Seagate Secure®

TCG Opal and Enterprise SSC Self-Encrypting Drives

Security Target

Version 1.0
10 March 2022

Revision History

Version	Date	Description	Author(s)
0.1	05/03/2021	Initial Revision	Leidos
0.2	09/20/2021	Updated for new KMD information	Leidos
0.3	03/07/2022	Updated to address evaluation findings	Leidos
1.0	03/10/2022	Final for Check-out	Leidos

TABLE OF CONTENTS

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE comprises Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives provided by Seagate Technology, LLC.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives Security Target

ST Version – Version 1.0

ST Date – 10 March 2022

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

Product Name	Model #	Standard	Firmware
Exos X18 3.5” SAS HDD	ST18000NM007J ST16000NM007J ST14000NM007J ST12000NM007J ST10000NM016G	Enterprise SSC	EF02
Exos X18 3.5” SATA HDD	ST18000NM025J	Opal SSC ATA Security	MF01
Exos X18 3.5” SAS HDD	ST18000NM026J	Opal SSC	KF01
Exos 7E10 3.5” SAS HDD	ST10000NM022B ST10000NM011B ST8000NM022B ST8000NM011B ST6000NM024B ST6000NM013B ST4000NM013B ST4000NM029B ST4000NM017B	Enterprise SSC	EF01 KF01 NF01

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

Table 1: TOE Models and Firmware Versions

TOE Developer – Seagate Technology, LLC

Evaluation Sponsor – Seagate Technology, LLC

CC Identification – *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017*

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following Protection Profile:

- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata* 20190201, February 1, 2019, [CPPFDE_EE], including the following optional and selection-based SFRs: FCS_CKM.1(b), FCS_CKM.4(b), FCS_CKM.4(c), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(f), FCS_KDF_EXT.1, FCS_RBG_EXT.1, FCS_CKM.4(e), FPT_FAC_EXT.1, FPT_FUA_EXT.1, and FPT_RBP_EXT.1.

The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:

- TD0458: FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities
- TD0460: FIT Technical Decision for FPT_PWR_EXT.1 non-compliant power saving states
- TD0464: FIT Technical Decision for FPT_PWR_EXT.1 compliant power saving states.

The following NIAP Technical Decision issued for [CPPFDE_EE] is not applicable to this evaluation, for the reason stated:

- TD0606: FIT Technical Recommendation for Evaluating a NAS against the FDE AA and FDEE—this TD provides a technical recommendation regarding evaluation Network Attached Storage (NAS) devices against the FDE EE and FDE AA cPPs, but the devices comprising the TOE are not NAS devices.

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017
    - Part 3 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by appending the SFR with parentheses that contain a letter that is unique for each iteration, e.g. (a), (b), (c) and a descriptive string for the SFR's purpose, e.g. Server. For a component that has already been iterated in the PP, and is iterated again (double iteration) in the ST, the convention above is used for the PP iteration. An additional identifier is added after the first identifying parentheses, containing additional parenthesis with a number that is unique for each iteration, e.g. (1), (2), (3). The descriptive string goes after this set of parenthesis identifiers and identifies the SFR's purpose, e.g. Server. An example of a double iteration would be "(a) (1) descriptive string".
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
  - The SFRs have all been drawn from the Protection Profile (PP): collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201, February 1, 2019, [CPPFDE_EE]. As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Abbreviations and Acronyms

AES	Advanced Encryption Standard
ASIC	Application-Specific Integrated Circuit
ATA	Advanced Technology Attachment
BEV	Border Encryption Value
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CLI	Command Line Interface
CPP	Collaborative Protection Profile
CPPFDE_EE	Collaborative Protection Profile for Full Drive Encryption – Encryption Engine
CRNGT	Continuous Random Number Generator Test
CSPSK	Critical Security Parameter Sanitization Key
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
EE	Encryption Engine
FDE	Full Drive Encryption
FIPS	Federal Information Processing Standard

FW	Firmware
GCM	Galois Counter Mode
HDD	Hard Disk Drive
HMAC	Hashed Message Authentication Code
ISE	Instant Secure Erase
IT	Information Technology
IV	Initialization Vector
KEK	Key Encryption Key
KMD	Key Management Description
LBA	Logical Block Addressing
MEK	Media Encryption Key
MEKEK	Media Encryption Key Encryption Key
MK	Master Key
NIST	National Institute of Standards and Technology
PP	Protection Profile
PSID	Physical SID (public drive-unique value)
RBG	Random Bit Generator
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
RTU	Root of Trust for Update
SAR	Security Assurance Requirement
SAS	Serial Attached SCSI
SATA	Serial ATA (Serial AT Attachment)
SCSI	Small Computer Systems Interface
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SID	Security Identifier, (aka Drive Owner PIN)
SFR	Security Functional Requirement
SPD	Security Problem Definition
SPI	Serial Peripheral Interface
SSC	Security Subsystem Class
SSD	Solid State Drive
ST	Security Target
TCG	Trusted Computer Group
TOE	Target of Evaluation
TSF	TOE Security Functions
XOR	Exclusive or
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

2. TOE Description

The TOE comprises Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives (SEDs) provided by Seagate Technology, LLC. The TOE model numbers and firmware versions are identified in Section 1.1.

The Seagate SEDs implement FIPS-approved and NIST-recommended cryptographic algorithms. All algorithms implementing cryptographic security functional requirements have applicable NIST Cryptographic Algorithm Validation Program (CAVP) certificates, which are identified in Section 6.2. The SEDs provide an Instant Secure Erase (ISE) function and full protection of customer data-at-rest with self-encrypting drive locking. The Seagate Secure Drives are designed in accordance with Trusted Computing Group (TCG) specifications.

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

2.1 TOE Overview

Communication between the host system and the device occurs via an interface protocol. Products included in the TOE support either the Serial ATA (SATA) or Serial Attached SCSI (SAS) interface. The distinction between SATA and SAS generally is not significant. The drives behave the same independent of interface type, except for handling failed authentication attempts as part of the process of validating the Border Encryption Value (BEV) (see Section 6.2.8). While the physical form factor of the drives differ, all models included in the TOE support the requirements defined in [CPPFDE_EE].

Management of the device security subsystem occurs via a security protocol which is encapsulated by the interface protocol. The device will support the protocol for either TCG Enterprise SSC or TCG Opal SSC as defined by the Storage Work Group (SWG), which is a subgroup of the Trusted Computing Group (TCG). Additionally, SATA devices may support the protocol for the ATA Security feature set as defined by the INCITS T13 Technical Committee

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

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

2.2 TOE Architecture

2.2.1 Physical Boundaries

The TOE model series includes SSC Opal and SSC Enterprise and support either SATA or SAS interfaces. SEDs can be a hard-disk drive (HDD) or a solid-state drive (SSD). All models in the TOE are HDD. All SEDs meet the requirements set forth in this document and behave the same except for handling failed authentication attempts as part of the process of validating the BEV (see Section 6.2.8).

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

Product Name	Standard	Firmware	Model #	Capacity
Exos™ X18, 3.5-Inch, SAS HDD	Enterprise SSC	EF02	ST18000NM007J ST16000NM007J ST14000NM007J ST12000NM007J ST10000NM016G	18 TB 16 TB 14 TB 12 TB 10 TB
Exos™ X18, 3.5-Inch, SATA HDD	Opal SSC	MF01	ST18000NM025J	18 TB
Exos™ X18, 3.5-Inch, SAS HDD	Opal SSC	KF01	ST18000NM026J	18 TB
Exos™ 7E10, 3.5-Inch, SAS HDD	Enterprise SSC	EF01 KF01 NF01	ST10000NM022B ST10000NM011B ST8000NM022B ST8000NM011B ST6000NM024B ST6000NM013B ST4000NM013B ST4000NM029B ST4000NM017B	10 TB 10 TB 8 TB 8 TB 6 TB 6 TB 4 TB 4 TB 4 TB
Exos™ 7E10, 3.5-Inch, SATA HDD	Enterprise SSC	SF01 TF01	ST10000NM021B ST8000NM021B ST6000NM023B ST4000NM012B ST4000NM028B	10 TB 8 TB 6 TB 4 TB 4 TB

Table 2: TOE Hardware and Firmware

The TOE models and firmware all provide the same basic set of security functionality, differing mainly in capacity and supported interface standards, as identified in Table 2.

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

2.2.2 Logical Boundaries

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

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

2.2.2.1 Cryptographic Support

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

2.2.2.2 User Data Protection

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

2.2.2.3 Security Management

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

2.2.2.4 Protection of the TSF

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

2.3 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, the following Common Criteria specific guides reference the security-related guidance material for all devices in the evaluated configuration:

Guidance Documentation:

- Seagate Secure® TCG Enterprise and TCG Opal SSC Self-Encrypting Drive Common Criteria Evaluated Configuration Guide, Version 1.0, 9 March 2022

3. Security Problem Definition

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

In general, the [CPPFDE_EE] has presented a Security Problem Definition appropriate for Full Drive Encryption - Encryption Engines and as such is applicable to the Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives.

4. Security Objectives

As with the Security Problem Definition, this security target includes by reference the Security Objectives from the [CPPFDE_EE]. The [CPPFDE_EE] security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the [CPPFDE_EE] has presented a Security Objectives statement appropriate for Full Drive Encryption - Encryption Engines and as such is applicable to the Seagate Secure® TCG Opal and Enterprise SSC Self-Encrypting Drives.

4.1 Security Objectives for the Operational Environment

OE.TRUSTED_CHANNEL	Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure.
OE.INITIAL_DRIVE_STATE	The OE provides a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption.
OE.PASSPHRASE_STRENGTH	An authorized administrator will be responsible for ensuring that the passphrase authorization factor conforms to guidance from the Enterprise using the TOE.
OE.POWER_DOWN	Volatile memory is cleared after entering a Compliant power saving state or turned off so memory remnant attacks are infeasible.
OE.SINGLE_USE_ET	External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization factor.
OE.PHYSICAL	The Operational Environment will provide a secure physical computing space such that an adversary is not able to make modifications to the environment or to the TOE itself.
OE.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
OE.TRAINED_USERS	Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors.

Note:

All of the cryptographic functionality is implemented by the TOE and the TOE does not rely on its Operational Environment to provide any cryptographic services. Therefore, OE.STRONG_ENVIRONMENT_CRYPTO is not included in the ST.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile (PP): *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201*, February 1, 2019, [CPPFDE_EE]. As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the [CPPFDE_EE] made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in [CPPFDE_EE] with the required selection made for ASE_TSS as identified in Section 5.3.

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [CPPFDE_EE]. The [CPPFDE_EE] defines the following extended SFRs and since they are not redefined in this ST, the [CPPFDE_EE] should be consulted for more information in regard to those CC extensions.

- 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.6: Cryptographic Key Destruction Types
- FCS_KDF_EXT.1: Cryptographic Key Derivation
- FCS_KYC_EXT.2: Key Chaining (Recipient)
- FCS_RBG_EXT.1: Random Bit Generation
- FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
- FCS_VAL_EXT.1(a): Validation of Cryptographic Elements (SATA)
- FCS_VAL_EXT.1(b): Validation of Cryptographic Elements (SAS)
- FDP_DSK_EXT.1: Protection of Data on Disk
- FPT_FAC_EXT.1: Firmware Access Control
- FPT_FUA_EXT.1: Firmware Update Authentication
- FPT_KYP_EXT.1: Key and Material Protection
- FPT_PWR_EXT.1: Power Saving States
- FPT_PWR_EXT.2: Timing of Power Saving States
- FPT_RBP_EXT.1: Rollback Protection
- FPT_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Trusted Update

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE.

Requirement Class	Requirement Component
FCS: Cryptographic support	FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)
	FCS_CKM.1(c): Cryptographic Key Generation (Data Encryption Key)
	FCS_CKM.4(a): Cryptographic Key Destruction (Power Management)
	FCS_CKM.4(b): Cryptographic Key Destruction (TOE-Controlled Hardware)
	FCS_CKM.4(c): Cryptographic Key Destruction (General Hardware)
	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(b): Cryptographic Key and Key Material Destruction (Power Management)
	FCS_CKM_EXT.6: Cryptographic Key Destruction Types
	FCS_COP.1(a): Cryptographic Operation (Signature Verification)
	FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(c): Cryptographic Operation (Message Authentication)
	FCS_COP.1(d): Cryptographic Operation (Key Wrapping)
	FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_KDF_EXT.1: Cryptographic Key Derivation
	FCS_KYC_EXT.2: Key Chaining (Recipient)
	FCS_RBG_EXT.1: Random Bit Generation
	FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
	FCS_VAL_EXT.1(a): Validation (SATA)
	FCS_VAL_EXT.1(b): Validation (SAS)
FDP: User Data Protection	FDP_DSK_EXT.1: Protection of Data on Disk
FMT: Security Management	FMT_SMF.1: Specification of Management Functions
FPT: Protection of the TSF	FPT_FAC_EXT.1: Firmware Access Control
	FPT_FUA_EXT.1 Firmware Update Authentication
	FPT_KYP_EXT.1: Protection of Key and Key Material
	FPT_PWR_EXT.1: Power Saving States
	FPT_PWR_EXT.2: Timing of Power Saving States
	FPT_RBP_EXT.1: Rollback Protection
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Trusted Update

Table 3: TOE Security Functional Components

5.2.1 Cryptographic Support (FCS)

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

FCS_CKM.1.1(b) Refinement: The TSF shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [***256 bit***] that meet the following: [no standard].

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

FCS_CKM.1.1(c) Refinement: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation method **[**

- ***generate a DEK using the RBG as specified in FCS_RBG_EXT.1*]**

and specified cryptographic key sizes [***256 bits***].

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

FCS_CKM.4.1(a) Refinement: The TSF shall [***erase***] cryptographic keys and key material from volatile memory when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1 that meets the following: [a key destruction method specified in FCS_CKM_EXT.6].

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

FCS_CKM.4.1(b) Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- ***For volatile memory, the destruction shall be executed by a [***
  - ***single overwrite consisting of [***
    - ***zeroes,***
    - ***a new value of a key],***
  - ***removal of power to the memory*]**

] that meets the following: [no standard].

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

FCS_CKM.4.1(c) Refinement**:** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[**

- ***For non-volatile memory the destruction shall be executed by a [single] overwrite consisting of [***
  - ***a new value of a key of the same size***

  ]

] that meets the following: [no standard].

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

FCS_CKM.4.1(e) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [by using the appropriate method to destroy all encryption keys encrypting the key intended for destruction] that meets the following: [no standard].

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

FCS_CKM_EXT.4.1(a) The TSF shall destroy all keys and keying material when no longer needed.

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

FCS_CKM_EXT.4.1(b) The TSF shall destroy all key material, BEV, and authentication factors stored in plaintext when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1.

5.2.1.9 Cryptographic Key Destruction Types (FCS_CKM_EXT.6)

FCS_CKM_EXT.6.1 The TSF shall use **[*FCS_CKM.4(b)*, *FCS_CKM.4(c)*]** key destruction methods.

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

FCS_COP.1.1(a) Refinement: The TSF shall perform [cryptographic signature services (verification)] in accordance with a [

- ***RSA Digital Signature Algorithm with a key size (modulus) of [2048-bit]***

]
that meet the following: [

- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes***

].

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

FCS_COP.1.1(b) Refinement: The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [***SHA-256***] that meet the following: [*ISO/IEC 10118-3:2004*].

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

FCS_COP.1.1(c): Refinement: The TSF shall perform cryptographic [message authentication] in accordance with a specified cryptographic algorithm **[*HMAC-SHA-256*]** and cryptographic key sizes [**256 bit used in *[HMAC]***] that meet the following: [***ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"***].

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

FCS_COP.1.1(d) Refinement: The TSF shall perform [key wrapping] in accordance with a specified cryptographic algorithm [AES] in the following modes **[*KW, GCM*]** and the cryptographic key size [***256 bits***] that meet the following: [AES as specified in ISO/IEC 18033-3***, [NIST SP 800-38F, ISO/IEC 19772]***].

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

FCS_COP.1.1(f): Refinement: The TSF shall perform [data encryption and decryption] in accordance with a specified cryptographic algorithm [AES used in ***[GCM, XTS]*** *mode*] and cryptographic key sizes [***256 bits***] that meet the following: [AES as specified in ISO /IEC 18033-3*, **[GCM as specified in ISO/IEC 19772, XTS as specified in IEEE 1619]***].

5.2.1.15 Cryptographic Key Derivation (FCS_KDF_EXT.1)

FCS_KDF_EXT.1.1 The TSF shall accept [***imported submask***] to derive an intermediate key, as defined in [

- ***NIST SP 800-132***],

using the keyed-hash functions specified in FCS_COP.1(c), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

5.2.1.16 Key Chaining (Recipient) (FCS_KYC_EXT.2)

FCS_KYC_EXT.2.1 The TSF shall accept a BEV of at least [***256 bits***] from [the AA].

FCS_KYC_EXT.2.2 The TSF shall maintain a chain of intermediary keys originating from the BEV to the DEK using the following method(s): [

- ***key derivation as specified in FCS_KDF_EXT.1,***
- ***key wrapping as specified in FCS_COP.1(d)]***

]

while maintaining an effective strength of [***256 bits***] for symmetric keys and an effective strength of [***not applicable***] for asymmetric keys.

5.2.1.17 Random Bit Generation (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [***[NIST SP 800-90A]***] using [***CTR_DRBG (AES)***].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [

- [*2*] ***hardware-based noise source(s)***]

with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

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

FCS_SNI_EXT.1.1 The TSF shall use [***use salts that are generated by a*** [***DRBG as specified in FCS_RBG_EXT.1***].

FCS_SNI_EXT.1.2 The TSF shall use [***no nonces***].

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner [

- ***XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer;***
- ***GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key***].

5.2.1.19 Validation (for SATA) (FCS_VAL_EXT.1(a))

FCS_VAL_EXT.1.1(a) The TSF shall perform validation of the [BEV] using the following method(s): [

- ***decrypt a known value using the [intermediate key] as specified in FCS_COP.1(f) and compare it against a stored known value***]

FCS_VAL_EXT.1.2(a) The TSF shall require the validation of the [BEV] prior to [allowing access to TSF data after exiting a Compliant power saving state].

FCS_VAL_EXT.1.3(a) The TSF shall [

- ***require power cycle/reset the TOE after [5 (see Table 7: Try Limits Summary for details)] of consecutive failed validation attempts].***

5.2.1.20 Validation (for SAS) (FCS_VAL_EXT.1(b))

FCS_VAL_EXT.1.1(b) The TSF shall perform validation of the [BEV] using the following method(s): [

- ***decrypt a known value using the [intermediate key] as specified in FCS_COP.1(f) and compare it against a stored known value*]].**

FCS_VAL_EXT.1.2(b) The TSF shall require the validation of the [BEV] prior to [allowing access to TSF data after exiting a Compliant power saving state].

FCS_VAL_EXT.1.3(b) The TSF shall [

- ***block validation after [***
  - ***5 retries for Common PSID credentials,***
  - ***100 retries for all other credentials.***

    (see Table 7: Try Limits Summary for details)]

  of consecutive failed validation attempts

].

5.2.2 User Data Protection (FDP)

5.2.2.1 Protection of Data on Disk (FDP_DSK_EXT.1)

FDP_DSK_EXT.1.1 The TSF shall perform Full Drive Encryption in accordance with FCS_COP.1(f), such that the drive contains no plaintext protected data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

.

5.2.3 Security Management (FMT)

5.2.3.1 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 Refinement: The TSF shall be capable of performing the following management functions: [

a) change the DEK, as specified in FCS_CKM.1, when re-provisioning or when commanded,
b) erase the DEK, as specified in FCS_CKM.4(a),
c) initiate TOE firmware/software updates,
d) **[*configure a password for firmware update, configure the number of failed validation attempts required to trigger corrective behavior (TCG Opal only*)]**

].

5.2.4 Protection of the TSF (FPT)

5.2.4.1 Firmware Access Control (FPT_FAC_EXT.1)

FPT_FAC_EXT.1.1 The TSF shall require [***a password***] before the firmware update proceeds.

5.2.4.2 Firmware Update Authentication (FPT_FUA_EXT.1)

FPT_FUA_EXT.1.1 The TSF shall authenticate the source of the firmware update using the digital signature algorithm specified in FCS_COP.1(a) using the RTU that contains [***the public key***].

FPT_FUA_EXT.1.2 The TSF shall only allow installation of update if the digital signature has been successfully verified as specified in FCS_COP.1(a).

FPT_FUA_EXT.1.3 The TSF shall only allow modification of the existing firmware after the successful validation of the digital signature, using a mechanism as described in FPT_TUD_EXT.1.2.

FPT_FUA_EXT.1.4 The TSF shall return an error code if any part of the firmware update process fails.

Note: RTU stands for Root of Trust for Update. The RTU in this case is the RSA public key in ROM.

5.2.4.3 Protection of Key and Key Material (FPT_KYP_EXT.1)

FPT_KYP_EXT.1.1 The TSF shall [

- ***only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d), or encrypted, as specified in FCS_COP.1(g) or FCS_COP.1(e)***
- ***only store plaintext keys that meet any one of the following criteria [***
  - ***The plaintext key is [***
    - ***used to wrap a key as specified in FCS_COP.1(d)]***

    that is already [
    - ***wrapped as specified in FCS_COP.1(d)]]***.

Note: The MEK CSPSK is the only key material that is stored in plain text in non-volatile memory.

5.2.4.4 Timing of Power Saving States (FPT_PWR_EXT.1)

FPT_PWR_EXT.1.1 The TSF shall define the following Compliant power saving states: [***D3***].

5.2.4.5 Power Saving States (FPT_PWR_EXT.2)

FPT_PWR_EXT.2.1 For each Compliant power saving state defined in FPT_PWR_EXT.1.1, the TSF shall enter the Compliant power saving state when the following conditions occur: user-initiated request, [***shutdown***].

5.2.4.6 Rollback Protection (FPT_RBP_EXT.1)

FPT_RBP_EXT.1.1 The TSF shall verify that the new firmware package is not downgrading to a lower security version number by [**the internal block point mechanism**].

FPT_RBP_EXT.1.2 The TSF shall generate and return an error code if the attempted firmware update package is detected to be an invalid version.

5.2.4.7 TSF Testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [***during initial start-up (on power on), at the conditions [before the function is first invoked]***] to demonstrate the correct operation of the TSF: [

- **Power on Self-Tests:**
  - **ASIC AES: Encrypt and Decrypt KATs performed**
  - **ASIC SHA: Digest KAT performed**
  - **ASIC RSA: Verify KAT performed**
  - **ASIC HMAC: HMAC KAT performed**
  - **ASIC 800-90 DRBG: DRBG KAT performed**
  - **Firmware HMAC: HMAC KAT performed**
  - **Firmware AES-GCM, AES-GCM (large block size): Encrypt and Decrypt KATs performed**
  - **Firmware RSA: Verify KAT performed**
  - **Firmware 800-38F Key Wrap: AES Key Wrap and Unwrap KATs performed**
  - **Firmware SHA: SHA KATs performed**
  - **Firmware Integrity Check: Signature Verification**
  - **Secure boot process**
- **Conditional tests:**
  - **Firmware Load Check,**
  - **Hardware 800-90 DRBG Continuous Random Number Generator Test (CRNGT), and**
  - **Hardware 800-90 DRBG Entropy (CRNGT)]**.

5.2.4.8 Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 Refinement: The TSF shall provide [authorized users] the ability to query the current version of the TOE **[*firmware*]**.

FPT_TUD_EXT.1.2 Refinement: The TSF shall provide [authorized users] the ability to initiate updates to TOE **[*firmware*]**.

FPT_TUD_EXT.1.3 Refinement: The TSF shall verify updates to the TOE [***firmware***] using a [***authenticated firmware update mechanism as described in FPT_FUA_EXT.1***] by the manufacturer prior to installing those updates.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the [CPPFDE_EE].

Requirement Class	Requirement Component
ASE: Security Target	ASE_CCL.1 Conformance Claims
	ASE_ECD.1 Extended Components Definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security Objectives for the Operational Environment
	ASE_REQ.1 Stated Security Requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE Summary Specification
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 4: Assurance Components

Consequently, the assurance activities specified in the [CPPFDE_EE] apply to the TOE evaluation. This ST completes ASE_TSS.1.1C as follows:

ASE_TSS.1.1C Refinement: The TOE summary specification shall describe how the TOE meets each SFR, including a proprietary Key Management Description (Appendix E of the [CPPFDE_EE]), and [***Entropy Essay***].

6. TOE Summary Specification

This chapter provides an overview of the TOE operations and describes the security functions:

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

6.1 Overview of TOE Operations

Seagate SEDs use logical block addressing (LBA) to support the user addressable non-volatile memory space from LBA0 to LBAMax. The TOE accepts SATA or SCSI commands to read or write user data in this memory space. All user data in the user addressable non-volatile memory space is encrypted.

The TOE supports a non-volatile memory space that is only available to the TOE. It is referred to as the system area. The system area is used to store keys, key material and CSPs. There is no logical or physical access to the system area from outside of the TOE. The TOE accepts TCG commands to indirectly access or modify values in the system area.

The TOE also supports a non-volatile memory space known as the TCG Data Store Tables. This area is not available to the user but is accessible by an administrator through access-controlled TCG commands. Data in the TCG Data Store Tables is unencrypted. The TOE places no restriction on what data is stored in this area. Guidance provides a warning that directs administrators not to store protected data in the tables.

Seagate SEDs support subdividing user storage. The storage ranges are called bands. Each band is secured with its own authentication key and DEK and has its own key chain. The key chain begins with a drive lock PIN-also known as a TCG PIN or authentication key. The drive lock PIN is used as an input to the PBKDF function to generate an intermediate key. This intermediate key is used as an input to the AES GCM mode function to generate an intermediate wrap key. On TCG Enterprise SSC devices, 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). On TCG Opal SSC devices operating in TCG mode, the wrap key protects a second intermediate key that is used as input to the AES KW function to wrap the MEK. On TCG Opal SSC devices operating in ATA Security mode, the wrap key is used as input to the AES KW function to wrap the MEK.

The SEDs use PINs, passwords, and authentication keys as BEVs. This ST and Seagate uses these terms interchangeably. The SED receives an authentication PIN from the host Authorization Acquisition (AA) component, which could be whatever form or content the AA allows. The Seagate SEDs support authentication PINs with length up to 32 bytes. Multiple PINs are required to control different functionality/resources within the SED. All Seagate SEDs are shipped with a default set of PIN values that allow for open-access of the SED until new PINs and locking settings are established.

The minimum pin length requirement for FIPS 140-2 is 4 bytes. Some CC environments may require the use of full 32 byte PIN values. Seagate supports this and it can be enforced by setting the minimum PIN length value '_MinPINLength' to 32. The '_MinPINLength' is not part of the TCG specification. There is a '_MinPINLength' value associated with each credential and they must be set independently.

For TCG Enterprise, there are four authentication PINs needed in order to gain access to all of the drive's operational resources. These are 32-byte passwords which are identified by the credential names SID (Security Identifier), PSID (Physical Security ID), BandMaster, and EraseMaster.

For TCG Opal, there are five authentication PINs needed in order to gain access to all of the drive's operational resources. These are up to 32-byte passwords which are identified by the credential names SID, PSID, AdminSP Admins, LockingSP Admins, and Users. In addition, for ATA security mode, there are also the User and Master passwords.

The following PINs are BEVs and provide access to encrypted user data: SATA Master Password; SATA User Password; Band Masters 1-32; Erase Master; Locking SP Admin 1-4 Passwords; and User 1-16 Passwords. The following PINs are management passwords, which provide access to SED management functions: SID; PSID; and AdminSP Admin 1-4 Passwords. Further details regarding these PINs are provided in **Table 6: Try Limits Summary**

.

PIN values are never stored directly on the SED. Instead, an entered PIN value is passed to the process that unwraps an intermediate key. If this process is successful then the entered PIN value is valid.

Names of PINs are tied to Enterprise and Opal SSC. This applies to all user PINs (Admins and Users (Opal), and BandMaster (Enterprise)). PSIDs and SIDs never constitute a BEV.

6.2 Cryptographic Support

The TOE includes CAVP-certified cryptographic algorithms providing supporting cryptographic functions. The following functions have been certified in accordance with the identified standards.

Functions	**Standards**	**Certificates**	**Security Functional Requirement**
Cryptographic signature services			
• RSA: 2048 bits	RSASSA-PKCS1-v1_5	A1086, A1093	FCS_COP.1(a), FPT_FUA_EXT.1, FPT_TUD_EXT.1
Cryptographic hashing			
• SHA-256	ISO/IEC 10118-3:2004	A1088, A1092	FCS_COP.1(b)
Message authentication			
• HMAC-SHA-256: 256 bit used in HMAC	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”	A1083, A1091	FCS_COP.1(c)
Key Wrapping			
• AES in KW mode: 256 bits	NIST SP 800-38F	A1094	FCS_COP.1(d)
• AES in GCM mode: 256 bits	ISO/IEC 19772	A1080	FCS_COP.1(d)
Encryption/Decryption			
• AES in GCM Mode: 256 bits	ISO/IEC 19772	A1080	FCS_COP.1(f)
• AES in XTS Mode: 256 bits	IEEE 1619	A1090	FCS_COP.1(f)
Random-bit Generation			
• CTR_DRBG (AES): 256 bits entropy	NIST SP 800-90A	A1082	FCS_RBG_EXT.1, FCS_SNI_EXT.1

Table 5: Cryptographic Functions

6.2.1 Cryptographic Key Generation (FCS_CKM.1(b), FCS_CKM.1(c))

The TOE generates symmetric cryptographic keys using a Random Bit Generator (CTR_DRBG (AES)). The specified symmetric cryptographic key size is always 512 bits for MEKs (FCS_CKM.1(c)). The specified cryptographic key size for all other symmetric keys is 256 bits (FCS_CKM_1(b)).

The TOE uses AES GCM mode to encrypt/decrypt the MEKEKs. This process is also used to decrypt the GCM tag (the known value) for FCS_VAL_EXT.1 Validation. The MEK CSPSKs are stored in plaintext in non-volatile memory. The TOE uses AES XTS-AES-256 mode for data encryption. AES XTS-AES-256 mode requires 512 bit Media Encryption Keys. The MEKs are protected using a two-step AES-KW process that uses the MEKEKs and MEK CSPSKs before storage in non-volatile memory.

6.2.2 Cryptographic Key Destruction (FCS_CKM.4(a), FCS_CKM.4(b), FCS_CKM.4(c), FCS_CKM.4(e), FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_CKM_EXT.6)

The TSF destroys cryptographic keys in accordance with a specified cryptographic key destruction method by using the appropriate method to destroy all encryption keys encrypting the key intended for destruction. (FCS_CKM.4(e))

There are two key destruction scenarios, one for volatile memory and one for non-volatile memory. For volatile memory the TOE uses key destruction methods as specified in FCS_CKM.4.1(b).

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, Verify PIN Function) as described below. The keys are removed immediately after they are used or when they are no longer needed, using a single overwrite of zeroes. Keys are permanently stored by the firmware in the following manner. All keys stored in non-volatile memory are wrapped, except for the second intermediate AES KW key on TCG Enterprise SSC devices. It is stored in non-volatile memory in plaintext form.

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 (D3). When power is removed from the drive, the device goes off and keys are removed. (FCS_CKM_EXT.4(b))

For non-volatile memory, the TOE always writes a new value of the key. All keys and key material are stored in the system area on the media. If the TOE commands the HDD sequencer to write a block in the system area, it can rely on the status bits returned by the sequencer to know that the data was written correctly. The TOE does not have to read the block back to verify that it was written correctly.

TCG Enterprise SED drives use the BandMaster 1-32 or EraseMaster passwords to lock and unlock user bands. TCG Opal SED drives use the Locking SP Admin 1-4 or User passwords 1-16 to lock and unlock user bands.

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))

The TOE performs RSA Digital Signature Algorithm verification with a key size (modulus) of 2048 bits. The function complies with FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes. Seagate uses RSASSA-PKCS1-v1_5. SEDs do not generate RSA keys. RSA Digital Signature Algorithm verification is used to perform updates to the TOE firmware.

The TOE performs SHA-256 cryptographic hashing services that meet the following: ISO/IEC 10118-3:2004. The hash function is used with HMAC-SHA-256 message authentication functions. The TOE also uses the SHA-256 hash functions as part of the RSA signature verification function.

The TOE performs HMAC-SHA-256 message authentication using cryptographic key sizes 256 bit that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". The block size is 64 bytes and the output MAC length size is 32 bytes.

The TOE performs AES GCM mode encryption and decryption using cryptographic key size 256 bits that meet the following: AES as specified in ISO/IEC 18033-3 and NIST SP 800-38F, ISO/IEC 19772 (see also Section 6.1.8 Validation).

The TOE performs AES KeyWrap per SP 800-38F. The inputs to the AES-256 KeyWrap function are a plaintext media encryption key (payload) or an intermediate key, the integrity check value ICV and a plaintext intermediate key. All values are passed on the stack in DRAM. The output of the AES-256 KeyWrap function is a wrapped key or an intermediate key and an integrity check value. Both are returned on the stack in DRAM.

The TOE performs AES KeyUnwrap per SP 800-38F. The inputs to the AES-256 KeyUnwrap function are a wrapped media encryption key (payload) or an intermediate key, the integrity check value ICV and a plaintext intermediate key. All values are passed on the stack in DRAM. The output of the AES-256 KeyUnwrap function is a plaintext key or an intermediate key-if the integrity check PASSES. The media encryption key is returned on the stack in DRAM and then finally programmed into the FDE hardware as the XTS-AES-256 mode encryption key for data encryption/decryption.

The TOE supports both secure FW download and a secure boot procedure. These require PKCS #1, v1.5 RSA signed firmware (FW) packages. The modulus and key size is 2048 bits.

Firmware packages are signed using a secure server using the appropriate RSA private key.

Access to firmware download is controlled by the Firmware Download Port. The Firmware Download Port is a non-standard TCG port that has been added by Seagate to control access to the firmware download function and to prevent unauthorized firmware updates. All Seagate drives ship with the Firmware Download port in the default unlocked state, which allows firmware updates. The Firmware Download port is set to the locked state and set to lock on reset as part of FIPS/CC configuration.

For secure FW download, the TOE receives a signed FW update package from the host and stores it in DRAM. The TOE then verifies the RSA signature of the FW update package using FW routines and the public key in ROM. If the signature is verified to be correct then the new FW package is accepted and stored from DRAM into flash. If the signature does not verify then the FW download is aborted with an error.

For the secure boot process, the TOE first loads the FW from flash into DRAM using FW routines in ROM. The TOE then verifies the RSA signature of the FW in DRAM using FW routines and the public key in ROM. If the signature is verified to be correct then the ROM FW code transfers control to the FW in DRAM. If the signature does not verify then a fatal error is indicated by the TOE.

6.2.4 Cryptographic Key Derivation (FCS_KDF_EXT.1)

TOE SEDs obtain an Authentication PIN from a host Authorization Acquisition (AA) component, which could be any form or content the AA allows. Seagate SEDs support Authentication PINs with length up to 256 bits.

The TOE accepts the imported submask (the Authentication PIN) to derive an intermediate key (MK), as defined in NIST SP 800-132 and uses the keyed-hash function HMAC-SHA-256. The output is at least of equivalent security strength (in number of bits) to the BEV.

6.2.5 Key Chaining (Recipient) (FCS_KYC_EXT.2)

The TOE accepts BEVs of at least 256 bits from the AA, maintaining a chain of intermediary keys originating from the BEV to the DEK and using the following methods:

- key derivation as specified in FCS_KDF_EXT.1—the TOE derives the MK with PBKDF and Authentication PIN
- key wrapping as specified in FCS_COP.1(d)—the process varies depending on the device type and mode, as follows:

- TCG Enterprise SSC devices (TCG mode or ATA Security mode)—the TOE unwraps an intermediate key using AES in GCM mode. The TOE unwraps the media encryption key with a two-step AES KW process
    - TCG Opal SSC devices in TCG mode—the TOE unwraps a chain of two intermediate keys using AES in GCM mode. The TOE then unwraps the media encryption key using AES-KW
    - TCG Opal SSC devices in ATA Security mode—the TOE unwraps an intermediate key using AES in GCM mode. The TOE then unwraps the media encryption key using AES-KW
- the TOE decrypts disk data using 256 bit AES in XTS mode and the MEK.

The TOE maintains an effective strength of 256 bits for symmetric keys.

6.2.6 Random Bit Generation (FCS_RBG_EXT.1)

The TOE performs all deterministic random bit generation services in accordance with NIST SP 800-90A using CTR_DRBG (AES).

The deterministic RBG is seeded by two hardware entropy sources that accumulate a minimum of 256 bits of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

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

The TOE uses 128-bit salt values generated using its CTR_DRBG (AES) implementation (as specified in FCS_RBG_EXT.1) as inputs to the Password Based Key Derivation (PBKDF) function. There is a 128-bit salt value associated with each PIN value in the drive.

The tweak values used for XTS are non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer. The TOE uses DRBG randomly generated 96-bit IV values as inputs to the AES GCM Key Wrap/Unwrap function (FCS_COP.1(d)). There is a 96-bit IV value associated with each PIN value in the drive.

6.2.8 Validation (FCS_VAL_EXT.1(a), FCS_VAL_EXT.1(b))

PINs (BEVs) are used as authentication factors or authorization factors by the TOE. The PINs are not stored in the TOE. Instead, for each PIN (BEV), the PIN is validated by first calling the PBKDF function with the PIN and the associated plaintext salt value as inputs. The output of the PBKDF function is the intermediate key associated with that PIN. Next, call the AES GCM Key Unwrap function with the intermediate key, 8 bits of Additional Authenticated Data (AAD) and IV, TAG and Wrapped wrap key associated with that PIN. If the AES GCM function returns PASS then the PIN is valid and authentication is successful, else the PIN is invalid and authentication is unsuccessful. Many PINs do not have an associated wrap key; in these cases, a null wrap key is used. The complete list of PINs (authorization factors), otherwise known as credentials, is in Table 6 below.

The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a compliant power saving state.

The TOE maintains a separate failure count for each PIN that keeps track of the number of failed authentication attempts. The counter is reset to zero after a successful authentication. For some TCG Opal PINs (as specified in Table 6 below), the maximum allowed failure count is settable to a value in the range 1 to 5. The failure counters either reset to zero on power cycle or are persistent across power cycles. The persistence settings are set in the factory and are not configurable. For SATA credentials, the TOE requires a power cycle/reset of the TOE after 5 consecutive failed validation attempts (FCS_VAL_EXT.1(a)). For all other credentials, the TOE is required to block validation after a number of consecutive failed validation attempts.

The following table identifies the failure count maximum values, persistence and configuration options for each PIN type.

Credential Name	Credential Type	Try Limit	Try Limit Settable	Persistent
ATA Master Password (BEV)	ATA	5 retries	NO	NO
ATA User Password (BEV)	ATA	5 retries	NO	NO
SID	TCG Enterprise (SAS)	100 retries	NO	YES
SID	TCG Enterprise (SATA)	5 retries	NO	NO
PSID	TCG Enterprise	5 retries	NO	NO
Band Masters 1-32 (BEV)	TCG Enterprise (SAS)	100 retries	NO	YES
Band Masters 1-32 (BEV)	TCG Enterprise (SATA)	5 retries	NO	NO
Erase Master (BEV)	TCG Enterprise (SAS)	100 retries	NO	YES
Erase Master (BEV)	TCG Enterprise (SATA)	5 retries	NO	NO
SID	TCG Opal	5 retries	YES	NO
PSID	TCG Opal	5 retries	NO	NO
Locking SP Admin 1-4 Passwords (BEV)	TCG Opal	5 retries	YES	NO
Admin SP Admin 1-4 Passwords (BEV)	TCG Opal	5 retries	YES	NO
User 1-16 Passwords (BEV)	TCG Opal	5 retries	YES	NO

Table 6: Try Limits Summary

6.3 Security Management

The TOE supports management functions for changing and erasing the DEK and for initiating the TOE firmware updates.

6.3.1 Specification of Management Functions (FMT_SMF.1)

The TOE is capable of performing the following management functions:

a) change the DEK, as specified in FCS_CKM.1, when re-provisioning or when commanded

b) erase the DEK, as specified in FCS_CKM.4(a)

c) initiate TOE firmware/software update

d) configure a password for firmware update

e) configure the number of failed validation attempts required to trigger corrective behavior.

The TOE changes a DEK when re-provisioning or when commanded. The Seagate SEDs generate each MEK (the DEK) on the drive by using the drive's SP 800-90A Counter DRBG (256 bits).

MEK destruction is described in Section 6.2.2 (Cryptographic Key Destruction).

Firmware updates are initiated using either the ATA Download Micro Code command (for SATA); or the Write Buffer command (for SAS (SCSI)).

To perform a firmware download, an administrator performs the following steps:

1) Unlock firmware download port.
2) Obtain a genuine Seagate Secure firmware update package from: https://www.seagate.com/support-home
3) The signed firmware package is downloaded to the drive. It is received by the drive firmware and placed into DRAM.
4) The signature is verified using PKCS #1, v1.5 RSA signature algorithm and public key in ROM. If the verification fails an error is returned and the update is not performed. The RSA key/modulus size for all current generation Seagate products is 2048 bits.
5) The firmware update package is written to flash. This overwrites the original firmware.
6) The FW performs a soft reset which loads and runs the new firmware.
7) At this point the firmware download port is unlocked. It can be locked by either performing a power on reset or by resetting the _PortLocking Object PortLocked Column to TRUE.

The password required for firmware updates is the SID. The initial value for SID is a 32-byte manufactured SID (MSID), public drive-unique value that is used as the default PIN. The drive must be "personalized" to change the initial value of the SID to private values. Once the administrator takes ownership of the drive, the SID value is set to the administrator-configured value. The commands to configure the SID value are ATA SECURITY SET PASSWORD, and TCG Set Method.

The TOE provides functions to configure the number of failed validation attempts required to trigger corrective behavior. On TCG Opal devices, an administrator can configure Try limits using the Try Limit command, but only for the following credentials, as identified in Table 6 above: SID; Locking SP Admin 1-4 passwords; Admin SP Admin 1-4 passwords; and User 1-16 passwords.

6.4 User Data Protection

The TOE performs Full Drive Encryption such that the drive contains no plaintext protected data. The TOE is encrypted by default and without user intervention using XTS-AES-256 mode.

6.4.1 Protection of Data on Disk (FDP_DSK_EXT.1)

The TOE is encrypted by default without user intervention using AES in XTS mode (as described in Sections 6.2). There is no restriction on reading or writing data to the SED until a user takes ownership using a TCG controller. Taking ownership locks a drive and constitutes the initialization process providing data-at-rest protection. A locked drive restricts data reads and writes based on the settings of the BandMasters (TCG Enterprise), Locking SP Users (TCG Opal) and User or Master (ATA security mode).

There are three categories of storage: unencrypted for OS use, unencrypted for drive use, and encrypted. On Opal SEDs, unencrypted for OS use includes shadow MBR, which is used for boot. On both Opal and Enterprise SEDs, the system area of disk is not encrypted.

There is no host access to the system area. TCG Data Store tables are available unencrypted in the system area. Administrators can store data in these tables through access-controlled TCG commands. An SED places no restriction on what data is stored. Guidance documentation instructs administrators not to store protected data in the tables.

6.5 Protection of the TSF

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

6.5.1 Firmware Access Control and Update Authentication (FPT_FAC_EXT.1, FPT_FUA_EXT.1)

This section assumes that the firmware download port is in the locked state. Seagate drives all ship with the firmware download port in the unlocked state. The firmware download port is placed into the locked state as part of the steps to enable the CC operating mode.

The TOE's Firmware Access Control requires the administrator to unlock the firmware download port. This requires authentication with the SID credential (password) in order for the firmware update to proceed. To enable firmware download an administrator performs the following steps:

1) Open session to Admin SP.
2) Authenticate with SID credential (password).
3) Set FW download _PortLocking Object PortLocked Column to FALSE.
4) Close Session.

To perform a firmware download, an administrator performs the following steps:

1) Unlock firmware download port.
2) Obtain a genuine Seagate Secure firmware update package from: https://www.seagate.com/support-home
3) The signed firmware package is downloaded to the drive. It is received by the drive firmware and placed into DRAM.
4) The signature is verified using PKCS #1, v1.5 RSA signature algorithm and public key in ROM. If the verification fails an error is returned and the update is not performed. The RSA key/modulus size for all current generation Seagate products is 2048 bits.
5) The firmware update package is written to flash. This overwrites the original firmware.
6) The FW performs a soft reset which loads and runs the new firmware.
7) At this point the firmware download port is unlocked. It can be locked by either performing a power on reset or by resetting the _PortLocking Object PortLocked Column to TRUE.

An error code is returned if any part of the firmware update process fails. The TOE only allows installation of an update if the digital signature has been successfully verified.

The firmware key store and the signature verification algorithm is stored in a write protected area on the TOE. The firmware can only be updated using the authenticated update mechanism by an authorized user where the authorized source that signs TOE updates is Seagate. The TOE authenticates the source of the firmware update using the RSA digital signature algorithm: with a key size (modulus) of 2048 bits. The mechanism uses the Root of Trust for Update RTU key stored in ROM that contains the public key to verify the signature on an update image. An error code is returned if any part of the firmware update process fails. The TOE only allows installation of an update if the digital signature has been successfully verified.

6.5.2 Protection of Key and Key Material (FPT_KYP_EXT.1)

The TOE stores all wrapped keys in non-volatile memory only when the keys have been wrapped. Key wrapping is performed using AES KW and AES GCM, as specified in FCS_COP.1(d).

Intermediate keys are not generated using submask combining.

6.5.3 Power Saving States and Timing (FPT_PWR_EXT.1, FPT_PWR_EXT.2)

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.

"A user-initiated request" is removing the power in the context of a SED.

Separately, the drive can be locked, but remains in a power on state. The requirement does not apply in this case.

6.5.4 RollBack Protection (FPT_RBP_EXT.1)

The TOE supports the functional capability to assure that downgrading to a lower security version number is not possible. With this mechanism if a flaw in FW 1 is found then FW 2 is generated and downloaded to the drive. Using the internal block point mechanism, FW 1 will no longer be compatible with the drive and cannot be downloaded.

If a firmware update package is downloaded to the drive with an invalid firmware revision number, the RollBack protection firmware in the TOE generates and returns an error code and the firmware update package is rejected with one of the following error codes.

Roll back Error Message:

Error Number	Message
0x0B740800	"Invalid Field Parameter"
0x05269920	"Trying to download older firmware over newer firmware"

6.5.5 TSF Testing (FPT_TST_EXT.1)

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

The TOE runs the following Power on Self-Tests:

- ASIC AES: Encrypt and Decrypt KATs performed
- ASIC SHA: Digest KAT performed
- ASIC RSA: Verify KAT performed
- ASIC HMAC: HMAC KAT performed
- ASIC 800-90 DRBG: DRBG KAT performed
- Firmware HMAC: HMAC KAT performed

- Firmware AES-GCM, AES-GCM (large block size): Encrypt and Decrypt KATs performed
- Firmware RSA: Verify KAT performed
- Firmware 800-38F Key Wrap: AES Key Wrap and Unwrap KATs performed
- Firmware SHA: SHA KATs performed
- Firmware Integrity Check: Signature Verification
- Secure boot process.

For each of the cryptographic Known Answer Tests (KATs) listed above, the TOE uses known inputs to calculate an expected cryptographic result, and compares that result to the known result. If the calculated result matches the expected result, the test passes; if it does not match, the test fails.

The TOE performs the Firmware Integrity Check as part of the secure boot process. For the secure boot process, the TOE first loads the FW from flash into DRAM using FW routines in ROM. The TOE then verifies the RSA signature of the FW in DRAM using FW routines and the public key in ROM. If the signature is verified to be correct then the ROM FW code transfers control to the FW in DRAM. If the signature does not verify then a fatal error is indicated by the TOE. This test uses cryptography but is not a test of cryptography per se and is considered a non-cryptographic test.

Additionally, the following Conditional tests are run:

- Firmware Load Check: RSA PKCS#1, v1.5 signature verification of new firmware image is performed before it can be loaded. The new firmware is accepted only if the signature is verified. This test is run when new firmware is downloaded.
- Hardware 800-90 DRBG (CRNGT): Newly generated random number is compared to the previously generated random number. Test fails if they are equal. This test is run when a random number is generated.
- Hardware 800-90 DRBG Entropy (CRNGT): Newly retrieved entropy value is compared to previously retrieved entropy value. Test fails if they are equal. This test is run when entropy is retrieved from entropy pool.

Health tests as described above (the conditional DRBG tests) are run for by all deterministic random bit generation services consistent with section 11.3 NIST SP 800-90A. The self-tests demonstrate the correct operation of the TSF.

6.5.6 Trusted Update (FPT_TUD_EXT.1)

The TOE provides authorized users with the ability to query the current version of the TOE firmware, the ability to initiate the TOE firmware updates, and the ability to verify updates (prior to installing those updates) using the RSA digital signature algorithm (with a key size (modulus) of 2048 bits) provided by Seagate.

For SATA SED drives the TOE firmware version is queried with the SATA Identify command. For SAS SED drives the TOE firmware version is queried with the SAS Inquiry command.

See Section 6.5.1 for more details.

7. Protection Profile Claims

This ST conforms to the *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201*, 1 February 2019, [CPPFDE_EE], including the following optional and selection-based SFRs: FCS_CKM.1(b), FCS_CKM.4(b), FCS_CKM.4(c), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(f), FCS_KDF_EXT.1, FCS_RBG_EXT.1, FCS_CKM.4(e), FPT_FAC_EXT.1, FPT_FUA_EXT.1, and FPT_RBP_EXT.1.

As explained in Section 3, Security Problem Definition, the Security Problem Definition of the [CPPFDE_EE] has been included by reference into this ST, and excludes A.STRONG_CRYPTO.

As explained in Section 4, Security Objectives, the Security Objectives of the [CPPFDE_EE] has been included by reference into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from the [CPPFDE_EE]. The only operations performed on the SFRs drawn from the [CPPFDE_EE] are assignment and selection operations.

Requirement Class	Requirement Component	Source
FCS: Cryptographic Support	FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)	CPPFDE_EE
	FCS_CKM.1(c): Cryptographic Key Generation (Data Encryption Key)	CPPFDE_EE
	FCS_CKM.4(a): Cryptographic Key Destruction (Power Management)	CPPFDE_EE
	FCS_CKM.4(b): Cryptographic Key Destruction (TOE-Controlled Hardware)	CPPFDE_EE
	FCS_CKM.4(c): Cryptographic Key Destruction (General Hardware)	CPPFDE_EE
	FCS_CKM.4(e): Cryptographic Key Destruction (Key Cryptographic Erase)	CPPFDE_EE
	FCS_CKM_EXT.4(a): Cryptographic Key and Key Material Destruction (Destruction Timing)	CPPFDE_EE
	FCS_CKM_EXT.4(b): Cryptographic Key and Key Material Destruction (Power Management)	CPPFDE_EE
	FCS_CKM_EXT.6: Cryptographic Key Destruction Types	CPPFDE_EE
	FCS_COP.1(a): Cryptographic Operation (Signature Verification)	CPPFDE_EE
	FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)	CPPFDE_EE
	FCS_COP.1(c): Cryptographic Operation (Message Authentication)	CPPFDE_EE
	FCS_COP.1(d): Cryptographic Operation (Key Wrapping)	CPPFDE_EE
	FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption)	CPPFDE_EE
	FCS_KDF_EXT.1: Cryptographic Key Derivation	CPPFDE_EE

Requirement Class	Requirement Component	Source
	FCS_KYC_EXT.2: Key Chaining (Recipient)	CPPFDE_EE
	FCS_RBG_EXT.1: Random Bit Generation	CPPFDE_EE
	FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	CPPFDE_EE
	FCS_VAL_EXT.1(a): Validation (SATA)	CPPFDE_EE
	FCS_VAL_EXT.1(b): Validation (SAS)	CPPFDE_EE
FDP: User Data Protection	FDP_DSK_EXT.1: Protection of Data on Disk	CPPFDE_EE
FMT: Security Management	FMT_SMF.1: Specification of Management Functions	CPPFDE_EE
FPT: Protection of the TSF	FPT_FAC_EXT.1: Firmware Access Control	CPPFDE_EE
	FPT_FUA_EXT.1 Firmware Update Authentication	CPPFDE_EE
	FPT_KYP_EXT.1: Protection of Key and Key Material	CPPFDE_EE
	FPT_PWR_EXT.1: Power Saving States	CPPFDE_EE
	FPT_PWR_EXT.2: Timing of Power Saving States	CPPFDE_EE
	FPT_RBP_EXT.1: Rollback Protection	CPPFDE_EE
	FPT_TST_EXT.1: TSF Testing	CPPFDE_EE
	FPT_TUD_EXT.1: Trusted Update	CPPFDE_EE

Table 7: SFR Protection Profile Sources

8. Rationale

This security target includes by reference the [CPPFDE_EE] Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the [CPPFDE_EE] assumptions and excludes A.STRONG_CRYPTO. [CPPFDE_EE] security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow [CPPFDE_EE] application notes and assurance activities. Consequently, [CPPFDE_EE] rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 9 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Cryptographic Support	**User Data Protection**	**Security Management**	**Protection Of The TSF**
FCS_CKM.1(b)	X			
FCS_CKM.1(c)	X			
FCS_CKM.4(a)	X			
FCS_CKM.4(b)	X			
FCS_CKM.4(c)	X			
FCS_CKM.4(e)	X			
FCS_CKM_EXT.4(a)	X			
FCS_CKM_EXT.4(b)	X			
FCS_CKM_EXT.6	X			
FCS_COP.1(a)	X			
FCS_COP.1(b)	X			
FCS_COP.1(c)	X			
FCS_COP.1(d)	X			
FCS_COP.1(f)	X			
FCS_KDF_EXT.1	X			
FCS_KYC_EXT.2	X			
FCS_RBG_EXT.1	X			

	Cryptographic Support	User Data Protection	Security Management	Protection Of The TSF
FCS_SNI_EXT.1	X			
FCS_VAL_EXT.1(a)	X			
FCS_VAL_EXT.1(b)	X			
FDP_DSK_EXT.1		X		
FMT_SMF.1			X	
FPT_FAC_EXT.1				X
FPT_FUA_EXT.1				X
FPT_KYP_EXT.1				X
FPT_PWR_EXT.1				X
FPT_PWR_EXT.2				X
FPT_RBP_EXT.1				X
FPT_TST_EXT.1				X
FPT_TUD_EXT.1				X

Table 8: Security Functions vs. Requirements Mapping