Seagate® Secure NVMe Self-Encrypting Drives Security Target

Version 0.24
March 7, 2024

Prepared for:

47488 Kato Road
Fremont, CA 94538

Phison Electronics Corporation
No.1, Qun-Yi Road, Jhunan, Miaoli County,
Taiwan 350, R.O.C.

Prepared by:
Leidos Inc.
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

Revision History

Version	Date	Description	Author(s)
0.1	07/18/2022	Initial Revision	Leidos
0.2	09/09/2022	Updates provided by the vendor	Leidos
0.3	09/15/2022	Updates provided by the vendor	Leidos
0.4	09/22/2022	Updates provided by the vendor	Leidos
0.5	11/15/2022	Updates provided by the vendor	Leidos
0.6	12/05/2022	Updates provided by the vendor	Leidos
0.7	1/9/2023	Updates provided by the vendor	Leidos
0.8	2/13/2023	Modify context from Leidos' input	Phison
0.9	3/22/2023	Updates provided by the vendor	Leidos
0.10	4/18/2023	Modify context	Phison
0.11	5/10/2023	Confirm Firmware version	Phison
0.12	6/6/2023	Updates provided by the vendor	Leidos
0.13	6/12/2023	Modify context	Phison
0.14	7/6/2023	Modify context	Leidos
0.15	7/18/2023	Incorporated the latest TDs.	Leidos
0.16	8/7/2023	Modify context	Leidos
0.17	8/20/2023	Modify context	Leidos
0.18	9/3/2023	Modify Context	Leidos
0.19	9/7/2023	Modify Context	Leidos
0.20	9/9/2023	Modify Context	Leidos
0.21	10/24/2023	Modify context per NIAP validator comments	Leidos
0.22	12-22/2023	Modified context per Evaluator comments	Leidos
0.23	2/5/2024	Modified context per Evaluator comments	Leidos
0.24	3/7/2024	Modified context information	Phison

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 the Seagate® Secure NVMe Self-Encrypting Drives provided by Seagate Technology, LLC, and developed by Phison.

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 NVMe Self-Encrypting Drives Security Target

ST Version – Version 0.24

ST Date – March. 7, 2024

TOE Identification – Seagate® Secure NVMe Self-Encrypting Drives

The specific TOE products and models include:

Product Name	Model #	Standard	Firmware
Nytro 5550H 15mm U.2/U.3 Mixed Use (3 DWPD)	XP800LE70025 XP1600LE70025 XP3200LE70025 XP6400LE70025 XP12800LE70025	SED with TCG Opal	SE4SA530 SGEBHG02
Nytro 5350H 15mm U.2/U.3 Read Intensive (1 DWPD)	XP1920SE70025 XP3840SE70025 XP7680SE70025 XP15360SE70025	SED with TCG Opal	SE4SA530 SGEBHG02
Nytro 5550M 15mm U.2/U.3 Mixed Use (3 DWPD)	XP800LE70055 XP1600LE70055 XP3200LE70055 XP6400LE70055 XP12800LE70055	SED with TCG Opal	SE4SA530 SGEBHG02

Product Name	Model #	Standard	Firmware
Nytro 5350M 15mm U.2/U.3 Read Intensive (1 DWPD)	XP1920SE70055 XP3840SE70055 XP7680SE70055 XP15360SE70055	SED with TCG Opal	SE4SA530 SGEBHG02
Nytro 5550M 7mm U.2/U.3 Mixed Use (3 DWPD)	XP800LE10025 XP1600LE10025 XP3200LE10025 XP6400LE10025	SED with TCG Opal	SE4SA530 SGEBHG02
Nytro 5350M 7mm U.2/U.3 Read Intensive (1 DWPD)	XP1920SE10025 XP3840SE10025 XP7680SE10025	SED with TCG Opal	SE4SA530 SGEBHG02

Table 1: TOE Models and Firmware Versions

TOE Developer – Phison Electronics Corporation

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 demonstrate exact conformance to the following CC specifications:

- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201, February 1, 2019,* [CPPFDE_EE] and including the following optional and selection-based SFRs: FCS_CKM.1(b), FCS_CKM.4(b), 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, 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.
- **TD0769:** FIT Technical Decision for FPT_KYP_EXT.1.1 – Although the Security Target claims FP_KYP_EXT.1.1.

The following NIAP Technical Decisions issued for [CPPFDE_EE] are 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.
- **TD0766:** FIT Technical Decision for FCS_CKM.4(d) Test Notes – this TD modifies the tests for FCS_CKM.4(d). This Security Target does not claim compliance to FCS_CKM.4(d).

This ST and the TOE conform 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
BEV	Border Encryption Value
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CPP	Collaborative Protection Profile

CPPFDE_EE	Collaborative Protection Profile for Full Drive Encryption – Encryption Engine
CRNGT	Continuous Random Number Generator Test
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
HDD	Hard Disk Drive
HMAC	Hashed Message Authentication Code
ICV	integrity check value for the KW function.
IT	Information Technology
IV	Initialization Vector
KEK	Key Encryption Key
KMD	Key Management Description
LBA	Logical Block Addressing
MSID	Manufacturer's Secure ID (MSID) PIN
NVMe	Nonvolatile Memory Express
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
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SID	Security Identifier, (aka Drive Owner PIN)
SFR	Security Functional Requirement
SP	Security Provider
SPD	Security Problem Definition
SPI	Serial Peripheral Interface
SSC	Security Subsystem Class
SSD	Solid State Drive
ST	Security Target
TEK	Transfer Encryption Key
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 the Seagate® Secure NVMe Self-Encrypting Drives by Seagate Technology, LLC. The TOE model numbers and firmware versions are identified in Section 1.1.

The Seagate® Secure NVMe Self-Encrypting Drives implement NIST-recommended cryptographic algorithms. The CAVP certificates 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 NVMe Self-Encrypting 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.

2.1 TOE Overview

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

The Opal SSC supports NVMe (PCIe). While the physical form factor and firmware of the drives differ, all models included in the TOE support the requirements defined in [CPPFDE_EE].

Seagate® Secure NVMe Self-Encrypting Drives 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 comprises SSC Opal devices. The Opal SSC series supports NVMe interfaces of a solid-state drive (SSD). (see Table 2). All SEDs meet the requirements set forth in this document and provide the same security functionality.

The following table identifies each TOE model along with its capacity, firmware, and ASIC. All models implement the TCG Opal interface.

All drives include the PS5020-E20 Module V1.00 (firmware) and Phison PS5020-E20 (hardware) cryptomodules. The cryptomodule is implemented on an ARM Cortex-R5 processor, which is based upon the ARMv7-R architecture.

Product Name	Model #	Capacity User (GB)	Firmware
Nytro 5550H 15mm U.2/U.3 Mixed Use (3 DWPD)	XP800LE70025 XP1600LE70025 XP3200LE70025 XP6400LE70025 XP12800LE70025	800 1600 3200 6400 12800	SE4SA530 SGEBHG02
Nytro 5350H 15mm U.2/U.3 Read Intensive (1 DWPD)	XP1920SE70025 XP3840SE70025 XP7680SE70025 XP15360SE70025	1920 3840 7680 15360	SE4SA530 SGEBHG02
Nytro 5550M 15mm U.2/U.3 Mixed Use (3 DWPD)	XP800LE70055 XP1600LE70055 XP3200LE70055 XP6400LE70055 XP12800LE70055	800 1600 3200 6400 12800	SE4SA530 SGEBHG02
Nytro 5350M 15mm U.2/U.3 Read Intensive (1 DWPD)	XP1920SE70055 XP3840SE70055 XP7680SE70055 XP15360SE70055	1920 3840 7680 15360	SE4SA530 SGEBHG02
Nytro 5550M 7mm U.2/U.3 Mixed Use (3 DWPD)	XP800LE10025 XP1600LE10025 XP3200LE10025 XP6400LE10025	800 1600 3200 6400	SE4SA530 SGEBHG02
Nytro 5350M 7mm U.2/U.3 Read Intensive (1 DWPD)	XP1920SE10025 XP3840SE10025 XP7680SE10025	1920 3840 7680	SE4SA530 SGEBHG02

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 hardware as identified in Table 2.

All models can be installed with either firmware version SE4SA530 or SGEBHG02. The try limit value settings differ between the two versions, but the cryptographic algorithm designs are the same. The Seagate market type (either Channel, which is the retail market, or OEM) decides which version of firmware to deploy in a particular model.

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 NVMe Self-Encrypting Drives:

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

2.2.2.1 Cryptographic Support

The TOE includes NIST-validated 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, initiating the TOE firmware updates, and configuring a password for firmware updates.

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 power saving states. The TOE runs a suite of self-tests during initial start-up (on power on).

2.3 TOE Documentation

Seagate publishes a number of documents that provide information and guidance for the deployment of the TOE. In particular, the following Common Criteria specific guide references the security-related guidance material for all devices in the evaluated configuration:

Guidance Documentation:

- Seagate Secure® NVMe Self-Encrypting Drive Common Criteria Configuration Guide, Version Draft V1.1, February 9, 2023.

3. Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of 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[1]. The TOE implements all cryptographic functionality, therefore there are no cryptographic functions in the Operational Environment as stated in 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 NVMe Self-Encrypting Drives.

[1] See Section 3 for the rationale to exclude the A.STRONG_CRYPTO assumption.

4. Security Objectives

Like 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 NVMe 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.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: Validation of Cryptographic Elements
- 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_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: Validation
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) 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) 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) 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) 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]***
- ***For non-volatile memory [***
  - ***that employs a wear-leveling algorithm, the destruction shall be executed by a [***
    - ***overwrite with a new value of a key of the same size,***
    - ***block erase]]***

] that meets the following: [no standard].

5.2.1.5 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.

5.2.1.6 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.

5.2.1.7 Cryptographic Key Destruction Types (FCS_CKM_EXT.6)

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

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

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

- ***RSA Digital Signature Algorithm with a key size (modulus) of [4096-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***

].

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

FCS_COP.1.1(b) The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [***SHA-256, SHA-512***] that meet the following: [*ISO/IEC 10118-3:2004*].

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

FCS_COP.1.1(c) The TSF shall perform [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"***].

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

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

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

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

5.2.1.13 Cryptographic Key Derivation (FCS_KDF_EXT.1)

FCS_KDF_EXT.1.1 The TSF shall accept [***a conditioned password 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.

5.2.1.14 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.

5.2.1.15 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 [***HMAC_DRBG (any)***].

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

- [***At least one] 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.

5.2.1.16 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***].

5.2.1.17 Validation (FCS_VAL_EXT.1)

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

- ***key wrap as specified in FCS_COP.1 (d)***
- ***]***

FCS_VAL_EXT.1.2 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 The TSF shall [

- ***require power cycle/reset the TOE after [the number of try limits defined in Table 10: Try Limits Summary 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 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 the number of failed validation attempts required to trigger corrective behavior, configure a password for firmware update]

].

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 digest of the RSA public key in ROM.

5.2.4.3 Protection of Key and Key Material (FPT_KYP_EXT.1)[2]

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)*****].**

5.2.4.4 Timing of Power Saving States (FPT_PWR_EXT.1)[3]

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 [**comparing the security version in the new firmware package to the security version of the installed firmware and ensuring the update version is not less than the installed version**].

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 SHA-256, SHA-512: Digest KAT performed**
  - **ASIC RSA: Verify KAT performed**
  - **Firmware HMAC-SHA-256: HMAC KAT performed**
  - **Firmware XTS-AES-256: Encrypt and Decrypt KATs performed**
  - **Firmware RSA: Verify KAT performed**
  - **Firmware 800-90 DRBG: DRBG KAT performed**
  - **Firmware 800-132 PBKDF: PBKDF KAT performed**
  - **Firmware Integrity Check: Signature Verification**
  - **Firmware SHA-512: SHA-512 KAT performed**
  - **Secure boot process**

- **Conditional tests:**

[2] Modified per TD0769.
[3] Modified per TD0464.

- **Firmware Load Check: RSA PSS signature verification of new firmware image is done before it can be loaded.**
- **Firmware 800-90 DRBG: Newly generated random number is compared to the previously generated random number. Test fails if they are equal.**
- **Firmware 800-90 DRBG Entropy: Newly generated random number is compared to the previously generated random number. Test fails if they are equal.**
- **Firmware 800-38F Key Wrap: AES Key Wrap and Unwrap KATs performed**

].

5.2.4.8 Trusted Update (FPT_TUD_EXT.1)

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

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

FPT_TUD_EXT.1.3 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 The TOE summary specification shall describe how the TOE meets each SFR, including a proprietary Key Management Description (Appendix E), 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

When shipped from the factory, the drive is configured with a single data band called Band 0 (also known as the Global Data Band) which comprises LBA 0 through LBA max. The host may allocate Band1 by specifying a start LBA and an LBA range. Seagate SEDs (TOE) use logical block addressing (LBA) to support the user-addressable non-volatile memory space from LBA0 to LBAMax. The TOE accepts NVMe commands to read or write user data in this memory space. All user data in the user-addressable non-volatile memory space is encrypted.

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

Seagate SEDs support subdividing user storage. The storage ranges are called locking ranges. Each locking range is secured with its own authentication key and Data Encryption Key (DEK). Seagate's proprietary Key Management Description Document Section 3 provides more details on the keys that make up the key hierarchy and describes the connection between pairs of keys.

Seagate's Key Management Description Document shows the key chain from Authentication key to the DEK. Each locking range has its own key chain. A chain contains five keys: Drive Lock PIN (a.k.a. TCG PIN and Authentication key), Transfer Key(TEK), Key Encryption Key (KEK) and DEK. The TEK is wrapped and unwrapped with the Authentication key using AES-KW. The KEK is wrapped and unwrapped with TEK using AES-KW. The DEK is wrapped and unwrapped with the KEK using AES-KW.

The SEDs use PINs, passwords, and authentication keys as BEVs. This ST and Seagate use 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 of 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.

For TCG Opal, there are five 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: User's Security Identifier (SID); Physical SID (public drive-unique value (PSID); Admin SP Admins; Locking SP Admins; and Users.

The drive has two security providers (SPs) called the "Admin SP" and the "Locking SP." These act as gatekeepers to the drive security services. Security-related commands will not be accepted unless they also supply the correct credentials to prove the requester is authorized to perform the command.

The following PINs are BEVs and provide access to encrypted user data: Locking SP Admin 1-4 Passwords; and User 1-9 Passwords. The following PINs are management passwords, which provide access to SED management functions:

SID; Physical Security ID (PSID); and Admin SP Admin 1-4 Passwords. Further details regarding these PINs are provided in Table 10: Try Limits Summary Details.

PIN values are never stored directly on the SED. Instead, an entered PIN value is verified via KW function defined per SP800-38F. If this process is successful then the entered PIN value is valid.

Names of PINs are tied to Opal SSC. This applies to all user PINs (admins and users (Opal)). PSIDs (Physical Security IDs) and SIDs (User's Security Identifier) are never going to be a BEV. The PSID corresponds to the known unique value printed on the device.

Encrypting drives use one in-line encryption engine for each port, employing AES XTS-AES-256 mode to encrypt all data prior to being written on the media and to decrypt all data as it is read from the media. The encryption engines are always in operation and cannot be disabled.

6.2 Cryptographic Support

The TOE includes NIST-validated 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: 4096 bits	Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS	A3307, A3308	FCS_COP.1(a), FPT_FUA_EXT.1, FPT_TUD_EXT.1
Cryptographic hashing			
• SHA-256, SHA-512	ISO/IEC 10118-3:2004	A3307, A3308 (SHA-512 only)	FCS_COP.1(b)
Message authentication			
• HMAC-SHA-256: 256 bit used in HMAC	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”	A3307	FCS_COP.1(c)
Key Wrapping			
• AES in KW mode: 256 bits	NIST SP 800-38F	A3307	FCS_COP.1(d)
Encryption/Decryption			
• AES in CBC Mode: 256 bits (implemented as a prerequisite for AES Key Wrap, not as a separate encryption/decryption function)	FIPS Pub 197, Advanced Encryption Standard	A3307	Prerequisite to FCS_COP.1(d)
• AES in XTS Mode: 256 bits	IEEE 1619	A3307	FCS_COP.1(f)
Random-bit Generation			
• HMAC_DRBG (any): 256 bits entropy	NIST SP 800-90A	A3307	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 uses its CAVP-validated implementation of HMAC_DRBG(any) to generate symmetric keys.

The specified symmetric cryptographic key size is always 512 bits for DEKs (FCS_CKM.1(c)). AES in XTS-256 mode uses separate 256 bit keys for Initialization Vector (IV) and block encryption, which results in the need to

provide 512 bits of key material for AES-XTS-256 mode. The DEKs are protected using a two-step AES-KW process that uses the KEK before storage in non-volatile memory.

The specified cryptographic key size for all other symmetric keys is 256 bits (FCS_CKM_1(b)).

The TOE uses AES-KW to encrypt/decrypt the TEKs/KEKs/DEKs. This process is also used to decrypt the C_PIN (the known value) for FCS_VAL_EXT.1 Validation.

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

There are two key destruction scenarios, one for volatile memory and one for non-volatile memory. Both types of memory used by the TOE implement 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 locking range. 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 locking range, the existing key is overwritten with a new value of a key. Unlocked locking range keys are stored in plaintext form in volatile memory but cyphertext in non-volatile memory for use by the FDE engine as needed. All other plaintext keys are temporarily stored in volatile memory 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.

The 64-byte Data Encryption Key (DEK) is a random number which is generated by the drive, never leaves the drive, and is inaccessible to the host system. The TOE does not import any DEK from the outside of the SSD. The DEK is itself encrypted when it is stored on the media and decrypted (i.e. plaintext) when it is in volatile temporary storage. A unique data encryption key is used for each of the drive's possible 9 data ranges. The drive has two security providers (SPs) called the "Admin SP" and the "Locking SP." These act as gatekeepers to the drive security services. Security-related commands will not be accepted unless they also supply the correct credentials to prove the requester is authorized to perform the command.

The Admin SP allows the drive's owner to enable or disable firmware download operations (see Section 6.4). Access to the Admin SP is available using the SID (Secure ID) password or the MSID (Manufacturers Secure ID) password. The Locking SP controls read/write access to the media and the cryptographic erase feature.

Description	Type	Generation	Storage	Zeroization
Data Encryption/Decryption Key(Global Range) Data Encryption/Decryption Key(LBA Range 1 – 8)	XTS-AES-256 (encrypt/decrypt unit is 512 byte)	SP800-90A HMAC-SHA256-DRBG	Stored encrypted by Key Encryption Key and stored in non-volatile memory. Stored as plaintext in volatile memory and registers.	Overwritten by SP800-90A HMAC-SHA256-DRBG in non-volatile memory. Actively overwritten with a new key value in volatile memory. TCG_Revert TCG_Revert SP TCG_GenKey
Firmware Decryption Key	XTS-AES-256 (encrypt/decrypt unit is 512 byte)	Generated outside the module	Stored as plaintext in volatile memory	N/A

Description	Type	Generation	Storage	Zeroization
			and non-volatile memory.	
Key Encryption Key(Global Range) Key Encryption Key(LBA Range 1 – 8)	AES Key Wrap 256	SP800-90A HMAC-SHA256-DRBG	Encrypted by Transfer Encryption Key with AES Key Wrap 256 and stored in non-volatile memory. Stored as plaintext in volatile memory.	Upon receiving the TCG_Revert command, the key will be replaced by zeros in volatile memory.
Transfer Encryption Key(Admin1 – Admin4) Transfer Encryption Key(User1 – User9)	AES Key Wrap 256	SP800-90A HMAC-SHA256-DRBG	Encrypted by Password-base-key with AES Key Wrap 256 and stored in non-volatile memory. Plaintext in volatile memory.	Upon receiving the TCG_Revert command, the key will be replaced by zeros in volatile memory.
Password-based-key of admin1 – admin 4 password in Locking SP Password-based-key of user1 – user9 password in Locking SP	AES Key Wrap 256	SP800-132 PBKDF2	Plaintext in volatile memory.	Overwritten with zeroes in volatile memory.
Admin SP SID Password	32 bytes	this value is initially generated during manufacturing for initialization only; after initialization the operator can generate and enter this value	PBKDF and AES Key Wrap dummy data and stored in non-volatile memory. Stored as plaintext in volatile memory.	Overwritten with zeroes in volatile memory via TCG End of Session Command
Locking SP Admin1 – Admin4 Password	32 bytes	N/A TCG Set C_PIN Command	PBKDF and AES Key Wrap dummy data and stored in non-volatile memory.	Overwritten with zeroes in volatile memory via TCG End of Session Command

Description	Type	Generation	Storage	Zeroization
			Stored as plaintext in volatile memory.	
Password-based key of Locking SP User password 1-9	32 bytes	N/A TCG Set C_PIN Command	PBKDF and AES Key Wrap dummy data and stored in non-volatile memory. Stored as plaintext in volatile memory.	Overwritten with zeroes in volatile memory via TCG End of Session Command.
PBKDF2 Internal State	SP800-132 PBKDF2 with HMAC SHA 256	SP800-132 PBKDF2 with HMAC SHA 256	Stored as plaintext in volatile memory.	Overwritten with zeroes in volatile memory.
Last seed value for TRNG	4 bytes seed	HW RNG(TRNG)	Stored as plaintext in volatile memory.	Overwritten with zeroes in volatile memory.
Last seed value for DRBG	256 bits seed	SP800-90A HMAC-SHA256-DRBG	Stored as plaintext in volatile memory.	Overwritten with zeroes in volatile memory.
Seed Material	SP800-90A HMAC-SHA256-DRBG	HW RNG(TRNG)	Stored as plaintext in volatile memory.	Overwritten with zeroes in volatile memory.
Internal State (V and Key) of SP800-90A	SP800-90A HMAC-SHA256-DRBG K is 32 bytes V is 32 bytes	Initialized via DRBG instantiation	Stored as plaintext in volatile memory.	Overwritten with zeroes in volatile memory.
RSA Code Sign Public Key	RSA-4096 + SHA 512	N/A - generated outside of the module. 1.During mass production flow, the hashed value of the public key is stored to the OTP-ROM of the controller 2.Signed FW binary file contains public key and will be	Stored as plaintext in volatile memory. hashed value is stored in OTP-ROM	N/A

Description	Type	Generation	Storage	Zeroization
		stored to non-volatile memory.		

Table 6: Key Table

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 uses key destruction methods as specified in FCS_CKM.4.1(b). This is described in more detail below.

The TOE always writes a new value of the DEKs/KEKs and TEKs keys. All keys and key material including the DEKs/KEKs and TEKs, but excluding the Authentication Key (PIN) are stored in the system area on the media.

There are separate areas for system data and user data in non-volatile memory. The non-volatile memory key destruction on the solid state drives is used only for system data. For non-volatile memory the TOE performs a write of a new value of a key to the system areas used for key storage. The non-volatile memory system performs any erase or wear leveling functions as necessary. All keys and key material including the DEKs/KEKs and TEKs are stored in the non-volatile memory.

TCG Opal SED drives use the Locking SP Admin 1-4 or User passwords 1-9 to lock and unlock user locking range.

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 4096 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. The SEDs do not generate RSA keys. RSA Digital Signature Algorithm verification is used to verify updates to the TOE firmware.

The TOE performs SHA-256 cryptographic hashing services that meet the following: ISO/IEC 10118-3:2004. The TOE uses SHA-256 with HMAC-SHA-256 as part of the HMAC_DRBG function. The TOE also uses the SHA-512 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 table below provides a summary of the Seagate® Secure NVMe Self-Encrypting Drives keys.

Name	Use	Type	Source	Storage
BEV	Authentication factor	256-bit conditioned password	Input from AA	Volatile memory
TEK	Used to encrypt KEK	AES KW 256	HMAC-SHA256-DRBG	non-volatile & volatile memory
KEK	Used to encrypt DEK	256-bit AES AES KW 256	HMAC-SHA256-DRBG	non-volatile & volatile memory
DEK	Data encryption key	256-bit AES	HMAC-SHA256-DRBG	non-volatile & volatile memory

Table 7 TOE Key Summary

The TOE performs AES Key Wrap per SP 800-38F. The inputs to the AES-256 Key Wrap function are shown in the table below. The output of the AES-256 Key Wrap function is a wrapped key or intermediate key.

The plaintext TEK is wrapped using the Password Based-Key consisting of a 256-bit cryptographic hash of password and AES-KW 256. The plaintext KEK is wrapped using the AES-KW 256 encrypted TEK. The plaintext DEK is encrypted using the AES-KW 256 encrypted KEK. The TOE performs AES XTS mode encryption using a key size of 256-bits that meet the following: AES as specified in ISO /IEC 18033-3 and XTS as specified in IEEE 1619.

AES Wrap Function	Key	Input (Data)	Output (Data)
1st AES Wrap	Password Based-Key	Plaintext TEK	Encrypted TEK
2nd AES Wrap	TEK	Plaintext KEK	Encrypted KEK
3rd AES Wrap	KEK	Plaintext DEK	Encrypted DEK

Table 8 TOE AES Wrap Functions

The TOE performs AES Key Unwrap per SP 800-38F. The inputs to the AES-256 Key Unwrap are shown in the table below. When an administrator or user enters a PIN, the TOE validates the PIN 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 ephemeral plaintext Authentication Key (identified as the Password Based-Key in Table 9) associated with that PIN. The second call performs the AES-KW unwrap with the Authentication Key. A successful unwrap function will result in the correct integrity check value for the KW function (ICV), indicating that the PIN is valid and authentication is successful. Otherwise, the PIN is invalid and authentication is unsuccessful. The complete list of PINs (authorization factors), otherwise known as credentials is in Table 10.

The encrypted TEK is unwrapped using the Password Based-Key consisting of a 256-bit cryptographic hash of password and AES-KW 256 unwrap function, if the unwrap function unwraps the result with the correct ICV then the unwrap TEK is valid and this plaintext TEK authentication is successful.

The encrypted KEK is unwrapped using the plaintext TEK and the AES-KW 256 unwrap function. A successful unwrap operation will result with the correct ICV indicating that the unwrapped KEK is valid and this plaintext KEK authentication is successful.

The encrypted DEK is unwrapped using the plaintext KEK and AES-KW 256 unwrap function. A successful unwrap operation will result with the correct ICV indicating that the unwrapped DEK is valid and this plaintext DEK authentication is successful. The TOE performs AES XTS mode encryption using a key size of 256-bits that meet the following: AES as specified in ISO /IEC 18033-3 and XTS as specified in IEEE 1619.

AES Unwrap Function	Key	Input (Data)	Output (Data)
1st AES Unwrap	Password Based-Key	Encrypted TEK	Plaintext TEK
2nd AES Unwrap	TEK	Encrypted KEK	Plaintext KEK
3rd AES Unwrap	KEK	Encrypted DEK	Plaintext DEK

Table 9 TOE AES Unwrap Functions

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 of 256 bits.

The TOE accepts a conditioned password submask (the Authentication PIN) to derive an Authentication Key, as defined in NIST SP 800-132 using the PBKDF2 function with the keyed-hash function HMAC-SHA-256 algorithm. The TOE uses randomly generated 256 bit salt values as inputs to the Password Based Key Derivation (PBKDF) function. There is a 256 bit salt value associated with each PIN value in the drive. The key output is 256-bits in length.

The key output of the derivation function will always be 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 256 bits from the AA, maintaining a chain of intermediate 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 Authentication Key with PBKDF and Authentication PIN,
- key wrapping as specified in FCS_COP.1(d): The TOE Decrypts the TEK with Authentication Key. The TOE Unwraps the DEK with a two-step process. First the KEK is unwrapped with the TEK using AES-KW. The DEK is then unwrapped with the KEK loaded from non-volatile memory--using AES-KW.
- the TOE Decrypts disk data with XTS-AES-256 mode and DEK.

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 HMAC_DRBG (any) and SHA-256 cryptographic hashing services.

The SSD SEDs use one hardware entropy source to seed the RBG 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.

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

The TOE uses randomly generated 256 bit salt values using an RBG described in FCS_RBG_EXT.1 as inputs to the Password Based Key Derivation (PBKDF) function. There is a 256 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 does not use nonces or IV values.

6.2.8 Validation (FCS_VAL_EXT.1)

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 ephemeral plaintext Authentication Key associated with that PIN. The second call is the AES-KW unwrap function with the Authentication Key. If unwrap function check results in the correct integrity check value for the KW function (ICV), the PIN is valid and authentication is successful, else the PIN is invalid and authentication is unsuccessful. The complete list of PINs (authorization factors), otherwise known as credentials is in Table 10 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. The persistence settings are set in the factory and are not configurable.

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

All models can be installed with either firmware version SE4SA530 or SGEBHG02. The try limit value settings differ for between the two versions, but the cryptographic algorithm designs are the same.

The Seagate market type (either Channel, which is the retail market, or OEM) decides which version of firmware to deploy in a particular model. It is not up to the final end-user to select the firmware to deploy; rather, this decision is made by the Seagate's market types. The channel market refers to the retailer market, which is different compared to the OEM market.

The difference between firmware versions is the number Try Limit retries that are permissible:

- Firmware version SE4SA530 – 5 retries
- Firmware version SGEBHG02 – 100 retries

All versions of the TOE implement the same cryptographic module and the firmware variants do not have any impact on the cryptographic functionality.

Credential Name / Firmware	Credential Type	Try Limit	Try Limit Settable	Persistent
SID (SE4SA530)	TCG Opal	5 retries	YES	NO
SID (SGEBHG02)	TCG Opal	100 retires	YES	YES
PSID (SE4SA530)	TCG Opal	5 retries	YES	NO
PSID (SGEBHG02)	TCG Opal	100 retires	YES	YES
Locking SP Admin 1-4 Passwords (BEV) (SE4SA530)	TCG Opal	5 retries	YES	NO
Locking SP Admin 1-4 Passwords (BEV) (SGEBHG02)	TCG Opal	100 retires	YES	YES
Admin SP Admin 1-4 Passwords (BEV) (SE4SA530)	TCG Opal	5 retries	YES	NO
Admin SP Admin 1-4 Passwords (BEV) (SGEBHG02)	TCG Opal	100 retires	YES	YES
User 1-9 Passwords (BEV) (SE4SA530)	TCG Opal	5 retries	YES	NO
User 1-9 Passwords (BEV) (SGEBHG02)	TCG Opal	100 retries	YES	YES

Table 10: Try Limits Summary Details

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 try limit defaults to 5 or 100 and it is modifiable. The non-persistent failure counters are reset to zero on power cycle.

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

DEK destruction is described in Section 6.2.2: Cryptographic Key Destruction.

Firmware updates are initiated using NVMe Firmware Image Download/Firmware Image Commit Command.

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

1) Unlock firmware download port.

2) The signed firmware package is downloaded to the drive. It is received by the drive firmware and placed into volatile memory.

3) The signature is verified using PKCS #1, v2.1 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 4096 bits.

4) The firmware update package is written to non-volatile memory. This overwrites the original firmware.

5) The FW performs a soft reset which loads and runs the new firmware.

6) 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 the 32-byte Manufacturer's SID (MSID), a fixed value when fresh out of the box 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 NVME SECURITY SET PASSWORD, and TCG Set Method.

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:XTS (as described in Section 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 Locking SP Users (TCG Opal).

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 an Opal-SED, 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).

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

Seagate drives are shipped 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. This section assumes that the firmware download port is in the locked state.

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 volatile memory.

4) The signature is verified using PKCS #1, v2.1 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 4096 bits.

5) The firmware update package is written to non-volatile memory. 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 are 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 4096 bits. The mechanism uses the Root of Trust for Update RTU key stored in ROM that contains the hashed public key. This key will be used for verifying with the public key that comes along with the signed firmware (FW) binary file. After successful verification, the public key in the binary will then be used 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 keys in non-volatile memory only when the keys have been wrapped. Key wrapping is performed using AES KW, as specified in FCS_COP.1(d).

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 Messag

Error Stat	Message
StatusType = 1h; StatusCode = 07h	“Invalid Firmware Image”

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:

- Power on Self-Tests:
  - ASIC SHA-256, SHA-512: Digest KAT performed

  - ASIC RSA: Verify KAT performed
  - Firmware HMAC-SHA-256: HMAC KAT performed
  - Firmware XTS-AES-256: Encrypt and Decrypt KATs performed
  - Firmware RSA: Verify KAT performed
  - Firmware 800-90 DRBG: DRBG KAT performed
  - Firmware 800-132 PBKDF: PBKDF KAT performed
  - Firmware Integrity Check: Signature Verification
  - Firmware SHA-512: SHA-512 KAT performed
  - Secure boot process
- Conditional tests:
  - Firmware Load Check: RSA PSS signature verification of new firmware image is done before it can be loaded.
  - Firmware 800-90 DRBG: Newly generated random number is compared to the previously generated random number. Test fails if they are equal.
  - Firmware 800-90 DRBG Entropy: Newly generated random number is compared to the previously generated random number. Test fails if they are equal.
  - Firmware 800-38F Key Wrap: AES Key Wrap and Unwrap KATs performed.

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 non-volatile memory into volatile memory using FW routines in ROM. The TOE then verifies the RSA signature of the FW in volatile memory 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 volatile memory. If the signature does not verify then a fatal error is indicated by the TOE.

The Continuous RNG test for the DRBG generates a new random number which is compared to the previously generated random number. The test fails if they are equal. This test is run when a random number is generated.

The TSF performs RSA PKCS#1, v1.5 signature verification of a new firmware image 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.

Health tests as described above (the conditional DRBG tests) are run for 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 4096 bits) provided by Seagate.

See Section 6.5.1 for more details.

7. Protection Profile Claims

This ST is conformant 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_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, 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_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
	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 Validation	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_FAC_EXT.1: Firmware Access Control	CPPFDE_EE

Requirement Class	Requirement Component	Source
FPT: Protection of the TSF	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 11: 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 12: Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	CryptographicSupport	**UserDataProtection**	**SecurityManagement**	**ProtectionOfTheTSF**
FCS_CKM.1(b)	X			
FCS_CKM.1(c)	X			
FCS_CKM.4(a)	X			
FCS_CKM.4(b)	X			
FCS_CKM_EXT.4(a)	X			
FCS_CKM_EXT.4(b)	X			
FCS_CKM_EXT.6	X			

	CryptographicSupport	UserDataProtection	SecurityManagement	ProtectionOfTheTSF
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			
FCS_SNI_EXT.1	X			
FCS_VAL_EXT.1	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 12: Security Functions vs. Requirements Mapping