Western Digital Technologies, Inc.

Ultrastar DC HC560 TCG Enterprise HDD, SED and Ultrastar DC HC570 TCG Enterprise HDD, SED

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.20
Date: December 19, 2025

Protection of Data at Rest

Table of Contents

Tables

Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Ultrastar® DC HC560 TCG Enterprise HDD SED and Ultrastar® DC HC570 TCG Enterprise HDD SED. It contains the security rules under which each module must operate and describes how each module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows.

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

The Western Digital Ultrastar DC HC560 TCG Enterprise HDD SED, hereafter referred to as Ultrastar DC HC560, Cryptographic Module, cryptographic module, or CM, and the Western Digital Ultrastar DC HC570 TCG Enterprise HDD SED, hereafter referred to as Ultrastar DC HC570, Cryptographic Module, cryptographic module, or CM are self-encryption drives (SED) that comply in general with the specifications listed in 13.2 Trusted Computing Group Specifications and specifically with the TCG Storage Architecture Core Specification [TCG Core] with the Trusted Computing Group (TCG) Storage Security Subsystem Class (SSC): Enterprise Specification [TCG Enterprise].

The TCG Storage SSC: Enterprise Specification defines a management interface for host application software to activate, provision, and manage encryption of user data. The specification includes data structures and their required content, and mechanisms for managing and configuring Authentication Credentials and access controls. The security architecture provides a locking mechanism by which an Authentication Credential (i.e., a password) can be set by an operator to enable control of access to user data. After an operator authenticates to the appropriate role and locks access to user data access user data is inaccessible. This implementation complies with the lock-based authentication model specified in IG 4.1.A.

2.1 Description

Purpose and Use

The Cryptographic Module's intended use is by US Federal agencies or other markets that require FIPS 140-3 validated hardware modules. The primary function of the Cryptographic Module is to provide data encryption, access control, and cryptographic erase of the data stored on the hard drive media within the CM. The operator of the Cryptographic Module interfaces with the Cryptographic Module through application software that resides within a host system.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

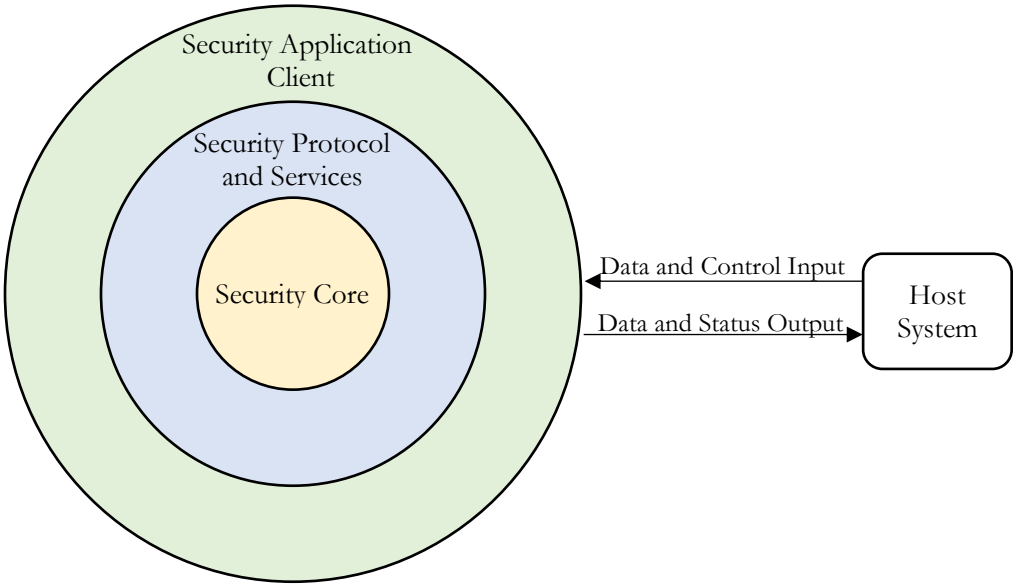

Figure 1 - Security Subsystem Components

Cryptographic Boundary

Figure 2 and Figure 3 depict the physical form of each CM within the scope of this security policy document. The CM is a multi-chip embedded embodiment. The hard opaque surface of the enclosure defines the cryptographic boundary. All components within this boundary satisfy FIPS 140-3 requirements. The Cryptographic Module firmware disables the SIO port pins outlined by the red box to the right of the SAS connector in Figure 2 and Figure 3.

Tested Operational Environment's Physical Perimeter (TOEPP)

Tested Operational Environment's Physical Perimeter (TOEPP) – The physical enclosure of the CM defines the TOEPP's physical perimeter.

TOEPP and Cryptographic Boundary - The cryptographic boundary consists of CM's physical enclosure, the externally attached PCBA, all firmware implementations within the immutable Security Core firmware that resides within the ROM of the Western Digital SoC9B ASIC, and the mutable Security Protocol and Services and Security Application Client firmware layers. The Cryptographic Module writes mutable firmware from disk media into DRAM memory on power up.

Photographs

Figure 2 - Ultrastar DC HC560

Figure 3 - Ultrastar DC HC570

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification - Hardware

The Ultrastar DC HC560 and Ultrastar DC HC570 cryptographic modules are tested on the operational environments listed below.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Ultrastar DC HC560/0F38603	WUH722020BL4205	RY07, R5G4, RG01, VM18	ARM Cortex M3, ARM Cortex-R8, Synopsys ARC HS36	20 TB, 4Kn
Ultrastar DC HC560/0F38653	WUH722020BL5205	RY07, R5G4, RG01, VM18	ARM Cortex M3, ARM Cortex-R8, Synopsys ARC HS36	20 TB, 512e
Ultrastar DC HC570/0F48003	WUH722222AL4205	R7J4, RG01	ARM Cortex M3, ARM Cortex-R8, Synopsys ARC HS36	22 TB, 4Kn
Ultrastar DC HC570/0F48053	WUH722222AL5205	R7J4, RG01	ARM Cortex M3, ARM Cortex-R8, Synopsys ARC HS36	22 TB, 512e

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

The Ultrastar DC HC560 components listed below and identified in Figure 4 and Figure 5 are excluded from the cryptographic boundary.

Table Ultrastar DC HC560 Exclusions

Exclusion*	Rationale
-3V via	The -3V via connects to the Negative Switching Regulator (NSR) output of the PLSI device. It supplies -3V to the preamp chip in the head assembly through an inductor. If the PLSI device fails or inductor opens the preamp voltage input drops to 0V. This disables disk media read/write functions and renders user data inaccessible. Therefore, the -3V via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
5V via	The voltage level on the 5V circuit is dependent on the presence of voltage on the 5V_EFUSE circuit. An N-channel Power MOSFET isolates the 5V circuit from the 5V_EFUSE circuit. A MOSFET failure will cause the voltage on the 5V circuit to drop to 0V. This results in the immediate shutdown of the CM. Therefore, the 5V via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
5V_EFUSE via	The 5V_EFUSE circuit connects to the output of an integrated dual electronic eFuse, designed to protect circuitry from overcurrent and overvoltage events, in applications that require hot swap operation and in-rush current control. If the electronic eFUSE device fails, the voltage on the 5V_EFUSE circuit drops to 0V. This results in the immediate shutdown of the CM. Therefore, the 5V _EFUSE via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
5V_PREAMP via	The 5V_PREAMP via connects to the 5V_EFUSE circuit though a zero-ohm resistor. Any failure of the 5V_EFUSE circuit to supply 5V or a failure of the zero-ohm resistor causes the voltage on the 5V_PREAMP circuit to drop 0V. This results in the immediate shutdown of the CM. Therefore, the 5V_PREAMP via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
INAND_VCCQ2 via	The voltage level of the INAND_VCCQ2 depends on a functioning synchronous step-down DC/DC converter, which is dependent on the presence of voltage on the 5V_EFUSE circuit and V3.3_PLR3 circuit. A 5V_EFUSE circuit failure, V3.3_PLR3 circuit failure, or DC/DC converter component failure causes the voltage on the INAND_VCCQ2 circuit to drop to 0V. The INAND_VCCQ2 circuit supplies power to the serial boot flash device. The CM fails to bootup if the INAND_VCCQ2 drops to 0V. Therefore, the INAND_VCCQ2 via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
V3.3_PLR3 via	V3.3_PLR3 is dependent on the presence of 5 volts on the +5V_EFUSE net, which supplies power to a Power Large Scale Integrated (PLSI) circuit device. Any failure of the 5V_EFUSE circuit to supply 5V or a failure of the PLSI device causes the voltage on the V3.3_PLR3 circuit to drop 0V. This results in the immediate shutdown of the CM. Therefore, the V3.3_PLR3 via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
AUX_IN via	The voltage level on the AUX_IN circuit allows the SoC9 ASIC to determine the temperature of the disk enclosure. The CM initiates a thermal safety shutdown if the temperature is outside the normal operating range the CM automatically shuts down. Therefore, the AUX_IN via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
Drive Motor Control Cable	The Drive Motor Control Cable is a three-conductor ribbon cable that serves a mechanical purpose. The three conductors, designated SPN_A, SPN_B, and SPN_C provide drive spindle rotor position data to the Spindle Driver within PLSI device. Therefore, the Drive Motor Control Cable satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.

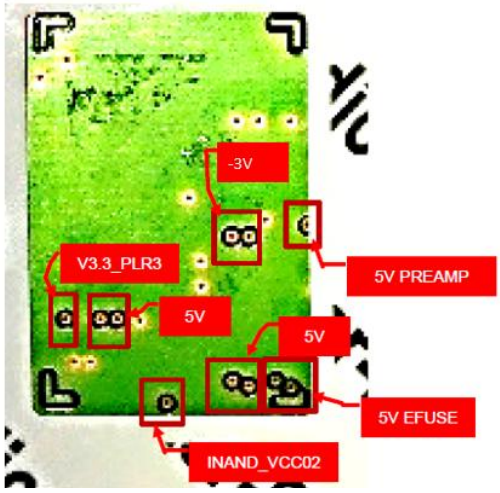

Figure 4 - Excluded Components, Ultrastar DC HC560

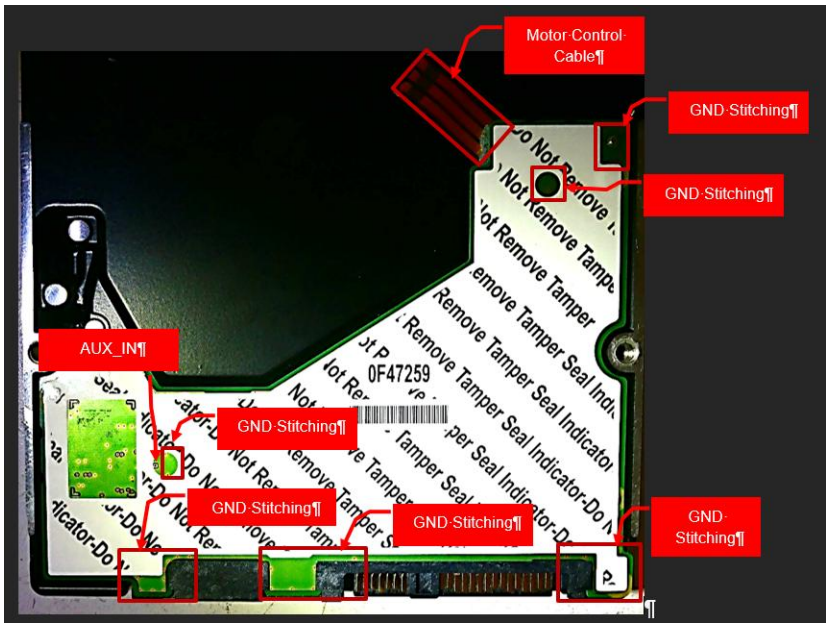

Figure 5 - Excluded Components, Ultrastar DC HC560

The Ultrastar DC HC570 components listed below and identified in Figure 6, Figure 7 and Figure 8 are excluded from the cryptographic boundary.

Table Ultrastar DC HC570 Exclusions

Exclusion*	Rationale
5V_EFUSE via	The 5V_EFUSE circuit connects to the output of an integrated dual electronic eFuse, which connects to ground through a capacitor. The eFuse device protects circuitry from overcurrent and overvoltage events, in applications that require hot swap operation and in-rush current control. If the electronic eFUSE device fails or the capacitor shorts to ground, the voltage on the 5V_EFUSE circuit drops to 0V. This results in the immediate shutdown of the CM. Therefore, the 5V _EFUSE via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.

Exclusion*	Rationale
INAND_VCC_X via	INAND_VCC_X circuit powers the OptiNAND device. INAND_VCC_X derives from INAND_VCC through a fuse. The output of the fuse connects to ground through two capacitors. If the fuse opens or either capacitor shorts to ground, the OptiNAND loses power and shuts down. CM responds by inhibiting writes to the CM. Therefore, the INAND_VCC_X via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
J2_VEE via	J2_VEE supplies -3V supply to the preamp chip in the head assembly through an inductor. If the inductor fails and the preamp input voltage drops to 0V, read/write functions to the disk media are disabled. This renders user data inaccessible. Therefore, the J2_VEE via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
READY_LED via	READY_LED circuit serves as a status indicator that is within the scope of the Status Port. Therefore, the READY_LED via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
SIOEN_AE via	The SIOEN_AE signal enables serial communication between the SoC9 ASIC and the preamp chip in the head assembly. A malfunction by the SoC ASIC or lose of the direct connection between the SoC9 ASIC to the preamp chip prevents the proper setup of read/write functionality. This renders user data inaccessible. Therefore, the SIOEN_AE via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
SWDCLK via	SWDCLK circuit provides a debug clock signal for the ARM JTAG Interface port. The ARM JTAG Interface port is disabled in production drives for use in the field. Therefore, the SWDCLK via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
V3.3_PLR3 via	V3.3_PLR3 is dependent on the presence of 5V on the +5V_EFUSE net, which supplies power to a Power Large Scale Integrated (PLSI) circuit device. V3.3_PLR3 is sourced from the 3.3V linear regulator output of the KOI PLSI. Any failure of the 5V_EFUSE circuit to supply 5V or a failure of the PLSI device causes the voltage on the V3.3_PLR3 circuit to drop 0V. V3.3_PLR3 connects to ground through a capacitor. If the capacitor shorts to ground the PLSI immediately shuts down. Either failure mode results in the immediate shutdown of the CM. Therefore, the V3.3_PLR3 via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
WRP via	WRP and WRM form a differential pair connected to the head assembly's Write Channel. The loss of the direct connection between the WRP output of the SoC9 ASIC to the head assembly significantly reduces the robustness of the transmitted data. The inability to cancel electromagnetic interface present on the differential pair could cause the corruption of user data written to disk media. The corruption of user data cannot compromise the SSPs stored within CM. Therefore, the WRP via satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.
Drive Motor Control Cable	The Drive Motor Control Cable is a three-conductor ribbon cable that serves a mechanical purpose. The three conductors, designated SPN_A, SPN_B, and SPN_C provide drive spindle rotor position data to the Spindle Driver within PLSI device. Therefore, the Drive Motor Control Cable satisfies the excluded components requirements in 7.2.3.1 Cryptographic boundary general requirements.

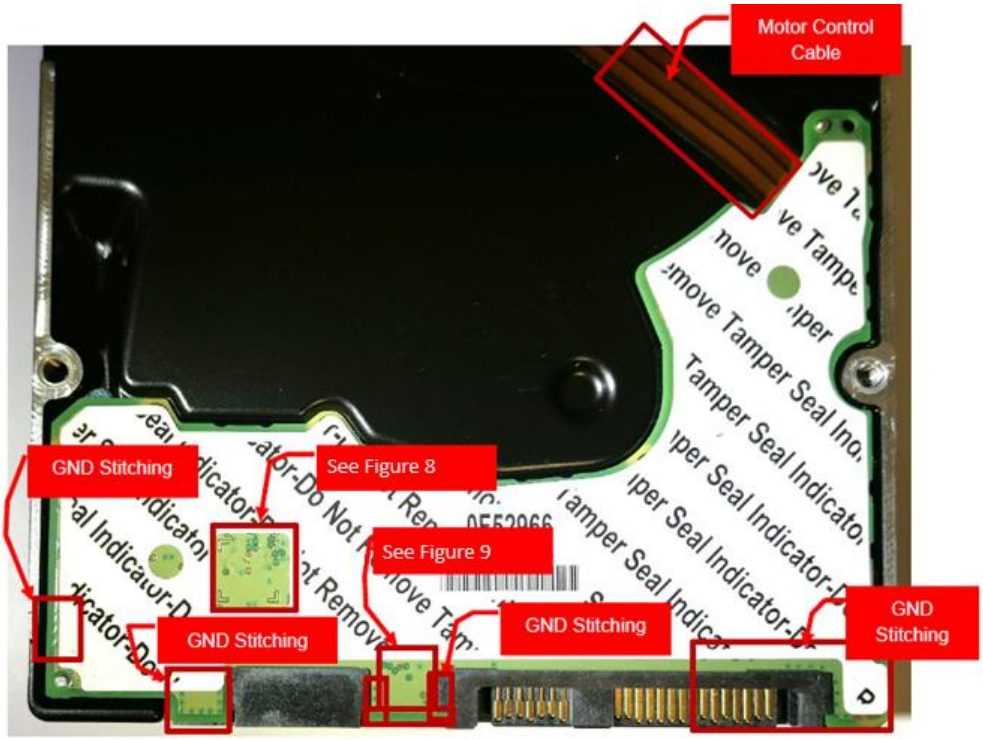

Figure 6 - Excluded Components, Ultrastar DC HC570

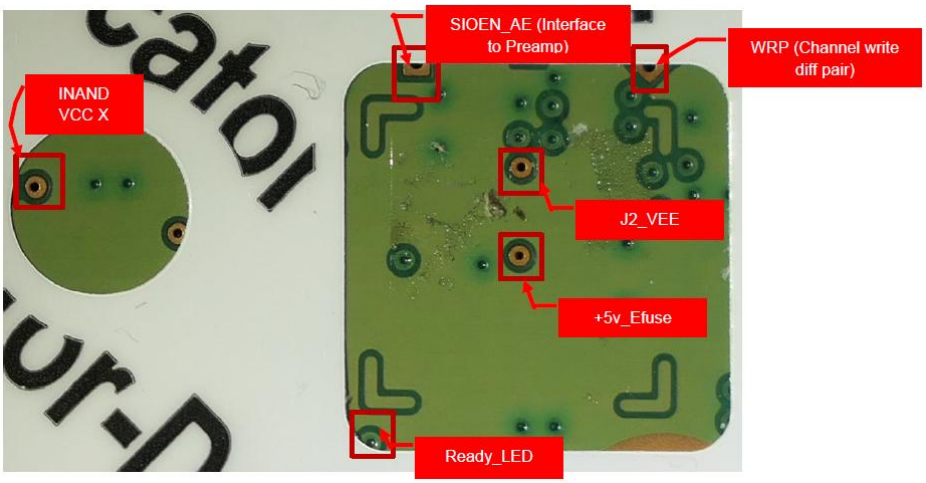

Figure 7 - Excluded Components, Ultrastar DC HC570

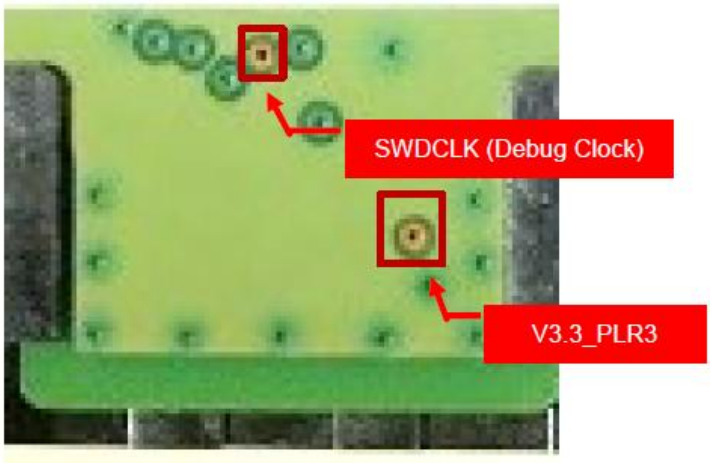

Figure 8 - Excluded Components, Ultrastar DC HC570

2.4 Modes of Operation

Mode Name	Description	Type	Status Indicator
isFIPS	The cryptographic module is operating as a compliant FIPS 140-3 module	Approved	1. The Level 0 Discovery service returns a value of 1 from the in FIPS global indicator data field and 2. The Firmware Download Control LockOnReset field is set to PowerCycle and 3. For each configured BandMaster, the state of each listed attribute is set as shown below. * LockOnReset = PowerCycle * ReadLockEnabled = True * WriteLockEnabled = True

Table 3: Modes List and Description

Section 11.1 (Installation, Initialization and Startup Procedures) specifies the recommended and mandatory steps necessary for the secure installation, initialization, and start-up of the cryptographic module as a FIPS 140-3 SL2 compliant module. The Crypto Officer is responsible for assuring that the mandatory configuration requirements remain unchanged. When correctly configured the Cryptographic Module always powers up isFIPS mode.

The cryptographic module does not support non-approved or non-allowed security functions.

Mode Change Instructions and Status:

The table above specifies the conditions that must be true for the Cryptographic Module to operate in isFIPS mode. Any action by the operator that negates the PowerCycle setting of the Firmware Download Control's LockOnReset field transitions the CM to a noncompliant state. Any action by the operator that negates the attribute setting, specified in the Modes List and Description table for LockOnReset, ReadLockEnabled, or WriteLockEnabled for any configured BandMaster transitions the CM to a noncompliant state.

Degraded Mode Description:

The Cryptographic Module does not support a degraded operational mode.

2.5 Algorithms

The Cryptographic Module supports NIST SP 800-131A compliant approved algorithms listed in the Approved Algorithms table.

Approved Algorithms

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2099	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CBC	AES 3580	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A2101	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	AES 3580	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-KWP	A2098	Direction - Decrypt Key Length - 256	SP 800-38F
AES-XTS	A2101	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
Counter DRBG	A2098	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
HMAC-SHA2-256	HMAC 2280	Key sizes < block size - Yes Key size = block size - Yes Key sizes > block size - Yes	FIPS 198-1
PBKDF	A2100	Iteration Count - Iteration Count: 2-1024 Increment 1 Password Length - Password Length: 32	SP 800-132
RSA SigVer (FIPS186-4)	A2098	Signature Type - PKCSPSS Modulo - 3072	FIPS 186-4
RSA SigVer (FIPS186-4)	A2099	Signature Type - PKCSPSS Modulo - 3072	FIPS 186-4
SHA2-256	A2099	Message Length - Message Length: 256, 0-65536 Increment 8	FIPS 180-4
SHA2-256	SHS 2942	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor Affirmed Algorithms

The Cryptographic Module implements the FIPS Vendor Affirmed cryptographic algorithms listed in the Vendor-Affirmed Algorithms table.

Name	Properties	Implementation	Reference
CKG-Direct	Key Type:Symmetric Key Generation	N/A	SP 800-133rev2 Section 4 example #1 and IG D.H
CKG-XTS	Key Type:Symmetric Key Generation	N/A	SP 800-133rev2 Section 6.3 example #2 and IG C.I

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms

The Cryptographic Module does not implement non-Approved but allowed algorithms.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed

The Cryptographic Module does not implement non-Approved but allowed algorithms with no security claimed.

N/A for this module.

Non-Approved, Not Allowed Algorithms

None. The cryptographic module does not implement algorithms that are not NIST SP 800-131A compliant.

N/A for this module.

2.6 Security Function Implementations

The Cryptographic Module implements the Security Function Implementations listed in the Security Function Implementations table..

Name	Type	Description	Properties	Algorithms
Decryption	BC-UnAuthDecrypt	Block Cipher Decryption	:	AES-CBC: (AES 3580)
Derived_Key_Generation	PBKDF	Password-Based Key Derivation	Publications: [IG D.N]	PBKDF: (A2100) HMAC-SHA2-256: (HMAC 2280) SHA2-256: (SHS 2942)
Digest_Generation	SHA	Secure Hash Standard	Publications: [IG C.B]	SHA2-256: (SHS 2942)
Digest_Verification	SHA	Secure Hash Standard	Publications: [IG C.B]	SHA2-256: (SHS 2942)
Encryption	BC-UnAuthEncrypt	Block Cipher Encryption	Publications: [IG 10.3.A]	AES-CBC: (AES 3580)
Entropy	ENT-ESV	Entropy Source	Publications: [IG 9.3.A] [IG D.J] [IG D.L] [IG D.O]	
FW_Authenticity	DigSig-SigVer	Digital Signature Verification. Verifies the authenticity of a	Publications: [IG C.E], [IG C.F]	RSA SigVer (FIPS186-4): (A2098)

Name	Type	Description	Properties	Algorithms
		CM firmware image.		SHA2-256: (SHS 2942)
FW_Integrity	DigSig-SigVer	Digital Signature Verification. Verifies the integrity of a CM firmware image	Publications: [IG C.E] [IG C.F]	RSA SigVer (FIPS186-4): (A2098) SHA2-256: (SHS 2942)
Key Wrap_D	BC-Auth	Symmetric Authentication Decryption	:	AES-KWP: (A2098) AES-ECB: (AES 3580)
Keyed_Digest_Generation	MAC	Message Authentication Generation	Publication: [IG C.B]	HMAC-SHA2-256: (HMAC 2280) SHA2-256: (SHS 2942)
Keyed_Digest_Verification	MAC	Message Authentication Verification	Publications: [IG C.B]	HMAC-SHA2-256: (HMAC 2280) SHA2-256: (SHS 2942)
LRK_NSK Generation	CKG	Symmetric Key Generation	Publication: [IG C.I]	CKG-Direct: ()
MEK Generation	CKG	Symmetric Key Generation	Publication: [IG D.H]	CKG-XTS: ()
OptiNAND_Descrambler	BC-UnAuth	Block Cipher	:	AES-CBC: (A2099)
FW_Auth_OptiNAND	DigSig-SigVer	Digital Signature Verification	Publication: [IG C.E] [IG C.F]	RSA SigVer (FIPS186-4): (A2099) SHA2-256: (A2099)
FW_Integrity _OptiNAND	DigSig-SigVer	Digital Signature Verification.	Publication: [IG 10.3.A] [IG C.E] [IG C.F]	RSA SigVer (FIPS186-4): (A2099) SHA2-256: (A2099)
RBG	DRBG	Random bit generator	Publication: [IG D.L]	Counter DRBG: (A2098)
SecureLoader_Integrity	DigSig-SigVer	Digital Signature Verification.	Publication: [IG C.F] [IG C.E]	RSA SigVer (FIPS186-4): (A2098) SHA2-256: (SHS 2942)

Name	Type	Description	Properties	Algorithms
Symmetric_Key_Generation	CKG	Generates AES 256 symmetric cryptographic keys	Publications: [IG D.H]	CKG-Direct: ()
User_Data_Decryption	BC-UnAuthDecrypt	Block Cipher Decryption	Publication: [IG C.I]	AES-XTS: (A2101) AES-ECB: (A2101)
User_Data_Encryption	BC-UnAuthEncrypt	Block Cipher Encryption	Publication: [IG C.I]	AES-XTS: (A2101) AES-ECB: (A2101)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES-XTS Key Pair Generation

The Cryptographic Module performs a key comparison test on each LRK.AESKey/LRK.XTS keyset and NSK.AESKey/NSK.XTS keyset to assure compliance with FIPS 140-3 IG C.I XTS-AES Key Generation Requirements every time the CM generates an LRK.AESKey/LRK.XTS keyset and a NSK.AESKey/NSK.XTS keyset, to assure compliance for all derived MEKs. The only use of any AES-XTS key pair is the encryption and decryption of data-at-rest within the cryptographic module in a storage application.

PBKDF2

The password consists of a minimum of twelve (12) hexadecimal bytes values and a maximum of thirty-two (32) hexadecimal bytes values that range from 0x00 to 0xFF. The probability that a random attempt correctly guesses a twelve (12) byte password, or a false acceptance occurs is equal to 1 in 7.92E+28. The probability that a random attempt correctly guesses a thirty-two (32) byte password, or a false acceptance occurs is equal to 1 in 1.16E+7728.

The default 1024 iteration count, 256-bit Salt and HMAC-SHA2-256 (Cert #HMAC 2280) algorithm conforms to SP 800-132, Option 2a. The Master key (MK) encrypts and decrypts data protection keys.

The PBKDF2 derived keys, K_u, and K_a, are only used in a data storage application.

2.8 RBG and Entropy

The SP 800-90A rev1-compliant Deterministic Random Bit Generator (DRBG), implemented as a CTR_DRBG mechanism, uses an AES-256 block cipher derivation function to generate encryption keys for use within the cryptographic boundary of the Cryptographic Module. Paragraphs titled Entropy Information and RBG Information summarize the characteristics of the entropy noise source that resides within the cryptographic boundary and seeds the CTR_DRBG.

Cert Number	Vendor Name
E13	Western Digital Corporation

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
ESV, E13	Physical	0L23689, IC SOC9, Rev 2.1; ARM Cortex M3, ARM Cortex R8	32 bits	2.7	None

Table 8: Entropy Sources

Entropy Information

The hardware-based ring oscillator noise source referenced in the Entropy Sources table consist of eight (8) identical groups of four (4) independent ring oscillator circuits. Within each group, there are four (4) distinct logic inverter gate designs that consist of 19, 23, 31, and 39 gates. The oscillators are physically isolated from other active traces within the SoC9 ASIC. No configuration steps are necessary to operate the entropy source in a compliant manner. As stated in the Public Use Document for E13, on power up the Cryptographic Module executes an entropy source initialization sequence that collects sufficient samples of raw noise to verify the health of its entropy source prior to seeding the DRBG. If the initialization sequence returns false, the Cryptographic Module transitions to an error state that blocks the execution of all security services.

RBG Information

The output of the entropy source referenced in the Entropy Sources table consists of the raw data generated from thirty-two (32) free running ring oscillators. Eight identical groups of four variable length inverter chains define the implementation. Each 32-bit sample produces at least 2.7 bits of entropy. Each time the DRBG is instantiated or reseeded, the CM concatenates one hundred sixty (160) 32-bit samples to seed the DRBG. This equates to 5120 bits of entropy data and translates to at least 431.379 bits of min-entropy. This seeds the CTR_DRBG with approximately 287 bits of security strength (~287.59 bits of entropy input and ~143.79 bits of nonce). Seeding the DRBG with at least 287 bits of security strength exceeds the requirement to seed the DRBG with 256 bits of security strength.

2.9 Key Generation

The cryptographic module utilizes an SP 800-90A rev1-compliant CTR_DRBG to generate symmetric cryptographic keys, which comply with sections 6.1, 6.2.3 and 6.3 of SP 800-133r2. Each symmetric keyset consists of an encryption and a signing key. Specifically,

- the Root Keyset consists of a 256-bit Root Encryption Key and 256-bit Root Signing Key
- the Global Active Keyset (AEK) consists of a 256-bit Global Active Encryption Key and a 256-bit Global Active Signing Key
- the SED Active Keyset consists of a 256-bit SED Active Encryption Key and a 256-bit SED Active Signing Key
- the SED AdminSP Active Keyset consists of a 256-bit SED AdminSP Active Encryption Key and a 256-bit SED AdminSP Active Signing Key
- SED LockingSP Active Keyset consists of a 256-bit SED LockingSP Active Encryption Key and a 256-bit SED LockingSP Active Signing Key

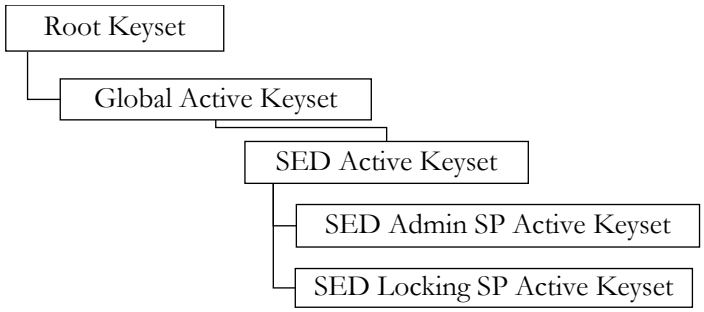

Figure 9 - Symmetric Key Tree

2.10 Key Establishment

Key Agreement Information

The cryptographic module does not support a key establishment scheme.

Key Transport Information

The cryptographic module does not support a key transport scheme.

2.11 Industry Protocols

The cryptographic module does not implement any Industry Protocol.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

As a hardware module, the Cryptographic Module uses the standard 29-pin Serial Attached SCSI (SAS) connector that conforms to the mechanical requirements of SFF 8680. The Ports and Interfaces table identifies the Cryptographic Module's physical ports and associated FIPS defined logical interfaces. The two-wire SIO Serial Port connector consists of signal and ground. Prior to shipment, Western Digital disables the SIO port. The Cryptographic Module does not provide a maintenance access interface.

The Cryptographic Module does not support a trusted channel communication link between the CM and a host system.

The Cryptographic Module does not support a Control Output logical interface.

Physical Port	Logical Interface(s)	Data That Passes
SAS Connector	Control Input	Used to transmit SCSI commands from the host system to the CM.
UART	Control Input	The UART port vias are covered by a tamper evident seal.
SAS Connector	Data Input	Used to transmit data and firmware update images from the host system to the CM.
UART	Data Input	The UART port vias are covered by a tamper evident seal.
SAS Connector	Data Output	Used to transmit data from the Cryptographic Module to the host system.
UART	Data Output	The UART port vias are covered by a tamper evident seal.
Power Connector	Power	Power connector
SAS Connector	Status Output	Used to transmit status data from the CM to the host system. READY_LED
UART		The UART port vias are covered by a tamper evident seal.
None	Status Output	Download Port: This logical port has two valid states, locked, and unlocked. If locked, the CM logically blocks firmware downloads. If unlocked, the CM logically allows the Cryptographic Officer to download firmware.

Table 9: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

The Cryptographic Module implements the authentication methods listed in the Authentication Methods table.

.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Credential PIN Authentication	After first authenticating with module unique data, the CO role authenticates to the Module with a 12-to-32 bytes Authentication Credential PIN password. Byte value range (ea.): 0x00 to 0xFF.	Authority_Digest_Verification	12-byte PIN: 96 bits- Permutations: 7.92E+28; 32-byte PIN: 256 bits- Permutations: 1.16E+77	Permutations: 7.92E+28 Authentication Time: 2.094965 msec Guess Probability (1 min): 3.61E-25; For 32-byte Permutations: 1.16E+77 Authentication Time: 2.094965 msec Guess Probability (1 min): 2.47E-73

Table 10: Authentication Methods

Note: E = log2(RL), where E = authentication strength, R = pool of unique characters and L = password length defines the security strength of an Authentication Credential PIN. See Calculating Password Entropy [PW].

4.2 Roles

The Module supports distinct User and Cryptographic Officer (CO) operator roles. The Cryptographic Module enforces role separation by requiring a role identifier and authentication credential in the form of a Personal Identification Number (PIN). The Cryptographic Module enforces role dependent service access rules. The Approved Services table maps services to Crypto Officer and User roles. The Cryptographic Module implements Access Control in layers. The top layer of the implementation consists of Access Control Lists (ACLs). ACLs are lists of Access Control Elements (ACEs). The boolean state of an ACE associated with an authority within a role determines access to a service. After authentication, an authority's associated ACE boolean expression is set to be True. Prior to authentication, an authority's associated ACE boolean expression is set to False. Closing a TCG session or powering off the Cryptographic Module disables all previously authenticated authorities by setting the ACE Boolean expression associated with all authenticated authorities to False. After powering up the CM and opening a new TCG session, the operator must execute the Authenticate service to enable an authority within the Crypto Officer and User roles.

The module does not support a maintenance role

The Cryptographic Module does not support concurrent operators.

The Cryptographic Module encrypts and signs all authentication data, associated with a role, stored outside the ACM. The ACM imports the encrypted and signed authentication, verifies the signature, and decrypts the authentication data. Before validating the operator supplied authentication data, the ACM checks for try limit violations.

The lock-based authentication method implemented by the Cryptographic Module remains secure because the purpose of the implementation is to protect data-at-rest and the host operating system in communication with the CM acts as the operator and is considered a trusted machine.

The Cryptographic Module implements the roles listed in the Roles table.

Name	Type	Operator Type	Authentication Methods
Anybody	Role	User	None
BandMaster [0-15]	Role	CO	Credential PIN Authentication
EraseMaster	Role	CO	Credential PIN Authentication
SCSI User	Role	User	None
SID	Role	CO	Credential PIN Authentication

Table 11: Roles

4.3 Approved Services

The Approved Services table lists approved services implemented by the Cryptographic Module.

The SSPs modes of access shown in the table below are defined as:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The CM uses the SSP to perform a cryptographic operation.

Z = Zeroise: The CM zeroises the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authenticate PSID	PSID character string authentication	isFIPS mode is true	PSID authentication request	UEC success or failure code	Decryption Keyed_Digest_Verification Keyed_Digest_Generation	SID - PSID Digest: E - PSID: W,E - SED Active Encryption Key: E - SED Active Signing Key: E Anybody - PSID Digest: E - PSID: W,E - SED Active Encryption Key: E - SED Active Signing Key: E
Authenticate TCG Authority	Authentication Credential authentication	isFIPS mode is true	Crypto Officer or User authentication request	UEC success or failure code	Decryption Derived_Key_Generation Keyed_Digest_Verification Keyed_Digest_Generation	SID - SID PIN Digest: E - SID PIN: E,W - MSID: E,W - MSID Digest: E - SED AdminSP Active Signing Key: E - SED AdminSP Active Encryption Key: E - Global Active

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Key: E BandMaster [0-15] - Global Active Signing Key: E - MSID Digest: E - SED LockingSP Active Signing Key: E - Locking SP CSP Blob: E - Non-Admin Authority Key (Ku) (BandMaster unique): E,G - KDF Salt (EraseMaster and BandMaster unique): E - MSID: W,E - BandMaster PIN (16 total): W,E - BandMaster PIN Digest (16 total): E EraseMaster - EraseMaster PIN Digest: E - SED LockingSP Active Signing Key: E - MSID Digest: E - Locking SP CSP Blob: E - EraseMaster PIN: W,E - Global Active Signing Key: E - Admin Authority

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key (Ka): E,G - KDF Salt (EraseMaster and BandMaster unique): E - MSID: W,E Anybody - SID PIN Digest: E - EraseMaster PIN Digest: E - BandMaster PIN Digest (16 total): E - MSID Digest: E - SED AdminSP Active Signing Key: E - SED AdminSP Active Encryption Key: E - SED LockingSP Active Encryption Key: E - SID PIN: W,E - EraseMaster PIN: W,E - BandMaster PIN (16 total): W,E - MSID: W,E - SED LockingSP Active Signing Key: E - Global Active Signing Key: E - Admin SP CSP Blob: E - Locking SP CSP Blob: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Admin Authority Key (Ka): E,G - Non-Admin Authority Key (Ku) (BandMaster unique): E,G - KDF Salt (EraseMaster and BandMaster unique): E
BootFlashIntegrity	An RSA digital signature that verifies the authenticity of a binary firmware image.	isFIPS mode is true	RSA 3072 PSS Signed firmware image	UEC success or failure code	SecureLoader_Integrity Digest_Generation Digest_Verification	Unauthenticated - Storage Device Certification Authority Key (SD_CA Key): E - SD CA Key Digest: E
FIPS 140 Compliance Descriptor	This service reports the FIPS 140 revision as well as the Cryptographic Module's overall security level, hardware revision, firmware revision and module name.	isFIPS mode is true	Security Protocol Command to read FIPS 140 Compliance	FIPS 140 Compliance Descriptor table data or UEC failure code	None	SCSI User
Firmware Download	Digital signature verification of a binary firmware image.	isFIPS mode is true	Command to load a new firmware image	UEC success or failure code	FW_Authenticity	SCSI User - OEM Firmware Key (OEM_FW Key): E - OEM_Release Key (OEM_Release Key):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - Storage Device Certification Authority Key (SD_CA Key): E - Product Group Key (PROD_GROUP Key): E
Firmware Download Control	Enable or disable access to the Firmware Download service	isFIPS mode is true	Command to set the state of the FW_DOWNLOAD_PORT bit	UEC success or failure code	None	SID
Firmware Integrity	An RSA digital signature verifies the authenticity of a binary firmware image.	isFIPS mode is true	RSA 3072 PKCSPSS Signed firmware image	UEC success or failure code	FW_Integrity	Unauthenticated - OEM Firmware Key (OEM_FW Key): E - Security Core Firmware Key (SC_FW Key): E - Security Protocol Firmware Key (SP_FW Key): E - OEM Original Factory State Key (OEM_OFS Key): E - Storage Device Boot FW Key (SD_BFW Key): E - Storage Device Certification Authority Key (SD_CA Key): E - Product Group Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(PROD_GROUP Key): E
Generate Random	TCG Random method that generates a random number from the SP 800-90A CTR_DRBG	isFIPS mode is true	Command to generate a string of random byte values	String of random byte values or UEC failure code.	RBG	Anybody - DRBG.Key: E - DRBG.V: G,E EraseMaster - DRBG.Key: E - DRBG.V: G,E BandMaster [0-15] - DRBG.Key: E - DRBG.V: G,E SID - DRBG.Key: E - DRBG.V: G,E
Get MSID	Reads data structure; access control enforcement occurs per data structure field.	isFIPS mode is true	Command to read MSID. [TCG Core]	MSID character string or UEC failure code. [TCG Core]	Keyed_Digest_Verification	SID - MSID: R,E - Global Active Signing Key: E EraseMaster - MSID: R,E - Global Active Signing Key: E BandMaster [0-15] - MSID: R,E - Global Active Signing Key: E Anybody - MSID: R,E - Global Active Signing Key: E
Get Band Attributes	Returns the data stored in the Locking SP table for an LBA Range	isFIPS mode is true	Command to read selected LBA attribute table cells. [TCG Enterprise]	Requested LBA attribute data or UEC failure code.	None	BandMaster [0-15] Anybody

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				[TCG Enterprise]		
Get Data Store	Read a stream of bytes from unstructured storage	isFIPS mode is true	Command to read DataStore table data [TCG SIIS].	Requested DataStore table data or UEC failure code	None	Anybody BandMaster [0-15]
Level 0 Discovery	TCG 'Level 0 Discovery' discloses basic configuration data about the Cryptographic Module, both current and potential [TCG Core Product Manual]	isFIPS mode is true	Command to read Level 0 Discovery table cells [TCG Core]	Requested Level 0 Discovery table data or UEC failure code. [TCG Core]	None	Anybody
OptiNAND Firmware Download	Digital signature verification of a binary firmware image.	isFIPS mode is true and firmware loading status message	Command to load a new firmware image	UEC success or failure code	FW_Auth_OptiNAND	SID - sFFUPublicKey: E
OptiNAND Firmware Integrity	Digital signature verification of a binary firmware image.	isFIPS mode is true	RSA 3072 PSS Signed firmware image	UEC success or failure code	OptiNAND_Descrambler FW_Integrity _OptiNAND	Unauthenticated - sFFUPublicKey: E - SecureBootPublicKey: E - sFFU_EncKey: E
Read User Data	Reads ciphertext from a LBA Ranges	isFIPS mode is true	Command to read user data within an LBA range [SBC-4]	Requested user data or	User_Data_Decryption Decryption	SCSI User - Media Encryption Keyset (MEK) - MEK.AESEnc Key,

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and output user plaintext data.			UEC failure code		MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - Anybody User Access Key (UAKa): E
Reset Module	Power on Reset	isFIPS mode is true	None	READY_LED state and UEC success or failure code	Derived_Key_Generation Encryption Key Wrap_D RBG Symmetric_Key_Generation Entropy Decryption Keyed_Digest_Generation Keyed_Digest_Verification MEK Generation	Unauthenticated - DRBG.Seed: G,E,Z - DRBG.Key: G,E,Z - DRBG.V: G,E,Z - SED Volatile Encryption Key: G,E - SED Volatile Signing Key: G,E - ESV: E,Z,G - Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): G - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - Locking Range Keyset (LRK) - LRK.AES Key,

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						LRK.XTS Key (BandMaster unique): E - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique): E - Range Access Key (RAK) (BandMaster unique): E - Root Encryption Key: E - Root Signing Key: E
Revert	The Revert method cryptographically erases CSPs and returns the Cryptographic Module to its original manufactured state.	isFIPS mode is true	Command to execute Revert [TCG Opal]	READY_LED state and UEC success or failure code	Derived_Key_Generation Encryption Keyed_Digest_Generation MEK Generation RBG Symmetric_Key_Generation FW_Integrity Key Wrap_D LRK_NSK Generation	SID - SID PIN Digest: G,Z - EraseMaster PIN Digest: G,Z - BandMaster PIN Digest (16 total): G,Z - KDF Salt (EraseMaster and BandMaster unique): G,E,Z - DRBG.Key: E - DRBG.V: G,E - Admin Authority Key (Ka): G,E,Z - Non-Admin Authority Key (Ku) (BandMaster unique): G,E,Z - Locking Range Keyset (LRK) -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						LRK.AES Key, LRK.XTS Key (BandMaster unique): G,E,Z - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique): G,E,Z - Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): G,Z - Range Access Key (RAK) (BandMaster unique): G,E,Z - User Access Key (UAK) (BandMaster unique): G,E,Z - User Management Key (UMK): G,E,Z - Root Encryption Key: E - Root Signing Key: E - Global Active Encryption Key (AEK): G,E,Z - Global Active Signing Key: G,E,Z - SED Active Encryption Key: G,E,Z - SED Active

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Key: G,E,Z - SED AdminSP Active Encryption Key: G,E,Z - SED AdminSP Active Signing Key: G,E,Z - SED LockingSP Active Encryption Key: G,E,Z - SED LockingSP Active Signing Key: G,E,Z - Admin SP CSP Blob: G,E,Z - Locking SP CSP Blob: G,E,Z - SED Volatile Encryption Key: G,E,Z - SED Volatile Signing Key: G,E,Z - PSID Digest: G,Z - MSID Digest: G,Z - Anybody User Access Key (UAKa): E - MSID: E - PSID: E - OEM Original Factory State Key (OEM_OFS Key): E Anybody - SID PIN Digest: G,Z - EraseMaster PIN Digest: G,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- BandMaster PIN Digest (16 total): G,Z - KDF Salt (EraseMaster and BandMaster unique): G,E,Z - DRBG.Key: E - DRBG.V: G,E - Admin Authority Key (Ka): G,E,Z - Non-Admin Authority Key (Ku) (BandMaster unique): G,E,Z - Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique): G,E,Z - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique): G,E,Z - Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): G,Z - Range Access Key (RAK) (BandMaster unique): G,E,Z - User Access Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(UAK) (BandMaster unique): G,E,Z - User Management Key (UMK): G,E,Z - Root Encryption Key: E - Root Signing Key: E - Global Active Encryption Key (AEK): G,E,Z - Global Active Signing Key: G,E,Z - SED Active Encryption Key: G,E,Z - SED Active Signing Key: G,E,Z - SED AdminSP Active Encryption Key: G,E,Z - SED AdminSP Active Signing Key: G,E,Z - SED LockingSP Active Encryption Key: G,E,Z - SED LockingSP Active Signing Key: G,E,Z - Admin SP CSP Blob: G,E,Z - Locking SP CSP Blob: G,E,Z - SED Volatile Encryption Key: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SED Volatile Signing Key: G,E,Z - PSID Digest: G,Z - MSID Digest: G,Z - Anybody User Access Key (UAKa): E - MSID: E - PSID: E - OEM Original Factory State Key (OEM_OFS Key): E
RevertSP	The RevertSP method cryptographically erases CSPs and returns the Cryptographic Module to its original manufactured state.	isFIPS mode is true	Command to execute RevertSP [TCG Opal]	READY_LED state and UEC success or failure code	Derived_Key_Generation Encryption Key Wrap_D Keyed_Digest_Generation MEK Generation RBG Symmetric_Key_Generation FW_Integrity LRK_NSK Generation	SID - EraseMaster PIN Digest: G,Z - BandMaster PIN Digest (16 total): G,Z - DRBG.Key: E - DRBG.V: E,G - Admin Authority Key (Ka): G,E,Z - Non-Admin Authority Key (Ku) (BandMaster unique): G,E,Z - Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique): G,E,Z - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique): G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): G,Z - Range Access Key (RAK) (BandMaster unique): G,E,Z - User Access Key (UAK) (BandMaster unique): G,E,Z - User Management Key (UMK): G,E,Z - KDF Salt (EraseMaster and BandMaster unique): G,E,Z - Root Encryption Key: E - Root Signing Key: E - Global Active Encryption Key (AEK): G,E,Z - Global Active Signing Key: G,E,Z - SED Active Encryption Key: G,E,Z - SED Active Signing Key: G,E,Z - SED AdminSP Active Encryption Key: G,E,Z - SED AdminSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Active Signing Key: G,E,Z - SED LockingSP Active Encryption Key: G,E,Z - SED LockingSP Active Signing Key: G,E,Z - Locking SP CSP Blob: G,E,Z - Admin SP CSP Blob: G,E,Z - SED Volatile Encryption Key: G,E,Z - SED Volatile Signing Key: G,E,Z - PSID Digest: G,Z - PSID: E - OEM Original Factory State Key (OEM_OFS Key): E Anybody - EraseMaster PIN Digest: G,Z - BandMaster PIN Digest (16 total): G,Z - DRBG.Key: E - DRBG.V: E,G - Admin Authority Key (Ka): G,E,Z - Non-Admin Authority Key (Ku) (BandMaster unique): G,E,Z - Locking Range

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique): G,E,Z - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique): G,E,Z - Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): G,Z - Range Access Key (RAK) (BandMaster unique): G,E,Z - User Access Key (UAK) (BandMaster unique): G,E,Z - User Management Key (UMK): G,E,Z - KDF Salt (EraseMaster and BandMaster unique): G,E,Z - Root Encryption Key: E - Root Signing Key: E - Global Active Encryption Key (AEK): G,E,Z - Global Active

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Key: G,E,Z - SED Active Encryption Key: G,E,Z - SED Active Signing Key: G,E,Z - SED AdminSP Active Encryption Key: G,E,Z - SED AdminSP Active Signing Key: G,E,Z - SED LockingSP Active Encryption Key: G,E,Z - SED LockingSP Active Signing Key: G,E,Z - Locking SP CSP Blob: G,E,Z - Admin SP CSP Blob: G,E,Z - SED Volatile Encryption Key: G,E,Z - SED Volatile Signing Key: G,E,Z - PSID Digest: G,Z - PSID: E - OEM Original Factory State Key (OEM_OFS Key): E
SCSI Command	The SCSI command set provides an efficient peer-to-peer	isFIPS mode is true	Command to execute SCSI command [SCSI Core], [SCSI Block]	Return device data as defined within [SCSI Core] and [SCSI	None	SCSI User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	operation for SCSI devices.			Block] or UEC failure code		
Self-Test	The Cryptographic Module performs self-tests when it powers up.	N/A	None	READY_LED state and UEC success or failure code	Decryption Derived_Key_Generation Digest_Generation Digest_Verification Encryption Entropy FW_Integrity Key Wrap_D Keyed_Digest_Generation Keyed_Digest_Verification RBG	Unauthenticated - DRBG.Key: G,E,Z - DRBG.V: G,E,Z - DRBG.Seed: E,Z - ESV: G,Z
Set Password	Write data structures; access control enforcement occurs per data structure field. This service can change Authentication Credential PINs.	isFIPS mode is true	Command to update the password for a TCG Authority. SID PIN, BandMaster PIN, and EraseMaster PIN. See [TCG Core]	UEC success or failure code	Derived_Key_Generation Encryption Keyed_Digest_Generation	SID - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - SED Active Encryption Key: E - SED Active Signing Key: E - SED AdminSP Active Encryption Key: E - SED AdminSP Active Signing Key: E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - SID PIN: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SID PIN Digest: G EraseMaster - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - SED Active Encryption Key: E - SED Active Signing Key: E - SED LockingSP Active Encryption Key: E - SED LockingSP Active Signing Key: E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - Admin Authority Key (Ka): E,G - EraseMaster PIN: W,E - EraseMaster PIN Digest: G - KDF Salt (EraseMaster and BandMaster unique): E BandMaster [0-15] - Global Active Encryption Key (AEK): E - Global Active Signing Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SED Active Encryption Key: E - SED Active Signing Key: E - SED LockingSP Active Encryption Key: E - SED LockingSP Active Signing Key: E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - Non-Admin Authority Key (Ku) (BandMaster unique): G,E - BandMaster PIN Digest (16 total): G - KDF Salt (EraseMaster and BandMaster unique): E - BandMaster PIN (16 total): W,E Anybody
Set Band Attributes	Set the starting location, size, and attributes of an LBA range.	isFIPS mode is true	Command to update LBA range attribute configuration data. See [TCG Enterprise]	UEC success or failure code	Encryption Keyed_Digest_Generation MEK Generation User_Data_Encryption	BandMaster [0-15] - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - SED Active Encryption Key: E - SED Active Signing Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SED LockingSP Active Encryption Key: E - SED LockingSP Active Signing Key: E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - User Access Key (UAK) (BandMaster unique): E - Range Access Key (RAK) (BandMaster unique): E - Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique): E - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique): E - Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): G - Locking SP CSP Blob: G Anybody

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SED Volatile Encryption Key: E - SED Volatile Signing Key: E - Anybody User Access Key (UAKa): E - Range Access Key (RAK) (BandMaster unique): E - Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique): E - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique): E - Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): G
Set Data Store	Write a stream of bytes to unstructured storage.	isFIPS mode is true	Command to write data to the DataStore table. [TCG Enterprise]	UEC Success or failure code	None	BandMaster [0-15] Anybody
Show Status	The status inquiry command requests SCSI	isFIPS mode is true	Command to read and display module status data [SCSI Core], [SCSI Block].	Return requested module data	None	SCSI User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	device (e.g., Cryptographic Module) status information.			or UEC failure code		
TCG Erase	TCG Erase cryptographically erases user data by regenerating and replacing a Locking Range Key associated with an LBA range.	isFIPS mode is true	Command to execute Erase method. [TCG Enterprise], [TCG Ent App Notes]	UEC success or failure code	Encryption Decryption User_Data_Encryption MEK Generation RBG Keyed_Digest_Generation LRK_NSK Generation	EraseMaster - Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): G,E,Z - Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique): G,E,Z - DRBG.Key: E - DRBG.V: E - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique): E - Range Access Key (RAK) (BandMaster unique): E - User Management Key (UMK): E - User Access Key (UAK) (BandMaster unique): E - Locking SP CSP Blob: G,E - Global Active Encryption Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(AEK): E - Global Active Signing Key: E - SED LockingSP Active Encryption Key: E - SED LockingSP Active Signing Key: E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E
Write User Data	Transform plaintext user data into ciphertext and writes to an LBA range.	isFIPS mode is true	Operation Code, LBA, Transfer Length, Data-Out Buffer [SBC-4]	UEC success or failure code	User_Data_Encryption Decryption	SCSI User - Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique): E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - Anybody User Access Key (UAKa): E

Table 12: Approved Services

4.4 Non-Approved Services

The Cryptographic Module does not support non-approved services.

N/A for this module.

4.5 External Software/Firmware Loaded

The Cryptographic Module utilizes RSA public key cryptography to verify the authenticity of firmware downloaded to the CM. The Cryptographic Module uses RSA 3072 PKCSPSS with SHA2-256 to verify the digital signature of a downloaded firmware binary image. A Hardware Security Module (HSM), which resides in a secure Western Digital facility, generates, and stores the RSA Public/Private key pairs used in the firmware signing process. The Cryptographic Module rejects a downloaded firmware binary image if the digital signature verification process fails.

5 Software/Firmware Security

5.1 Integrity Techniques

The Cryptographic Module utilizes RSA public key cryptography to verify the integrity of all firmware binary images within the CM prior to execution. An operator may initiate the integrity test on demand by power cycling the CM.

The firmware integrity tests ensure that prior to executing any firmware image the storage device verifies the firmware is from an authenticated Western Digital source. Current storage devices typically implement a multi-stage loader system to boot the drive. Each loader stage is responsible for loading and verifying the next image before transferring control to the next image. This process establishes a chain of trust during the boot process.

The Cryptographic Module's Boot ROM code loads the secure loader image. The SD_CA Key signed secure loader, enables the boot process to use other keys besides the SD_CA Key for boot time signature checking (i.e., SD_BFW Key). For example, the secure loader loads the SD_BFW public key certificate and verifies the SD_CA Key signature of the certificate. The secure loader then loads the next image(s) from boot flash, verifies the signature of the next image(s) using the SD_BFW public key, and transfers control to the next image.

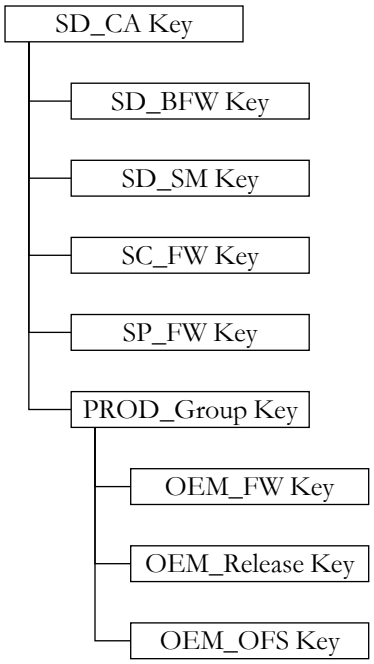

Figure 10 - Asymmetric Key Tree

5.2 Initiate on Demand

The operator initiates the integrity test on demand by power cycling the Cryptographic Module.

5.3 Open-Source Parameters

The Western Digital firmware development process does not utilize open-source firmware to build executable code installed within the Cryptographic Module.

6 Operational environment

6.1 Operational Environment Type and Requirements

Type of Operating Environment: Limited

How Requirements are Satisfied

While operational, the Cryptographic Module prohibits additions, deletions, or modification of the code working set. For firmware upgrades, the Cryptographic Module uses an authenticated download service to upgrade its mutable firmware in its entirety. The immutable security firmware stored in ROM, which is essential and integral to the operation of the module is non-modifiable. If the download operation is successful, authorized, and verified, the Cryptographic Module will begin operating with the new code working set after successfully executing all pre-operational self-tests.

Firmware loaded into the cryptographic module that is not on the FIPS 140-3 certificate is out of the scope of this validation and requires a separate FIPS 140-3 validation.

6.2 Configuration Settings and Restrictions

The Cryptographic Module blocks the installation of firmware images that contain a Code ID that is inconsistent with the Cryptographic Module's SoC, hardware interface type (e.g., SAS or SATA) and security type (e.g., TCG Enabled, FIPS Enabled, etc.).

The Crypto Officer is responsible for assuring that the LockOnReset parameter of the logical firmware download port is set to PowerCycle. The Cryptographic Module is in a noncompliant state when the LockOnReset parameter is not set to PowerCycle. The Crypto Officer is responsible for assuring the logical firmware download port remains locked unless the CO intends to execute the Firmware Download service. The CO shall lock the firmware download port after the Firmware Download service completes. Consult the Ports section of the Ultrastar DC HC560 3.5-inch Serial Attached SCSI Hard Disk Drive Specification [Product Manual] or Ultrastar DC HC570 3.5-inch Serial Attached SCSI Hard Disk Drive Specification [Product Manual] for guidance.

The Crypto Officer is responsible for assuring that the BandMaster Authentication PIN Credential for all configured BandMasters does not equal the MSID value. LBA ranges associated with BandMasters with module unique authentication PIN values are considered unsecure.

The Crypto Officer is responsible for assuring that the LockOnReset attribute for any configured BandMaster is set to PowerCycle. The Cryptographic Module is in a noncompliant state when the state of the LockOnReset attribute of any configured BandMaster is not set to PowerCycle.

The Crypto Officer is responsible for assuring that the ReadLockEnabled and WriteLockEnabled attribute for any configured BandMaster is set to True. The Cryptographic Module is in a noncompliant state when the state of the ReadLockEnabled or WriteLockEnabled attribute of any configured BandMaster is set to False.

Consult the TCG Storage SSC: Enterprise Specification [TCG Enterprise] for guidance.

7 Physical Security

The Cryptographic Module is a multi-chip embedded module that complies with FIPS 140-3 Level 2 security. An ambient temperature from 5° to 60°C defines the Cryptographic Module's environmental operating range [Datasheet]

7.1 Mechanisms and Actions Required

The Cryptographic Module does not make claims in the Physical Security area beyond FIPS 140-3 Level 2 security. Therefore, the CM does not employ any fault induction mitigation techniques or EFP feature to immediately zeroise all unprotected SSPs if the temperature or voltage falls outside of the cryptographic module's normal operating range. The CM initiates a thermal safety shutdown if the temperature drops below -40°C or exceeds 70°C but does not zeroize SSPs if either trip point is exceeded.

- All components are production-grade materials with standard passivation techniques.
- The enclosure is opaque.
- Engineering design supports opacity requirements.
- An attacker cannot penetrate or remove and reapply a tamper-evident security seal without evidence of tampering. In addition, it is difficult to replicate the tamper-evident security seal.

Mechanism	Inspection Frequency	Inspection Guidance
During the manufacturing process, specialized equipment applies one tamper-evident security seal to the CM's PCBA.	Annually	The Cryptographic Module's owner shall inspect the Cryptographic Module for evidence of tampering. If tamper evidence is apparent, the owner should return the module to Western Digital.

Table 13: Mechanisms and Actions Required

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature			
HighTemperature			
LowVoltage			
HighVoltage			

Table 14: EFP/EFT Information

Temperature Type	Temperature
LowTemperature	
HighTemperature	

Table 15: Hardness Testing Temperatures

Figure 11 - Tamper-Evident Seal for Ultrastar DC HC560

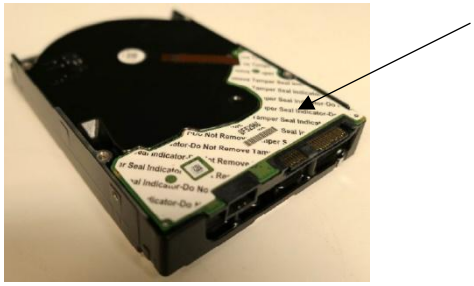

Figure 12 - Tamper-Evident Seal for Ultrastar DC HC570

Figure 13 - Tamper Evidence on Tamper Seal

8 Non-invasive Security

8.1 Mitigation Techniques

The Cryptographic Module lacks features to mitigate any non-invasive security attacks beyond the scope of the requirements within FIPS 140-3 Security Level 2.

9 Sensitive Security Parameters Management

The Cryptographic Module manages the SSPs listed in Section 0 of this document. The Cryptographic Module does not support the output of SSPs beyond the cryptographic boundary. The Cryptographic Module does not support non-approved algorithms or key lengths.

9.1 Storage Areas

Calling processes implemented in firmware control Cryptographic Module access to SSPs. Zeroization services destroy or cryptographically erase SSPs.

Storage Area Name	Description	Persistence Type
DRAM	General purpose system memory	Dynamic
IRAM	Memory internal to the ACM	Dynamic
NOR Flash	SSP and boot code storage	Static

Storage Area Name	Description	Persistence Type
Disk Media (Reserved Area)	SSP and operation firmware image storage	Static
One-time Programable (OTP)	Root Key and Certificate Authority Key storage	Static
Masked ROM	A type of non-volatile memory that is programmed with a specific set of data or instructions during the IC fabrication process.	Static
NAND Flash	SSP storage and firmware image	Static

Table 16: Storage Areas

9.2 SSP Input and Output Methods

The CM limits the input of SSPs to plaintext Authentication Credential PINs and RSA-3072 public keys. RSA-3072 public key insertion occurs during the manufacturing process. Instead of storing PIN values as plaintext, the CM stores an HMAC SHA-256 Digest of the PIN. A Hardware Security Module (HSM), which resides within a secure Western Digital facility, generates, and stores RSA Public/Private key pairs utilized during the manufacturing process. The CM does not support the output of intermediate values generated during key generation. The module does not support the output of SSPs beyond the cryptographic boundary of the module.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Authentication Credential PIN	Operator	CM	Plaintext	Manual	Electronic	
Public Key Input	Operator	CM	Plaintext	Manual	Electronic	
Public Key Output	CM	Operator	Plaintext	Manual	Electronic	

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization of persistent SSPs complies with the cryptographic erasure requirements for SCSI Hard Disk drives within [SP 800 88], Guidelines for Media Sanitization. The Cryptographic Module zeroizes ephemeral SSPs by overwriting the SSP memory location with all zeros within the scope of the function call.

Zeroization Method	Description	Rationale	Operator Initiation
Power Cycle	Power cycling involves disconnecting and reconnecting the CM to its source of power.	Plaintext SSPs stored in IRAM memory within the ACM are destroyed instantaneously when power is removed.	Physically or remotely disconnects the CM from its source of power.
Revert Zeroization Command	The Revert method cryptographically erases CSPs, removes the owner's Authentication Credentials and returns the Cryptographic Module to its original manufactured state.	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	Transmits a command to the CM as the TPer tto execute the Revert method.
RevertSP Zeroization Command	The RevertSP method cryptographically erases CSPs. RevertSP removes the owner's Authentication Credentials and returns the Cryptographic Module to its original manufactured state. The CM preserves Global Range data if the KeepGlobalRangeKey parameter is set to True.	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	Transmit a command to the CM, as the TPer, to execute the RevertSP method.
Secure Manufacturing Reconfiguration Process	The secure manufacturing reconfiguration processes incorporates a hardware security module (HSM) and supporting security software to inject cryptographic keys, digital certificates and assure only authentic firmware is installed on the Cryptographic Module.	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	Transmit proprietary commands to the CM to initiate a rebuild process that zeroizes and regenerates the symmetric and asymmetric key trees.
TCG Erase	The TCG Erase method cryptographically erases user data by regenerating the Locking Range Key (LRK) and Media Encryption Key (MEK) associated with a data range.	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	Transmit a command to the CM, as the TPer, to execute the Erase method.
Ephemeral SSP Zeroization	Module zeroizes ephemeral SSPs after use.	Plaintext SSPs stored in IRAM memory within the ACM are overwritten with 0s.	Automatic after use.

Table 18: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Admin Authority Key (Ka)	The Ka key encrypts and decrypts the UMK.	256 bits - 256 bits	Derived Symmetric Key - CSP	Derived_Key_Generation		Decryption Encryption
Admin SP CSP Blob	An Admin SP CSP Blob stores configuration data and CSPs that bind a set of methods and access controls to an Admin SP.	N/A - N/A	N/A - CSP			
Anybody User Access Key (UAKa)	The Anybody Authority uses UAKa to decrypt and encrypt the RAK of unlocked LBA Ranges.	256 bits - 256 bits	Symmetric Key - CSP	Manufacturing		Decryption Encryption
BandMaster PIN (16 total)	Authentication Credential PIN for a Locking SP Bandmaster Authority	96 to 256 bits - 96 to 256 bits	Plaintext - CSP			Keyed_Digest_Generation Derived_Key_Generation
BandMaster PIN Digest (16 total)	Authenticates BandMaster PIN.	256 bits - 256 bits	Message Digest - CSP	Keyed_Digest_Generation		Keyed_Digest_Verification
DRBG.Key	Internal state associated with the [SP 800-90A] CTR_DRBG using AES-256	256 bits - 256 bits	Entropy - CSP	RBG		RBG
DRBG.Seed	Internal state associated with the [SP 800-90A] CTR_DRBG using AES-256.	5120 bits - 432 bits	Entropy - CSP	Entropy		RBG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG.V	Internal state associated with the [SP 800-90A] CTR_DRBG using AES-256.	128 bits - 128 bits	Entropy - CSP	RBG		RBG
EraseMaster PIN	Authentication Credential PIN for the Locking SP EraseMaster Authority.	96 to 256 bits - 96 to 256 bits	Plaintext - CSP			Keyed_Digest_Generation Derived_Key_Generation
EraseMaster PIN Digest	Authenticates the EraseMaster PIN	256 bits - 256 bits	Message Digest - CSP	Keyed_Digest_Generation		Keyed_Digest_Verification
ESV	Entropy source input to the [SP 800-90A] CTR_DRBG	32-bit sample - 2.7 bits per 32-bit sample	Entropy - CSP	Entropy		RBG
Global Active Encryption Key (AEK)	The Global Active Encryption Key encrypts and decrypts the SED Active Keyset, NSK and the UAKa key.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Decryption Encryption
Global Active Signing Key	Signs the encrypted SED Active Keyset.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Keyed_Digest_Generation Keyed_Digest_Verification
KDF Salt (EraseMaster and BandMaster unique)	KDF Salts are integral to the PBKDF2 generation of each Ka and Ku derived authority key.	256 bits - 256 bits	Symmetric Key - PSP	Symmetric_Key_Generation		Derived_Key_Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique)	LRKs in combination with the NSKs derive MEKs, which encrypt LBA Ranges	256 bits - 256 bits	Symmetric Key - CSP	LRK_NSK Generation		MEK Generation
Locking SP CSP Blob	Locking SP CSP Blob store configuration data and CSPs that bind a set of methods and access controls to a Locking SP.	N/A - N/A	N/A - CSP			
Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique)	MEKs encrypt and decrypt LBA Ranges.	256 bits - 256 bits	Derived Symmetric Key - CSP	MEK Generation		User_Data_Decryption User_Data_Encryption
MSID	The MSID string is the module unique password for the SID, EraseMaster and BandMaster authorities. Stored during the manufacturing process.	32 bytes - 162.8 bits	Plaintext - PSP	Manufacturing		Keyed_Digest_Generation Keyed_Digest_Verification
MSID Digest	Authenticates the MSID PIN	256 bits - 256 bits	Message Digest - CSP	Keyed_Digest_Generation		Keyed_Digest_Verification
Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique)	NSKs in combination with the LRKs derive MEKs, which encrypt LBA Ranges.	256 bits - 256 bits	Symmetric Key - CSP	LRK_NSK Generation		MEK Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Non-Admin Authority Key (Ku) (BandMaster unique)	Ku keys encrypt and decrypt all UAKs.	256 bits - 256 bits	Derived Symmetric Key - CSP	Derived_Key_Generation		Decryption Encryption
OEM Firmware Key (OEM_FW Key)	The OEM_FW Key verifies OEM firmware images and packages	3072-bits - 128 bits	Public Key - Neither	HSM, External		FW_Integrity FW_Authenticity
OEM Original Factory State Key (OEM_OFS Key)	The OEM_OFS Key verifies the OEM Original Factory Settings files.	3072-bits - 128 bits	Public Key - Neither	HSM, External		FW_Integrity
OEM_Release Key (OEM_Release Key)	The OEM_Release Key verifies the outer signature of an OEM firmware package.	3072-bits - 128 bits	Public Key - Neither	HSM, External		FW_Authenticity
Product Group Key (PROD_GROUP Key)	The PROD_GROUP Key verifies OEM_FW Key certificates.	3072-bits - 128 bits	Public Key - Neither	HSM, External		FW_Authenticity FW_Integrity
PSID	The PSID string serves as authentication data and proof of physical presence for the Revert and RevertSP services. Stored during the manufacturing process.	256 bits - 162.8 bits	Plaintext - PSP	Manufacturing		Keyed_Digest_Generation
PSID Digest	Authenticates the PSID	256 bits - 256 bits	Message Digest - CSP	Keyed_Digest_Generation		Keyed_Digest_Verification

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Range Access Key (RAK) (BandMaster unique)	RAKs encrypt and decrypt LRKs.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Decryption Encryption
Root Encryption Key	The Root Encryption Key encrypts the Global Active Encryption key and Key Wraps the Root Signing Key.	256 bits - 256 bits	Symmetric Key - CSP	Manufacturing		Decryption Encryption Key Wrap_D
Root Signing Key	Signs the encrypted Global Active Key.	256 bits - 256 bits	Symmetric Key - CSP	Manufacturing		Keyed_Digest_Generation Keyed_Digest_Verification
SecureBootPublicKey	The SecureBootPublicKey verifies the OptiNAND Firmware download image.	3072 bits - 128 bits	Public Key - Neither	HSM, External		FW_Integrity _OptiNAND
Security Core Firmware Key (SC_FW Key)	The SC_FW Key verifies Access Control Module (ACM) security core firmware.	3072 bits - 128 bits	Public key - Neither	HSM, External		FW_Integrity
Security Protocol Firmware Key (SP_FW Key)	The SP_FW Key verifies ACM security protocol and services firmware.	3072 bits - 128 bits	Public Key - Neither	HSM, External		FW_Integrity
SED Active Encryption Key	Encrypts and decrypts the SED AdminSP Active Keyset and the SED LockingSP Active Keyset.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Decryption Encryption
SED Active Signing Key	Signs the encrypted SED AdminSP Active Keyset and the SED	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Keyed_Digest_Generation Keyed_Digest_Verification

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	LockingSP Active Keyset.					
SED AdminSP Active Encryption Key	Encrypts and decrypts Admin SP CSP Blobs.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Decryption Encryption
SED AdminSP Active Signing Key	Signs encrypted Admin SP CSP Blobs.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Keyed_Digest_Generation Keyed_Digest_Verification
SED LockingSP Active Encryption Key	Encrypts and decrypts Locking SP CSP Blob.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Decryption Encryption
SED LockingSP Active Signing Key	Signs encrypted Locking SP CSP Blob.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Keyed_Digest_Generation Keyed_Digest_Verification
SED Volatile Encryption Key	Encrypts, and decrypts LRKs and MEKs.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Decryption Encryption
SED Volatile Signing Key	Signs encrypted LRKs and MEKs.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Keyed_Digest_Generation Keyed_Digest_Verification
sFFU_EncKey	Descrambles a Secure Field Firmware Update (sFFU) image	256 bits - 256 bits	Public Key - Neither	HSM, External		OptiNAND_Descrambler
sFFUPublicKey	The sFFUPublicKey verifies OptiNAND Secure Field Firmware Update (sFFU) images.	3072 bits - 128 bits	Public Key - Neither	HSM, External		FW_Integrity _OptiNAND FW_Auth_OptiNAND
SID PIN	Authentication Credential PIN for the Admin SP SID Authority.	96 to 256 bytes - 96 to 256 bits	Plaintext - CSP			Keyed_Digest_Generation Keyed_Digest_Verification
SID PIN Digest	Authenticates the SID PIN.	256 bits - 256 bits	Message Digest - CSP	Keyed_Digest_Generation		Keyed_Digest_Verification

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Storage Device Boot FW Key (SD_BFW Key)	The SD_BFW Key is public key used to verify all boot flash images.	3072-bits - 128 bits	Public Key - Neither	HSM,External		FW_Integrity
Storage Device Certification Authority Key (SD_CA Key)	The SD_CA Key is the Master RSA 3072 public key used to verify the Secure Loader image	3072-bits - 128 bits	Public Key - Neither	HSM, External		FW_Integrity FW_Authenticity SecureLoader_Integrity
SD CA Key Digest	SHA-256 Digest of the SD CA Key	256 bits - 128 bits	Message Digest CSP - Neither	HSM, External		SecureLoader_Integrity
User Access Key (UAK) (BandMaster unique)	Encrypts and decrypts the RAK associated with a BandMasters.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Decryption Encryption
User Management Key (UMK)	Encrypts and decrypts UAKs.	256 bits - 256 bits	Symmetric Key - CSP	Symmetric_Key_Generation		Decryption Encryption

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Admin Authority Key (Ka)		IRAM:Plaintext	Ephemeral SSP Zeroization	N/A	User Management Key (UMK):Encrypts User Management Key (UMK):Decrypts EraseMaster PIN:Derived From KDF Salt (EraseMaster and BandMaster unique):Derived From
Admin SP CSP Blob		IRAM:Plaintext Disk Media	Power up to power down	Revert Zeroization Command	SED AdminSP Active Encryption Key:Encrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
		(Reserved Area):Encrypted		RevertSP Zeroization Command Power Cycle	SED AdminSP Active Signing Key:Signed by
Anybody User Access Key (UAKa)		IRAM:Plaintext Disk Media (Reserved Area):Encrypted	Power up to power down	Power Cycle Revert Zeroization Command RevertSP Zeroization Command	Range Access Key (RAK) (BandMaster unique):Encrypts Range Access Key (RAK) (BandMaster unique):Decrypts Global Active Encryption Key (AEK):Encrypted by Global Active Encryption Key (AEK):Decrypted by
BandMaster PIN (16 total)	Authentication Credential PIN	IRAM:Plaintext	Ephemeral SSP Zeroization	N/A	SED LockingSP Active Signing Key:Used With BandMaster PIN Digest:Generates KDF Salt (EraseMaster and BandMaster unique):Used With Non-Admin Authority Key (Ku) (BandMaster unique):Derives
BandMaster PIN Digest (16 total)		IRAM:Plaintext Disk Media (Reserved Area):Plaintext	Ephemeral SSP Zeroization	Power Cycle Revert Zeroization Command RevertSP Zeroization Command	BandMaster PIN (16 total):Generated from SED LockingSP Active Signing Key:Generated from
DRBG.Key		IRAM:Plaintext	Power up to power down	Power Cycle	DRBG.Seed:Derived from DRBG.V:Paired With
DRBG.Seed		IRAM:Plaintext	Power up to power down	Power Cycle	DRBG.V:Derives DRBG.Key:Derives ESV:Derived from
DRBG.V		IRAM:Plaintext	Power up to power down	Power Cycle	DRBG.Seed:Derived from DRBG.Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
EraseMaster PIN	Authentication Credential PIN	IRAM:Plaintext	Ephemeral SSP Zeroization	N/A	SED LockingSP Active Signing Key:Used With EraseMaster PIN Digest:Generate KDF Salt (EraseMaster and BandMaster unique):Used With Admin Authority Key (Ka):Derive
EraseMaster PIN Digest		IRAM:Plaintext Disk Media (Reserved Area):Plaintext	Ephemeral SSP Zeroization	Power Cycle Revert Zeroization Command RevertSP Zeroization Command	EraseMaster PIN:Generated From SED LockingSP Active Signing Key:Generated From
ESV		IRAM:Plaintext	Power up to power down	Power Cycle	DRBG.Seed:Derives
Global Active Encryption Key (AEK)		NOR Flash:Encrypted		Secure Manufacturing Reconfiguration Process	SED Active Encryption Key:Encrypts SED Active Encryption Key:Decrypts SED Active Signing Key:Encrypts SED Active Signing Key:Decrypts Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique):Encrypts Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique):Decrypts User Access Key (UAK) (BandMaster unique):Encrypts User Access Key (UAK) (BandMaster unique):Decrypts Root Encryption Key:Encrypted by Root Encryption Key:Decrypted by Root Signing Key:Signed by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Global Active Signing Key		NOR Flash:Encrypted		Secure Manufacturing Reconfiguration Process	SED Active Encryption Key:Signs SED Active Signing Key:Signs Root Encryption Key:Encrypted by Root Encryption Key:Decrypted by Root Signing Key:Signed by
KDF Salt (EraseMaster and BandMaster unique)		IRAM:Plaintext Disk Media (Reserved Area):Plaintext	Ephemeral SSP Zeroization	Power Cycle Revert Zeroization Command RevertSP Zeroization Command	BandMaster PIN (16 total):Used With Non-Admin Authority Key (Ku) (BandMaster unique):Derives EraseMaster PIN:Used With Admin Authority Key (Ka):Derives
Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique)		DRAM:Encrypted Disk Media (Reserved Area):Encrypted	Generation to power down	Power Cycle Revert Zeroization Command RevertSP Zeroization Command TCG Erase	Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique):Used With Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique):Generates SED Volatile Encryption Key:Encrypted by SED Volatile Encryption Key:Decrypted by Range Access Key (RAK) (BandMaster unique):Encrypted by Range Access Key (RAK) (BandMaster unique):Decrypted by
Locking SP CSP Blob		IRAM:Plaintext Disk Media (Reserved Area):Encrypted	Power up to power down	Power Cycle Revert Zeroization Command RevertSP Zeroization Command	SED LockingSP Active Encryption Key:Encrypted by SED LockingSP Active Encryption Key:Signed

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique)		DRAM:Encrypted	Generation to power down	Power Cycle Revert Zeroization Command RevertSP Zeroization Command TCG Erase	Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique):Generated From Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique):Generated From SED Volatile Encryption Key:Encrypted by SED Volatile Encryption Key:Decrypted by
MSID	Public Key Input Public Key Output	IRAM:Plaintext NOR Flash:Obfuscated	IRAM: Ephemeral SSP Zeroization. NOR Flash: N/A	N/A	SED Active Signing Key:Signed by SED Active Signing Key:Used with MSID Digest:Generate
MSID Digest		Disk Media (Reserved Area):Plaintext		Revert Zeroization Command RevertSP Zeroization Command	MSID:Generated From SED Active Signing Key:Generated From
Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (BandMaster unique)		DRAM:Encrypted Disk Media (Reserved Area):Encrypted	Generation to power down.	Power Cycle Revert Zeroization Command RevertSP Zeroization Command	Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique):Used With Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique):Generate Global Active Encryption Key (AEK):Encrypted by Global Active Encryption Key (AEK):Decrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Non-Admin Authority Key (Ku) (BandMaster unique)			Ephemeral SSP Zeroization	N/A	BandMaster PIN (16 total):Derived From KDF Salt (EraseMaster and BandMaster unique):Derived From User Access Key (UAK) (BandMaster unique):Encrypts User Access Key (UAK) (BandMaster unique):Decrypts
OEM Firmware Key (OEM_FW Key)		NOR Flash:Obfuscated		N/A	Product Group Key (PROD GROUP Key):Verified by
OEM Original Factory State Key (OEM_OFS Key)		NOR Flash:Obfuscated		N/A	Product Group Key (PROD GROUP Key):Verified By
OEM_Release Key (OEM_Release Key)		NOR Flash:Obfuscated		N/A	Product Group Key (PROD_GROUP Key):Verified By
Product Group Key (PROD_GROUP Key)		NOR Flash:Obfuscated		N/A	Storage Device Certification Authority Key (SD_CA Key):Verified By OEM Firmware Key (OEM_FW Key):Verifies OEM Original Factory State Key (OEM_OFS Key):Verifies OEM_Release Key (OEM_Release Key):Verifies
PSID	Public Key Input	NOR Flash:Encrypted IRAM:Plaintext	NOR Flash: N/A. IRAM: Ephemeral, destroyed after use	Power Cycle	PSID Digest:Generates SED Active Encryption Key:Encrypted by SED Active Encryption Key:Decrypted by SED Active Signing Key:Paired with SED Active Signing Key:Signed by
PSID Digest		Disk Media (Reserved Area):Plaintext		Revert Zeroization Command RevertSP	PSID:Generated From SED Active Signing Key:Generated From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Zeroization Command	
Range Access Key (RAK) (BandMaster unique)		Disk Media (Reserved Area):Encrypted		Revert Zeroization Command RevertSP Zeroization Command	User Access Key (UAK) (BandMaster unique):Encrypted by User Access Key (UAK) (BandMaster unique):Decrypted by Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique):Encrypts Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique):Decrypts
Root Encryption Key		One-time Programable (OTP):Plaintext		Secure Manufacturing Reconfiguration Process	Global Active Encryption Key (AEK):Encrypts Global Active Encryption Key (AEK):Decrypts Root Signing Key:Wraps Root Signing Key:Unwraps
Root Signing Key		NOR Flash:Encrypted		Secure Manufacturing Reconfiguration Process	Global Active Encryption Key (AEK):Signs Root Encryption Key:Wrapped by Root Encryption Key:Unwrapped by
SecureBootPublicKey	Public Key Input	Disk Media (Reserved Area):Encrypted		N/A	sFFUPublicKey:Verifies sFFU_EncKey:Verifies
Security Core Firmware Key (SC_FW Key)	Public Key Input	NOR Flash:Obfuscated			Storage Device Certification Authority Key (SD_CA Key):Verified by
Security Protocol Firmware Key (SP_FW Key)	Public Key Input	NOR Flash:Obfuscated			Storage Device Certification Authority Key (SD_CA Key):Verified by
SED Active Encryption Key		NOR Flash:Encrypted		Revert Zeroization Command	SED AdminSP Active Encryption Key:Encrypts SED AdminSP Active Signing

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				RevertSP Zeroization Command	Key:Encrypts SED AdminSP Active Encryption Key:Decrypts SED AdminSP Active Signing Key:Decrypts SED LockingSP Active Encryption Key:Encrypts SED LockingSP Active Signing Key:Encrypts SED LockingSP Active Encryption Key:Decrypts SED LockingSP Active Signing Key:Decrypts Global Active Encryption Key (AEK):Encrypted by Global Active Encryption Key (AEK):Decrypted by Global Active Signing Key:Signed by
SED Active Signing Key		NOR Flash:Encrypted		Revert Zeroization Command RevertSP Zeroization Command	SED AdminSP Active Encryption Key:Signs SED AdminSP Active Signing Key:Signs SED LockingSP Active Encryption Key:Signs SED LockingSP Active Signing Key:Signs MSID:Signs PSID:Signs Global Active Encryption Key (AEK):Encrypted by Global Active Encryption Key (AEK):Decrypted by Global Active Signing Key:Signed by
SED AdminSP Active Encryption Key		NOR Flash:Encrypted		Revert Zeroization Command	Admin SP CSP Blob:Encrypts Admin SP CSP Blob:Decrypts SED Active Encryption

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				RevertSP Zeroization Command	Key:Encrypted by SED Active Encryption Key:Decrypted by SED Active Signing Key:Signed by
SED AdminSP Active Signing Key		NOR Flash:Encrypted		Revert Zeroization Command RevertSP Zeroization Command	Admin SP CSP Blob:Signs SED Active Encryption Key:Encrypted by SED Active Encryption Key:Decrypted by SED Active Signing Key:Signed by
SED LockingSP Active Encryption Key		NOR Flash:Encrypted		Revert Zeroization Command RevertSP Zeroization Command	Locking SP CSP Blob:Encrypts Locking SP CSP Blob:Decrypts SED Active Encryption Key:Encrypted by SED Active Encryption Key:Decrypted by SED Active Signing Key:Signed by
SED LockingSP Active Signing Key		NOR Flash:Encrypted		Revert Zeroization Command RevertSP Zeroization Command	Locking SP CSP Blob:Signs SED Active Encryption Key:Encrypted by SED Active Encryption Key:Decrypted by SED Active Signing Key:Signed by BandMaster PIN (16 total):Used With BandMaster PIN Digest (16 total):Generates EraseMaster PIN:Used With EraseMaster PIN Digest:Generates
SED Volatile Encryption Key		IRAM:Plaintext	Power up to power down	Power Cycle Revert Zeroization Command RevertSP	Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique):Encrypts Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Zeroization Command	(BandMaster unique):Encrypts Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique):Decrypts Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique):Decrypts
SED Volatile Signing Key		IRAM:Plaintext	Power up to power down	Power Cycle Revert Zeroization Command RevertSP Zeroization Command	Locking Range Keyset (LRK) - LRK.AES Key, LRK.XTS Key (BandMaster unique):Signs Media Encryption Keyset (MEK) - MEK.AESEnc Key, MEK.AESDec Key, MEK.XTS Tweak Key (BandMaster unique):Signs
sFFU_EncKey	Public Key Input	NAND Flash:Plaintext		N/A	SecureBootPublicKey:Verified by
sFFUPublicKey	Public Key Input	NAND Flash:Plaintext		N/A	SecureBootPublicKey:Verified by
SID PIN	Authentication Credential PIN	IRAM:Plaintext	Ephemeral SSP Zeroization	N/A	SED AdminSP Active Signing Key:Used With SID PIN Digest:Generate
SID PIN Digest		Disk Media (Reserved Area):Plaintext		Revert Zeroization Command RevertSP Zeroization Command	SID PIN:Generated From SED AdminSP Active Signing Key:Generated From
Storage Device Boot FW Key (SD_BFW Key)		NOR Flash:Obfuscated		N/A	Storage Device Certification Authority Key (SD_CA Key):Verified by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Storage Device Certification Authority Key (SD_CA Key)		NOR Flash:Obfuscated		N/A	Storage Device Boot FW Key (SD_BFW Key):Verifies Security Core Firmware Key (SC_FW Key):Verifies Security Protocol Firmware Key (SP_FW Key):Verifies Product Group Key (PROD_GROUP Key):Verifies
SD CA Key Digest		One-time Programable (OTP):Plaintext		N/A	Storage Device Certification Authority Key (SD_CA Key):Verifies
User Access Key (UAK) (BandMaster unique)		Disk Media (Reserved Area):Encrypted		Revert Zeroization Command RevertSP Zeroization Command	Range Access Key (RAK) (BandMaster unique):Encrypts Range Access Key (RAK) (BandMaster unique):Decrypts Non-Admin Authority Key (Ku) (BandMaster unique):Encrypted by Non-Admin Authority Key (Ku) (BandMaster unique):Decrypted by
User Management Key (UMK)		Disk Media (Reserved Area):Encrypted		Revert Zeroization Command RevertSP Zeroization Command	User Access Key (UAK) (BandMaster unique):Encrypts User Access Key (UAK) (BandMaster unique):Decrypts Admin Authority Key (Ka):Encrypted by Admin Authority Key (Ka):Decrypted by

Table 20: SSP Table 2

10 Self-Tests

The Cryptographic Module performs pre-operational self-tests automatically at powered up and after installing a new firmware image. Pre-operational self-tests tests ensure that the Cryptographic Module is not corrupted, and all cryptographic algorithms work as expected. The Cryptographic Module

inhibits all data output via the "data output" interface and the execution of loaded or modified approved security functions while executing the pre-operational self-tests.

10.1 Pre-Operational Self-Tests

Cryptographic Module

The Cryptographic Module performs pre-operational self-tests listed in the Pre-Operational Self-Tests table at power up, in response to a self-initiated reset and prior to booting to a new firmware image. The execution of the ESV Critical Function test and the RSA SigVer SW/FW Integrity self-test, associated with Cert # A2098, satisfy AS10.23. Upon failure the Cryptographic Module transitions to a Device Unavailable error state.

OptiNAND Device

The OptiNAND device performs a pre-operational self-test listed in the Pre-Operational Self-Tests table at power up, in response to a self-initiated reset and prior to booting to a new firmware image. Upon failure, the device returns a UEC error code, aborts booting to the firmware image and transitions to a Device Unavailable error state. The execution of the SW/FW Integrity self-test associated with Cert # A2099 satisfies AS10.23.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity using RSA SigVer (FIPS186-4) (A2098)	3072-bit, PSS w/SHA2-256	KAT	SW/FW Integrity	Pass: Boot to the firmware image, Fail: Device Unavailable	Executed on all firmware stored in NOR Flash and on disk media before the Module transition to Security Subsystem (SSM) initialization state.
Firmware Integrity using RSA SigVer (FIPS186-4) (A2099)	3072-bit, PSS w/SHA2-256, SecureBootPublicKey	KAT	SW/FW Integrity	Pass: Boot to the firmware image, Fail: Device Unavailable	Executed on all firmware stored in NAND Flash before the OptiNAND device transitions to the Device Ready state.

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Cryptographic Module Conditional Self-Tests

The Cryptographic Module performs conditional self-tests listed in the Conditional Self-Tests table. Upon failure the Cryptographic Module, with exception of the ESV self-tests, transitions to a Device Degraded error state. Conditional ESV self-test failures cause the CM to transition to a Device Unavailable error state.

OptiNAND Conditional Self-Tests

The OptiNAND device performs conditional self-tests listed in the Conditional Self-Tests table. If any conditional self-test fails, the OptiNAND device executes a self-initiated reset or enters a Device Degraded error state. If the OptiNAND device enters a Device Degraded error state, the Cryptographic Module reports the error condition by transmitting an UEC error code to the host system. After entering the Device Degraded error state, the OptiNAND device does not process functional commands unless a power cycle occurs and clears the error state.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A2099) Encrypt	AES-256, CBC	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Encrypt, verify.	At bootup
AES-CBC (A2099) Decrypt	AES-256, CBC	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Decrypt, verify.	At bootup
AES-CBC (AES 3580) Encrypt	AES-256	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Encrypt, verify.	At bootup
AES-CBC (AES 3580) Decrypt	AES-256	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Decrypted, verify.	At bootup
AES-ECB (AES 3580) Encrypt	AES-256	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Encrypt, verify.	At bootup
AES-ECB (AES 3580) Decrypt	AES-256	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Decrypted, verify.	At bootup
AES-KWP (A2098) Encrypt	256-bit	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Authenticated Encrypt, verify.	At bootup
AES-KWP (A2098) Decrypt	256-bit	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Authenticated Decrypt, verify.	At bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS (A2101) Encrypt	AES-256	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Encrypt, verify.	At bootup
AES-XTS (A2101) Decrypt	AES-256	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	Decrypt, verify.	At bootup
AES-XTS (A2101) Non-equivalence test	AES-256	Non-equivalence test	Critical Function	Fail: UEC error code	Verify	LRK and NSK generation
Counter DRBG (A2098)	Counter DRBG, AES-256	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Unavailable	Counter DRBG SP800-90A Health Tests Instantiation, generate, and reseed KATs performed before the first random data generation	At bootup
ESV RCT	Repetition Count Test (RCT)	RCT	CAST	Pass: UEC success code/Next test, Fail: Device Unavailable	As specified in [90B] section 4.4 for continuous tests.	Continuous when entropy is requested. After the CTR_DRBG generates 2^32 keys.
ESV APT	Adaptive Proportion Test (APT)	APT	CAST	Pass: UEC success code/Next test, Fail: Device Unavailable	As specified in [90B] section 4.4 for continuous tests.	Continuous when entropy is requested. After the CTR_DRBG generates 2^32 keys.
ESV (Cert # ESV13) RCT	Repetition Count Test (RCT)	SP 800-90B Health-Test	CAST	Pass: Next test, Fail: Device Unavailable	An RCT as specified in [90B] section 4.4 are executed before generation of the DRBG entropy input.	At bootup
ESV (Cert # ESV13) APT	Adaptive Proportion Test (APT)	SP 800-90B Health-Test	CAST	Pass: Next test, Fail: Device Unavailable	An APT as specified in [90B] section 4.4 are executed before generation of the DRBG entropy input.	At bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Firmware Loading (A2098)	3072-bit Signature Verification	KAT	SW/FW Load	UEC success or error code	SHA-256 is computed on the loaded firmware and compared with the expected value.	Firmware download
Firmware Loading (A2099)	3072-bit Signature Verification	KAT	CAST	UEC success or error code	SHA-256 is computed on the loaded firmware and compared with the expected value.	Firmware download
HMAC-SHA2-256 (HMAC 2280)	HMAC-SHA2-256	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	HMAC-SHA2-256 KAT.	At bootup
PBKDF (A2100)	256-bit Salt Iteration Count: 1024	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	PBKDF2 KAT	At bootup
RSA SigVer (FIPS186-4) (A2098)	3072-bit RSA	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	3072-bit RSA PSS with SHA-226 Signature Verification.	At bootup
RSA SigVer (FIPS186-4) (A2099)	3072-bit RSA	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	3072-bit RSA PSS with SHA-226 Signature Verification	At bootup
SHA2-256 (A2099)	Message, 256-bit hash digest	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	HASH	At bootup
SHA2-256 (SHS 2942)	Message, 256-bit hash digest	KAT	CAST	Pass: UEC success code/Next test, Fail: Device Degraded	HASH	At bootup

Table 22: Conditional Self-Tests

10.3 Periodic Self-Test Information

The Cryptographic Module does not enforce a policy that would result in the interruption of the module's operations due to a periodic self-test.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity using RSA SigVer (FIPS186-4) (A2098)	KAT	SW/FW Integrity	On Demand	Device Reset
Firmware Integrity using RSA SigVer (FIPS186-4) (A2099)	KAT	SW/FW Integrity	On Demand	Device Reset

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A2099) Encrypt	KAT	CAST	On Demand	Device Reset
AES-CBC (A2099) Decrypt	KAT	CAST	On Demand	Device Reset
AES-CBC (AES 3580) Encrypt	KAT	CAST	On Demand	Device Reset
AES-CBC (AES 3580) Decrypt	KAT	CAST	On Demand	Device Reset
AES-ECB (AES 3580) Encrypt	KAT	CAST	On Demand	Device Reset
AES-ECB (AES 3580) Decrypt	KAT	CAST	On Demand	Device Reset
AES-KWP (A2098) Encrypt	KAT	CAST	On Demand	Device Reset
AES-KWP (A2098) Decrypt	KAT	CAST	On Demand	Device Reset
AES-XTS (A2101) Encrypt	KAT	CAST	On Demand	Device Reset
AES-XTS (A2101) Decrypt	KAT	CAST	On Demand	Device Reset

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS (A2101) Non-equivalence test	Non-equivalence test	Critical Function	On Demand	Programmatically
Counter DRBG (A2098)	KAT	CAST	On Demand	Device Reset
ESV RCT	RCT	CAST	On Demand	Device Reset, Programmatically
ESV APT	APT	CAST	On Demand	Device Reset, Programmatically
ESV (Cert # ESV13) RCT	SP 800-90B Health-Test	CAST	On Demand	Device Reset
ESV (Cert # ESV13) APT	SP 800-90B Health-Test	CAST	On Demand	Device Reset
Firmware Loading (A2098)	KAT	SW/FW Load		
Firmware Loading (A2099)	KAT	CAST		
HMAC-SHA2-256 (HMAC 2280)	KAT	CAST	On Demand	Device Reset
PBKDF (A2100)	KAT	CAST	On Demand	Device Reset
RSA SigVer (FIPS186-4) (A2098)	KAT	CAST	On Demand	Device Reset
RSA SigVer (FIPS186-4) (A2099)	KAT	CAST	On Demand	Programmatically
SHA2-256 (A2099)	KAT	CAST	On Demand	Device Reset
SHA2-256 (SHS 2942)	KAT	CAST	On Demand	Device Reset

Table 24: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Device Degraded	This error indicates that one of the conditional self-tests listed in the Conditional Self-Test table. In this state, the module no longer services any I/O command. The module only responds to non-I/O status inquiry commands.	Conditional test failure	Power Cycle	UEC failure code
Device Unavailable	This error indicates that a boot initialization, security subsystem initialization or firmware integrity failure event occurred. See the operational Self-Test table. In this state, the module no longer responds to any operator commands.	Pre-operational test failure	Power Cycle	Module is unresponsive

Table 25: Error States

10.5 Operator Initiated Self-Tests

The operator may initiate an on-demand periodic self-test by power cycling the CM.

11 Life-Cycle Assurance

11.1 Installation, Initialization and Startup Procedures

After initialization, the CM operates and powers up in isFIPS mode. Prior to configuring the CM to comply with isFIPS mode configuration requirements, it operates in a noncompliant state. Regardless, the CM functions as a Secure Erase Drive (SED) that is compliant with the TCG Storage SSC: Enterprise Specification [TCG Enterprise].

Installation and Initialisation:

The Crypto Officer is responsible for executing a Take-Ownership scenario to configure the Cryptographic Module to operationally comply with operator site requirements and assure that the Cryptographic Module is compliant with FIPS 140-3 at SL2.

Informative

Having the MSID Authentication Credential PIN electronically available to the operator constitutes a risk to the overall security of the Cryptographic Module. Therefore, the Crypto Officer should execute a Take-Ownership scenario the first time the Cryptographic Module is inserted into a system that replaces Authentication Credential PIN values that are set to the module unique MSID value with a value that is different from the MSID value and between 12 and 32 bytes in length. This assures compliance with ISO/IEC19790, Section 7.4.4 and IG 4.4.B.

Take-Ownership Scenario Example

1. Authenticate to the SID.
    a. If the CM authenticated to the SID with the module unique MSID value, change the SID PIN to a random value between 12 and 32 bytes in length.
2. Use the Get service to determine if the logical firmware download port is set to lock on PowerCycle.
    a. If the logical firmware download port's LockOnReset attribute is not set to PowerCycle utilize the Set service to set the LockOnReset attribute to PowerCycle.
3. Authenticate to each BandMaster that is within the scope of the operator site requirements.
    a. If the CM authenticated to a BandMaster with the module unique MSID value, change the BandMaster PIN to a random value between 12 and 32 bytes in length.
    b. Utilize the Get Band Attributes service to determine the state of a BandMaster's LockOnReset attribute. If the LockOnReset attribute is not set to PowerCycle, use the Set Band Attribute service to set the LockOnReset attribute to PowerCycle.
    c. Utilize the Get Band Attributes service to determine the state of a BandMaster's ReadLockEnabled attribute. If the ReadLockEnabled attribute is not set to True, use the Set Band Attribute service to set the ReadLockEnabled attribute to True.
    d. Utilize the Get Band Attributes service to determine the state of a BandMaster's WriteLockEnabled attribute. If the WriteLockEnabled attribute is not set to True, use the Set Band Attribute service to set the WriteLockEnabled attribute to True.
4. Authenticate to the EraseMaster.
    a. If the CM authenticated to the EraseMaster with the module unique MSID value, change the EraseMaster PIN to a random value between 12 and 32 bytes in length.

Delivery:

The Cryptographic Officer shall inspect the tamper evident seal that covers the Cryptographic Module's PCBA for evidence of tampering. See Figure 13 for an example of tamper evidence. If tamper evidence is apparent, the CO should return the module to Western Digital.

11.2 Administrator Guidance

Hard disk drives are fragile. Do not drop or jar the drive. Hold the drive only by the enclosure.

HDD electronics are sensitive to static electricity. Do not remove the CM from its antistatic container until ready to install. The operator engaged in the installation process should wear an antistatic wrist strap to ground to assure the discharge static electricity from any item or surface that my touch the CM. Hold the drive only by the metal case surrounding the drive. Avoid contacting with the SAS connector.

To assure proper installation and operation, verify all cooling requirements are met prior to initiating the installation instructions within the Ultrastar DC HC560 3.5-inch Serial Attached SCSI Hard Disk Drive Specification [Product Manual] and Ultrastar DC HC570 3.5-inch Serial Attached SCSI Hard Disk Drive Specification [Product Manual].

The Ultrastar DC HC560 3.5-inch Serial Attached SCSI Hard Disk Drive Specification [Product Manual] and Ultrastar DC HC570 3.5-inch Serial Attached SCSI Hard Disk Drive Specification [Product Manual] provides additional administrator guidance.

11.3 Non-Administrator Guidance

Inspect the CM for damage to the case or SAS connector. If the CM exhibits damage, return the CM for warranty replacement service.

The Ultrastar DC HC560 3.5-inch Serial Attached SCSI Hard Disk Drive Specification [Product Manual] and Ultrastar DC HC570 3.5-inch Serial Attached SCSI Hard Disk Drive Specification [Product Manual] provide non-administrator guidance.

11.4 Design and Rules

On power-up, if previously configured to comply with isFIPS mode, the Cryptographic Module automatically initializes to isFIPS mode without operator intervention. After successfully completing pre-operational and conditional self-tests, the CM transitions to an Approved mode operational state. In this state, the module awaits service requests from the operator.

The implemented security features protect against remote and physical attacks across the complete product cycle from manufacturing build time to returns and failure analysis. The secure firmware boot and firmware download process assure firmware image integrity and prevents compromised firmware attacks. These features prevent the counterfeiting of the CM, hacking and unauthorized access to CM ports. The authentication scheme enforces port restrictions for processes that are only allowed within a secure manufacturing environment. These security features utilize cryptographically secure messages to block unauthorized access to CM ports and imposes manufacturing command set restrictions. The CM utilizes a cryptographic encryption and HMAC signing scheme to assure the protection of all SSPs stored outside the ACM.

Rules of Operation

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
2. The Module provides role-based authentication.
3. On power cycle the Module clears previous authentications.
4. The Module complies with the lock-based authentication model. On power cycle, the Module locks unlocked services that require authentication to unlock (IG 4.1.A).
5. Accept as allowed under the lock-based authentication model, the operator does not have access to any cryptographic services prior to assuming an authorized role.
6. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.

7. All self-tests do not require any operator action.
8. The Cryptographic Module inhibits data output during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
10. The Module implements multiple zeroization service that vary in scope. The SSP Zeroization Methods table defines scope of each zeroization service.
11. The Module does not support concurrent operators.
12. The Module does not support a maintenance interface or role.
13. The Module does not support manual SSP establishment method.
14. The Module does not have any proprietary external input/output devices used for entry/output of data.
15. The Module does not enter or output plaintext CSPs.
16. The Module does not store any plaintext CSPs in non-volatile memory.
17. The Module does not output intermediate key values.
18. The Module does not provide bypass services or ports/interfaces.

11.5 Maintenance Requirements

The CM does not require periodic maintenance actions to maintain functional or secure operation.

11.6 End of Life

All CSPs stored within the volatile memory of the CM's ACM are inaccessible from outside the ACM. The CM encrypts and signs all CSPs before storing them in volatile or non-volatile memory outside the ACM. Removing power instantaneously erases all CSPs stored within the CM's volatile memory.

Prior to the environmentally disposal of the CM owner should cryptographically erase the CM. For this purpose, the CM supports the TCG Opal Revert method [TCG Opal]. Revert enables the CM's owner to cryptographically erase all CSPs and overwrite existing TCG settings to the module unique values that were set during manufacturing. If environmental disposal requirements require the zeroization of the Root Keyset, which consists of the Root Encryption Key and Root Signing Key, the CM owner must return the CM to Western Digital. Western Digital's proprietary Secure Manufacturing Reconfiguration Process supports Root Keyset zeroization.

12 Mitigation of Other Attacks

The Cryptographic Module lacks features to mitigate any specific attacks beyond the scope of the requirements within FIPS 140-3 SL2.

13 References and Definitions

The Security Policy refers to the following specifications, references, and definitions.

13.1 NIST Specifications

Abbreviation*	Specification Name
[FIPS 197]	Advanced Encryption Standard, FIPS PUB 197, NIST, May 2023
[FIPS 186]	Digital Signature Standard, FIPS PUB 186-4, NIST, July 2013
[FIPS 140]	Security Requirements for Cryptographic Modules, FIPS PUB 140-3, NIST, March 2019
[FIPS 140 IG]	Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program, September 2025

Abbreviation*	Specification Name
[FIPS 198]	The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, July 2008
[FIPS 180]	Secure Hash Standard (SHS), FIPS PUB 180-4, NIST, August 2015
[SP 800 38A]	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST, December 2001
[SP 800 38E]	Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, NIST, January 2010
[SP 800 38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, NIST, December 2012
[SP 800 57]	Recommendation for Key Management – Part I General (Revision 5), NIST, May 2020
[SP 800 88]	Guidelines for Media Sanitization (Revision 1), NIST, December 2014
[SP 800 90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revision 1), NIST, June 2015
[SP 800 90B]	Recommendation for the Entropy Sources Used for Random Bit Generation, NIST, January 2018
[SP 800 131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (Revision 2), NIST, March 2019
[SP 800 132]	Recommendation for Password-Based Key Derivation, NIST, December 2010
[SP 800 133]	Recommendation for Cryptographic Key Generation (Revision 2), NIST, June 2020
[SP 800 140B]	Cryptographic Module Validation Program (CMVP) Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B (Revision 1), NIST, November 2023
[SP 800 140C]	CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 (Revision 2), NIST, July 2023
[SP 800 140D]	CMVP Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759 (Revision 2), NIST, July 2023

13.2 Trusted Computing Group Specifications

Abbreviation*	Specification Name
[TCG Core]	TCG Storage Architecture Core Specification, Version 2.01 Revision 1.00 (August 5, 2015))
[TCG Enterprise]	TCG Storage Security Subsystem Class: Enterprise Specification, Version 1.01 Revision 1.00 (August 5, 2015)
[TCG Ent App Notes]	TCG Storage Application Note: Encrypting Storage Devices Compliant with SSC: Enterprise, Version 1.00 Revision 1.00 Final
[TCG Opal]	TCG Storage Security Subsystem Class: Opal Specification, Version 2.01, Final Revision 1.00 (August 5, 2015)
[TCG SIIS]	TCG Storage Interface Interactions Specification (SIIS), Version 1.07, (January 30, 2018)
[PSID]	TCG Storage Opal SSC Feature Set: PSID, Specification Version 1.00, Final Revision 1.00 (August 5, 2015)

13.3 SCSI Specifications

Abbreviation*	Specification Name
[SCSI Core]	SCSI Primary Commands (SPC-6), Revision 6, October 2021
[SCSI Block]	SCSI Block Commands (SBC-4), Revision 22, 29 September 2020
[SAS]	Serial Attached SCSI (SAS-3), Revision 6, November 2013

Abbreviation*	Specification Name
[SFSC]	Security Features for SCSI Commands, Revision 2, September 2015

13.4 Corporate References

Abbreviation*	Specification Name
[Product Manual]	Ultrastar DC HC560 3.5-inch Serial Attached SCSI Hard Disk Drive Specification, Version 1.1 (April 2022), https://www.westerndigital.com/support
[Product Manual]	Ultrastar DC HC570 3.5-inch Serial Attached SCSI Hard Disk Drive Specification, Version 1.2 (September 2023), https://www.westerndigital.com/support
[Datasheet]	Ultrastar DC HC560 Datasheet, (July 2022), D018-000383-AA02, https://www.westerndigital.com/support
[Datasheet]	Ultrastar DC HC570 Datasheet, (August 2022), D018-000537-AA01, https://www.westerndigital.com/support

13.5 Other References

Abbreviation*	Reference Name
[IETF]	IETF RFC 2119, 1997, "Key words for use in RFCs to Indicate Requirement Levels."
[PW]	Calculating Password Entropy: https://www.pleacher.com/mp/mlessons/algebra/entropy.html
[ISO 19790]	ISO/IEC 19790, Information technology - Security techniques - Security requirements for cryptographic modules, International Organization for Standardization (ISO), December 2015

14 Definitions

Name*	Definition
Access Control Entry (ACE)	Access control entries are entries in an access control list containing information describing the access rights related to a particular security identifier or user.
Access Control List (ACL)	Access control list refers to the permissions attached to an object that specify which users have access to that object and the operations the user can perform.
Allowed	NIST approved, i.e., recommended in a NIST Special Publication, or acceptable, i.e., no known security risk as opposed to deprecated, restricted, and legacy use. [SP 800 131A]
Anybody	A formal TCG term for an unauthenticated role. [TCG Core]
Approved mode of operation	A mode of the Cryptographic Module that employs only approved security functions. [FIPS 140]
Approved	[FIPS 140] approved or recommended in a NIST Special Publication.
Authenticate	Prove the identity of an Operator or the integrity of an object.
Authentication Credential PIN	An authentication credential (i.e., a password) associated with the SID, Admin SP Admin1, Locking SP Admin or Locking SP User Authority as defined in the TCG Storage Security Subsystem Class Opal, Specification [TCG Core].
Authorize	Grant an authenticated Operator access to a service or an object.
Ciphertext	Encrypted data transformed by an Approved security function.
Confidentiality	A cryptographic property that blocks disclosure of sensitive information to unauthorized parties.
Credential	A formal TCG term for data used to authenticate an Operator. [TCG Core]
Critical Security Parameter (CSP)	Security-related information (e.g., secret, and private cryptographic keys, and authentication data such as credentials and PINs) whose disclosure or modification can compromise the security of a Cryptographic Module. [FIPS 140]
Crypto Officer	An Operator performing cryptographic initialization and management functions. [FIPS140]

Name*	Definition
Cryptographic Boundary	An explicitly defined perimeter that establishes the boundary of all components (i.e. set of hardware, software, or firmware components) of the cryptographic module. [FIPS 140]
Cryptographic Key	A sequence of symbols that controls the operation of a cryptographic transformation. A cryptographic transformation can include but not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification.
Cryptographic Module	The set of hardware, software, and/or firmware used to implement approved security functions contained within the cryptographic boundary. [FIPS 140]
CSP Blob	The term CSP Blob is used to indicate an external stored object that contains one or more CSPs. The CSP Blob is a protected unit and contains metadata such as version and UID. The contents of the CSP Blob may be visible outside the ACM. Some contents may be hidden and encrypted outside the ACM boundary. In all cases, the CSP Blob is only modifiable from within the ACM. When CSPs are stored externally to the ACM and/or accepted from outside the ACM boundary, tamper protection is implemented. Secret keys are used to AES encrypt and HMAC-SHA256 sign the entire CSP Blob before being stored outside the ACM boundary.
Data at Rest	User data residing on the storage device media rather than in transition.
Discovery	A TCG method that provides the properties of the TCG device. [TCG Enterprise]
Download and Execute module (DLE)	The DLE verifies the OptiNAND firmware RSA signature.
Field Firmware Update (sFFU)	A secure Field Firmware Update replaces the firmware within an iNAND device.
Global Active Keyset (AEK)	Set defined by the 256-bit Global Active Encryption Key and the 256-bit Global Active Signing Key
Hardware Security Module (HSM)	A hardware security module is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication, and other cryptographic functions.
IF-RECV	An interface command used to retrieve security protocol data from the TPer [TCG Core].
IF-SEND	An interface command used to transmit security protocol data to the TPer [TCG Core].
OptiNAND®	A Universal Flash Storage (UFS) embedded flash device.
Integrity	A cryptographic property that blocks the modification or deletion of sensitive in an unauthorized and undetected manner.
Interface	A logical entry or exit point of a Cryptographic Module that provides access to the Cryptographic Module for logical information flows. [FIPS 140]
Key Derivation Function (KDF)	An Approved cryptographic algorithm that derives one or more keys from a secret value and other information.
Key Encrypting Key (KEK)	A cryptographic key used to encrypt or decrypt other keys.
Key management	The activities involving the handling of cryptographic keys and other related security parameters during the entire life cycle of the Cryptographic Module. The handling of authentication data is representative of a key management activity.
Key Wrap	An Approved cryptographic algorithm that uses a KEK to provide Confidentiality and Integrity.
LBA Range	A formal term that defines a contiguous logical block range (sequential LBAs) to store encrypted User Data; bands do not overlap, and each has its own unique encryption key and other settable properties.
Manufactured SID (MSID)	A unique module unique value assigned to each SED during manufacturing. An externally visible MSID value is not required if the user can derive the MSID from other information printed on the drive. The MSID is readable with the TCG protocol. It is the initial and module unique value for all Authentication Credentials. [TCG Core]
Method	A remote procedure call to an SP that initiates an action on the SP. [TCG Core]

Name*	Definition
Object	An object is any row of an object table. The object type is defined by the object table in which the object occurs. The columns of the object table define the contents of each object in it. [TCG Core]
Object Table	Object tables provide storage for data that binds a set of methods and access controls to that data. [TCG Core]
ObjectUID	The Unique ID (UID) of an Object. Each object table has a column named UID. This column contains an 8-byte unique identifier for that row. [TCG Core]
OFS file	The CM uses an OFS file to reset the Cryptographic Module's configuration back to its original factory setting during Revert and RevertSP operations.
One Time Programable (OTP)	OTP memory is a special type of write once read only non-volatile memory.
Operator	A consumer, either human or automation, of cryptographic services that is external to the Cryptographic Module. [FIPS 140]
Personal Identification Number (PIN)	A formal TCG term designating a string of octets used to authenticate an identity. [TCG Core]
Plaintext	Unencrypted data.
Port	A physical entry or exit point of a Cryptographic Module that. A port provides access to the Cryptographic Module's physical signals. [FIPS 140]
PSID (Physical Security Identifier)	A SED unique value printed on the Cryptographic Module's label used as authentication data and proof of physical presence for the Zeroise Service.
Public Security Parameters (PSP)	Public information, that if modified can compromise the security of the Cryptographic Module (e.g., a public key).
Read Data	An external request to transfer User Data from the SED. [SCSI Block]
Reserved Area	Internal data on the storage medium within the cryptographic boundary that is not accessible to an operator.
Root Keyset	A set of 256-bit keys that consist of the Root Encryption Key and Root Signing Key.
SD_CA Key	Storage Device Certification Authority Key (X509v3). This key serves as the Cryptographic Module's Master RSA Public Key and is the root source of verification for all other key certificates. The SD_CA Key signs the SecureLoader. A manufacturing process injects the SD_CA Key within the CM and stores a hash of the SD_CA Key in OTP memory
Secure Field Firmware Update (sFFU)	OptiNAND firmware update image.
Security Identifier (SID)	The authority that represents the TPer owner. Crypto Officer serves in this role. [TCG Core]
Security Provider (SP)	A TCG term used to define a collection of Tables and Methods with access control.
SED Active Keyset	A set of 256-bit keys that consists of the SED Active Encryption Key and the SED Active Signing Key.
SED AdminSP Active Keyset	A set of 256-bit keys that consists of the SED AdminSP Active Encryption Key and the SED AdminSP Active Signing Key.
SED Global Active Keyset	A set of 256-bit keys that consists of the Global Active Encryption Key (AEK) and the Global Active Signing Key.
SED LockingSP Active Keyset	A set of 256-bit keys that consists of the SED LockingSP Active Encryption Key and the SED LockingSP Active Signing Key. The keyset protects TCG protocol LockingSP CSPs.
SED Volatile Keyset	A set of 256-bit keys that consists of the SED Volatile Key and the SED Volatile Signing Key.
Self-Encrypting Drive (SED)	A storage device that provides data storage services, which automatically encrypts all user data written to the device and automatically decrypts all user data read from the device.
Session	A formal TCG term that envelops the lifetime of an Operator's authentication. [TCG Core]
Small Form Factor (SFF)	Small form factor is a computer form factor designed to minimize the volume and footprint of a desktop computer.

Name*	Definition
Storage Medium	The non-volatile, persistent storage location within a SED partitioned into disjointed sets defined by a User Data area, and a Reserved Area.
Table	The basic data structures within a Security Provider (SP). Object tables store persistent SP state data defined in TCG Core specification. [TCG Core]
TableUID	The Unique ID (UID) of a Table. Each object table has a column named UID. This column contains an 8-byte unique identifier for that row. [TCG Core]
TPer	A Trusted Peripheral. The TPer manages trusted storage-related functions and data structures. [TCG Core]
TPer Owner	The SID Authority (Crypto Officer) represents TPer Owner.
Triple Level Cell (TLC)	Triple level cells refer to NAND flash devices that store three bits of information per cell, with eight total voltage states.
User Data	Data transferred from/to a SED using the Read Data and Write Data commands. [SCSI Block]
User	An Operator that consumes cryptographic services. [FIPS 140]
Write Data	An external request to transfer User Data to a SED. [SCSI Block]
Zeroise	Invalidate a Critical Security Parameter. [FIPS 140]

15 Acronyms

Acronym*	Definition
AEK	Active Encryption Key
AEN	Asynchronous Event Notification
AES	Advanced Encryption Standard (FIPS 197)
ACE	Access Control Entry
ACL	Access Control List
CBC	Cipher Block Chaining, an operational mode of AES
CM	Cryptographic Module
CO	Crypto Officer [FIPS 140]
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter [FIPS 140]
DEE	Data Encryption Engine
DLE	OptiNAND Download and Execute firmware
DRAM	Dynamic Random Access Memory
DRBG	Deterministic Random Bit Generator
EDC	Error Detection Code
EMI	Electromagnetic Interference
FID	Flash Internal Data
FIPS	Federal Information Processing Standard
FSEC	Flash Security Data
HDD	Hard Disk Drive
HSM	Hardware Security Module
IV	Initialization Vector
KAT	Known Answer Test
KDF	Key Derivation Function

Acronym*	Definition
KEK	Key Encrypting Key
LBA	Logical Block Address
MEK	Media Encryption Key
MSID	Manufactured Security Identifier
NAND	**N**egative AND Flash Memory technology
NIST	National Institute of Standards and Technology
NOR	**N**egative OR Flash Memory technology
OFS	Original Factory Setting
OTP	One Time Programable
PBKDF2	Password Base Key Derivation Function
PIN	Personal Identification Number
POR	Power on Reset
PSID	Physical Security Identifier
PSP	Public Security Parameter
RID	Reserved Area Internal Data
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SD_CA	Storage Device Certification Authority
SECD	Security Data
SED	Self-Encrypting Drive
SFF	Small Form Factor
sFFU	Secure Field Firmware Update
SID	Security Identifier, The TCG authority representing the TPer Owner (Cryptographic Officer)
SIO	Serial Input/Output
SOC	System-on-a-Chip
SP	Security Provider [TCG Core], also Security Policy [FIPS 140]
SSC	Subsystem Class
SWG	Storage Work Group
TCG	Trusted Computing Group
TLC	Triple Level Cell
UEC	Universal Error Code
UID	Unique Identifier
XTS	A mode of AES that utilizes "Tweakable" block ciphers