the TOE is a software product, the ST author selects ‘digital signature’. If the TOE is a hardware product, the ST author selects ‘authenticated firmware update mechanism as described in FPT_FUA_EXT.1’.

The secure firmware update mechanism is used for verifying the authenticity and integrity of the new update package and for ensuring that it is protected from modification outside of the secure update process. The authenticated firmware update mechanism shall be protected from unintended or malicious modification by a mechanism that is at least as strong as that protecting the RTU and the firmware.

The intent of this requirement is to ensure that an authenticated firmware update mechanism will be provided. Authentication verifies that the firmware package was generated by an authentic source and is unaltered. All updates to the existing firmware shall go through an authenticated update mechanism as described in FPT_FUA_EXT.1.

2.4.8.2 TSS Assurance Activities

The evaluator shall examine the TSS to ensure that it describes information stating that an authorized source signs TOE updates and will have an associated digital signature.

[ST] section 6.5.1 “Firmware Access Control and Update Authentication (FPT_FAC_EXT.1, FPT_FUA_EXT.1)” indicates Seagate digitally signs all firmware updates with an RSA key corresponding to an RSA public key stored in drive ROM.

The evaluator shall examine the TSS contains a definition of an authorized source along with a description of how the TOE uses public keys for the update verification mechanism in the Operational Environment.

[ST] section 6.5.1 “Firmware Access Control and Update Authentication (FPT_FAC_EXT.1, FPT_FUA_EXT.1)” identifies Seagate as the authorized source of firmware updates (search for “the authorized source that signs TOE updates is Seagate”).

The evaluator ensures the TSS contains details on the protection and maintenance of the TOE update credentials.

[ST] section 6.5.1 “Firmware Access Control and Update Authentication (FPT_FAC_EXT.1, FPT_FUA_EXT.1)” indicates Seagate digitally signs all firmware updates with an RSA key corresponding to an RSA public key stored in drive ROM.

If the Operational Environment performs the signature verification, then the evaluator shall examine the TSS to ensure it describes, for each platform identified in the ST, the interface(s) used by the TOE to invoke this cryptographic functionality.

The TOE verifies digital signatures of firmware updates. Thus, this assurance activity is not applicable.

2.4.8.3 Guidance Assurance Activities

The evaluator ensures that the operational guidance describes how the TOE obtains vendor updates to the TOE ….

[Guide] section "Firmware Access Control and Firmware Trusted Update" describes obtaining a signed firmware update package from Seagate and gives the URL https://www.seagate.com/support-home.

The evaluator ensures that the operational guidance describes … the processing associated with verifying the digital signature of the updates (as defined in FCS_COP.1(a)) ...

[Guide] section "Firmware Access Control and Firmware Trusted Update" covers signature verification (search for "4. The signature is verified using PKCS #1, v1.5 RSA signature algorithm and public key in ROM.").

The evaluator ensures that the operational guidance describes … the actions that take place for successful and unsuccessful cases.

[Guide] section "Firmware Access Control and Firmware Trusted Update" describes Seagate SED behavior in both the successful (update installed) and unsuccessful (error code returned) cases.

2.4.8.4 KMD Assurance Activities

There are no KMD evaluation activities for this SFR.

2.4.8.5 Test Assurance Activities

The evaluators shall perform the following tests (if the TOE supports multiple signatures, each using a different hash algorithm, then the evaluator performs tests for different combinations of authentic and unauthentic digital signatures and hashes, as well as for digital signature alone):

Test 1: *The evaluator performs the version verification activity to determine the current version of the TOE. After the update tests described in the following tests, the evaluator performs this activity again to verify that the version correctly corresponds to that of the update.*

The evaluator combined tests 1 and 2. See test 2 below.

Test 2: *The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that an update successfully installs on the TOE. The evaluator shall perform a subset of other evaluation activity tests to demonstrate that the update functions as expected.*

The evaluator queried the current version of the TOE firmware. The evaluator then obtained an unsigned TOE firmware update and attempted to upgrade the TOE. The TOE rejected the update and the evaluator queried the TOE firmware version again and confirmed it went unchanged. The evaluator acquired a valid, signed update and attempted to upgrade the TOE. The evaluator confirmed that the TOE accepted the update and updated successfully via querying the firmware version and observing the increased TOE firmware version increased.

3 SECURITY ASSURANCE REQUIREMENTS

3.1 Development (ADV)

3.1.1 ADV_FSP.1 Basic Functional Specification

The EAs for this assurance component focus on understanding the interfaces (e.g., application programing interfaces, command line interfaces, graphical user interfaces, network interfaces) described in the AGD documentation, and possibly identified in the TOE Summary Specification (TSS) in response to the SFRs. Specific evaluator actions to be performed against this documentation are identified (where relevant) for each SFR in Section 2 (Evaluation Activities for SFRs), and in EAs for AGD, ATE and AVA SARs in other parts of Section 5.

The EAs presented in this section address the CEM work units ADV_FSP.1-1, ADV_FSP.1-2, ADV_FSP.1-3, and ADV_FSP.1-5.

The EAs are reworded for clarity and interpret the CEM work units such that they will result in more objective and repeatable actions by the evaluator. The EAs in this SD are intended to ensure the evaluators are consistently performing equivalent actions.

The documents to be examined for this assurance component in an evaluation are therefore the Security Target, AGD documentation, and any required supplementary information required by the cPP: no additional "functional specification" documentation is necessary to satisfy the EAs. The interfaces that need to be evaluated are also identified by reference to the EAs listed for each SFR, and are expected to be identified in the context of the Security Target, AGD documentation, and any required supplementary information defined in the cPP rather than as a separate list specifically for the purposes of CC evaluation. The direct identification of documentation requirements and their assessment as part of the EAs for each SFR also means that the tracing required in ADV_FSP.1.2D (work units ADV_FSP.1-4, ADV_FSP.1-6 and ADV_FSP.1-7 is treated as implicit and no separate mapping information is required for this element.

Table 10 SD Table 1: Mapping of ADV_FSP.1 CEM Work Units to Evaluation Activities

CEM ADV_FSP.1 Work Units	Evaluation Activities
ADV_FSP.1-1 The evaluator ***shall examine*** the functional specification to determine that it states the purpose of each SFR-supporting and SFR-enforcing TSFI.	5.2.1.1 Evaluation Activity: *The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.*

ADV_FSP.1-2 The evaluator ***shall examine*** the functional specification to determine that the method of use for each SFR-supporting and SFR-enforcing TSFI is given.	5.2.1.1 Evaluation Activity: *The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.*
ADV_FSP.1-3 The evaluator ***shall examine*** the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing and SFR supporting TSFI.	5.2.1.2 Evaluation Activity: *The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.*
ADV_FSP.1-4 The evaluator ***shall examine*** the rationale provided by the developer for the implicit categorisation of interfaces as SFR-non-interfering to determine that it is accurate.	Paragraph 561 from the CEM: "In the case where the developer has provided adequate documentation to perform the analysis called for by the rest of the work units for this component without explicitly identifying SFR-enforcing and SFR-supporting interfaces, this work unit should be considered satisfied." Since the rest of the ADV_FSP.1 work units will have been satisfied upon completion of the EAs, it follows that this work unit is satisfied as well.
ADV_FSP.1-5 The evaluator ***shall check*** that the tracing links the SFRs to the corresponding TSFIs.	5.2.1.3 Evaluation Activity: The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.
ADV_FSP.1-6 The evaluator ***shall examine*** the functional specification to determine that it is a complete instantiation of the SFRs.	EAs that are associated with the SFRs in Section 2, and, if applicable, Sections 3 and 4, are performed to ensure that all the SFRs where the security functionality is externally visible (i.e., at the TSFI) are covered. Therefore, the intent of this work unit is covered.
ADV_FSP.1-7 The evaluator ***shall examine*** the functional specification to determine that it is an accurate instantiation of the SFRs.	EAs that are associated with the SFRs in Section 2, and, if applicable, Sections 3 and 4, are performed to ensure that all the SFRs where the security functionality is externally visible (i.e., at the TSFI) are addressed, and that the description of the interfaces is accurate with respect to the specification captured in the SFRs. Therefore, the intent of this work unit is covered.

3.1.1.1 Supporting Document 5.2.1.1 Evaluation Activity

The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant. In this context, TSFI are deemed security relevant if they are used by the administrator to configure the TOE, or to perform other administrative functions (e.g., audit review or performing updates). Additionally, those interfaces that are identified in the ST, or guidance documentation, as adhering to

the security policies (as presented in the SFRs), are also considered security relevant. The intent, is that these interfaces will be adequately tested, and having an understanding of how these interfaces are used in the TOE is necessary to ensure proper test coverage is applied.

The set of TSFI that are provided as evaluation evidence are contained in the Administrative Guidance and User Guidance.

The TOE is a set of Seagate self-encrypting drives. As described in [ST], an end user interacts with the TOE through a TCG host controller. Seagate SEDs implement TCG Enterprise Security Subsystem Class (SSC), TCG Opal SSC, and ATA Security specifications. These specifications determine TOE behavior including the interfaces each Seagate SED presents to host controllers.

[Guide] identifies TCG methods and ATA Security commands relevant to the TSF. In particular, [Guide] section "Setup and Configuration" describes the steps necessary to put a Seagate SED into the evaluated configuration. Each step includes examples to illustrate interactions between a host controller and a SED. The examples are based on Seagate TCG and ATA Security libraries. A host controller developer would adapt the examples to the developer's own libraries.

TCG SSCs and ATA Security have mature, widely used, well documented specifications. Please see section 1.3 above. Briefly, [TCG Core] specifies aspects TCG Storage common to all SSCs. The specification covers device architecture (components and core operations) and architectural elements (data structures, interface communication, and security provider (SP) operation descriptions) as well an SP reference. [TCG SIIS] provides a mapping between concepts and features of [TCG Core] and ATA and SCSI interfaces. [TCG Ent] specializes [TCG Core] for enterprise-class use cases. Similarly, [TCG Opal] specializes [TCG Core] for storage devices built to protect the confidentiality of stored user data against unauthorized access once a device leaves the owner's control. [TCG SUDR] defines Single User Mode for the Opal SSC. [ATA-8 ACS2] specifies the AT Attachment command set used to communicate between host systems and storage devices, which includes ATA security commands.

The evaluator used [ST] and [Guide] to identify TCG methods and ATA Security commands relevant to each TOE security function. [ST] section 6.2.2 "Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c)(1) HDD, FCS_CKM.4(c)(2) SSH and Hybrid FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)" provides convenient labels for most TOE security functions. Examples in [Guide] section "TCG Enterprise Setup & Configuration" show additional configuration functions. [Guide] tables 4.1 through 4.6 contain security service names along with TCG methods and ATA Security comments for TOE security functions. Table 11 summarizes the correspondence between SFRs and externally visible security functions. Table 12, Table 13, and Table 14 trace each security function through TCG methods and ATA Security commands to applicable descriptions in TCG Storage and ATA Security specifications. The evaluation team used the mappings to confirm [Guide] and the public specifications adequately document the purpose and method of use for each TOE security function interface.

Table 11 Mapping from SFR to Security Functions

SFR	Security Function
FCS_CKM.1(b)	No external interface
FCS_CKM.1(c)	No external interface
FCS_CKM.4(a)	Device full off

SFR	Security Function
FCS_CKM.4(b)	No external interface
FCS_CKM.4(1)(c) HDD	No external interface
FCS_CKM.4(2)(c) SDD and Hybrid	No external interface
FCS_CKM.4(e)	No external interface
FCS_CKM_EXT.4(a)	No external interface
FCS_CKM_EXT.4(b)	Device full off
FCS_CKM_EXT.6	Take Ownership
FCS_CKM_EXT.6	Change PIN
FCS_CKM_EXT.6	EraseMaster
FCS_CKM_EXT.6	Revert SP
FCS_CKM_EXT.6	Lock Band
FCS_CKM_EXT.6	Unlock Band
FCS_COP.1(a)	No external interface
FCS_COP.1(b)	No external interface
FCS_COP.1(c)	No external interface
FCS_COP.1(d)	No external interface
FCS_COP.1(f)	No external interface
FCS_KDF_EXT.1	Verify PIN
FCS_KYC_EXT.2	Verify PIN
FCS_RBG_EXT.1	No external interface
FCS_SNI_EXT.1	No external interface
FCS_VAL_EXT.1(a)	Verify PIN
FCS_VAL_EXT.1(b)	Verify PIN
FDP_DSK_EXT.1	Read/Write data
FMT_SMF.1	EraseMaster
FMT_SMF.1	RevertSP
FMT_SMF.1	FW Download
FMT_SMF.1	Set PIN (FW Download)
FMT_SMF.1	Set Try Limit
FPT_FAC_EXT.1	Authenticate (FW Download)
FPT_FUA_EXT.1	FW Download
FPT_KYP_EXT.1	No external interface
FPT_PWR_EXT.1	No external interface
FPT_PWR_EXT.2	Device full off
FPT_RBP_EXT.1	FW Download
FPT_TST_EXT.1	Power-on Reset

SFR	Security Function
FPT_TUD_EXT.1	Query Firmware Version
FPT_TUD_EXT.1	FW Download

Table 12 Mapping from Security Function to TCG Enterprise SSC Interface Specification

Security Function	Security Service	Example Step	Interface	Specification	Section
Change PIN	Set PIN	2	TCG Set	[TCG Core]	5.3.3.7 Basic Table Method Group - Set (Table and Object Method)
				[TCG Core]	5.3.4.2 Table Management
				[TCG Ent]	10.3.3.2 Set
Disable Authority	See example	6	TCG Set	See above	See Change PIN
				[TCG Core]	5.3.2.10 Access Control Metadata Group - Authority (Object Table)
				[TCG Ent]	11.3.1 Authorities & Credentials
Erase Band	Cryptographic Erase	N/A	TCG Erase	[TCG Ent]	10.5.4.1 Erase
FW Download	Firmware Download	N/A	TCG Set	See above	See Change PIN
			SCSI Write Buffer	[TCG SIIS]	3 SCSI Interface
FW Download (Port Lock/Unlock)	See "Firmware Access Control and Firmware Trusted Update"	10	TCG Set	See above	See Change PIN Note: Firmware Download Port is a Seagate-defined port. See sections “TCG Enterprise Setup & Configuration” and “Firmware Access Control and Firmware Trusted Update”.
FW Download (Set Lock on Reset)	See example	9	TCG Set	See above	See Change PIN Note: Firmware Download Port is a Seagate-defined port. See sections “TCG Enterprise Setup & Configuration” and “Firmware Access Control and Firmware Trusted Update”.
FW Download (Authenticate)	See example	1	TCG Authenticate	[TCG Core]	5.3.3.12 Access Control Method Group - Authenticate (SP Method)
				[TCG Core]	5.3.4.1 Authentication
				[TCG Ent]	11.2.2 Authenticate Method Deviations
Get Object	See example	1, 2, 4	TCG Get	[TCG Core]	5.3.3.6 Basic Table Method Group - Get (Table and

Security Function	Security Service	Example Step	Interface	Specification	Section
					Object Method)
				[TCG Core]	5.3.4.2 Table Management
				[TCG Ent]	10.3.3.1 Get
Lock Band	Lock / Unlock User Data Range for Read and/or Write	N/A	TCG Set	See above	See Change PIN
				[TCG Core]	5.7 Locking Template
				[TCG Ent]	11.4.5 Locking Objects Definition
				[TCG Ent]	11.4.10 Device Behavior Under Locking
Query Firmware Version	See "Firmware Access Control and Firmware Trusted Update"	N/A	SAS Inquiry	[TCG SIIS]	3 SCSI Interface
			SATA Identify	[TCG SIIS]	4 ATA Interface
			Ditto	[ATA-8 ACS2]	7.17 IDENTIFY DEVICE - ECh, PIO Data-In
Read/Write data	User Data Read / Write	N/A	SCSI Read	[TCG SIIS]	3 SCSI Interface
			SCSI Write	[TCG SIIS]	3 SCSI Interface
				[TCG Core]	5.7.2.2 Locking (Object Table)
				[TCG Core]	5.7.3.2 Reading/Writing User Data
				[TCG Ent]	11.4.5.1 Locking Objects Deviations
				[TCG Ent]	11.4.10 Device Behavior Under Locking
Revert SP	Exit CC Security Mode	N/A	TCG RevertSP	[TCG Opal]	5.2.2 Revert – Admin Template SP Object Method See note in [Guide] Table 4.6
Set Minimum PIN Length	See example	4, 9	TCG Set	See above	See also [Guide] section TCG Enterprise Setup & Configuration
Set PIN (Setup)	Set PIN	2, 3, 5	TCG Set	See above	See Change PIN

Security Function	Security Service	Example Step	Interface	Specification	Section
Set PIN (FW Download)	See "Firmware Access Control and Firmware Trusted Update"	2	TCG Set	See above	See Change PIN
Take Ownership	See "Protection of Data on Disk & Specification of Management Functions"	1	TCG Authenticate	See above	See Firmware (Authenticate)
				[TCG Ent]	2 Overview
				[TCG Ent]	12.1 Use of MSID
Transition to TCG Security	See "Protection of Data on Disk & Specification of Management Functions"	1	TCG Authenticate	See above	See Take Ownership
Unlock Band	Lock / Unlock User Data Range for Read and/or Write	N/A	TCG Set	See above	See Lock Band
Verify PIN	See example	1	TCG Authenticate	See above	See Firmware (Authenticate)

Table 13 Mapping from Security Function to TCG Opal SSC Interface Specification

Security Function	Security Service	Example Step	Interface	Specification	Section
Change PIN	Set PIN	2	TCG Set	[TCG Core]	5.3.3.7 Basic Table Method Group - Set (Table and Object Method)
				[TCG Core]	5.3.4.2 Table Management
				[TCG Opal]	4.2.4 Admin Template Methods
				[TCG Opal]	4.3.6 Locking Template Methods

Disable Authority	See example	7	TCG Set	See above	See Change PIN
				[TCG Core]	5.3.2.10 Access Control Metadata Group - Authority (Object Table)
				[TCG Opal]	4.2.1.7 Authority (M)
Erase Band (non-SUDR)	Cryptographic Erase	N/A	TCG GenKey	[TCG Core]	5.3.3.16 Key Related Method Group - GenKey (Object Method)
				[TCG Opal]	4.3.1.5 MethodID (M)
Erase Band (SUDR Locking SP Admins)	Cryptographic Erase	N/A	TCG Erase	[TCG SUDR]	3.1.1.2 Erase
				[TCG SUDR]	2 Single User Mode Overview
Erase Band (SUDR Users)	Cryptographic Erase	N/A	TCG GenKey	See above	See Erase Band: Cryptographic Erase of SUDR Locking SP Admin1-4
FW Download	Load complete firmware image	N/A	ATA DOWNLOAD MICROCODE	[TCG Opal]	5.1.4 Examples
				[TCG SIIS]	4 ATA Interface
				[ATA-8 ACS2]	7.12 DOWNLOAD MICROCODE - 92h, PIO Data-Out/Non-Data
FW Download (Port Lock/Unlock)	See "Firmware Access Control and Firmware Trusted Update"	9	TCG Set	See above	See Change PIN Note: Firmware Download Port is a Seagate-defined port. See sections “TCG Enterprise Setup & Configuration” and “Firmware Access Control and Firmware Trusted Update”.
FW Download (Set Lock on Reset)	See example	8	TCG Set	See above	See Change PIN Note: Firmware Download Port is a Seagate-defined port. See sections “TCG Enterprise Setup & Configuration” and “Firmware Access Control and Firmware Trusted Update”.
FW Download (Authenticate)	See example	2	TCG Authenticate	[TCG Core]	5.3.3.12 Access Control Method Group - Authenticate (SP Method)
				[TCG Core]	5.3.4.1 Authentication
				[TCG Opal]	4.2.4 Admin Template Methods
				[TCG Opal]	4.3.6 Locking Template Methods

Get Object	See example	5, 6	TCG Get	[TCG Core]	5.3.3.6 Basic Table Method Group - Get (Table and Object Method)
				[TCG Core]	5.3.4.2 Table Management
				[TCG Opal]	4.2.4 Admin Template Methods
				[TCG Opal]	4.3.6 Locking Template Methods
Lock Band	Lock / Unlock User Data Range for Read and/or Write	N/A	TCG Set	See above	See Change PIN
				[TCG Core]	5.7 Locking Template
				[TCG Opal]	4.3.5 Locking Template Tables
				[TCG Opal]	4.3.7 SD Read/Write Data Command Locking Behavior
Query Firmware Version	See "Firmware Access Control and Firmware Trusted Update"	N/A	SATA Identify	[TCG SIIS]	4 ATA Interface
				[ATA-8 ACS2]	7.17 IDENTIFY DEVICE - ECh, PIO Data-In
Read/Write data	User Data Read / Write	N/A	ATA Read	[TCG SIIS]	4 ATA Interface
			ATA Write	[TCG SIIS]	4 ATA Interface
				[TCG Core]	5.7.2.2 Locking (Object Table)
				[TCG Core]	5.7.3.2 Reading/Writing User Data
				[TCG Opal]	4.3.7 SD Read/Write Data Command Locking Behavior
Revert SP (Drive Owner)	Exit CC Security Mode	N/A	TCG Admin SP Revert Locking SP Object	[TCG Opal]	5.2.2 Revert – Admin Template SP Object Method
			TCG Admin SP Revert Admin SP Object	[TCG Opal]	5.2.2 Revert – Admin Template SP Object Method
Revert SP (Admin SP Admins)	Exit CC Security Mode	N/A	TCG Admin SP Revert Admin SP Object	[TCG Opal]	5.2.2 Revert – Admin Template SP Object Method
Revert SP (Locking SP Admins)	Exit CC Security Mode	N/A	TCG Locking SP RevertSP	[TCG Opal]	5.2.3 RevertSP – Base Template SP Method

				[TCG Opal]	4.2.4 Admin Template Methods
				[TCG Opal]	4.3.6 Locking Template Methods
Set Minimum PIN Length	See example	3	TCG Set	See above	See also [Guide] section TCG Opal Setup & Configuration
Set PIN (Setup)	Set PIN	2, 4, 6	TCG Set	See above	See Change PIN
Set PIN (FW Download)	See "Firmware Access Control and Firmware Trusted Update"	2	TCG Set	See above	See Change PIN
Set Try Limit	See “Validation - Try Limits and Persistence Settings” and “TCG Opal Setting Try Limits”	N/A	TCG Set	[TCG Core]	5.3.4.1.1.2 Authentication Attempt Limits with C_PIN Objects
				[TCG Core]	5.3.2.12 Credential Table Group - C_PIN (Object Table)
				[TCG Opal]	4.2.1.8 C_PIN (M)
				[TCG Opal]	4.3.1.9 C_PIN (M)
Take Ownership	See "Protection of Data on Disk & Specification of Management Functions"	1	TCG Activate	[TCG Opal]	5.2.1 Activate – Admin Template SP Object Method
				[TCG SUDR]	3.1.2.1 Activate
Transition to TCG Opal Security Mode	See "Protection of Data on Disk & Specification of Management Functions"	1	TCG Activate	See above	See Take Ownership
Unlock Band	Lock / Unlock User Data Range for Read and/or Write	N/A	TCG Set	See above	See Lock Band
Verify PIN	See example	2	TCG Authenticate	See above	See Firmware (Authenticate)

Table 14 Mapping from Security Function to TCG Opal SSC and ATA Security Interface Specifications

Security Function	Security Service	Example Step	Interface	Specification	Section
Change PIN	Set PIN	1, 2	ATA SECURITY SET Password	[ATA-8 ASC2]	7.47 SECURITY SET PASSWORD - F1h, PIO Data-Out
		N/A	TCG set	[TCG Core]	5.3.2.4 Locking SP Life Cycle Interactions with the ATA Security Feature Set
				[TCG Core]	5.3.4.2 Table Management
				[TCG Opal]	4.2.4 Admin Template Methods
				[TCG Opal]	4.3.6 Locking Template Methods
Disable Authority	See example	3	TCG Set	See above	See Change PIN
				[TCG Core]	5.3.2.10 Access Control Metadata Group - Authority (Object Table)
				[TCG Opal]	4.2.1.7 Authority (M)
Erase Band	Cryptographic Erase	N/A	ATA SECURITY ERASE PREPARE	[ATA-8 ASC2]	7.44 SECURITY ERASE PREPARE - F3h, Non-Data
			ATA SECURITY ERASE UNIT	[ATA-8 ASC2]	7.45 SECURITY ERASE UNIT - F4h, PIO Data-Out
FW Download	Load complete firmware image	N/A	ATA DOWNLOAD MICROCODE	[TCG Opal]	5.1.4 Examples
				[ATA-8 ACS2]	7.12 DOWNLOAD MICROCODE - 92h, PIO Data-Out/Non-Data
FW Download (Port Lock/Unlock)	See "Firmware Access Control and Firmware Trusted Update"	5	TCG Set	See above	See Change PIN
FW Download (Set Lock on Reset)	See example	4	TCG Set	See above	See Change PIN
FW Download (Authenticate)	See example	3	TCG Authenticate	[TCG Core]	5.3.3.12 Access Control Method Group - Authenticate (SP Method)
				[TCG Core]	5.3.4.1 Authentication
				[TCG Opal]	4.2.4 Admin Template Methods

Security Function	Security Service	Example Step	Interface	Specification	Section
				[TCG Opal]	4.3.6 Locking Template Methods
Get Object	See example	3, 4	TCG Get	[TCG Core]	5.3.3.6 Basic Table Method Group - Get (Table and Object Method)
				[TCG Core]	5.3.4.2 Table Management
				[TCG Opal]	4.2.4 Admin Template Methods
				[TCG Opal]	4.3.6 Locking Template Methods
Lock Band	Reset Module	N/A	Power-on reset	[ATA-8 ACS2]	4.20.2.2 User Password
Query Firmware Version	See "Firmware Access Control and Firmware Trusted Update"	N/A	SATA Identify	[ATA-8 ACS2]	7.17 IDENTIFY DEVICE - ECh, PIO Data-In
Read/Write data	User Data Read / Write	N/A	ATA READ commands	[ATA-8 ACS2]	7.24 READ BUFFER - E4h, PIO Data-In to 7.40 READ VERIFY SECTOR(S) EXT - 42h, Non-Data
		N/A	ATA WRITE Commands	[ATA-8 ACS2]	7.62 WRITE BUFFER - E8h, PIO Data-Out to 7.75 WRITE STREAM DMA EXT - 3Ah, DMA
Revert SP	Exit CC Security Mode	N/A	ATA SECURITY ERASE PREPARE	[ATA-8 ASC2]	7.44 SECURITY ERASE PREPARE - F3h, Non-Data
			ATA SECURITY ERASE UNIT	[ATA-8 ASC2]	7.45 SECURITY ERASE UNIT - F4h, PIO Data-Out
Set PIN (Setup)	Set PIN	1, 2	TCG Set	See above	See Change PIN
Set PIN (FW Download)	See "Firmware Access Control and Firmware Trusted Update"	2	ATA SECURITY SET Password	See above	See Change PIN
Take Ownership	See "Protection of Data on Disk & Specification of Management Functions"	1	ATA SECURITY SET Password	See above	See Change PIN

Security Function	Security Service	Example Step	Interface	Specification	Section
Transition to ATA Security Mode	See "Protection of Data on Disk & Specification of Management Functions"	1	ATA SECURITY SET Password	See above	See Take Ownership
				[ATA-8 ASC2]	See Take Ownership
Unlock Band	Unlock User Data	N/A	ATA SECURITY UNLOCK	[ATA-8 ASC2]	4.20 Security feature set
Verify PIN	See example	3	TCG Authenticate	See above	See Firmware (Authenticate)

3.1.1.2 Supporting Document 5.2.1.2 Evaluation Activity

The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.

Please see section 3.1.1.1 above, which summarizes the evaluation team's examination of TOE security function interfaces. The evaluation team used the mappings to confirm [Guide] and the public specifications adequately identify and describe the parameters for each TOE security function interface.

3.1.1.3 Supporting Document 5.2.1.3 Evaluation Activity

The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.

The evaluator uses the provided documentation and first identifies, and then examines a representative set of interfaces to perform the EAs presented in Section 2 (Evaluation Activities for SFRs), including the EAs associated with testing of the interfaces.

It should be noted that there may be some SFRs that do not have an interface that is explicitly "mapped" to invoke the desired functionality. For example, generating a random bit string, destroying a cryptographic key that is no longer needed, or the TSF failing to a secure state, are capabilities that may be specified in SFRs, but are not invoked by an interface.

However, if the evaluator is unable to perform some other required EA because there is insufficient design and interface information, then the evaluator is entitled to conclude that an adequate functional specification has not been provided, and hence that the verdict for the ADV_FSP.1 assurance component is a 'fail'.

Please see Table 11 Mapping from SFR to Security Functions in section 3.1.1.1 above

3.2 Guidance Documents (AGD)

It is not necessary for a TOE to provide separate documentation to meet the individual requirements of AGD_OPE and AGD_PRE. Although the Evaluation Activities in this section are described under the traditionally separate AGD families, the mapping between real TOE documents and AGD_OPE and AGD_PRE requirements may be many-to-many, as long as all requirements are met in documentation that is delivered to administrators and users (as appropriate) as part of the TOE.

3.2.1 AGD_OPE.1 Operational User Guidance

Specific requirements and checks on the user guidance documentation are identified (where relevant) in the individual Evaluation Activities for each SFR, and for some other SARs (e.g. ALC_CMC.1).

Evaluation Activity:

The evaluator shall check the requirements below are met by the operational guidance. It should be noted that operational guidance may take the form of an "integrator's guide", where the TOE developer provides a description of the interface (e.g., commands that the Host Platform may invoke to configure a SED).

Operational guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.

Operational guidance must be provided for every Operational Environment that the TOE supports as claimed in the Security Target and must adequately address all platforms claimed for the TOE in the Security Target. This may be contained all in one document.

The contents of the operational guidance will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in ***sections 2, 3, and 4.***

In addition to SFR-related Evaluation Activities, the following information is also required.

- *The operational guidance shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.*

Each Seagate SED firmware and hardware contain the drive's cryptographic engine, which is not configurable.

In addition to SFR-related Evaluation Activities, the following information is also required.

- *The operational guidance shall describe how to configure the IT environments that are supported to shut down after an administratively defined period of inactivity.*

The TOE is a set of Seagate SEDs, which rely on the host platform for power management. Thus, this assurance activity is not applicable.

In addition to SFR-related Evaluation Activities, the following information is also required.

- *The operational guidance shall identify system "sleeping" states for all supported operating environments and for each environment, provide administrative guidance on how to disable the sleep state. As stated above, the TOE developer may be providing an integrator's guide and "power states" may be an abstraction that SEDs provide at various levels – e.g., may simply provide a command that the Host Platform issues to manage the state of the device, and the Host Platform is responsible for providing a more sophisticated power management scheme.*

[Guide] sections "Power Saving States and Timing of Power Saving States" and "Cryptographic Key and Key Material Destruction (Power Management)" provide sufficient information for a host platform to manage a Seagate SED's power states.

In addition to SFR-related Evaluation Activities, the following information is also required.

- *The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The operational guidance shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.*

The TCG Storage and ATA Security Specifications identified in section 1.3 above specify interfaces and behaviors for self-encrypting drives, which include the Seagate SEDs. [Guide] serves to identify the interfaces and behaviors related to the security functional requirements and security functions in [ST].

3.2.2 AGD_PRE.1 Preparative Procedures

As for the operational guidance, specific requirements and checks on the preparative procedures are identified (where relevant) in the individual Evaluation Activities for each SFR.

Evaluation Activity:

The evaluator shall check the requirements below are met by the preparative procedures.

The contents of the preparative procedures will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in sections 2, 3, and 4.

Preparative procedures shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.

Seagate wrote [Guide] to provide administrators and users with guidance to configure and operate a Seagate SED in the evaluated configuration. Applicable sections in [Guide] are "Setup and Configuration" and "TCG Enterprise, TCG Opal and ATA Enhanced Mode Security Mode Services". Section "Setup and Configuration" covers each of TCG Enterprise, TCG Opal, and ATA Mode devices. Section "TCG Enterprise, TCG Opal and ATA Enhanced Mode Security Mode Services" describes the correspondence from device services to ATA and TCG commands.

The NIAP Product Compliant List entry for this evaluation includes a copy of [Guide].

TCG and ATA public specifications supplement [Guide] with detailed interface information. Please see section 1.3 above for a list of specifications. Section 3.1.1 above presents results of the evaluation team's check of the specifications.

The contents of the preparative procedures will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in sections 2, 3, and 4

In addition to SFR-related Evaluation Activities, the following information is also required.

Preparative procedures must include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target). The documentation should be in an informal style and should be written with sufficient detail and explanation that they can be understood and used by the target audience (which will typically include IT staff who have general IT experience but not necessarily experience with the TOE itself).

[ST] section 2.2.1 Physical Boundaries describes a Seagate SED's dependence on a host system (search for 'A host system using the standard protocol defined by the Trusted Computing Group (TCG) is required in the operational environment.")

[Guide] section "Operational Environment" restates the security objectives for the operational environment as shown in Table 15.

Table 15 Operational Environment Information

Security Objective	Information
OE.TRUSTED_CHANNEL	Authorized administrators and users must ensure that the communication channel between the host and the storage device is sufficiently protected to prevent information disclosure. For example extremely long unprotected interface cables from the host to the device are not permitted.
OE.INITIAL_DRIVE_STATE	An authorized administrator must ensure that a newly provisioned or initialized storage device is free of protected data in areas not targeted for encryption.
OE.PASSPHRASE_STRENGTH	An authorized administrator must be responsible for ensuring that the allowed passphrase authorization factors configuration conforms to the local storage device environment requirements.
OE.POWER_DOWN	Administrators must ensure that guidance is given to users regarding the amount of time it takes for the storage device volatile memory to clear after entering the Compliant power saving state (power off in this case) so memory remnant attacks are infeasible.
OE.SINGLE_USE_ET	Authorized administrators must ensure that authorized users are trained in the proper storage of external tokens that contain authorization factors and that they will be used for no other purpose than to store the external token authorization factor.
OE.PHYSICAL	Authorized administrators and users must ensure that the storage device is used in a secure physical computing space such that an adversary is not able to make modifications to the environment or to the storage device itself.
OE.TRAINED_USERS	Authorized administrators must ensure that authorized users are properly trained and follow all guidance for securing the storage device and the proper use of authorization factors.

In addition to SFR-related Evaluation Activities, the following information is also required.

Preparative procedures must be provided for every Operational Environment that the TOE supports as claimed in the Security Target and must adequately address all platforms claimed for the TOE in the Security Target. . This may be contained all in one document.

[Guide] section "Introduction" states the need for host system that supports TCG or ATA security mode commands.

The preparative procedures must include

- *instructions to successfully install the TSF in each Operational Environment; and*

[Guide] section "Introduction" states the need for host system that supports TCG or ATA security mode commands. Section "Setup and Configuration" covers each of TCG Enterprise, TCG Opal, and ATA Mode devices.

The preparative procedures must include

- *instructions to manage the security of the TSF as a product and as a component of the larger operational environment; and*

[Guide] section "Protection of Data on Disk & Specification of Management Functions" covers managing security of Seagate SEDs. The section addresses personalization of a drive, interaction with an Authorization Acquisition component, supporting multiple users, and erasing a drive.

The preparative procedures must include

- *instructions to provide a protected administrative capability.*

[Guide] section "TCG Enterprise, TCG Opal and ATA Enhanced Mode Security Mode Services" identifies security services along with access restrictions on those services. Please see [Guide] tables 4.1, 4.3, and 4.5.

3.3 Life-Cycle Support (ALC)

3.3.1 ALC_CMC.1 Labeling of the TOE

When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.

The evaluator obtained the TOE from the vendor and observed it is labelled with a unique reference in the form of a serial number and identifiers to match the model number and firmware in the Security Target.

3.3.2 ALC_CMS.1 TOE CM Coverage

When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.

The evaluator confirmed via the Security Target that the developer provided an identification of the TOE defined as: Product Name, model number, standard, capacity and firmware. [ST] uniquely identifies each of [ST], [KMD], and [Guide] by title, version and date.

3.4 Security Target Evaluation (ASE)

An evaluation activity is defined here for evaluation of Exact Conformance claims against a cPP in a Security Target. Other aspects of ASE remain as defined in the CEM.

3.4.1 Conformance Claims (ASE_CCL.1)

The table below indicates the actions to be taken for particular ASE_CCL.1 elements in order to determine exact conformance with a cPP.

3.4.1.1 ASE_CCL.1.8C

Evaluator Action

The evaluator shall check that the statements of security problem definition in the PP and ST are identical.

[ST] section 3 "Security Problem Definition" includes by reference the security problem definition from [CPP FDE EE] excluding A.STRONG_CRYPTO. The exclusions is consistent with the instructions in [CPP FDE EE] section A.1 Internal Cryptographic Implementation.

3.4.1.2 ASE_CCL.1.9C

Evaluator Action

The evaluator shall check that the statements of security objectives in the PP and ST are identical.

[ST] section 4.1 "Security Objectives for the Operational Environment" reproduces security objectives verbatim from [CPP FDE EE] section 4.1 "Security Objectives for the Operational Environment".

- OE.TRUSTED_CHANNEL
- OE.INITIAL_DRIVE_STATE
- OE.PASSPHRASE_STRENGTH
- OE.POWER_DOWN
- OE.SINGLE_USE_ET
- OE.TRAINED_USERS
- OE.PHYSICAL

[ST] section 4.1 explicitly excludes OE. STRONG_ENVIRONMENT_CRYPTO, which is consistent with instructions in [CPP FDE EE] section A.1 "Internal Cryptographic Implementation" (search for "ST author shall omit OE.STRONG_ENVIRONMENT_CRYPTO and its corresponding assumption').

3.4.1.3 ASE_CCL.1.10C

Evaluator Action

The evaluator shall check that the statements of security requirements in the ST include all the

mandatory SFRs in the cPP, and all of the selection-based SFRs that are entailed by selections made in other SFRs (including any SFR iterations added in the ST). The evaluator shall check that if any other SFRs are present in the ST (apart from iterations of SFRs in the cPP) then these are taken only from the list of optional SFRs specified in the cPP (the cPP will not necessarily include optional SFRs, but may do so). If optional SFRs from the cPP are included in the ST then the evaluator shall check that any selection-based SFRs entailed by the optional SFRs adopted are also included in the ST.

[ST] section 5 "IT Security Requirements" states the SFRs and SARs are from [CPP FDE EE]. Table 16 below confirms all SFRs in [ST] come from [CPP FDE EE]. The correct reproduction of SFRs and completion of operations on SFRs is assessed in the ASE_REQ.1 work units. Table 17 below confirms the correspondence between [ST] SARs and [CPP FDE EE] SARs.

Table 16 ST Security Functional Requirements

PP SFR	ST SFR
FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)	FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)
FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key)	FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key)
FCS_CKM.4(a) Cryptographic Key Destruction (Power Management)	FCS_CKM.4(a) Cryptographic Key Destruction (Power Management)
FCS_CKM.4(b) Cryptographic Key Destruction (TOE-Controlled Hardware)	FCS_CKM.4(b) Cryptographic Key Destruction (TOE-Controlled Hardware)
FCS_CKM.4(c) Cryptographic Key Destruction (General Hardware)	FCS_CKM.4(c)(1) HDD Cryptographic Key Destruction (General Hardware)
FCS_CKM.4(c) Cryptographic Key Destruction (General Hardware)	FCS_CKM.4(c)(2) SDD and Hybrid Cryptographic Key Destruction (General Hardware)
FCS_CKM.4(e) Cryptographic Key Destruction (Key Cryptographic Erase)	FCS_CKM.4(e) Cryptographic Key Destruction (Key Cryptographic Erase)
FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)	FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)
FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)	FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)
FCS_CKM_EXT.6 Cryptographic Key Destruction Types	FCS_CKM_EXT.6 Cryptographic Key Destruction Types
FCS_COP.1(a) Cryptographic Operation (Signature Verification)	FCS_COP.1(a) Cryptographic Operation (Signature Verification)
FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)	FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(c) Cryptographic Operation (Message Authentication)	FCS_COP.1(c) Cryptographic Operation (Message Authentication)
FCS_COP.1(d) Cryptographic Operation (Key Wrapping)	FCS_COP.1(d) Cryptographic Operation (Key Wrapping)

PP SFR	ST SFR
FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)	FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)
FCS_KDF_EXT.1 Cryptographic Key Derivation	FCS_KDF_EXT.1 Cryptographic Key Derivation
FCS_KYC_EXT.2 Key Chaining (Recipient)	FCS_KYC_EXT.2 Key Chaining (Recipient)
FCS_RBG_EXT.1 Random Bit Generation	FCS_RBG_EXT.1 Random Bit Generation
FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
FCS_VAL_EXT.1 Validation	FCS_VAL_EXT.1(a) Validation (SATA)
FCS_VAL_EXT.1 Validation	FCS_VAL_EXT.1(b) Validation (SAS)
FDP_DSK_EXT.1 Protection of Data on Disk	FDP_DSK_EXT.1 Protection of Data on Disk
FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 Specification of Management Functions
FPT_FAC_EXT.1 Firmware Access Control	FPT_FAC_EXT.1 Firmware Access Control
FPT_FUA_EXT.1 Firmware Update Authentication	FPT_FUA_EXT.1 Firmware Update Authentication
FPT_KYP_EXT.1 Protection of Key and Key Material	FPT_KYP_EXT.1 Protection of Key and Key Material
FPT_PWR_EXT.1 Power Saving States	FPT_PWR_EXT.1 Power Saving States
FPT_PWR_EXT.2 Timing of Power Saving States	FPT_PWR_EXT.2 Timing of Power Saving States
FPT_RBP_EXT.1 Rollback Protection	FPT_RBP_EXT.1 Rollback Protection
FPT_TST_EXT.1 TSF Testing	FPT_TST_EXT.1 TSF Testing
FPT_TUD_EXT.1 Trusted Update	FPT_TUD_EXT.1 Trusted Update

Table 17 ST Security Assurance Requirements

PP SAR	ST SAR
Basic Functional Specification (ADV_FSP.1)	ADV_FSP.1 Basic functional specification
Operational User Guidance (AGD_OPE.1)	AGD_OPE.1: Operational user guidance
Preparative Procedures (AGD_PRE.1)	AGD_PRE.1: Preparative procedures
Labeling of the TOE (ALC_CMC.1)	ALC_CMC.1 Labelling of the TOE
TOE CM Coverage (ALC_CMS.1)	ALC_CMS.1 TOE CM coverage
Independent Testing – Sample (ATE_IND.1)	ATE_IND.1 Independent testing - sample
Vulnerability Survey (AVA_VAN.1)	AVA_VAN.1 Vulnerability survey
Conformance Claims (ASE_CCL.1)	ASE_CCL.1 Conformance Claims
Extended Components Definition (ASE_ECD.1)	ASE_ECD.1 Extended Components Definition
ST Introduction (ASE_INT.1)	ASE_INT.1 ST Introduction
Security Objectives for the Operational Environment (ASE_OBJ.1)	ASE_OBJ.1 Security Objectives for the Operational Environment

PP SAR	ST SAR
Stated Security Requirements (ASE_REQ.1)	ASE_REQ.1 Stated Security Requirements
Security Problem Definition (ASE_SPD.1)	ASE_SPD.1 Security Problem Definition
TOE Summary Specification (ASE_TSS.1)	ASE_TSS.1 TOE Summary Specification

[ST] contains all unconditional requirements from [CPP FDE EE] along with all three optional requirements.

- FCS_CKM.4(e) Cryptographic Key Destruction (Key Cryptographic Erase)
- FPT_FAC_EXT.1 Firmware Access Control
- FPT_RBP_EXT.1 Rollback Protection

Table 18 Security Functional Requirement Completeness Check lists security functional requirements in [CPP FDE EE]. For each requirement that depends on selection-based requirements, the table groups related selection-based requirements with the requirement. The first column identifies each requirement as unconditional (U), selection-based (SB), optional (Op), or objective (Ob). The security target omits the following selection-based requirements since no selection implies inclusion of any of these requirements.

- FCS_CKM.1(a) Cryptographic Key Generation (Asymmetric Keys)
- FCS_CKM.4(d) Cryptographic Key Destruction (Software TOE, 3rd Party Storage)
- FCS_COP.1(e) Cryptographic Operation (Key Transport)
- FCS_COP.1(g) Cryptographic Operation (Key Encryption)
- FCS_SMC_EXT.1 Submask Combining

Table 18 Security Functional Requirement Completeness Check

Type	Security Functional Requirement
U	FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key)
SB	FCS_RBG_EXT.1 Random Bit Generation
SB	FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)
U	FCS_CKM.4(a) Cryptographic Key Destruction (Power Management)
U	FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)
U	FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)
U	FCS_CKM_EXT.6 Cryptographic Key Destruction Types
SB	FCS_CKM.4(b) Cryptographic Key Destruction (TOE-Controlled Hardware)
SB	FCS_CKM.4(c)(1) HDD Cryptographic Key Destruction (General Hardware)
SB	FCS_CKM.4(c)(2) SDD and Hybrid Cryptographic Key Destruction (General Hardware)
U	FCS_KYC_EXT.2 Key Chaining (Recipient)
SB	FCS_KDF_EXT.1 Cryptographic Key Derivation
SB	FCS_COP.1(c) Cryptographic Operation (Message Authentication)
SB	FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)
SB	FCS_COP.1(d) Cryptographic Operation (Key Wrapping)

U	FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
SB	FCS_RBG_EXT.1 Random Bit Generation
SB	FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)
SB	FCS_COP.1(d) Cryptographic Operation (Key Wrapping)
SB	FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)
SB	FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)
U	FCS_VAL_EXT.1(a) Validation (SATA)
SB	FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)
SB	FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)
U	FCS_VAL_EXT.1(b) Validation (SAS)
SB	FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)
SB	FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)
U	FDP_DSK_EXT.1 Protection of Data on Disk
SB	FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)
SB	FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)
U	FMT_SMF.1 Specification of Management Functions
U	FPT_KYP_EXT.1 Protection of Key and Key Material
SB	FCS_COP.1(d) Cryptographic Operation (Key Wrapping)
U	FPT_PWR_EXT.1 Power Saving States
U	FPT_PWR_EXT.2 Timing of Power Saving States
U	FPT_TST_EXT.1 TSF Testing
U	FPT_TUD_EXT.1 Trusted Update
SB	FPT_FUA_EXT.1 Firmware Update Authentication
SB	FCS_COP.1(a) Cryptographic Operation (Signature Verification)
SB	FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)
Op	FCS_CKM.4(e) Cryptographic Key Destruction (Key Cryptographic Erase)
Op	FPT_FAC_EXT.1 Firmware Access Control
Op	FPT_RBP_EXT.1 Rollback Protection

3.5 Tests (ATE)

3.5.1 ATE_IND.1 Independent Testing – Sample

Testing is performed to confirm the functionality described in the TSS as well as the operational guidance documentation. The focus of the testing is to confirm that the requirements specified in the SFRs are being met.

The evaluator should consult Appendix B FDE Equivalency Considerations when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under

evaluation.

The SFR-related Evaluation Activities in the SD identify the specific testing activities necessary to verify compliance with the SFRs. The tests identified in these other Evaluation Activities constitute a sufficient set of tests for the purposes of meeting ATE_IND.1.2E. It is important to note that while the Evaluation Activities identify the testing that is necessary to be performed, the evaluator is responsible for ensuring that the interfaces are adequately tested for the security functionality specified for each SFR.

Evaluation Activity:

The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.

The evaluator received the TOE from the vendor and confirmed that it conforms with the hardware, configuration and firmware describe in the ST.

Evaluation Activity:

The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.

The evaluator received the TOE from the vendor and powered it on. The evaluator confirmed it presented no errors and entered a running state. The evaluator performed a version and model verification activity prior to testing.

Evaluation Activity:

The evaluator shall prepare a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must show in the test plan that each applicable testing requirement in the SFR-related Evaluation Activities is covered.

The test plan identifies the platforms to be tested, and for any platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition and configuration of each platform to be tested, and any setup actions that are necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of any cryptographic engine to be used (e.g. for cryptographic protocols being evaluated).

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives, and the expected results.

The test report (which could just be an updated version of the test plan) details the activities that took

place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure, so that a fix was then installed and then a successful re-run of the test was carried out, then the report would show a "fail" result followed by a "pass" result (and the supporting details), and not just the "pass" result[2].

The evaluator prepared a test plan prior to testing outlining the required test activities to be performed. Throughout testing the test plan was updated with results to eventually become the test report.

The test plan laid out a subset of all instances of the TOE in the evaluation to be tested. Similar instances of the TOE were grouped together based on similar form factor, standard, type of storage memory and firmware. When an instance or instances of the TOE were not tested justification was provided in the test report via equivalency rationale.

The test report lists each instance of the TOE tested for each SFR and details it as defined in the ST. The test report also shows configuration performed on the TOE to place it into CC compliant mode as described in guidance.

The test plan established and set of procedures to follow with steps and configuration necessary to achieve the expected result.

The test report describes in detail the activities the evaluator performed along with actual results in the form of evidence to accomplish each test. Each test account in accompanied by a test result in the form of 'pass' or 'fail'. The test report also establishes an overall result for the cumulative test activities stated by a 'pass' or 'fail'.

The overall verdict for the testing effort for the Seagate Secure® TCG SSC Self-Encrypting Drives is a 'pass'.

Independent testing took place at Leidos facility from March 1, 2021 to November 12, 2021.

The evaluation team established a test configuration comprising:

- **TOE components**

The evaluation team carefully selected a subset of drives to be tested. The test platforms listed below cover a range of instances of the TOE to cover a variety of firmware, drive types, sector sizes, native interfaces, standards, form factors and media types.

The evaluation team carefully selected a subset of drives to be tested. The test platforms listed below cover a range of instances of the TOE to cover a variety of firmware, drive types, sector sizes, native interfaces, standards, form factors and media types. The three selected models below were chosen to exercise and verify the CAVP certs:

[2] It is not necessary to capture failures that were due to errors on the part of the tester or test environment. The intention here is to make absolutely clear when a planned test resulted in a change being required to the originally specified test configuration in the test plan, to the evaluated configuration identified in the ST and operational guidance, or to the TOE itself.

Product Name	Model #	Standard	Firmware
ExosTM 7E8, SAS Interface (Cimarron)	ST4000NM014A	Enterprise SSC	EF03
Nytro® 3032 SSD, 15mm, SAS Interface (LangeBP)	XS960SE70104	Enterprise SSC	0202
BarraCuda 2.5", SATA Interface (Rosewood)	ST1000LM050	Opal SSC ATA Security	RPE3

- **Test Configuration**

The evaluator configured default environment configurations for the Seagate Secure® TCG SSC Self-Encrypting Drives products as described in guidance.

The following non-TOE components were also used as part of the evaluation were:

- 010 Hex editor—Perform binary compare of flash files pulled from the TOE.
- Seagate FIPS test tool (internal)—Test tool to send TCG/ATA commands to the TOE.
- Seagate Workbench (internal)—Interface with the TOE to query firmware version
- Seagate Instrumented firmware (internal)—Specialty firmware to observe key destruction.
- Python Interpreter—manually send TCG/ATA commands to the TOE.
- Dell Optiplex 790, Windows 7, SAS controller—PC used to interface with TOE.

Equivalency Rationale

The evaluated products differ in the following aspects. The sections below explain the differences in each aspect and provide rationale that the set of devices used in testing cover all aspects.

- Firmware version
  - OEM—General Seagate firmware
  - Customer—Seagate engineered firmware for specific customer
  - Specialty Instrumented
- Drive type
  - SED
  - FIPS
- Disc sector size
  - 4k native
  - 512 emulation
  - 512 native
- Native interface

    - SAS
    - SATA
- Standard
    - Opal SSC ATA Security
    - Enterprise SSC
    - Enterprise SSC ATA Security
- Form factor
    - Platter size
    - Number of platters
    - Speed
    - Capacity
- Media Type
    - HDD
    - SSD
    - Hybrid

Firmware Equivalence

There are two types of firmware that comprise the TOE: controller firmware and crypto firmware. Controller firmware is the only firmware that differs between instances of the TOE. The sections below explain the differences in controller firmware. Crypto firmware however does not change between instances of the TOE. The table below shows that all crypto firmware is covered.

Firmware	**CAVP**	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST6000NM033A ST4000NM014A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
800-90 DRBG 1.0 (Firmware)	**DRBG #62**			**X**	**X**		**X**
ARMv7 AES in Firmware 3.0 (Firmware)	**AES #1343**	**X**	**X**	**X**	**X**	**X**	**X**
ARMv7 AES Key Wrap in Firmware 1.0 (Firmware)	**AES #2947**	**X**	**X**	**X**	**X**	**X**	**X**
ARMv7 GCM in Firmware 1.0 (Firmware)	**AES #2804**			**X**	**X**		**X**
ARMv7 GCM in Firmware 2.0 (Firmware)	**AES #2841**	**X**	**X**			**X**	
ARMv7 HMAC in Firmware 4.0 (Firmware)	**HMAC #1597**			**X**	**X**		**X**

Firmware	**CAVP**	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST6000NM033A ST4000NM014A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
ARMv7 HMAC in Firmware 5.0 (Firmware)	**HMAC #2613**	**X**	**X**			**X**	
ARMv7 RSA in Firmware 5.0 (Firmware)	**RSA #1934**			**X**	**X**		**X**
ARMv7 RSA in Firmware 5.1 (Firmware)	**RSA #2056**	**X**	**X**			**X**	
ARMv7 SHS in Firmware 3.0 (Firmware)	**SHS #1225**			**X**	**X**		**X**
ARMv7 SHS in Firmware 5.0 (Firmware)	**SHS #3304**	**X**	**X**			**X**	
Hash_Based DRBG 2.0 (Firmware)	**DRBG**	**X**	**X**			**X**	

Firmware	**CAVP**	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST6000NM033A ST4000NM014A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
	#1146						
Balto AES in Hardware	**AES #4843**	**X**					
Balto HMAC in Hardware	**HMAC #3243**	**X**					
Balto RSA in Hardware	**RSA #2662**	**X**					
Balto SHA in Hardware	**SHS #3984**	**X**					
Cheops AES in Hardware (cert #4279)	**AES #4279**			**X**	**X**		**X**

Firmware	**CAVP**	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST6000NM033A ST4000NM014A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
Cheops AES in Hardware (cert #3758)	**AES #3758**			**X**	**X**		**X**
Cheops HMAC in Hardware (cert #2815)	**HMAC #2815**			**X**	**X**		**X**
Cheops HMAC in Hardware (cert #2460)	**HMAC #2460**			**X**	**X**		**X**
Cheops RSA in Hardware	**RSA #1933**			**X**	**X**		**X**
Cheops SHA in Hardware (cert #3515)	**SHS #3515**			**X**	**X**		**X**
Cheops SHA in Hardware (cert	**SHS**			**X**	**X**		**X**

Firmware	**CAVP**	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST6000NM033A ST4000NM014A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
#3128)	**#3128**						
Myna AES in Hardware	**AES #3940**		**X**			**X**	
Myna HMAC in Hardware	**HMAC #2565**		**X**			**X**	
Myna RSA in Hardware	**RSA #2013**		**X**			**X**	
Myna SHA in Hardware	**SHS #3250**		**X**			**X**	

OEM Firmware

There are two types of firmware that comprise the TOE: controller firmware and crypto firmware. Controller firmware is the only firmware that differs between instances of the TOE.

Controller Firmware

The TOE implements two types of controller firmware.

- OEM Firmware: The OEM firmware selected for testing covers EF03, 0202, and RPE3. The OEM firmware consists of the following: 7539, 0001, 0002, 0003, 0004, 0005, 0202, A001, A003, CK10, CF04, CKF1, CS10, CSF2, CT10, CT12, CT14, CTF1, EF01, EF02, EF03, EFA2, LXM7, NFA2, NF04, RDE3, REE2, RPE2, RPE3, RSE3, RTE2, RXE2, RXE3, SDM2, SFA2, SF01, SSM1, TF01, TFA2 . Different OEM firmware versions do not differ between security functionality however they do differ to conform to the amount of bytes per sector. Bytes per sector does not impact security and is not SFR relevant.
- Customer Firmware: Customer firmware is modified OEM firmware to accommodate a specific customer of the vendor. The customer firmware included in the evaluation is RSE3, RDE3, and RXE2 and 0001. The modifications that customer firmware makes to OEM firmware are to make specific firmware for capacity and number of platters. These changes are made to accommodate physical differences in the TOE and are not considered security or SFR relevant.

The controller firmware does not impact the crypto firmware.

Crypto Firmware

- Seagate uses the ARM Cortex-R5(F) processor core with the ARMv7-R 32 bit architecture for all of its firmware cryptographic implementations for all of the TOE devices. Equivalency rationale is not required since the crypto firmware uses the same processor and architecture for all of the crypto implementations.
- Seagate provides hardware implementations for its self encryption drives (SEDs). The hardware implementations are identified by their part number:
    - Balto
    - Cheops
    - Myna

Drive Type Equivalence

There are two types of drives tested; SED and FIPS. The FIPS drive is a SED drive with exterior modifications to be FIPS compliant. The other change to the drive is the FIPS drive introduces a FIPS Indicator Bit and FIPS Feature Descriptor. These properties are changed to reflect whether or not the drive is in FIPS compliant mode. Both SED and FIPS drives may be configured to enter a FIPS compliant mode. The added properties to these drives are considered for reporting only and are not TSF relevant.

Sector size equivalence

Different drives support different sector sizes of 4k native, 512 emulation, and 512 native for how many bytes per physical sector. A variety of sector sizes were covered through sampling. Sector sizes are considered physical differences and are not TSF relevant.

Native interface equivalence

Two types of native interfaces were covered in testing; SAS and SATA. Through the tested sample of drives both were fully tested.

Standard equivalence

Three different standards are covered in the evaluation; Opal SSC ATA Security, Enterprise SSC, and Enterprise SSC ATA Security. Each standard was fully tested through the selected sample. The table below shows each instance of the TOE and the standard tested.

Tested Platforms:

Product Name	Model #	Standard	Firmware
ExosTM 7E8, SAS Interface (Cimarron)	ST4000NM014A	Enterprise SSC	EF03
Nytro® 3032 SSD, 15mm, SAS Interface (LangeBP)	XS960SE70104	Enterprise SSC	0202
BarraCuda 2.5", SATA Interface (Rosewood)	ST1000LM050	Opal SSC ATA Security	RPE3

Form Factor equivalence

Instances of the TOE varied in terms of platter size, number of platters, capacity and speed. Each of these properties are physical properties and are not security or TSF relevant.

Media Type

The set of devices included vary between types of media. HDD, SSD and Hybrid (both HDD and SSD) are all media types that comprise the TOE. All types of media were fully tested between Cimarron, LangeBP and Rosewood.

CAVP Certifications

The three drives identified above were chosen to exercise and validate the CAVP certifications of the firmware and hardware cryptographic implementations. Every CAVP certificate was tested at least one time.

3.5.2 Cryptographic Algorithm Validation Programming Testing

Seagate Secure TCG SSC Self-Encrypting Drives use algorithm implementations validated under the CAVP (http://csrc.nist.gov/groups/STM/cavp/index.html). NIAP Policy Letter #5 defines the applicability and relationship of NIST CAVP and CMVP testing to assurance activities associated with cryptography requirements in NIAP-approved protection profiles (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf). This section supplements the following AAR sections to confirm CAVP certificates cited in [ST] contain the information required by NIAP Policy Letter #5.

- 2.1.10 FCS_COP.1(a) Cryptographic Operation (Signature Verification
- 2.1.11 FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)
- 2.1.12 FCS_COP.1(c) Cryptographic Operation (Message Authentication)
- 2.1.13 FCS_COP.1(d) Cryptographic Operation (Key Wrapping)
- 2.1.14 FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)

- 2.1.17 FCS_RBG_EXT.1 Random Bit Generation

[ST] Table 2 TOE Hardware and Firmware and Table 6 Cryptographic Functions provide information on cryptographic implementations and CAVP certificates for each TOE device. Table 19, Table 20, and Table 21 verify the correspondence between each TOE device, its cryptographic implementations (hardware and firmware), and CAVP certificates. The tables confirm information required by NIAP Policy #5 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update4.pdf) for each TOE device.

[ST] Table 2 identifies the hardware and firmware cryptographic implementations for each product (see columns "ASIC" and "Firmware implementations (for each model) as identified by CAVP," respectively). The table identifies multiple models for each product. However, all the models for a product have the same hardware and firmware cryptographic implementations. Table 19 identifies the mapping from product name and model number to firmware implementation.

Table 19 Mapping from Product Name and Model Number to Firmware Implementation

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)

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
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 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) 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)
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 XS3840SE70024 XS7680SE70024 XS15360TE70024	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 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	XS400ME70104	Balto	Enterprise	400, 800,	0001	Hash_Based DRBG 2.0

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
SSD, 15mm SAS Interface	XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104		SSC	1600, 3200, 800, 1600, 3200, 6400, 960, 1920, 3840, 7680, 15360, 3840, 680	0002	(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 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

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						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 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 Hash_Based DRBG 2.0 (Firmware) ARMv7 HMAC in Firmware

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						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)
Exos™ 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 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™ 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

Product Name	Model #	ASIC	Standard	Capacity (GB)	Firmware	Firmware implementations (for each model) as identified by CAVP
						5.0 ARMv7 AES Key Wrap in Firmware 1.0 ARMv7 AES in Firmware 3.0 (Firmware)
Exos™ 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)
Exos™ 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 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™ 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

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® 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) 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)

Table 20 summarizes the firmware implementation, CAVP Certificate number to the drive model numbers.

Table 20 Firmware and CAVP Mapping to Model Number

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
800-90 DRBG 1.0 (Firmware)	DRBG #62			X	X		X

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
ARMv7 AES in Firmware 3.0 (Firmware)	AES #1343	X	X	X	X	X	X
ARMv7 AES Key Wrap in Firmware 1.0 (Firmware)	AES #2947	X	X	X	X	X	X

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
ARMv7 GCM in Firmware 1.0 (Firmware)	AES #2804			X	X		X
ARMv7 GCM in Firmware 2.0 (Firmware)	AES #2841	X	X			X	

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
ARMv7 HMAC in Firmware 4.0 (Firmware)	HMAC #1597			X	X		X
ARMv7 HMAC in Firmware 5.0 (Firmware)	HMAC	X	X			X	

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
	#2613						
ARMv7 RSA in Firmware 5.0 (Firmware)	RSA #1934			X	X		X
ARMv7 RSA in Firmware 5.1	RSA	X	X			X	

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
(Firmware)	#2056						
ARMv7 SHS in Firmware 3.0 (Firmware)	SHS #1225			X	X		X
ARMv7 SHS in Firmware 5.0	SHS	X	X			X	

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
(Firmware)	#3304						
Hash_Based DRBG 2.0 (Firmware)	DRBG #1146	X	X			X	

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
Balto AES in Hardware	AES #4843	X					
Balto HMAC in Hardware	HMAC #3243	X					

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
Balto RSA in Hardware	RSA #2662	X					
Balto SHA in Hardware	SHS #3984	X					

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
Cheops AES in Hardware (cert #4279)	AES #4279			X	X		X
Cheops AES in Hardware (cert #3758)	AES #3758			X	X		X

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
Cheops HMAC in Hardware (cert #2815)	HMAC #2815			X	X		X
Cheops HMAC in Hardware (cert #2460)	HMAC			X	X		X

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
	#2460						
Cheops RSA in Hardware	RSA #1933			X	X		X
Cheops SHA in Hardware (cert	SHS			X	X		X

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
#3515)	#3515						
Cheops SHA in Hardware (cert #3128)	SHS #3128			X	X		X
Myna AES in Hardware	AES		X			X	

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
	#3940						
Myna HMAC in Hardware	HMAC #2565		X			X	

Firmware	CAVP	XS1600ME10023 XS800ME10023 XS400ME10023 XS6400LE70023 XS1600LE10023 XS1920SE10123 XS3840TE10023 XS3200ME70023 XS15360SE70123 XS15360TE70023 XS7680TE70023 XS6400LE70024 XS400ME70024 XS800ME70024 XS3840TE70024 XS7680TE70024 XS1600ME70024 XS3200ME70024 XS800LE70024 XS1600LE70024 XS3200LE70024 XS960SE70024 XS1920SE70024 XS3840SE70024 XS7680SE70024 XS15360TE70024 XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	ST900MP0166 ST600MP0156 ST900MP0126 ST600MP0026	ST2000LX003 ST1000LX017	ST2000LM010 ST1000LM038 ST500LM033 ST1000LM050 ST500LM035	ST1200MM0069 ST2400MM0149 ST1800MM0149 ST1200MM0149 ST10000NM0246 ST10000NM0236 ST10000NM0186 ST10000NM0176 ST8000NM010A ST4000NM014A ST6000NM033A ST4000NM015A ST3000NM005A ST4000NM012A ST8000NM008A ST6000NM025A ST3000NM004A ST4000NM013A ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	ST2000DM011
Myna RSA in Hardware	RSA #2013		X			X	
Myna SHA in Hardware	SHS #3250		X			X	

Table 21 summarizes the correspondence between each cryptographic implementation and the certificate information required by NIAP Policy #5. Table 21 reproduced such dependencies in column Depend. Column 'Depend Met?' records a check of the dependencies.

All Seagate SEDs in the evaluation run firmware on ARM processors, which is consistent with the operational environments identified on the firmware CAVP certificates. Balto, Cheops, and Myna are hardware cryptographic implementations.

The evaluator found the CAVP certificates identified in [ST] are sufficient to satisfy NIAP Policy #5.

Table 21 Mapping from Firmware Implementation to CAVP Certificate

Implementation	Environment	Capabilities	CAVP List	Cert	Depend	Depend Met?
800-90 DRBG 1.0 (Firmware)	ARM Cortex-R Family	Hash based: Modes: SHA-256	DRBG	#62	SHS #1225	Yes
ARMv7 AES in Firmware 3.0 (Firmware)	ARM Cortex-R Family	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128, 256 (bits)	AES	#1343	None	Yes
ARMv7 AES Key Wrap in Firmware 1.0 (Firmware)	ARM Cortex-R Family	AES KW: Modes: Decrypt, Encrypt CIPHK transformation direction: Forward Key Lengths: 256 (bits) Plain Text Lengths: 128, 192, 256, 320, 4096 (bits)	AES	#2947	AES #1343	Yes
ARMv7 GCM in Firmware 1.0 (Firmware)	ARM Cortex-R Family	AES-GCM: Modes: Decrypt, Encrypt Key Lengths: 128, 256 (bits)	AES	#2804	AES #1343	Yes

Implementation	Environment	Capabilities	CAVP List	Cert	Depend	Depend Met?
		Tag Lengths: 128 (bits) Plain Text Lengths: 0, 8, 24, 128, 256 (bits) AAD Lengths: 0, 8, 24, 128, 256 (bits) 96 bit IV supported Other IV Lengths supported				
ARMv7 GCM in Firmware 2.0 (Firmware)	ARM Cortex-R Family	AES-GCM: Modes: Decrypt, Encrypt Key Lengths: 128, 256 (bits) Tag Lengths: 128 (bits) Plain Text Lengths: 0, 8, 24, 256 (bits) AAD Lengths: 0, 8, 24, 256 (bits) 96 bit IV supported Other IV Lengths supported	AES	#2841	AES #1343	Yes
ARMv7 HMAC in Firmware 4.0 (Firmware)	ARM Cortex-R Family	HMAC-SHA2-256: Key Sizes < Block Size Key Sizes > Block Size Key Sizes = Block Size	HMAC	#1597	SHS #1225	Yes
ARMv7 HMAC in Firmware 5.0	ARM Cortex-R Family	HMAC-SHA2-256:	HMAC	#2613	SHS #3304	Yes

Implementation	Environment	Capabilities	CAVP List	Cert	Depend	Depend Met?
(Firmware)		Key Sizes < Block Size Key Sizes > Block Size Key Sizes = Block Size HMAC-SHA2-384: Key Sizes < Block Size Key Sizes > Block Size Key Sizes = Block Size				
ARMv7 RSA in Firmware 5.0 (Firmware)	ARM Cortex-R Family	Signature Generation PKCS1.5: Mod 2048 SHA: SHA-256 Signature Verification PKCS1.5: Mod 2048 SHA: SHA-256	RSA	#1934	SHS #1225	Yes
ARMv7 RSA in Firmware 5.1 (Firmware)	ARM Cortex-R Family	Signature Generation PKCS1.5: Mod 2048 SHA: SHA-256 Signature Verification PKCS1.5: Mod 1024 SHA: SHA-256 Mod 2048 SHA: SHA-256	RSA	#2056	SHS #3304	Yes
ARMv7 SHS in Firmware 3.0 (Firmware)	ARM Cortex-R Family	SHA-1 SHA-256	SHS	#1225	None	Yes
ARMv7 SHS in Firmware 4.0 (Firmware)	ARM Cortex-R Family	SHA-512	SHS	#3129	None	Yes

Implementation	Environment	Capabilities	CAVP List	Cert	Depend	Depend Met?
ARMv7 SHS in Firmware 5.0 (Firmware)	ARM Cortex-R Family	SHA-256 SHA-384 SHA-512	SHS	#3304	None	Yes
Hash_Based DRBG 2.0 (Firmware)	ARM Cortex-R Family	Hash based: Prediction Resistance Modes: Enabled, Not Enabled Modes: SHA-256	DRBG	#1146	SHS #3304	Yes
Balto AES in Hardware	N/A	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 256 (bits) AES-GCM: Modes: Decrypt, Encrypt IV Generation: External Key Lengths: 256 (bits) Tag Lengths: 128 (bits) Plain Text Lengths: 8, 24, 256 (bits) AAD Lengths: 8, 24, 256 (bits) 96 bit IV supported AES-XTS: Key Size: 256: Modes: Decrypt, Encrypt Block Sizes: Full,	AES	#4843	None	Yes

Implementation	Environment	Capabilities	CAVP List	Cert	Depend	Depend Met?
		Partial				
Balto HMAC in Hardware	N/A	HMAC-SHA2-256: Key Sizes < Block Size Key Sizes > Block Size	HMAC	#3243	SHS #3984	Yes
Balto RSA in Hardware	N/A	Signature Generation PKCS1.5: Mod 2048 SHA: SHA-256 Signature Verification PKCS1.5: Mod 2048 SHA: SHA-256	RSA	#2662	SHS #3984	Yes
Balto SHA in Hardware	N/A	SHA-256	SHS	#3984	None	Yes
Cheops AES in Hardware	N/A	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128, 256 (bits) AES-XTS: Key Size: 256: Modes: Decrypt, Encrypt Block Sizes: Full, Partial	AES	#4279	None	Yes
Cheops AES in Hardware	N/A	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128, 256 (bits) AES-ECB: Modes: Decrypt, Encrypt	AES	#3758	None	Yes

Implementation	Environment	Capabilities	CAVP List	Cert	Depend	Depend Met?
		Key Lengths: 128, 256 (bits) AES-XTS: Key Size: 256: Modes: Decrypt, Encrypt Block Sizes: Full, Partial				
Cheops HMAC in Hardware	N/A	HMAC-SHA2-256: Key Sizes < Block Size Key Sizes > Block Size	HMAC	#2815	SHS #3515	Yes
Cheops HMAC in Hardware	N/A	HMAC-SHA2-256: Key Sizes < Block Size Key Sizes > Block Size	HMAC	#2460	SHS #1225	Yes
Cheops RSA in Hardware	N/A	Signature Generation PKCS1.5: Mod 2048 SHA: SHA-256 Signature Verification PKCS1.5: Mod 2048 SHA: SHA-256	RSA	#1933	SHS #1225, DRBG #62	Yes
Cheops SHA in Hardware	N/A	SHA-256	SHS	#3515	None	Yes
Cheops SHA in Hardware	N/A	SHA-256	SHS	#3128	None	Yes
Myna AES in Hardware	N/A	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128,	AES	#3940	None	Yes

Implementation	Environment	Capabilities	CAVP List	Cert	Depend	Depend Met?
		256 (bits) AES-XTS: Key Size: 256: Modes: Decrypt, Encrypt Block Sizes: Full, Partial				
Myna HMAC in Hardware	N/A	HMAC-SHA2-256: Key Sizes < Block Size Key Sizes > Block Size	HMAC	#2565	SHS #3250	Yes
Myna RSA in Hardware	N/A	Signature Generation PKCS1.5: Mod 2048 SHA: SHA-256 Signature Verification PKCS1.5: Mod 2048 SHA: SHA-256	RSA	#2013	SHS #3250	Yes
Myna SHA in Hardware	N/A	SHA-256	SHS	#3250	None	Yes

3.6 Vulnerability Assessment (AVA)

3.6.1 AVA_VAN.1 Vulnerability Survey

While vulnerability analysis is inherently a subjective activity, a minimum level of analysis can be defined and some measure of objectivity and repeatability (or at least comparability) can be imposed on the vulnerability analysis process. In order to achieve such objectivity and repeatability it is important that the evaluator follows a set of well-defined activities, and documents their findings so others can follow their arguments and come to the same conclusions as the evaluator. While this does not guarantee that different evaluation facilities will identify exactly the same type of vulnerabilities or come to exactly the same conclusions, the approach defines the minimum level of analysis and the scope of that analysis, and provides Certification Bodies a measure of assurance that the minimum level of analysis is being performed by the evaluation facilities.

In order to meet these goals some refinement of the AVA_VAN.1 CEM work units is needed. The following table indicates, for each work unit in AVA_VAN.1, whether the CEM work unit is to be performed as written, or if it has been clarified by an Evaluation Activity. If clarification has been provided, a reference to this clarification is provided in the table.

Table 22 SD Table 2. Mapping of AVA_VAN.1 CEM Work Units to Evaluation Activities

CEM AVA_VAN.1 Work Units	Evaluation Activities
AVA_VAN.1-1 The evaluator ***shall examine*** the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.	The evaluator shall perform the CEM activity as specified. *If the iTC specifies any tools to be used in performing this analysis in section A.3.4, the following text is also included in this cell: "The calibration of test resources specified in paragraph 1418 of the CEM applies to the tools listed in Appendix A, Section A.1.4."*
AVA_VAN.1-2 The evaluator ***shall examine*** the TOE to determine that it has been installed properly and is in a known state	The evaluator shall perform the CEM activity as specified.
AVA_VAN.1-3 The evaluator ***shall examine*** sources of information publicly available to identify potential vulnerabilities in the TOE.	Replace CEM work unit with activities outlined in Appendix A, Section A.1
AVA_VAN.1-4 The evaluator ***shall record*** in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.	Replace the CEM work unit with the analysis activities on the list of potential vulnerabilities in Appendix A, section A.1, and documentation as specified in Appendix A, Section A.3.
AVA_VAN.1-5 The evaluator ***shall devise*** penetration tests, based on the independent	Replace the CEM work unit with the activities specified in Appendix A, section A.2.

search for potential vulnerabilities.	
AVA_VAN.1-6 The evaluator **shall produce** penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: a) identification of the potential vulnerability the TOE is being tested for; b) instructions to connect and setup all required test equipment as required to conduct the penetration test; c) instructions to establish all penetration test prerequisite initialconditions; d) instructions to stimulate the TSF; e) instructions for observing the behaviour of the TSF; f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against g) expected results; h) instructions to conclude the test and establish the necessary post-test state for the TOE.	The CEM work unit is captured in Appendix A, Section A.3; there are no substantive differences.
AVA_VAN.1-7 The evaluator ***shall conduct*** penetration testing.	The evaluator shall perform the CEM activity as specified. See Appendix A, Section A.3, paragraph **(f)** for guidance related to attack potential for confirmed flaws.
AVA_VAN.1-8 The evaluator ***shall record*** the actual results of the penetration tests.	The evaluator shall perform the CEM activity as specified.
AVA_VAN.1-9 The evaluator ***shall report*** in the ETR the evaluator penetration testing effort, outlining the testing approach, configuration, depth and results.	Replace the CEM work unit with the reporting called for in Appendix A, Section A.3.
AVA_VAN.1-10 The evaluator ***shall examine*** the results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a Basic attack potential.	This work unit is not applicable for Type 1 and Type 2 flaws (as defined in Appendix A, Section A.1), as inclusion in this Supporting Document by the iTC makes any confirmed vulnerabilities stemming from these flaws subject to an attacker possessing a Basic attack potential. This work unit is replaced for Type 3 and Type 4 flaws by the activities defined in Appendix A, Section

	A.3, paragraph **(g).**
AVA_VAN.1-11 The evaluator **shall report** in the ETR all exploitable vulnerabilities and residual vulnerabilities, detailing for each: a) its source (e.g. CEM activity being undertaken when it was conceived, known to the evaluator, read in a publication); b) the SFR(s) not met; c) a description; d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual). e) the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using the tables 3 and 4 of Annex B.4.	Replace the CEM work unit with the reporting called for in Appendix A, Section A.3.

Because of the level of detail required for the evaluation activities, the bulk of the instructions are contained in Appendix A, while an "outline" of the assurance activity is provided below.

3.6.2 Supporting Document Assurance Activities

3.6.2.1 Supporting Document 5.6.1.1 Evaluation Activity (Documentation):

The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components apply to all systems claimed in the ST, and should identify at a minimum the processors used by the TOE. Software components include any libraries used by the TOE, such as cryptographic libraries. This additional documentation is merely a list of the name and version number of the components, and will be used by the evaluators in formulating hypotheses during their analysis.

The evaluator shall examine the documentation outlined below provided by the vendor to confirm that it contains all required information. This documentation is in addition to the documentation already required to be supplied in response to the EAs listed previously.

In addition to the activities specified by the CEM in accordance with Table 2 above, the evaluator shall perform the following activities.

Please see [ETR] section 2.6.1 AVA_VAN.1 and [VS] for results of the AVA_VAN.1 CEM work units as refined in [CPP FDE EE SD] Table 2 (which is reproduced as Table 22 above).

3.6.2.2 Supporting Document 5.6.1.2 Evaluation Activity

The evaluator formulates hypotheses in accordance with process defined in Appendix A.1. The evaluator documents the flaw hypotheses generated for the TOE in the report in accordance with the guidelines in Appendix A.3. The evaluator shall perform vulnerability analysis in accordance with Appendix A.2. The results of the analysis shall be documented in the report according to Appendix A.3.

The evaluators searched public sources of vulnerability information in accordance with [CPP FDE EE SD] section A.1.1 Type 1 Hypotheses — Public-Vulnerability-based. Sections 3.6.2.2.1.1, 3.6.2.2.1.3, 3.2.6.2.2.1.4 below list the identifiers of potential vulnerabilities returned by the searches. None of the hypotheses in [CPP FDE EE SD] A.1.2 Type 2 Hypotheses — iTC-Sourced apply to the Seagate Secure TCG SSC Self-Encrypting Drives TOE.

The evaluators examined the identified flaw hypotheses as documented in sections 3.6.2.2.1 and 3.6.2.2.2 below. The examination did not find any residual vulnerabilities in the Seagate Secure TCG SSC Self-Encrypting Drives TOE.

3.6.2.2.1 Vulnerability Searches

This section describes the search of public sources of vulnerability information. [CPP FDE EE SD] appendix A.1 Sources of vulnerability information identifies four types of flaw hypotheses:

- Type 1: Public-Vulnerability-based
- Type 2: iTC-Sourced
- Type 3: Evaluation-Team-Generated
- Type 4: Tool-Generated

Only Type 1 hypotheses are applicable to the Seagate Secure TCG SSC Self-Encrypting Drives TOE. [CPP FDE EE SD] appendix A.1.2 Type 2 Hypotheses — iTC-Sourced does not identify any flaw hypotheses applicable to hardware EE full-drive encryption products or generic full-drive encryption products. Appendix A.1.3 Type 3 Hypotheses — Evaluation-Team-Generated states, “Therefore, it is the intent of the iTC, for the evaluation to focus all effort on the Type 1 and Type 2 Hypotheses and has decided that Type 3 Hypotheses are not necessary.” Similarly, appendix A.1.4 Type 4 Hypotheses — Tool-Generated states, “Therefore, the relevant types of tools are referenced in Type 2.” Consequently, the evaluation team considered only potential vulnerabilities identified through searches of public sources of vulnerability information.

[CPP FDE EE SD] appendix A.1.1 Type 1 Hypotheses — Public-Vulnerability-based specifies the following public sources to search.

- 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/)

Table 23 Vulnerability Search Term List

Search Terms	Term Type
Seagate	Vendor

Search Terms	Term Type
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 vulnerability searches of the public vulnerability databases was performed on 11/11/2021.

3.6.2.2.2 Disposition of Flaw Hypotheses

The evaluators reviewed the search results. The review identified 17 CVEs that represent potential vulnerabilities. For of these CVEs, the evaluators hypothesized that the vulnerability exists in the Seagate TOE. In each case, the hypothesis that the CVE applies to the TOE is false.

3.6.2.2.3 Penetration Testing

[CPP FDE EE SD] requires the evaluator to conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

None of the vulnerabilities identified in the search of public sources are related to the TOE. Therefore, no testing is required to verify that an identified potential vulnerability has been mitigated.