Vendor name
Western Digital Technologies, Inc.

Module Name
Ultrastar DC HC560 TCG Enterprise HDD SED, Ultrastar DC HC570 TCG Enterprise HDD SED

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.6
Date: October 16, 2024

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.

Table 1 Security Levels

ISO/IEC 24759 Section 6	FIPS 140-3 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

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

Module Type
Hardware

Module Embodiment

Module Embodiment
Multiple-chip embedded

Module Characteristics

Module Characteristics
Figure 1 illustrates a logical view of the CM's firmware components. The Security Core partition is the most secure portion of the security subsystem. It forms a security boundary that provides assurances of firmware integrity and SSP integrity within the CM. The Security Protocol and Services partition contains the TCG Storage SSC: Enterprise SCC security protocol. Components in this ring communicate to the Security Core firmware through a Security Core API. The Security Application Client firmware, typically referred to as "Base Firmware" interfaces with the Security Protocol and Services firmware, provides adapters for the security subsystem support and implements a perimeter defense of the system based on security state. Specifically, the enforcement of port and command controls for manufacturing commands, firmware download control enforcement and boot up signature checks resides within the Security Application Client firmware layer. The Cryptographic Module operates within a limited operational environment. While operational, the Cryptographic Module prohibits operator or process-initiated additions, deletions, or modification of the code working set. For firmware upgrades, the Cryptographic Module uses an authenticated download service, which complies with ISO 19790 7.4.3.4, to upgrade the mutable firmware in its entirety. The immutable security firmware stored in ROM, which is essential and integral to the operation of the module is nonmodifiable. If the download operation is successful, authorized, and verified, the Cryptographic Module will begin operating with the new code working set after successfully executed all required pre-operational self-tests that comply with ISO 19790 7.10.2. Firmware loaded into the 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. The Cryptographic Module's security design utilizes common security protections, policies, and processes. It utilizes a hardware security Access Control Module (ACM) that incorporates a hardware Root of Trust (RoT). Security firmware leverages the RoT, hardware cryptographic algorithms and accelerators to implement a secure environment that assures firmware integrity, port access and the secure storage of plaintext secrets, user data, keys, and Sensitive Security Parameters (SSP) within the Cryptographic Module. The Cryptographic Module only supports approved security functions defined in NIST SP 800-140C and SP 800-140D. The hardware Root of Trust assures, 1) The isolation of security firmware and sensitive security parameters from Security Application Client firmware or firmware installed on embedded components within the cryptographic boundary, 2) The verification of cryptographic module firmware and security objects before usage, 3) A Key Management tree that secured by a root key stored in HW RoT OTP bits, 4) Support for a HW based Symmetric Key Generation, 5) Cryptographic Algorithm Acceleration and 6) End-to-End Protect between ACM & Key Server.

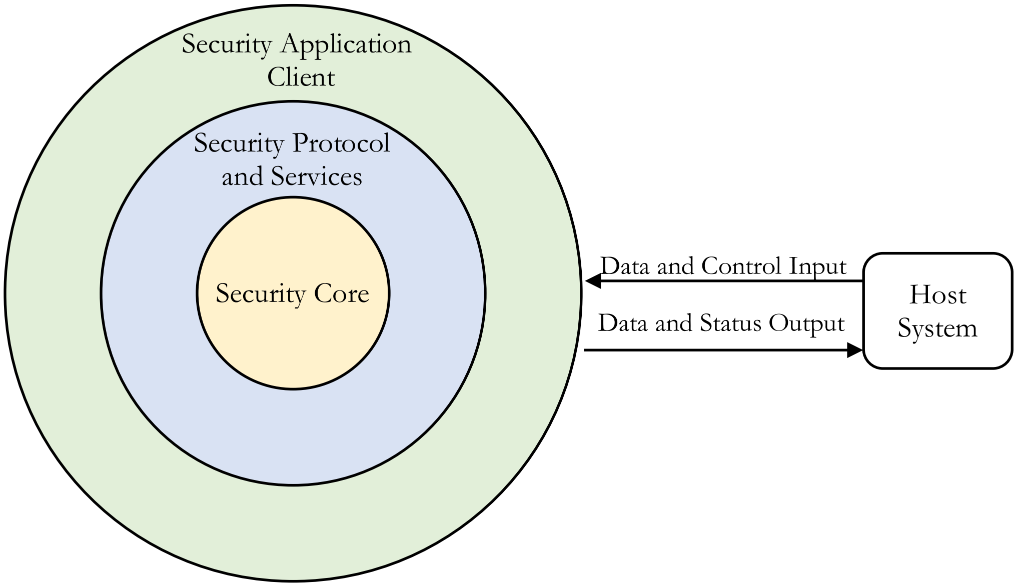

Figure 1 - Security Subsystem Components

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 and 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

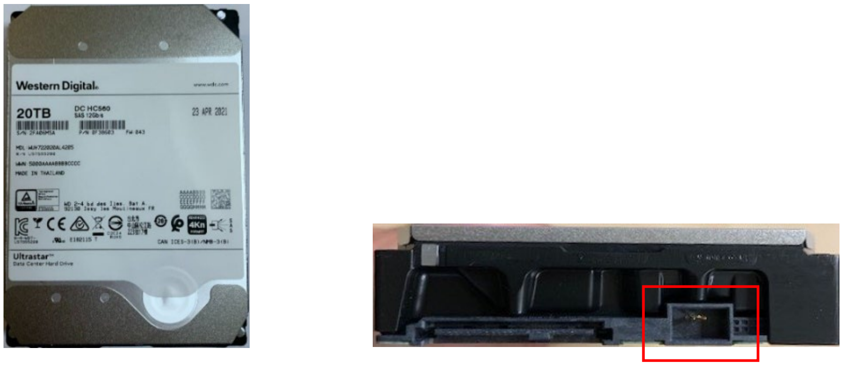

Figure 2 - Ultrastar DC HC560

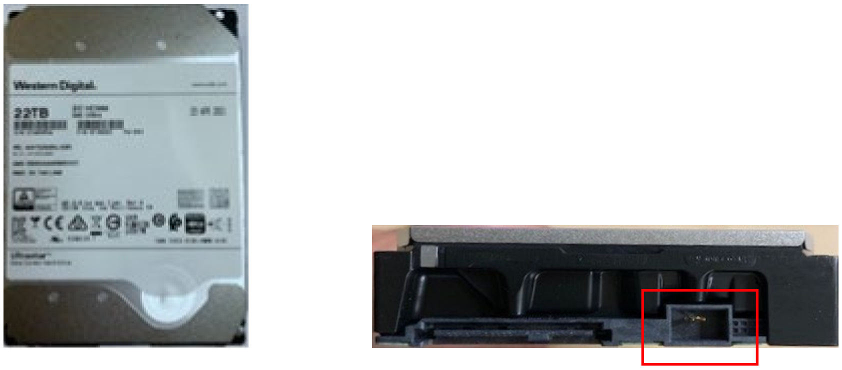

Figure 3 - Ultrastar DC HC570

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification - Hardware

The Ultrastar DC HC560 cryptographic module is tested on the following operational environment.

#	Model/Part Number	Hardware Versions	Firmware Versions	Processors	Non-Security Relevant Distinguishing Features
1	Ultrastar DC HC560	WUH722020BL4205	RY07, R5G4, RG01, VM18	ARM Cortex M3, ARM Cortex-R8, Synopsys ARC HS36	N/A
2	Ultrastar DC HC560	WUH722020BL5205	RY07, R5G4, RG01, VM18	ARM Cortex M3, ARM Cortex-R8, Synopsys ARC HS36	N/A

The Ultrastar DC HC570 cryptographic module is tested on the following operational environment.

#	Model/Part Number	Hardware Versions	Firmware Versions	Processors	Non-Security Relevant Distinguishing Features
1	Ultrastar DC HC570	WUH722222BL4205	R7J4, RG01	ARM Cortex M3, ARM Cortex-R8, Synopsys ARC HS36	N/A
2	Ultrastar DC HC570	WUH722222BL5205	R7J4, RG01	ARM Cortex M3, ARM Cortex-R8, Synopsys ARC HS36	N/A

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 2 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

Exclusion	Rationale
	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.

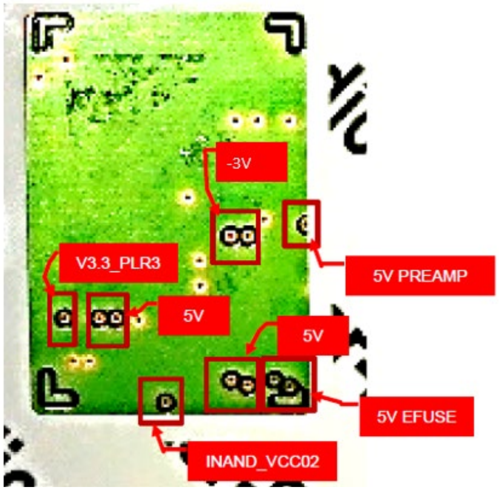

Figure 4 - Excluded Components, Ultrastar DC HC560

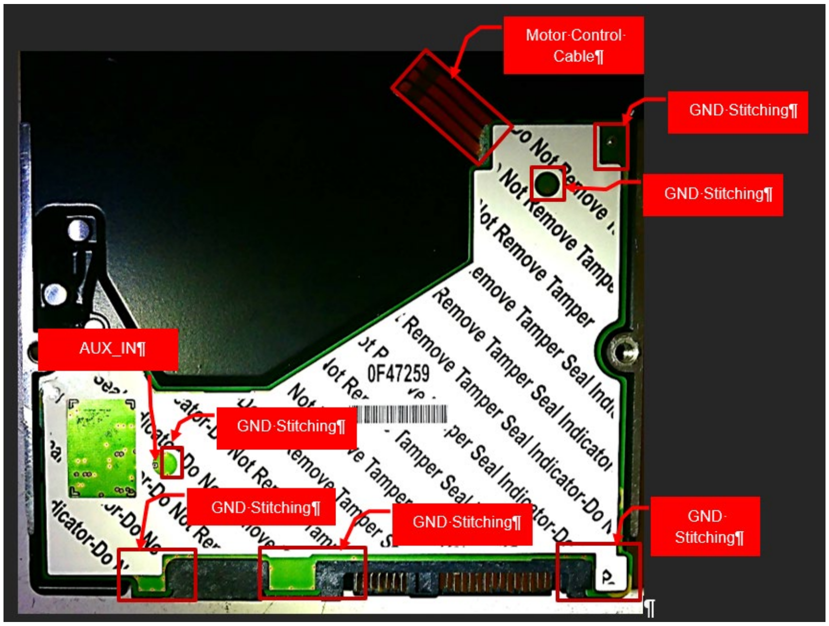

Figure 5 - Excluded Components, Ultrastar DC HC560

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

Table 3 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.

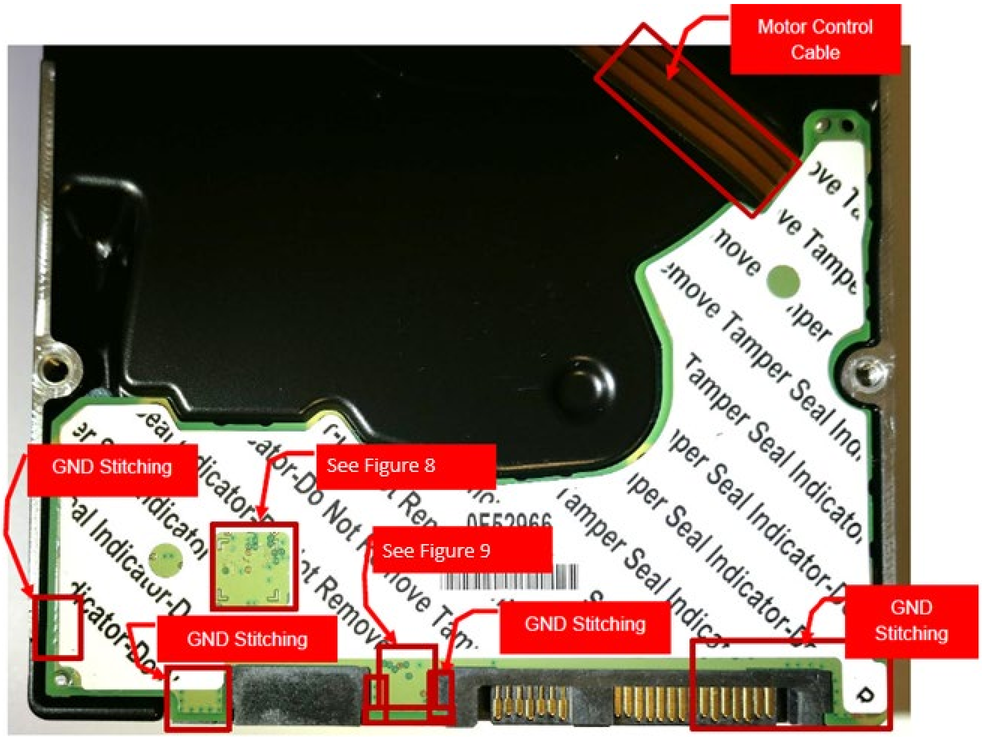

Figure 6 - Excluded Components, Ultrastar DC HC570

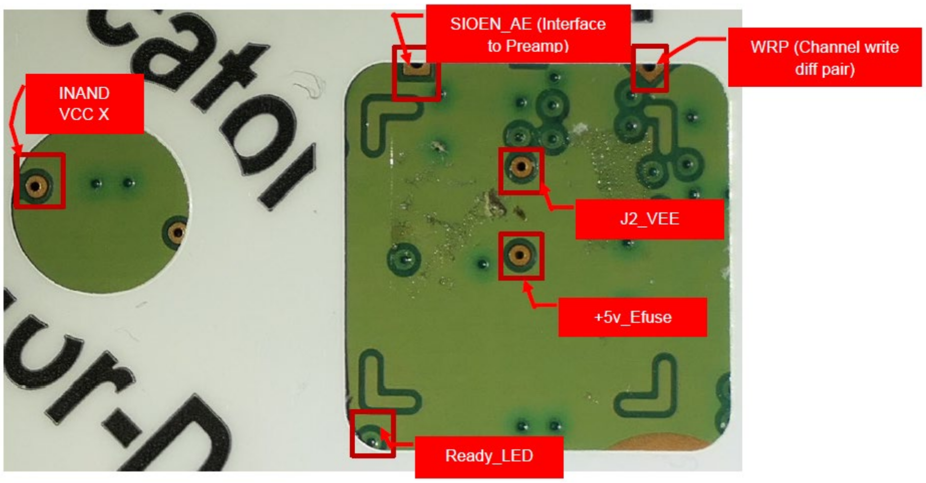

Figure 7 - Excluded Components, Ultrastar DC HC570

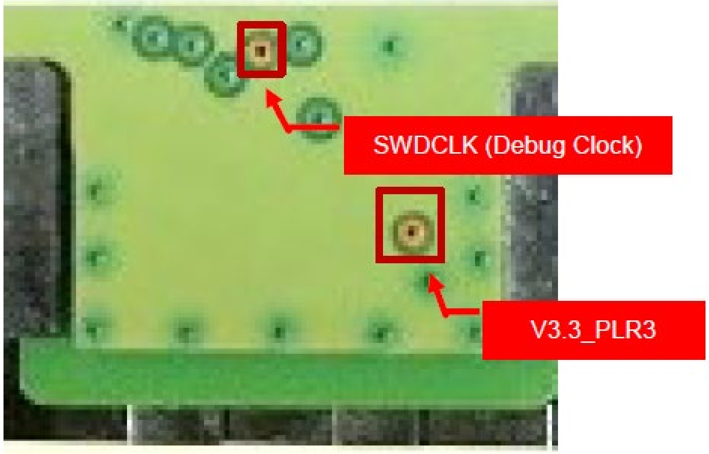

Figure 8 - Excluded Components, Ultrastar DC HC570

2.4 Modes of Operation

Table 4 Modes of Operation

Name	Description	FIPS	Status Indicator
isFIPS	The cryptographic module is operating as a compliant FIPS 140-3 module	Approved	1. The Level 0 Discovery[1] service returns a value of 1 from the in FIPS[2] global indicator data field and 2. The Firmware Download Control LockOnReset field is set to PowerCycle[3] and 3. For each configured BandMaster[4], the state of each listed attribute is set as shown below. • LockOnReset = PowerCycle • ReadLockEnabled = True • WriteLockEnabled = True

Section 11.1 of this document 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:

Table 4 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

[1] See the Level 0 Discovery' Vendor Specific Data 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.

[2] Global module-level indicator as defined in FIPS 140-3 IG 2.4.C Approved Security Service Indicator

[3] See 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.

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

Table 4 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 Table 5.

Approved Algorithms

Table 5 Approved Algorithms

Vendor Name	CAVP Cert	Algorithm and Standard	Mode/method	Description/Key Size/Key Strength	Use/Function
Avago Technologies	AES 3580[5]	AES [FIPS 197]	CBC [SP 800 38A]	Key Size: 128, 256 Key Strength: 128 bits, 256 bits	Encryption and Decryption of SSPs.
			ECB [SP 800 38A]	Key Size: 128, 256 Key Strength: 128 bits, 256 bits	Encryption and Decryption, AES KWP.
			XTS [SP 800 38E]	Key Size: 128, 256 Key Strength: 128 bits, 256 bits	Not used
Western Digital Corporation	A2098	AES [FIPS 197]	KWP [SP 800 38F] ECB [SP 800 38A]	Forward Payload Length: 96-1024, Increment 8 Key Size: 256 Key Strength: 256	Authenticated Encryption, Authenticated Decryption of Root Signing Key.
Western Digital Corporation	A2099	AES [FIPS 197]	CBC [SP 800 38A]	Key Size: 256 Key Strength: 256 bits	Descrambles OptiNAND sFFU firmware image.
Western Digital Corporation	A2101	AES [FIPS 197]	ECB [SP 800 38A]	Key Size: 128, 256 Key Strength: 128, 256 bits	Encryption, Decryption, DEE self-tests.
			XTS [SP 800 38E]	Payload Length: 4096 – 32768 Increment: 128 Tweak Mode: Number Key Size: 128, 256 Key Strength: 128, 256 bits	Encryption and Decryption of data-at-rest.
Western Digital Corporation	A2098	DRBG [SP 800 90A]	CTR	Mode: AES-256 Derivation Function: True Prediction Resistance: False Key Size: 256 Key Strength: 256 bits	Deterministic Random Bit Generation Security Strength = 256

[5] AES 3580 (2015) predates Testing Revision 2.0

Vendor Name	CAVP Cert	Algorithm and Standard	Mode/method	Description/Key Size/Key Strength	Use/Function
Avago Technologies	HMAC 2280	HMAC [FIPS 198]	SHA-1	Message Length: 8-51200, Increment: 8 Key Size: 160 Key Strength: 160 bits	Not used
			SHA2-224	Message Length: 8-51200, Increment: 8 Key Size: 224 Key Strength: 224 bits	Not used
			SHA2-256	Message Length: 8-51200, Increment: 8 Key Size: 256 Key Strength: 256 bits	Message Authentication of signed encrypted SSPs, PBKDF2 derived key generation
Western Digital Corporation	A2100	PBKDF2 [SP 800 132]	Option 2a	Master Key Generation Type: Option 2a Iteration Count: 2 - 1024 with Increment 1 HMAC Algorithm: SHA2-256 Password Length: 32 Salt Length: 128-512 with Increment 8 Key Data Length: 256 - 4096 with Increment: 256 Key Strength: 256	Password based key derivation function using HMAC-SHA2-256 (Cert #HMAC 2280). The derived generated keys, K_u, and K_a, encrypt data protection keys used in a data storage application.
Western Digital Corporation	A2098	RSA SigVer [FIPS 186]	PSS	Signature Type: PKCSPSS Hash Algorithm: SHA2-256 Modulo: 3072 Key Strength: 128 bits	SigVer within the ACM RoT.
Western Digital Corporation	A2099	RSA SigVer [FIPS 186]	PSS	Signature Type: PKCSPSS Hash Algorithm: SHA2-256 Modulo: 3072 Key Strength: 128 bits	SigVer within the OptiNAND device.
Avago Technologies	SHS 2942	SHS [FIPS 180]	SHA-1	Message Length: 8-51200, Increment: 8 Key Size: 160 Key Strength: 160 bits	Not used
			SHA2 - 224	Message Length: 8-51200, Increment: 8 Key Size: 224 Key Strength: 224 bits	Not used
			SHA2-256	Message Length: 8-51200, Increment: 8 Key Size: 256 Key Strength: 256 bits	Message digest generation. Digital signature verification within the ACM RoT

Vendor Name	CAVP Cert	Algorithm and Standard	Mode/method	Description/Key Size/Key Strength	Use/Function
Western Digital Corporation	A2099	SHS [FIPS 180]	SHA2-256	Message Length: 0-65536, Increment: 8 Key Size: 256 Key Strength: 256 bits	Message digest generation. Digital signature verification within the OptiNAND device.

Note: AES - XTS - The AES-XTS algorithm implementations include a check to ensure Key_1 ≠ Key_2

Vendor Affirmed Algorithms

The Cryptographic Module implements the FIPS Vendor Affirmed cryptographic algorithms listed in Table 6.

Table 6 Vendor Affirmed Algorithms

Algorithm Name	Algorithm Properties	Implementation	Reference
CKG-Direct	AES 256: Symmetric Key Generation	N/A	SP 800-133rev2 Section 4 example #1, Section 6.1 and IG D.H
CKG-Combined	AES 256: Symmetric Key Generation	N/A	SP 800-133rev2 Section 6.3 example #2 and IG D.H

Non-Approved, Allowed Algorithms

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

Non-Approved, Allowed Algorithms with No Security Claimed

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

Non-Approved, Not Allowed Algorithms

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

2.6 Security Function Implementations

The Cryptographic Module implements the Security Function Implementations listed in Table 7.

Table 7 Security Function Implementations

Name	Type	Description	SF Capabilities	Algorithms	Algorithm Properties
Authority_Digest_Generation	MAC	Generates an HMAC message digest of an Authentication Credential PIN	Publications: [IG 10.3.A]	HMAC-SHA2-256 (Cert #HMAC 2280)	Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits
Authority_Digest_Verification	MAC	Verifies the HMAC digest of an Authentication Credential PIN.	Publications: [IG 10.3.A]	HMAC-SHA2-256 (Cert #HMAC 2280)	Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits

Name	Type	Description	SF Capabilities	Algorithms	Algorithm Properties
Decryption	BC-UnAuth	Block Cipher	Publications: [IG 10.3.A]	AES-CBC (Cert #AES 3580)	Key Size: 128, 256, Key Strength: 128, 256 bits
Derived_Key_Generation	PBKDF2	Password-Based Key Derivation	Publications: [IG 10.3.A] [IG D.N]	PBKDF2 (Cert #A2100) HMAC-SHA2-256 (Cert #HMAC 2280)	**PBKDF2** Master Key Generation Type: Option 2a, Iteration Count: 2 - 1024 with Increment 1, HMAC Algorithm: SHA2-256. Password Length: 32, Salt Length: 128-512 with Increment 8, Key Data Length: 256 - 4096 with Increment: 256 **HMAC-SHA2-256** Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits Note: The CM uses keys derived from passwords only in a storage application.
Digest_Generation	SHA	Secure Hash Standard	Publications: [IG 10.3.A] [IG C.B]	SHA2-256 (Cert #SHS 2942)	Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits
Digest_Verification	SHA	Secure Hash Standard	Publications: [IG 10.3.A] [IG C.B]	SHA2-256 (Cert #SHS 2942)	Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits
Encryption	BC-UnAuth	Block Cipher	Publications: [IG 10.3.A]	AES-CBC (Cert #AES 3580)	Key Size: 128, 256, Key Strength: 128, 256 bits
Entropy	ESV	Entropy Source	Publications: [IG 9.3.A] [IG D.J] [IG D.O]	ESV Cert #13	Security Strength: 256

Name	Type	Description	SF Capabilities	Algorithms	Algorithm Properties
FW_Authenticity	DigSig-SigVer	Digital Signature Verification Verifies the authenticity of a CM firmware image	Publications: [IG 10.3.A] [IG C.B] [IG C.F]	RSA SigVer (Cert #A2098) SHA2-256 (Cert #SHS 2942)	**RSA SigVer** Signature Type: PKCSPSS Modulo: 3072. Key Strength: 128 bits **SHA2-256** Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits
FW_Integrity	DigSig-SigVer	Digital Signature Verification Verifies the integrity of a CM firmware image	Publications: [IG 10.3.A] [IG C.B] [IG C.F]	RSA SigVer (Cert #A2098) SHA2-256 (Cert #SHS 2942)	**RSA SigVer** Signature Type: PKCSPSS Modulo: 3072, Key Strength: 128 bits **SHA2-256** Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits
Key Wrap	KWP-AE KWP-AD	Key Wrapping Key Unwrapping	Publications: [IG 10.3.A] [IG D.G]	AES-KWP (Cert #A2098) AES-ECB (Cert #AES 3580)	**AES-KWP** Direction: Forward Authenticated Encrypt, Authenticated Decrypt, Payload Length: 96-1024, Increment 8, Key Length: 256 **AES-ECB** Key Size: 128, 256, Key Strength: 128, 256 bits
Keyed_Digest_Generation	MAC	Message Authentication Generation	Publications: [IG 10.3.A]	HMAC-SHA2-256 (Cert #HMAC 2280)	Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits
Keyed_Digest_Verification	MAC	Message Authentication Verification	Publications: [IG 10.3.A]	HMAC-SHA2-256 (Cert #HMAC 2280)	Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits

Name	Type	Description	SF Capabilities	Algorithms	Algorithm Properties
MEK Generation	CKG	Cryptographic Key Generation, XOR of LRK and NSK	Publications: [IG D.H]	DRBG (Cert # A2098) AES-XTS (A2101) CKG-Combined	Payload Length: 4096 – 32768 Increment: 128 Tweak Mode: Number Key Size: 128, 256 Key Strength: 128 bits, 256 bits
OptiNAND_Descrambler	BC-UnAuth	Block Cipher.	Publications: [IG 10.3.A]	AES-CBC (Cert #A2099)	Key Size: 256, Key Strength: 256 bits
FW_Auth_OptiNAND	DigSig-SigVer	Digital Signature Verification Verifies the authenticity of an OptiNAND firmware image	Publications: [IG 10.3.A] [IG C.B] [IG C.F]	RSA SigVer (Cert #A2099) SHA2-256 (Cert #A2099)	**RSA SigVer** Signature Type: PKCSPSS Modulo: 3072, Key Strength: 128 bits **SHA2-256** Message Length: 0-65536, Increment: 8, Key Size: 256, Key Strength: 256 bits
FW_Integrity_OptiNAND	DigSig-SigVer	Digital Signature Verification Verifies the integrity of an OptiNAND firmware image.	Publications: [IG 10.3.A] [IG C.B] [IG C.F]	RSA SigVer (Cert #A2099) SHA2-256 (Cert #A2099)	**RSA SigVer** Signature Type: PKCSPSS Modulo: 3072, Key Strength: 128 bits **SHA2-256** Message Length: 0-65536, Increment: 8, Key Size: 256, Key Strength: 256 bits
RBG	DRBG	Random bit generator	Publications: [IG 10.3.A] [IG D.L] [IG D.R]	CTR-DRBG (Cert #A2098)	Mode: AES-256 Derivation Function: True, Prediction Resistance: False, Key Size: 256, Key Strength: 256 bits
RBG_Seeding	ESV	Seeds DRBG with entropy data	Publications: [IG 9.3.A] [IG 10.3.A] [IG D.J] [IG D.K]	CTR-DRBG (Cert #A2098)	Mode: AES-256, Derivation Function: True, Prediction Resistance: False, Key Size: 256, Key Strength: 256 bits
	DRBG		Publications: [IG 10.3.A] [IG D.L] [IG D.R]		

Name	Type	Description	SF Capabilities	Algorithms	Algorithm Properties
SecureLoader_Integrity	DigSig-SigVer	Digital Signature Verification Verifies the integrity of the Secure Loader firmware image	Publications: [IG C.F] [IG 10.3.A] [IG C.B]	RSA SigVer (Cert #A2098)	**RSA SigVer** Signature Type: PKCSPSS Hash Algorithm: SHA2-256, Modulo: 3072, Key Strength: 128 bits **SHA2-256** Message Length: 8-51200, Increment: 8, Key Size: 256, Key Strength: 256 bits
	Secure Hash			SHA2-256 (Cert #SHS 2942)	
Symmetric_Key_Generation	CKG	Generates AES 256 symmetric cryptographic keys		CKG-Direct AES-CBC (Cert #AES 3580)	Key Size: 128, 256, Key Strength: 128, 256 bits
User_Data_Decryption	BC-UnAuth	Block Cipher	Publications: [IG 10.3.A] [IG C.I]	AES-XTS (Cert #A2101)	Payload Length: 4096 – 32768, Increment: 128, Tweak Mode: Number, Key Size: 128, 256, Key Strength: 128, 256 bits
User_Data_Encryption	BC-UnAuth	Block Cipher	Publications: [IG 10.3.A] [IG C.I]	AES-XTS (Cert #A2101)	Payload Length: 4096 – 32768, Increment: 128, Tweak Mode: Number, Key Size: 128, 256, Key Strength: 128, 256 bits

2.7 Algorithm Specific Information

AES-XTS Key Pair Generation

The Cryptographic Module performs a key comparison test on each LRK.AESKey/LRK.XTS 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 and 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, encrypt data protection keys 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.

Table 8 Entropy Certificates

Vendor Name	Certificate Number
Western Digital Corporation	E13

Table 9 Entropy Sources

Name	Type	Operating Environment	Sample Size	Entropy per sample	Conditioning Components
ESV, E13	Physical	0L23689, IC SOC9, Rev 2.1 ARM Cortex M3, ARM Cortex R8	32 bits	2.69612	None

Entropy Information

The hardware-based ring oscillator noise source referenced in Table 9 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 Documents 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 Table 9 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 2.69612 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 Locking SP Active Signing Key

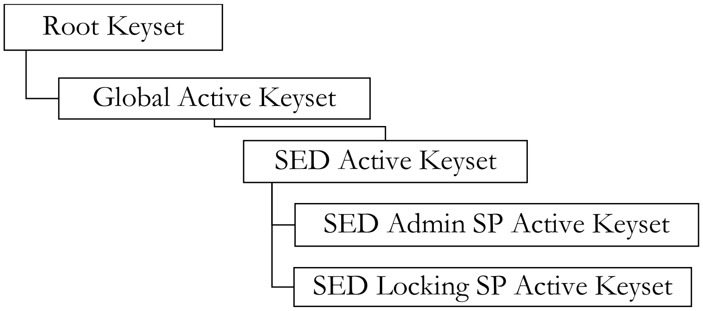

Figure 9 - Symmetric Key Tree

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 supports the TCG Storage SSC: Enterprise [TCG Enterprise] security 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. Table 10 identifies the Cryptographic Module's ports and 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 SCSI protocol [SCSI Core] [SCSI Block] provides the primary communication channel between the Cryptographic Module and a host system. Services provided by the Cryptographic Module that require the processing of operator issued commands include TCG Storage SSC: Enterprise configuration settings, the reading and writing of user data, and retrieval of status data.

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

Table 10 Ports and Interfaces

Physical Port	Logical Port	Data that passes over port/interface
SAS Connector SIO Serial Port Connector UART	Control Input	SAS connector: Used to transmit SCSI commands from the host system to the CM. SIO Serial Port: None, disabled. UART: Used to transmit SCSI commands from the host system to the CM.
SAS Connector SIO Serial Port Connector UART	Data Input	SAS connector: Used to transmit data and firmware update images from the host system to the CM. SIO Serial Port: FD_UART_RX, disabled. UART: Used to transmit data from the host system to the CM.
SAS Connector SIO Serial Port Connector UART	Data Output	SAS connector: Used to transmit data from the Cryptographic Module to the host system. SIO Serial Port: FD_UART_TX, disabled. UART: Used to transmitted data from the CM to the host system.
	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.
Power Connector	Power	Power connector
SAS Connector	Status Output	Used to transmit status data from the CM to the host system. READY_LED

4 Roles, Services, and Authentication

4.1 Authentication Methods

The Cryptographic Module implements the listed authentication methods.

Table 11 Authentication Methods

Name	Description	Security Mechanism	Strength Each Attempt	Strength per minute
Credential PIN Authentication	Authenticates a 12 to 32 bytes Authentication Credential PIN Byte value range (ea.): 0x00 to 0xFF.	Authority_Digest_Verification	12-byte PIN: 96 bits	Permutations: 7.92E+28 Authentication Time: 2.094965 msec Guess Probability (1 min): 3.61E-25
			32-byte PIN: 256 bits	Permutations: 1.16E+77 Authentication Time: 2.094965 msec Guess Probability (1 min): 2.47E-73

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. Table 13 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 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 Table 12.

Table 12 Roles

Name	Type	Operator Type	Authentication Methods
Anybody	Role	User	
BandMaster [0-15]	Role	CO	Credential PIN Authentication
EraseMaster	Role	CO	Credential PIN Authentication
SCSI User	Role	User	
SID	Role	CO	Credential PIN Authentication

The CM supports both Crypto Officer (CO) and User roles.

- Crypto Officer Roles
  - Secure ID (SID)
    - This Crypto Officer role corresponds to the Admin SP Secure ID (SID) Authority and serves as the TPer Owner is defined in the TCG Storage Architecture Core Specification [TCG Core]. The SID can access all services enabled by the Access Control Elements (ACE) assigned to the Admin SP Secure ID (SID) Authority.
  - EraseMaster
    - This Crypto Officer role corresponds to the Locking SP EraseMaster Authority defined in the TCG Storage Security Subsystem Class: Enterprise Specification [TCG Enterprise]. The EraseMaster can access all services enabled by the Access Control Elements (ACE) assigned to the EraseMaster. The EraseMaster is the single authority dedicated to resetting one or more LBA bands by invoking the TCG Erase service to regenerate the LRK and MEK associated with the LBA band. The EraseMaster can disable a BandMaster.
  - BandMaster
    - This Crypto Officer role corresponds to the Locking SP Bandmaster Authority as defined in the TCG Storage Security Subsystem Class: Enterprise Specification [TCG Enterprise]. BandMasters can access all services enabled by the Access Control Elements (ACE) assigned to a BandMaster. BandMasters lock and unlock LBA bands and configure LBA bands (user data regions) to control the ability of an operator to read and write data within the Cryptographic Module. The Cryptographic Module supports a maximum of sixteen (16) active BandMaster Authorities.

- User Roles
  - SCSI User
    - The SCSI User utilizes the SCSI interface protocol [SCSI Core] [SCSI Block], which is designed to provide an efficient peer-to-peer communication link, to communicate with a host system. The host system sends commands to the Cryptographic Module and waits for the Cryptographic Module to respond. The SCSI User may execute services that were previously enabled by another authenticated role in compliance with the lock-based authentication model specified in IG 4.1.A.
  - Anybody
    - This user role corresponds to the Locking SP Anybody Authority as defined in the TCG Storage Security Subsystem Class: Enterprise Specification [TCG Enterprise]. As specified in the TCG Storage Architecture Core Specification [TCG Core], the Anybody authority possess implicit authentication within a session. The Anybody authority executes services that do not require explicit authentication. The Anybody user role may execute services that were previously enabled by another authenticated role in compliance with the lock-based authentication model specified in IG 4.1.A.

4.3 Approved Services

Table 13 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.

Table 13 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
Authenticate PSID	PSID character string authentication	isFIPS mode is true	PSID	Success or UEC failure code	Decryption Keyed_Digest_Verification	CO: SID User: Anybody	**SID** **E:**PSID Digest, Global Active Keyset **W**: PSID **Anybody** **E:** PSID Digest, Global Active Keyset **W**: PSID
Authenticate TCG Authority	Authentication Credential authentication	isFIPS mode is true	Authentication Credential PIN	Success or UEC failure code	Authority_Digest_Verification	CO: SID, EraseMaster, BandMaster User: Anybody	**SID** E: SID PIN Digest, MSID Digest, SED AdminSP Active Signing Key **W**: SID PIN, MSID **EraseMaster** E: EraseMaster PIN Digest, BandMaster PIN Digests, MSID Digest, SED Active LockingSP Signing Key **W**: EraseMaster PIN, BandMaster PIN, MSID **BandMaster** **E**: BandMaster PIN Digests, EraseMaster

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
							PIN Digest, MSID Digest, SED LockingSP Active Signing Key **W**: BandMaster PIN, EraseMaster PIN, MSID **Anybody** E: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, MSID Digest, SED AdminSP Active Signing Key, SED LockingSP Signing Key **W**: SID PIN, EraseMaster PIN, BandMaster PIN, MSID
BootFlashIntegrity	An RSA digital signature verifies the authenticity of a binary firmware image.	isFIPS mode is true	RSA 3072 PSS signed firmware image	Success or UEC failure code	SecureLoader_ Integrity	Unauthenticated	**E**: SD_CA Key
FIPS 140 Compliance Descriptor[6]	This service reports the FIPS 140 revision as well as the Cryptographic Module's overall security level, hardware revision, firmware revision and module name.	N/A	Security Protocol IN (0x0, 0x2, 0x2)[7]	FIPS 140 Compliance Descriptor table data or UEC failure code	None	User: SCSI User	None

[6] See Security Features for SCSI Commands [SFSC] for further details

[7] See SCSI Primary Commands - 5 (SPC-5)

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
Firmware Download	Digital signature verification of a binary firmware image.	isFIPS mode is true	RSA 3072 PKCSPSS signed firmware image	Success or UEC failure code	FW_Authenticity	CO: SID	**E**: OEM_FW Key, OEM_Release Key
Firmware Download Control	Enable or disable access to the Firmware Download service	N/A	FW_DOWNLOAD_PORT bit within the AdminSP Logical Port Table	Success or UEC failure code	None	CO: SID	None
Firmware Integrity	An RSA digital signature verifies the authenticity of a binary firmware image.	isFIPS mode is true	RSA 3072 PKCSPSS signed firmware image	Success or UEC failure code	FW_Integrity	Unauthenticated	**E**: OEM_FW Key, SC FW Key, SP_FW Key, OEM_OFS Key, SD_BFW Key, SD_CA Key
Generate Random	TCG Random method that generates a random number from the SP 800-90A CTR_DRBG	isFIPS mode is true	Byte count	Byte string	RBG	User: Anybody	**G**: DRBG.Key, DRBG.V **E**: DRBG.Key, DRBG.V
Get	Reads data structure; access control enforcement occurs per data structure field	isFIPS mode is true	See §5.3.3.6 Basic Table Method Group - Get (Table and Object Method [TCG Core]	Requested table data. [TCG Core]	Decryption Keyed_Digest_Verification	CO: SID, EraseMaster, BandMaster, User: Anybody	**R**: MSID
Get Band Attributes	Returns the data stored in the Locking SP table for an LBA Band	N/A	Band_UID [TCG Enterprise]	LBA band attribute data [TCG Enterprise]	None	CO: BandMaster User: Anybody	None
Get Data Store	Read a stream of bytes from unstructured storage	N/A	See §3.2.13.9 Read data from the DataStore table [TCG SIIS]	DataStore plaintext data or UEC failure code	None	User: Anybody	None
Level 0 Discovery	TCG 'Level 0 Discovery' discloses basic configuration data about the	N/A	See §3.3.6 Level 0 Discovery, §3.3.6.2 IF-RECV Command [TCG Core]	Level 0 Discovery Response data [TCG Core]	None	User: Anybody	None

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
	Cryptographic Module, both current and potential [TCG Core] [Product Manual]						
OptiNAND Firmware Download	Digital signature verification of a binary firmware image.	isFIPS mode is true	RSA 3072 PSS signed firmware image	Success or UEC failure code	FW_Auth_OptiNAND OptiNAND_Descrambler	CO: SID	**E**: sFFUPublicKey
OptiNAND Firmware Integrity	Digital signature verification of a binary firmware image.	N/A	RSA 3072 PSS signed firmware image	Success or UEC failure code	FW_Integrity_OptiNAND OptiNAND_Descrambler	Unauthenticated	**E**: sFFUPublicKey
Read User Data	Reads ciphertext from a LBA band and output user plaintext data.	isFIPS mode is true	SCSI Operation Code, LBA, Transfer Length, Data-Out Buffer See [SBC-4]	Plaintext user data or UEC failure code	User_Data_Decryption	User: SCSI User	**E**: MEK
Reset Module	Power on Reset	isFIPS mode is true	None	Drive Ready Indicator or UEC failure code	Derived_Key_Generation Encryption Key Wrap RBG RBG_Seeding	Unauthenticated	**G**: DRBG.Seed, DRBG.Key, DRBG.V, ESV, SED Volatile Keyset **E:** ESV, DRBG.Key, DRBG.V, SED Volatile Keyset
Revert	The Revert method cryptographically erases CSPs and returns the Cryptographic Module to its original manufactured state.	isFIPS mode is true	PSID	Drive Ready Indicator or UEC failure code	Encryption Keyed_Digest_Generation RBG	CO: SID User: Anybody	**SID** **G**: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, DRBG.Key, DRBG.V, K_a, K_u, LRK, NSK, MEK, RAK, UAK, UMK, Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset,

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
							SED LockingSP Keyset, SED Volatile Keyset **W**: PSID **E**: DRBG.Key, DRBG.V, K_a, K_u, LRK, NSK, RAK, UAK, UMK, Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset **Z**: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, K_a, K_u, LRK, NSK, MEK, RAK, UAK, UMK, , Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset **Anybody** **G**: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, DRBG.Key, DRBG.V, K_a, K_u, LRK, NSK, MEK, RAK, UAK, UMK, Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset **W**: PSID

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
							E: DRBG.Key, DRBG.V, K_a, K_u, LRK, NSK, RAK, UAK, UMK, Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset **Z**: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, K_a, K_u, LRK, NSK, MEK, RAK, UAK, UMK, , Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset
RevertSP	The RevertSP method cryptographically erases CSPs and returns the Cryptographic Module to its original manufactured state.	isFIPS mode is true	See §5.1.3 RevertSP – Base Template SP Method [TCG Opal]	Drive Ready Indicator or UEC failure code	Encryption Key Wrap Keyed_Digest_Generation RBG	CO: SID User: Anybody	**SID** **G**: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, DRBG.Key, DRBG.V, K_a, K_u, LRK, NSK, MEK, RAK, UAK, UMK, , Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset SED AdminSP Keyset **E**: DRBG.Key, DRBG.V, K_a, K_u, LRK, NSK, RAK, UAK, UMK, Root Keyset,

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
							Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset **Z**: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, K_a, K_u, LRK, NSK, MEK, RAK, UAK, UMK, , Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset **Anybody** **G**: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, DRBG.Key, DRBG.V, K_a, K_u, LRK, NSK, MEK, RAK, UAK, UMK, Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset **E**: DRBG.Key, DRBG.V, K_a, K_u, LRK, NSK, RAK, UAK, UMK, , Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
							Z: SID PIN Digest, EraseMaster PIN Digest, BandMaster PIN Digests, K_a, K_u, LRK, NSK, MEK, RAK, UAK, UMK, , Root Keyset, Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, SED LockingSP Keyset, SED Volatile Keyset
SCSI Command	The SCSI command set provides an efficient peer-to-peer operation for SCSI devices.	N/A	Input parameters are defined within [SCSI Core] and [SCSI Block]	Return device data as defined within [SCSI Core] and [SCSI Block] or UEC failure code	None	User: SCSI User	None
Self-Test	The Cryptographic Module performs self-tests when it powers up	N/A	None	Drive Ready or UEC failure code	Decryption Derived_Key_Generation Digest_Generation Digest_Verification FW_Integrity Encryption Entropy Key Wrap Keyed_Digest_Generation Keyed_Digest_Verification RBG	Unauthenticated	**G**: DRBG.Key, DRBG.V **E**: DRBG.Key, DRBG.V
Set	Write data structures; access control enforcement occurs per data structure field. This service can	isFIPS mode is true	Set method table data. See [TCG Core]	Success or UEC failure code	Authority_Digest_Generation Encryption Keyed_Digest_Generation	CO: SID, EraseMaster, BandMaster User: Anybody	<u>**SID**</u> **E**: Global Active Keyset, SED Active Keyset, SED AdminSP Keyset, , SED Volatile Keyset **W**: SID PIN

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
	change Authentication Credential PINs.						**EraseMaster** **E**: Global Active Keyset, SED Active Keyset, SED LockingSP Keyset, SED Volatile Keyset, K_a **W**: EraseMaster PIN **BandMaster** **E**: Global Active Keyset, SED Active Keyset, SED LockingSP Keyset, SED Volatile Keyset, K_u W: BandMaster PIN **Anybody** **E**: Global Active Keyset, SED Active Keyset, SED Volatile Keyset
Set Band Attributes	Set the starting location, size, and attributes of an LBA band.	isFIPS mode is true	LBA band attribute configuration data See [TCG Enterprise]	Success or UEC failure code	Encryption Keyed_Digest_Generation	CO: BandMaster	**E**: Global Active Keyset, SED Active Keyset, SED LockingSP Keyset, SED Volatile Keyset, UAK
Set Data Store	Write a stream of bytes to unstructured storage.		DataStore byte table data See [TCG Enterprise]	Success or UEC failure code	None	CO: BandMaster User: Anybody	None
Show Status	The status inquiry command requests SCSI device (e.g., Cryptographic Module) status information	N/A	[SCSI Core] and [SCSI Block] define the input parameters.	Return requested module data or UEC failure code	None	User: SCSI User	None
TCG Erase	TCG Erase cryptographically erases user data	isFIPS mode is true	Band_UID See [TCG Enterprise], [TCG	Success or UEC failure code	Encryption Keyed_Digest_Generation	CO: EraseMaster	**G**: MEK, LRK **E**: DRBG.Key, DRBG.V, LRK, NSK,

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
	by regenerating and replacing a Locking Range Key associated with an LBA band.		Ent App Notes]		RBG		RAK, UMK, UAK, UAK_a **Z**: MEK, LRK
Write User Data	Transform plaintext user data into ciphertext and writes to an LBA band.	isFIPS mode is true	Operation Code, LBA, Transfer Length, Data-Out Buffer [SBC-4]	Success or UEC failure code	User_Data_Encryption	User: SCSI User	**E**: MEK

4.4 Non-Approved Services

The Cryptographic Module does not support non-approved services.

4.5 External Software/Firmware Loaded

The Cryptographic Module utilizes RSA public key cryptography to verify that firmware downloaded to the CM is authentic. 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.

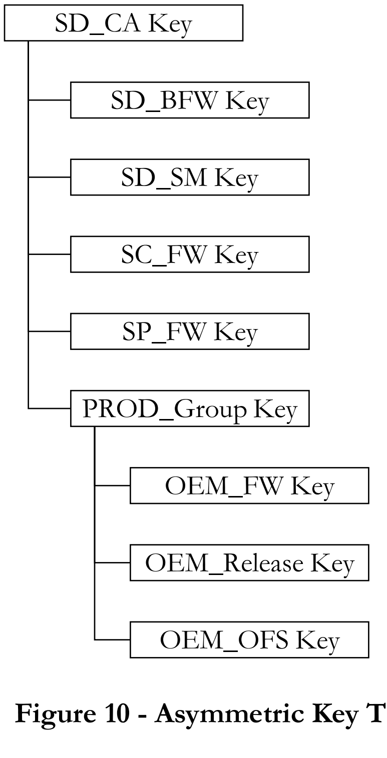

Figure 10 - Asymmetric Key Tree

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

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 bands associated with BandMasters with default authentication PIN values are considered plaintext.

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.

Table 14 Mechanisms and Actions Required

Physical Security Mechanism	Recommended Frequency of Inspection Testing	Inspection/Test Guidelines
During the manufacturing process, specialized equipment applies one tamper-evident security seal to the CM's PCBA. See Figure 11 and Figure 12.	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. See Figure 13.

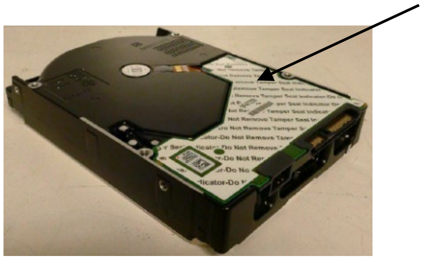

Figure 11 - Tamper-Evident Seal for Ultrastar DC HC560

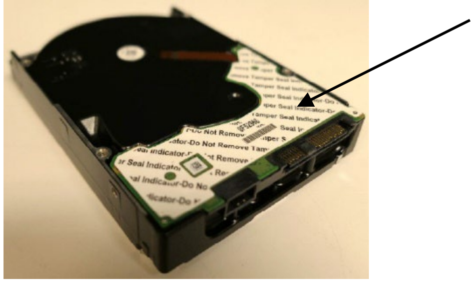

Figure 12 - Tamper-Evident Seal for Ultrastar DC HC570

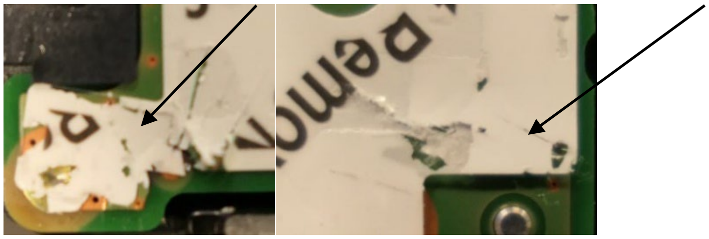

Figure 13 - Tamper Evidence on Tamper Seal

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 9.4 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.

Table 15 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
NAND Flash	SSP storage and firmware image	Static
Disk Media	SSP and operation firmware image storage	Static
One-time Programable (OTP)	Root Key and Certificate Authority Key storage	Static

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 input only 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 the RSA Public/Private key pairs input 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.

Table 16 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Authentication Credential PIN	Operator	CM	Plaintext	Automated	Electronic	Authenticate TCG Authority
Public Key	HSM	CM	Plaintext	Automated	Electronic	RSA SigVer

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.

Table 17 SSP Zeroization Methods

Method	Description	Rationale	Operator Initiation Capability
Power Cycle	Power cycling involves disconnecting and reconnecting the CM to its source of power.		The operator physically or remotely disconnects the CM from its source of power.
Revert	The Revert method cryptographically erases CSPs, removes the owner's Authentication Credentials and returns the Cryptographic Module to its original manufactured state.		The operator transmits a command to the CM as the TPer to initiate a zeroisation process.
RevertSP	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.		The operator transmits a command to the CM as the TPer to initiate a zeroisation process.
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.		The operator transmits 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.		The operator transmits a command to the CM as the TPer to initiate a user data erasure process.

9.4 SSPs

Table 18 SSPs Part 1

Name	Description	Size (in bits)	Strength (in bits)	Type	Generated By	Established By
Admin Authority Key (K_a)	The K_a key encrypts and decrypts UAKs and the UMK.	256 bits	256 bits	Derived Symmetric Key	PBKDF2, Internal	N/A
Anybody User Access Key (UAK_a)	The Anybody Authority uses UAK_a to decrypt the RAK of unlocked LBA bands.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A

Name	Description	Size (in bits)	Strength (in bits)	Type	Generated By	Established By
BandMaster PIN (16 total)	Authentication Credential PIN for a Locking SP Bandmaster Authority.	12 to 32 bytes	96 to 256 bits	Plaintext	N/A	N/A
BandMaster PIN Digest (16 total)	Authenticates BandMaster PIN.	256 bits	256 bits	Message Digest	HMAC-SHA2-256, Internal	N/A
DRBG.Key	Internal state associated with the [SP 800 90A] CTR_DRBG using AES-256	256 bits	256 bits	Entropy	CTR_DRBG, Internal	N/A
DRBG.Seed	Internal state associated with the [SP 800 90A] CTR_DRBG using AES-256	5120 bits	431.379 bits	Entropy	ESV Internal	N/A
DRBG.V	Internal state associated with the [SP 800 90A] CTR_DRBG using AES-256.	128 bits	128 bits	Entropy	CTR_DRBG, Internal	N/A
EraseMaster PIN	Authentication Credential PIN for the Locking SP EraseMaster Authority.	12 to 32 bytes	96 to 256 bits	Plaintext	N/A	N/A
EraseMaster PIN Digest	Authenticates the EraseMaster PIN	256 bits	256 bits	Message Digest	HMAC-SHA2-256, Internal	N/A
ESV	Entropy source input to the [SP 800 90A] CTR_DRBG	32-bit sample	2.69612 bits per 32-bit sample	Entropy	Ring oscillator noise source, Internal	N/A
Global Active Encryption Key (AEK)	The Global Active Encryption Key encrypts and decrypts the SED Active Keyset, NSK and the UAK$_a$ key.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
Global Active Signing Key	Signs the encrypted SED Active Keyset.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
KDF Salt (EraseMaster and BandMaster unique)	KDF Salts are integral to the PBKDF2 generation of each K$_a$ and K$_u$ derived authority key.	256-bits	256-bits	Symmetric Key	CKG-Direct	N/A
Locking Range Keyset (LRK) **LRK.AES Key** **LRK.XTS Key** **(BandMaster unique)**	LRKs in combination with the NSKs derive MEKs, which encrypt LBA bands	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
MEK - Media Encryption Keyset **MEK.AESEnc Key** **MEK.AESDec Key** **MEK.XTS Tweak Key** **(BandMaster unique)**	MEKs encrypt and decrypt LBA bands. An MEK.AESDec key is the last entry of the key schedule for an MEK.AESEnc key.	256 bits	256 bits	Derived Symmetric Key	CKG-Combined	N/A

Name	Description	Size (in bits)	Strength (in bits)	Type	Generated By	Established By
MSID	The MSID string is the default password for the SID, EraseMaster and BandMaster authorities. Stored during the manufacturing process, the CM generates this thirty-two-character value by processing a CTR-DRBG generated random number through an Alphanumeric Character Conversion algorithm. The algorithm draws from a thirty-four-element character set to generate the MSID.	32 bytes	162.8 bits	Plaintext	CKG-Direct	N/A
MSID Digest	Authenticates the MSID PIN	256 bits	256 bits	Message Digest	HMAC-SHA2-256, Internal	N/A
Namespace Keyset (NSK) **NSK.AES Key** **NSK.XTS Key** **(BandMaster unique)**	NSKs in combination with the LRKs derive MEKs, which encrypt LBA bands.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
Non-Admin Authority Key (K_u) (BandMaster unique)	K_u keys encrypt and decrypt all UAKs except UAK_a.	256 bits	256 bits	Derived Symmetric Key	PBKDF2, Internal	N/A
OEM Firmware Key (OEM_FW Key)	The OEM_FW Key verifies OEM firmware images and packages.	3072-bits	128-bits	Public Key	HSM, External	N/A
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	HSM, External	N/A
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	HSM, External	N/A
Product Group Key (PROD_GROUP Key)	The PROD_GROUP Key verifies OEM_FW Key certificates.	3072-bits	128-bits	Public Key	HSM, External	N/A

Name	Description	Size (in bits)	Strength (in bits)	Type	Generated By	Established By
PSID	The PSID string serves as authentication data and proof of physical presence for the Revert and RevertSP services. Stored during the manufacturing process, the CM generates this thirty-two-character value by processing a CTR-DRBG generated random number through an Alphanumeric Character Conversion algorithm. The algorithm draws from a thirty-four-element character set to generate the PSID.	32 bytes	162.8 bits[8]	Plaintext	CKG-Direct	N/A
PSID Digest	Authenticates the PSID	256 bits	256 bits	Message Digest	HMAC-SHA2-256, Internal	N/A
Range Access Key (RAK) (BandMaster unique)	RAKs encrypt and decrypt LRKs.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
Root Encryption Key	The Root Encryption Key encrypts the Global Active Keyset.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
Root Signing Key	Signs the encrypted Global Active Keyset.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
SecureBootPublicKey	The SecureBootPublicKey verifies the OptiNAND Boot Code, Static data structures and parameters. The OptiNAND Download and Execute (DLE) module uses the SecureBootPublicKey to verify the RSA 3072 PSS signature of OptiNAND firmware.	3072-bits	128-bits	Public Key	HSM, External	N/A
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	HSM, External	N/A
Security Protocol Firmware Key (SP_FW Key)	The SP_FW Key verifies ACM security protocol and services firmware.	3072-bits	128-bits	Public Key	HSM, External	N/A
SED Active Encryption Key	Encrypts and decrypts the SED AdminSP Active Keyset and the SED LockingSP Active Keyset.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A

[8] E = log2(RL), where E = authentication strength, R = pool of unique characters and L = password length, https://www.pleacher.com/mp/mlessons/algebra/entropy.html

Name	Description	Size (in bits)	Strength (in bits)	Type	Generated By	Established By
SED Active Signing Key	Signs the encrypted SED AdminSP Active Keyset and the SED LockingSP Active Keyset.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
SED AdminSP Encryption Key	Encrypts and decrypts CSPs associated with an Admin SP.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
SED AdminSP Signing Key	Signs encrypted CSPs associated with an Admin SP.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
SED LockingSP Encryption Key	Encrypts and decrypts CSPs associated with a Locking SP.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
SED LockingSP Signing Key	Signs encrypted CSPs associated with a Locking SP.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
SED Volatile Encryption Key	Encrypts, and decrypts LRKs and MEKs.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
SED Volatile Signing Key	Signs encrypted LRKs and MEKs.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
sFFU_EncKey	Descrambles a Secure Field Firmware Update (sFFU) image	256 bits	256 bits	Public Key	HSM, External	N/A
sFFUPublicKey	The sFFUPublicKey verifies OptiNAND Secure Field Firmware Update (sFFU) images.	3072-bits	128-bits	Public Key	HSM, External	N/A
SID PIN	Authentication Credential PIN for the Admin SP SID Authority.	12 to 32 bytes	96 to 256 bits	Plaintext	N/A	N/A
SID PIN Digest	Authenticates the SID PIN	256 bits	256 bits	Message Digest	HMAC-SHA2-256, Internal	N/A
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	HSM, External	N/A
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	HSM, External	N/A
Storage Device Secure Message Key (SD_SM Key)	The SD_SM Key verifies secure messages used for manufacturing, development, and failure analysis	3072-bits	128-bits	Public Key	HSM, External	N/A
SVSPublicKey	The SVSPublicKey verifies OptiNAND Unlock commands	3072-bits	128-bits	Public Key	HSM, External	N/A

Name	Description	Size (in bits)	Strength (in bits)	Type	Generated By	Established By
User Access Key (UAK) (BandMaster unique)	Encrypts and decrypts the RAK associated with a BandMasters.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A
User Management Key (UMK)	Encrypts and decrypts UAKs.	256 bits	256 bits	Symmetric Key	CKG-Direct	N/A

Table 19 SSPs Part 2

Name	Used By	Inputs and Outputs	Storage	Temporary Storage Duration	Zeroisation Methods	Category	Related SSPs
Admin Authority Key (K_a)	AES-CBC-256 (Cert #AES 3580)	N/A	IRAM, Plaintext	Ephemeral, destroyed after use.	N/A	CSP	Encrypts UAKs and the UMK, Derived from EraseMaster PIN and EraseMaster associated KDF Salt
Anybody User Access Key (UAK_a)	AES-CBC-256 (Cert #AES 3580)	N/A	IRAM - Plaintext	Power up to power down	Power Cycle	CSP	Decrypts RAKs
			Disk Media, Encrypted		Revert RevertSP		
BandMaster PIN (16 total)	PBKDF2 (Cert #A2100) HMAC-SHA2-256 (Cert #HMAC 2280)	Authentication Credential PIN	IRAM - Plaintext	Ephemeral, destroyed after use.	N/A	CSP	Paired with associated BandMaster PIN Digest, KDF Salt, and K_u key
BandMaster PIN Digest	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	Disk Media, Signed		Revert RevertSP	CSP	Generated from associated BandMaster PIN and the SED Active Signing Key
DRBG.Key	CTR_DRBG (Cert #A2098)	N/A	IRAM, Plaintext	Power up to power down	Power Cycle	CSP	Paired with DRBG.Seed and DRBG.V
DRBG.Seed	CTR_DRBG	N/A	IRAM -	Power up to	Power Cycle	CSP	Paired with

Name	Used By	Inputs and Outputs	Storage	Temporary Storage Duration	Zeroisation Methods	Category	Related SSPs
	(Cert #A2098)		Plaintext	power down			DRBG.Key and DRBG.V
DRBG.V	CTR_DRBG (Cert #A2098)	N/A	IRAM, Plaintext	Power up to power down	Power Cycle	CSP	Paired with DRBG.Seed and DRBG.V
ESV	CTR_DRBG (Cert #A2098)	N/A	IRAM, Plaintext	Power up to power down	Power Cycle	CSP	Paired with DRBG.Seed
EraseMaster PIN	PBKDF2 (Cert #A2100 HMAC-SHA2-256 (Cert #HMAC 2280)	Authentication Credential PIN	IRAM - Plaintext	Ephemeral Destroyed after use	N/A	CSP	Paired with EraseMaster PIN Digest, KDF Salt, and K_a key
EraseMaster PIN Digest	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	Disk Media, Signed		Revert RevertSP	CSP	Generated from EraseMaster PIN and SED Active Signing Key
Global Active Encryption Key (AEK)	AES-CBC-256 (Cert #AES 3580)	N/A	NOR Flash, Encrypted		Secure Manufacturing Reconfiguration Process	CSP	Encrypts and decrypts the SED Active Keyset, NSKs and UAK_a
Global Active Signing Key	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	NOR Flash, Encrypted		Secure Manufacturing Reconfiguration Process	CSP	Derived from AEK and SED Active Keyset
KDF Salt (EraseMaster and BandMaster unique)	HMAC-SHA2-256 (Cert #HMAC 2280) PBKDF2 (Cert #A2100)	N/A	Disk Media, Signed		Revert RevertSP	PSP	Paired with associated BandMaster PINs, the EraseMaster PIN, K_a key, and K_u keys
Locking Range Keyset (LRK) **LRK.AES Key** **LRK.XTS Key** **(BandMaster unique)**	XOR	N/A	DRAM, Encrypted	Generation to power down.	Power Cycle Revert RevertSP TCG Erase	CSP	Paired with associated NSK and MEK, Encrypted by SED Volatile Key

Name	Used By	Inputs and Outputs	Storage	Temporary Storage Duration	Zeroisation Methods	Category	Related SSPs
			Disk Media, Encrypted		Revert RevertSP TCG Erase		Paired with associated NSK and MEK, Encrypted by associated RAK
Media Encryption Keyset (MEK) **MEK.AESEnc Key** **MEK.AESDec Key** **MEK.XTS Tweak Key** **(BandMaster unique)**	AES-XTS-256 (Cert #A2101)	N/A	DRAM, Encrypted	Generation to power down.	Power Cycle	CSP	Generated from associated LRK and NSK, Encrypted by SED Volatile Key
MSID	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	IRAM, Plaintext	Ephemeral Destroyed after use.	N/A	PSP	Paired with MSID Digest, Signed by the SED Active Signing Key
			NOR Flash, Signed		N/A		
MSID Digest	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	Disk Media, Signed		Revert RevertSP	CSP	Generated from the MSID and the SED Active Signing Key
Namespace Keyset (NSK) **NSK.AES Key** **NSK.XTS Key** **(BandMaster unique)**	XOR	N/A	DRAM, Encrypted	Generation to power down.	Power Cycle	CSP	Paired with associated LRK and MEK, Encrypted by Global Active Encryption Key
			Disk Media, Encrypted	N/A	Revert RevertSP		
Non-Admin Authority Key (K_u) (BandMaster unique)	AES-CBC-256 (Cert #AES 3580)	N/A	N/A	Ephemeral, destroyed after use	N/A	CSP	Derived from associated BandMaster PIN and KDF Salt, Encrypts UAKs
OEM Firmware Key (OEM_FW Key)	RSA SigVer (Cert #A2098)	Public Key	NOR Flash, Signed		N/A	Neither	Verified by PROD_GROUP Key

Name	Used By	Inputs and Outputs	Storage	Temporary Storage Duration	Zeroisation Methods	Category	Related SSPs
OEM Original Factory State Key (OEM_OFS Key)	RSA SigVer (Cert #A2098)	Public Key	NOR Flash, Signed		N/A	Neither	Verified by PROD_GROUP Key
OEM_Release Key (OEM_Release Key)	RSA SigVer (Cert #A2098)	Public Key	NOR Flash, Signed		N/A	Neither	Verified by PROD_GROUP Key
Product Group Key (PROD_GROUP Key)	RSA SigVer (A2098)	Public Key	NOR Flash, Signed		N/A	Neither	Verified by SD_CA Key
PSID	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	IRAM, Plaintext	Generation to power down.	Power Cycle	PSP	Paired with PSID Digest Encrypted by SED Active Encryption Key, Signed by SED Active Signing Key
			NOR Flash, Encrypted and signed	N/A	N/A		
PSID Digest	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	Disk Media, Signed	N/A	Revert RevertSP	CSP	Generated from PSID and the SED Active Signing Key
Range Access Key (RAK) (BandMaster unique)	AES-CBC-256 (Cert #AES 3580)	N/A	Disk Media, Encrypted		Revert RevertSP	CSP	Encrypted by associated UAK, Encrypts associated LRK.
Root Encryption Key	AES-CBC-256 (Cert #AES 3580) AES-ECB-256 (Cert #AES 3580) KWP-AD (Cert #A2098) KWP-AE (Cert #A2098)	N/A	OTP		Secure Manufacturing Reconfiguration Process	CSP	Encrypts Global Active Keyset, Wraps Root Signing Key
Root Signing Key	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	NOR Flash, Encrypted		Secure Manufacturing Reconfiguration Process	CSP	Signs Global Active Encryption Key, Wrapped by Root Encryption

Name	Used By	Inputs and Outputs	Storage	Temporary Storage Duration	Zeroisation Methods	Category	Related SSPs
							Key
SecureBootPublicKey	RSA SigVer (Cert #A2099)	Public Key	Masked ROM, OptiNAND		N/A	Neither	Verifies OptiNAND firmware image, Signs sFFUPublicKey
Security Core Firmware Key (SC_FW Key)	RSA SigVer (Cert #A2098)	Public Key	NOR Flash, Signed		N/A	Neither	Verified by SD_CA Key
Security Protocol Firmware Key (SP_FW Key)	RSA SigVer (Cert #A2098)	Public Key	NOR Flash, Signed		N/A	Neither	Verified by SD_CA Key
SED Active Encryption Key	AES-CBC-256 (Cert #AES 3580)	N/A	NOR Flash, Encrypted		Revert RevertSP	CSP	Encrypts the SED AdminSP Active Keyset, Encrypts the SED LockingSP Active Keyset
SED Active Signing Key	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	NOR Flash, Encrypted		Revert RevertSP	CSP	Signs the SED AdminSP Active Keyset, Signs the SED LockingSP Active Keyset
SED AdminSP Encryption Key	AES-CBC-256 (Cert #AES 3580)	N/A	NOR Flash, Encrypted		Revert RevertSP	CSP	Encrypts CSPs associates with an Admin SP
SED AdminSP Signing Key	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	NOR Flash, Encrypted		Revert RevertSP	CSP	Signs CSPs associated with an Admin SP
SED LockingSP Encryption Key	AES-CBC-256 (Cert #AES 3580)	N/A	NOR Flash, Encrypted		Revert RevertSP	CSP	Encrypts CSPs associated with a Locking SP
SED LockingSP Signing Key	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	NOR Flash, Encrypted		Revert RevertSP	CSP	Signs CSPs associated with a Locking SP

Name	Used By	Inputs and Outputs	Storage	Temporary Storage Duration	Zeroisation Methods	Category	Related SSPs
SED Volatile Encryption Key	AES-CBC-256 (Cert #AES 3580)	N/A	IRAM, Plaintext	Power up to power down	Power Cycle Revert RevertSP	CSP	Encrypts LRKs and MEKs.
SED Volatile Signing Key	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	IRAM, Plaintext	Power up to power down	Power Cycle Revert RevertSP	CSP	Signs encrypted LRKs and MEKs.
sFFUEncKey	AES-CBC-256 (Cert #A2099)	Public Key	NAND Flash, OptiNAND, Signed		N/A	Neither	Signed by SecureBootPublic Key
sFFUPublicKey	RSA SigVer (Cert #A2099)	Public Key	NAND Flash, OptiNAND, Signed		N/A	Neither	Signed by SecureBootPublic Key
SID PIN	PBKDF2 (A2100) HMAC-SHA2-256 (Cert #HMAC 2280)	Authentication Credential PIN	IRAM - Plaintext	Ephemeral Destroyed after use	N/A	CSP	Paired with SID PIN Digest
SID PIN Digest	HMAC-SHA2-256 (Cert #HMAC 2280)	N/A	Disk Media - Encrypted		Revert RevertSP	CSP	Generated from SID PIN and SED Active Signing Key
Storage Device Boot FW Key (SD_BFW Key)	RSA SigVer (Cert #A2098)	Public Key	NOR Flash, Signed		N/A	Neither	Signed by SD_CA Key
Storage Device Certification Authority Key (SD_CA Key)	RSA SigVer (Cert #A2098)	Public Key	NOR Flash, Plaintext OTP, SHA-256 digest		N/A	Neither	Signs SD_BFW Key, SD_SM Key, SC_FW Key, SP_FW Key and PROD_GROUP Key
Storage Device Secure Message Key (SD_SM Key)	RSA SigVer (Cert #A2098)	Public Key	NOR Flash, Signed		N/A	Neither	Signed by SD_CA Key
SVSPublicKey	RSA SigVer (Cert #A2099)	Public Key	NAND Flash, OptiNAND, Signed		N/A	Neither	Signed by SecureBootPublic Key

Name	Used By	Inputs and Outputs	Storage	Temporary Storage Duration	Zeroisation Methods	Category	Related SSPs
User Access Key (UAK) (BandMaster unique)	AES-CBC-256 (Cert #AES 3580)	N/A	Disk Media, Encrypted		Revert RevertSP	CSP	Encrypts BandMaster associated RAK
User Management Key (UMK)	AES-CBC-256 (Cert #AES 3580)	N/A	Disk Media, Encrypted		Revert RevertSP	CSP	Encrypts UAKs

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 the pre-operational self-test listed in Table 20 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 and RSA SigVer SW/FW Integrity self-tests satisfy AS10.23. Upon failure the Cryptographic Module transitions to a Device Unavailable error state.

Table 20 CM Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Period	Periodic Method
RSA SigVer (Cert # A2098, Cert #SHS 2942)	3072-bit, PSS w/SHA2-256	Digital Signature Verification	SW/FW Integrity	Pass: Boot to the firmware image Fail: Device Unavailable	Verify Digital Signature.	On Demand	Manually
ESV (Cert # ESV13)	Repetition Count Test (RCT)	SP 800-90B Health-Test	Critical Function	Pass: Next test Fail: Device Unavailable	Verifies that the RCT Threshold was not exceeded as specified in [SP 800 90B]	On Demand	Manually
ESV (Cert # ESV13)	Adaptive Proportion Test (APT)	SP 800-90B Health-Test	Critical Function	Pass: Next test Fail: Device Unavailable	Verifies that the APT Threshold was not exceeded as specified in [SP 800 90B]	On Demand	Manually

OptiNAND Device

The OptiNAND device performs the pre-operational self-test listed below 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 satisfies AS10.23.

Table 21 OptiNAND Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Period	Periodic Method
RSA SigVer (Cert # A2099)	3072-bit, PSS w/SHA2-256, SecureBootPublicKey	Digital Signature Verification	SW/FW Integrity	Pass: Boot to the firmware image Fail: Device Unavailable	Verify Digital Signature.	On Demand	Manually

10.2 Conditional Self-Tests

Cryptographic Module Conditional Self-Tests

The Cryptographic Module performs the listed conditional self-tests. 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.

Table 22 CM Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Conditions	Coverage	Coverage Notes	Period	Periodic Method
AES-CBC	AES, 256-bit, CBC	Known Answer (KAT)	CAST	Pass: Next test Fail: Device Degraded	Encrypt, verify	Power up	Cert #AES 3580	IG 10.3.A	On Demand	Manually
AES-CBC	AES, 256-bit, CBC	KAT	CAST	Pass: Next test Fail: Device Degraded	Decrypted, verify	Power up	Cert #AES 3580	IG 10.3.A	On Demand	Manually
AES-ECB	AES, 256-bit, ECB	KAT	CAST	Pass: Next test Fail: Device Degraded	Encrypt, verify	Power up	Cert #AES 3580	IG 10.3.A	On Demand	Manually
AES-ECB	AES, 256-bit, ECB	KAT	CAST	Pass: Next test Fail: Device Degraded	Decrypted, verify	Power up	Cert #AES 3580	IG 10.3.A	On Demand	Manually
AES-ECB	AES, 256-bit, ECB, DEE	KAT	CAST	Pass: Next test Fail: Device Degraded	Encrypt, verify	Power up	Cert #A2101	IG 10.3.A	On Demand	Manually

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Conditions	Coverage	Coverage Notes	Period	Periodic Method
AES-ECB	AES, 256-bit, ECB, DEE	KAT	CAST	Pass: Next test Fail: Device Degraded	Decrypt, verify	Power up	Cert #A2101	IG 10.3.A	On Demand	Manually
AES-XTS	AES, 256-bit, XTS	Non-equivalence test[9]	Critical Function	Fail: UEC error code	Verify	LRK and NSK generation	Cert #A2101	IG C.I	On Demand	Programmatically
DRBG	5120-bit seed	KAT	CAST	Pass: Next test Fail: Device Unavailable	Verify	Power up	Cert #A2098	IG 10.3.A	On Demand	Programmatically
ESV	Repetition Count Test (RCT)	RCT	CAST	Pass: Next test Fail: Device Unavailable	Verifies that the RCT threshold was not exceeded as specified in [SP 800 90B]	Power up	Cert #ESV13	IG 10.3.A	On Demand	Manually
						After 2^{32} CTR_DRBG reseeds.				Programmatically
ESV	Adaptive Proportion Test (APT)	APT	CAST	Pass: Next test Fail: Device Unavailable	Verifies that the APT threshold was not exceeded as specified in [SP 800 90B]	Power up	Cert #ESV13	IG 10.3.A	On Demand	Manually .
						After 2^{32} CTR_DRBG reseeds				Programmatically
HMAC-SHA2-256	Message, 256-bit key, 256-bit hash digest	KAT	CAST	Pass: Next test Fail: Device Degraded	Verify	Power up	Cert #HMAC 2280	IG 10.3.A	On Demand	Manually
PBKDF2	256-bit Salt Iteration Count: 1024	KAT	CAST	Pass: Next test Fail: Device Degraded	Verify	Power up	Cert #A2100	IG 10.3.A	On Demand	Manually
RSA SigVer	3072-bit public key, 256-bit hash digest	KAT	CAST	Pass: Next test Fail: Device Degraded	Verify	Power up	Cert #A2098, Cert #SHS 2942	IG 10.3.A	On Demand	Manually

[9] IG C.I XTS-AES Key Generation Requirement

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Conditions	Coverage	Coverage Notes	Period	Periodic Method
RSA SigVer	3072-bit public key, 256-bit hash digest, OEM_Release Key	Digital Signature Verification	SW/FW Load Test	Pass: Boot to new image Fail: UEC error code	Verify	Firmware download	Cert #A2098, Cert #SHS 2942	IG 10.3.A	On Demand	Programmatically
SHA2-256	Message, 256-bit hash digest	KAT	CAST	Pass: Next test Fail: Device Degraded	Verify	Power up	Cert #SHS 2942	IG 10.3.A	On Demand	Manually
SP 800-38F KW	256-bit KEK	KAT	CAST	Pass: Next test Fail: Device Degraded	Authenticated Encrypt, verify	Power up	Cert #A2098	IG 10.3.A	On Demand	Manually
SP 800-38F KW	256-bit KEK	KAT	CAST	Pass: Next test Fail: Device Degraded	Authenticated Decrypt, verify	Power up	Cert #A2098	IG 10.3.A	On Demand	Manually

OptiNAND Conditional Self-Tests

The OptiNAND device performs the conditional self-test listed below. 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.

Table 23 OptiNAND Conditional Self-Tests

Algorithm Tested	Test Properties	Test Method	Type	Indicator	Details	Conditions	Coverage	Coverage Notes	Period	Periodic Method
AES-CBC	AES, 256-bit, CBC	KAT	CAST	Pass: Next test Fail: Device Degraded	Encrypt, verify	Power up	Cert #A2099	IG 10.3.A	On Demand	Manually
AES-CBC	AES, 256-bit, CBC	KAT	CAST	Pass: Exit self-test suite Fail: Device Degraded	Decrypt, verify	Power up	Cert #A2099	IG 10.3.A	On Demand	Manually

Algorithm Tested	Test Properties	Test Method	Type	Indicator	Details	Conditions	Coverage	Coverage Notes	Period	Periodic Method
RSA SigVer	3072-bit public key, 256-bit hash digest, sFFUPublicKey	Digital Signature Verification	CAST	Pass: Boot to new image Fail: UEC error code	Verify Digital Signature	Firmware download	Cert #A2099	IG 10.3.A	On Demand	Programmatically
SHA2-256	Message, 256-bit hash digest	KAT	CAST	Pass: Next test Fail: Device Degraded	Verify	Power up	Cert #A2099	IG 10.3.A	On Demand	Manually

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.

10.4 Error States

Table 24 Error States

Name	Description	Conditions	Recovery Method	Indicator
Device Degraded	This error indicates that one of the conditional self-tests listed in Table 22 or Table 23 failed. 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 Table 20 and Table 21. In this state, the module no longer responds to any operator commands.	Pre-operational test failure	Power cycle	Device is unresponsive

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 any Authentication Credential PIN that is set to the default 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 Authentication which states that, "…If default authentication data is used to control access to the module, then default authentication data shall [04.46] be replaced upon first-time authentication. This default authentication data does not need to meet the zeroisation requirements (7.9.7)."

Take-Ownership Scenario Example

1. Authenticate to the SID.
   a. If the CM authenticated to the SID with the default 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 default 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 default 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 RoT.

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 zeroisation service that vary in scope. Table 17 SSP Zeroization Methods defines scope of each zeroisation 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.
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 RoT are inaccessible from outside the ACM RoT. The CM encrypts and signs all CSPs before storing them in volatile or non-volatile memory outside ACM RoT. 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 default 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 186-5, NIST, February 2023
[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, August 2024
[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)

Abbreviation	Specification Name
[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
[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]

Name	Definition
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]
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]
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.

Name	Definition
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 Band	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 default 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 default value for all Authentication Credentials. [TCG Core]
Method	A remote procedure call to an SP that initiates an action on the SP. [TCG Core]
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.

Name	Definition
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.
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

Acronym	Definition
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
KEK	Key Encrypting Key
LBA	Logical Block Address
MEK	Media Encryption Key
MSID	Manufactured Security Identifier
NAND	Negative AND Flash Memory technology
NIST	National Institute of Standards and Technology
NOR	Negative 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

Acronym	Definition
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