Ultrastar® DC SN840 NVMe™ PCIe 3.0 Self Encrypting Drive
FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Protection of Data at Rest

Document Version: 1.1
2022-07-05

CONTENTS

Tables

Figures

1. Cryptographic Module Overview

The self-encrypting Ultrastar® DC SN840 NVMe™ PCIe 3.0 Self Encrypting Drive, hereafter referred to as Ultrastar DC SN840 or Cryptographic Module (CM) is a multiple-chip embedded module that complies with FIPS 140-2 Level 2 security. The drive enclosure defines the cryptographic boundary. See Figure 1: Ultrastar DC SN840 Cryptographic Module. The physical interface to the Cryptographic Module is the U.2[1] connector and a 2-pin UART port connector. All components within this boundary satisfy FIPS 140-2 requirements.

The Cryptographic Module complies with the Trusted Computing Group (TCG) Storage Security Subsystem Class: Ruby Specification [8]. The TCG Storage specifications [1, 2, 3, 4, 5, 6, 7, and 8] define the logical interface. The range of supported services, which utilize NIST approved algorithm, include 256-bit AES hardware-based data encryption, cryptographic erasure of user data, authenticated protection of LBA data ranges and RSA 2048 authenticated firmware download support.

The primary function of the module is to provide encrypted data storage, authenticated access control, and cryptographic erasure of the data stored on the solid-state media. The Cryptographic Module operator interfaces with the CM through a host system application.

Figure 1: Ultrastar DC SN840 Cryptographic Module

[1] Formally referred to as PCIe SSD SFF-8639

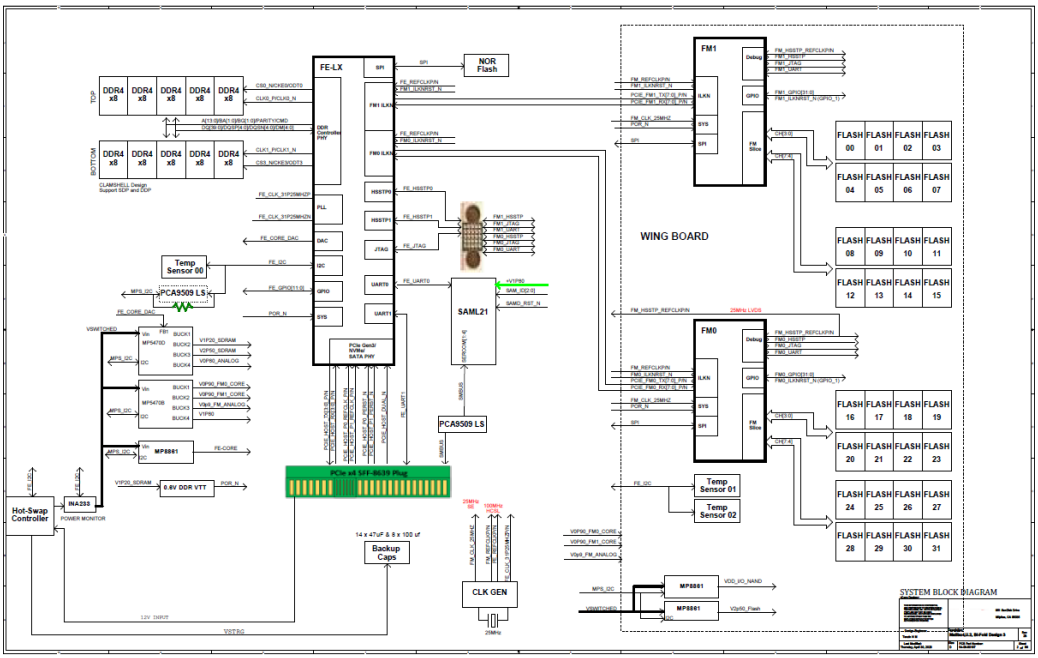

Figure 2: Ultrastar DC SN840 Block Diagram

1.1 Models

Multiple hardware versions define the scope of the Cryptographic Module. Storage capacity, write endurance, and overprovisioning define the differences. Table 1 provides the model numbers, characteristics, and firmware version associated with each validated model.

Hardware Version	Firmware Version	Description
WUS4C6416DSP3X5	R2210400, R2EF0003	SSD, BICS4, 1.6TB, PCIe, 3DW/D, 28% OP
WUS4BA119DSP3X5	R2210400, R2EF0003	SSD, BICS4, 1.92TB, PCIe, 1DW/D, 7% OP
WUS4C6432DSP3X5	R2210400, R2EF0003	SSD, BICS4, 3.2TB, PCIe, 3DW/D, 28% OP
WUS4BA138DSP3X5	R2210400, R2EF0003	SSD, BICS4, 3.84TB, PCIe, 1DW/D, 7% OP
WUS4C6464DSP3X5	R2210400, R2EF0003	SSD, BICS4, 6.4TB, PCIe, 3DW/D, 28% OP
WUS4BA176DSP3X5	R2210400, R2EF0003	SSD, BICS4, 7.68TB, PCIe, 1DW/D, 7% OP
WUS4BA1A1DSP3X5	R2210400, R2EF0003	SSD, BICS4, 15.36TB, PCIe, 1DW/D, 7% OP

Table 1 - Ultrastar DC SN840 Models

1.2 Security Level

The Cryptographic Module meets all requirements applicable to FIPS 140-2 Level 2 Security.

FIPS 140-2 Security Requirements Section	FIPS 140-2 Security Level Achieved
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2 - Module Security Level Specification

2. FIPS 140 Modes of Operation

2.1 FIPS Approved Mode of Operation

The Cryptographic Module has a single FIPS Approved mode of operation. Upon shipment from the vendor's manufacturing site the cryptographic module always operates in FIPS Approved Mode. See Section 7.2 for information on the recommended initialization instructions for the Cryptographic Module. The operator can confirm that the Cryptographic Module is operating in a FIPS Approved mode by invoking the Level 0 Discovery service and confirming that the inFIPS data field returns a value of 1.

2.2 TCG Ruby Security Mode

The TCG Ruby security mode utilizes NVMe commands as well as TCG commands that address the TCG Admin SP and TCG Locking SP to provide services. The Crypto Officer must execute the Activate service to enable the TCG Ruby security mode.

The TCG Ruby security mode allows multiple users with individualized access control to read, write, and erase data within independent data areas, which are referred to as LBA ranges. Access control tables define authorities, the secrets and authentication methods those authorities require, and the access control associations that permit method operation. Credential tables define the available encryption and decryption algorithms, authentication mechanisms, and store associated secrets or keys. Access control defines which authorities are permitted to successfully invoke which methods and modify ACLs.

The TCG Ruby security mode supports administrator functions within the Crypto Officer role to,

- Enable and disable Users
- Grant LBA range access to Users
- Create, configure, lock, and unlock LBA ranges
- Cryptographically erase data ranges

2.3 Single User Data Ranges

The Crypto Officer my elect to define one or more data ranges as a Single User Data Range (SUDR) when invoking the Activate service. The TCG Storage Opal SSC Feature Set: Single User Mode [5] defines Single User Data Ranges. As specified, the associated User role solely manages its assigned SUDR. Executing the Reactivate service allows an enabled Locking SP Admin to reclassify user data ranges.

2.4 Approved Algorithms

The Cryptographic Module supports the following FIPS Approved algorithms. All algorithms and key lengths comply with NIST SP 800-131A.

CAVP Cert	Algorithm Standards and Function
A1025	[SP 800-90A, SP 800-38A, SP 800-38D] DRBG Function: Deterministic random number generator (DRBG). Mode: CTR DRBG with AES-256 Derivation Function Key Size: 256 bits Key Length: 384 bits Security Strength: 256 bits Prerequisite: AES 3580
A1025	[SP 800-132] PBKDF2 Function: PBKDF2 utilizes a 32-byte PIN (password) and 256-bit KDF Salt to generate 256-bit Derived Authority Keys. Mode: HMAC-SHA2-256 Password Size: 32 bytes Salt Size: 256 bits Security Strength: 256 bits Prerequisite: SHS 2942, HMAC 2280
A1025, A1184	[FIPS 186-4] RSA Function: Digital signature verification with SHA2-256 Mode: PKCS#1 v1.5 Key Size: 2048 bits Security Strength: 112 bits Prerequisite: SHS 2942
A1025	[SP 800 38F] Key Wrapping Functions: Encryption, decryption, and key wrapping to protect the Root Signing Key Modes: KWP-AE, KWP-AD using AES-ECB-256 Key Size: 256 bits Security Strength: 256 bits Prerequisite: AES 3913
AES 3580[2]	[FIPS 197, SP 800-38A, SP 800-38E] AES Function: AES-CBC-256 encrypts and decrypts CSPs and PSPs. Mode: CBC Key Size: 256 Security Strength: 256 bits
AES 3913[3]	[FIPS 197] AES Function: AES-ECB-256 encryption and decryption. Supports SP 800-38F key wrapping Mode: ECB Key Size: 256 Security Strength: 256 bits

[2] The cryptographic module does not use the AES ECB-128, AES ECB-256, AES-CBC-128, AES-XTS-128, and AES-XTS-256 capabilities listed under Cert# AES 3580.

[3] The cryptographic module does not use the AES-ECB-128, AES-XTS-128 and AES-XTS-256 capabilities listed under Cert# AES 3913.

CAVP Cert	Algorithm Standards and Function
C1973	[FIPS 197, SP 800-38A, SP 800-38E] AES[4] Function: Used to encrypt and decrypt data-at-rest in a storage application Mode: XTS[5] • Per IG A.9, an LRK.AESKey/LRK.XTS keyset differs from its associated NSK.AESKey/NSK.XTS keyset Key Size: 256 Security Strength: 256 bits
ENT (P)	[SP800-90B] Function: Hardware entropy noise source seeds the Approved [SP800-90A] DRBG Type: Ring Oscillator DRBG Seed Length: 5120 bits DRBG Seed Entropy: 431.295 bits (2.6956 bits per 32 bits)
HMAC 2280[6]	[FIPS 198-1] HMAC Function: Used to sign and verify CSPs and PSPs and derive keys in PBKDF2. Mode: SHA2-256 Key Size: 256 Security Strength: 256 bits Prerequisite: SHS 2942
SHS 2942[7]	[FIPS 180-4] SHS Functions: Digital signature verification and in used in the HMAC function Mode: SHA2-256 Key Size: 256 Security Strength: 256 bits

Table 3 - FIPS Approved Algorithms

Algorithm	Description	Rationale
CKG	[SP800 133] Cryptographic Key Generation Function: Generated from the DRBG without further modification or post processing Reference: Table 9 and Table 10 list the Symmetric Keys	Vendor Affirmed [FIPS140] IG D.12 [SP 800 133] Sections 6.1, 6.2.3 and 6.3

Table 4 – Approved Cryptographic Functions Tested with Vendor Affirmation

2.5 Approved Random Number Generator

A validated [SP 800-90B] ENT (P) seeds the Approved [SP800-90A] DRBG. Available entropy does not modify the security strength of the cryptographic keys generated by the module. Each 32-bit sample block contains at least 2.6956 bits of entropy. Each time the DRBG is instantiated or reseeded, one hundred sixty (160) 32-bit samples seed the DRBG. This equates to 5120 bits of entropy data and translates to at least 431.295 bits of entropy. The nonce consumes approximately 143.7 bits. Therefore, approximately 287.5 bits of entropy remain to determine the bit strength of the keys generated by the DRBG. This exceeds the 384 bits (256-bit entropy input and 128-bit nonce) of min-entropy needed to seed the DRBG with 256-bits of security.

[4] AES-ECB-128 and AES-XTS-128 were tested. However, the cryptographic module does not use these algorithms.
[5] The length of the XTS-AES data unit does not exceed 2^{20} blocks
[6] The cryptographic module does not use the HMAC-SHA1, and HMAC-SHA2-224 capabilities listed under Cert# HMAC 2280.
[7] The cryptographic module does not use the SHA-1 and SHA2-224 capabilities listed under Cert# SHS 2942.

3. Ports and Interfaces

The drive uses the standard 68-pin PCIe U.2 connector that conforms to the mechanical requirements of SFF-8639. Table 5 identifies the Cryptographic Module's ports and interfaces. The UART port is a three-wire port that consists of transmit (Tx), receive (Rx) and ground. The UART connector is protected by the application of a tamper evident seal. The Cryptographic Module does not provide a removable maintenance access panel.

FIPS 140-2 Interface	Cryptographic Module Port Connector Pins
Power	Power connector
Control Input	U.2 connector, UART connector
Status Output	U.2 connector, UART connector
Data Input	U.2 connector, UART connector
Data Output	U.2 connector, UART connector

Table 5 - Ultrastar DC SN840 Ports and Interfaces

4. Identification and Authentication Policy

The Cryptographic Module enforces role separation by requiring a role identifier and an authentication credential in the form of a Personal Identification Number (PIN). The Cryptographic Module enforces the following FIPS140-2 operator roles. Table 6 maps TCG Storage authorities to FIPS 140-2 roles.

4.1 Crypto Officer Roles

4.1.1 Secure ID (SID)

This Crypto Officer role corresponds to the authority that represents the TPer owner within the Admin SP as defined in the TCG Storage Security Subsystem Class: Opal [2] specification. The Crypto Officer uses this role to transition the Cryptographic Module to the TCG Storage Ruby security mode. The Cryptographic Mode actively rejects firmware images that do not comply with FIPS 140 security requirements.

4.1.2 Admin SP Admin1

This Crypto Officer role corresponds to the Admin SP Admin1 authority defined in the TCG Storage Security Subsystem Class: Opal [2] specification. The Admin SP Admin1 authority can enable and disable Locking SP Admins.

4.1.3 Locking SP Admins

This Crypto Officer role corresponds to the Locking SP Admin Authority as defined in the TCG Storage Security Subsystem Class: Opal [2] specification. The CM enables Locking SP Admin1 by default. The CM can enable at most four (4) separate Locking SP Admins. By default, the CM disables Locking SP Admins beyond Admin1. When the Single User Data Range (SUDR) feature is disabled, a Locking SP Admin can enable and disable Users, create, and delete data ranges, set data range attributes, lock, unlock, and erase data ranges. A Locking SP Admin executes the Erase service to cryptographically erase a SUDR, by invoking TCG Erase. A Locking SP Admin executes the Erase service to cryptographically erase a non-SUDR, by invoking TCG GenKey. Both methods accomplish the same end by regenerating and replacing the Media Encryption Key (MEK) assigned to the data range.

4.2 User Roles

4.2.1 Locking SP Users

This user role corresponds to the Locking SP User Authority as defined in the TCG Storage Security Subsystem Class: Opal [2] specification. This role can lock and unlock LBA ranges to control the ability of the host to read and write data to and from the CM. By default, all Locking SP Users are disabled. The CM can enable at most nine (9) separate Users. Enabled Locking SP Admins enable Locking SP Users and assign them read/write/erase access to LBA data ranges. A Locking SP User executes the Erase service to cryptographically erase a SUDR by invoking TCG Erase or TCG GenKey. A Locking SP User executes the Erase service to cryptographically erase a non-SUDR by invoking TCG GenKey. Both methods accomplish the same end by regenerating and replacing the Media Encryption Key (MEK) assigned to the data range.

4.3 Anybody

The Anybody role can access services that do not require authentication. Apart from the Generate Random service, which provides output from an instance of the SP800-90A DRBG, unauthenticated services do not disclose, modify, or substitute Critical Security Parameters, use Approved security functions, or otherwise affect the security of the Cryptographic Module. If the operator has physical access to the drive, the Anybody role can use a power cycle to reset the Cryptographic Module, which results in the execution all the Power on Self-Tests (POST).

TCG Authority	Description	Authentication Type	Authentication Data
SID	The TCG Storage Security Subsystem Class: Opal [2] specification defines the SID authority.	Role-based	SID PIN
Admin SP Admin1	The TCG Storage Security Subsystem Class: Opal [2] specification defines the Admin SP Admin1 authority.	Role-based	Admin SP Admin1 PIN
Locking SP Admin	The TCG Storage Security Subsystem Class: Opal [2] specification] defines Locking SP Admin authority.	Role-based	Locking SP Admin PIN
Locking SP User	The TCG Storage Security Subsystem Class: Opal [2] specification defines the Locking SP User authority.	Role-based	Locking SP User PIN
Anybody	Anybody is a role that does not require authentication. The TCG Storage Security Subsystem Class: Opal [2] specification defines the Anybody authority.	Unauthenticated	N/A

Table 6 - Roles and Required Identification and Authentication

4.4 Authentication Method and Strength

Authentication occurs within a TCG session. At any one time, only a single session can be open. After opening an Admin SP session or a Locking SP session, an operator uses the Authenticate method to authenticate to a role. Authentications persist until the session closes or the Cryptographic Module powers down.

Operators utilize an Authority PIN to authenticate to a Crypto Officer or User role. Authority PINs are 32-byte TCG credentials. For a 32-byte PIN, there are 2^{256} possible values. Values from 0x00 to 0xFF are allowed for each byte position. Assuming all possible values have an equal chance of use, the probability of guessing the correct PIN is one chance in 2^{256} or approximately 8.64×10^{-78}, which is significantly less than 1/1,000,000.

The TCG Storage Ruby security model includes a TryLimit attribute for each TCG Authority, which if reached, locks out further attempts to authenticate to the TCG Authority. Assuming the TryLimit is non-zero[8], an Authority_Locked_Out state exists if the Tries count value equals the TryLimit value associated with a TCG Authority. Each authentication attempt consumes approximately 198 microseconds. Hence, at most, approximately 30,287 authentication attempts can occur within one minute when the TryLimit equals zero (0). Thus, the probability that a false acceptance occurs within a one-minute interval is approximately 2.62×10^{-73} ($8.64 \times 10^{-78} \times 30{,}287$), which is significantly less than 1/100,000.

5. Access Control Policy

5.1 Roles and Authenticated Services

Service	Description	Role(s)
Activate	The Activate method allows the TPer owner to "turn on" a Security Provider (SP) that was created in manufacturing. LBA ranges are configured, and data encryption and access control credentials (re)generated and/or set within the Cryptographic Module. Access control is configured for LBA range unlocking.	CO (SID, Admin SP Admin1)
Authenticate	Input a TCG Credential for authentication	CO (SID, Admin SP Admin1, Locking SP Admins) Users (Locking SP Users)
Disable User Set PIN	This service disables the ability of a non-SUDR User to modify its own PIN.	CO (Locking SP Admins)
Enable/Disable Admin SP Admin	This service enables and disables the Admin SP Admin1 authority.	CO (SID)
Enable/Disable Locking SP Admin	This service enables and disables a Locking SP Admin authority.	CO (Locking SP Admin1)
Enable/Disable Locking SP User	This service enables and disables a Locking SP User authority.	CO (Locking SP Admins)
Enable/Disable SUDR	This service enables and disables the classification of a data range as a SUDR.	CO (Locking SP Admins)
Erase non-SUDR	A cryptographic erasure service that utilizes the TCG GenKey method to generate and replace the MEK assigned to an LBA data range	CO (Locking SP Admins) Users (Locking SP Users)
Erase SUDR	A cryptographic erasure service that utilizes the TCG GenKey or TCG Erase method to generate and replace the MEK assigned to an LBA data range	CO (Locking SP Admins)[9] Users (Locking SP Users)[10]
Field FA	This service provides basic drive health analysis testing and media verification. The service does not leak any clear text user data to the host interface. This service is limited to performing the following functions: • Basic health tests • Media verification All Host Read/Write Commands are inhibited.	CO (SID, Admin SP Admin1, Locking SP Admins) Users (Locking SP Users)

[8] When TryLimit is set to zero (0), the CM places no limit on the number of authentication attempts.
[9] TCG Erase
[10] TCG GenKey or TCG Erase

Service	Description	Role(s)
Initialize Cryptographic Module[11]	Crypto Officer provisions the Cryptographic Module from the organizational policies	CO (SID, Admin SP Admin1)
Lock/Unlock Data Range	This service denies or permits read and write access to an LBA range	CO (Locking SP Admins)[12] Users (Locking SP Users)
Reactivate	In Single User Mode, the reactivate service allows the host to define which ranges are under the control of a single User authority. In addition, it allows the host to define range ownership within non-Global Range Locking objects.	CO (Locking SP Admins)
SecureDrive Command	TCG IF-SEND and IF-RECV transport secure commands to and from the Cryptographic Module.	CO (SID, Admin SP Admin1, Locking SP Admins) Users (Locking SP Users)
Set	Write data structures; access control enforcement occurs per data structure field. This service can change PINs.	CO (SID, Admin SP Admin1, Locking SP Admins) Users (Locking SP Users)
Set Data Range Attributes for a non-SUDR	This service sets the starting location, size, and locking attributes for a SUDR.	CO (Locking SP Admins) Users (Locking SP Users)
Set Data Range Attributes for a SUDR	This service sets the starting location, size, and locking attributes as well as the User access rights for a non-SUDR.	CO (Locking SP Admins) Users (Locking SP Users)
Zeroize	This service utilizes the TCG Revert method to zeroize the CM and return the CM to its original manufactured state. Execution of this service requires the operator to authenticate to the PSID[13] or SID PIN.	SID use case: CO (SID) PSID use case: CO (Admin SP Admin1, Locking SP Admins) Users (Locking SP Users) Anybody

Table 7 - Authenticated CM Services

[11] See the Cryptographic Module Acceptance and Provisioning section within 7.2 Initialization Rules.
[12] Applies only to non-SUDRs
[13] See TCG Storage Opal SSC Feature Set: PSID [3]

5.2 Unauthenticated Services

Table 8 - Unauthenticated Services lists the unauthenticated services the Cryptographic Module provides.

Service	Description
End Session	End a TCG session by clearing all session state
FIPS 140 Compliance Descriptor[14]	This service reports the FIPS 140 revision as well as the Cryptographic Module's overall security level, hardware revision, firmware revision and module name.
Firmware Download	RSA2048 PKCS#1 v1.5 and SHA-256 verify the entire firmware image.
Format NVM	This service changes an LBA data size and/or metadata size. This low-level format operation may cryptographically erase all data and metadata associated with all namespaces or specific namespaces.
Generate Random	TCG Random method generates a random number from the SP800-90A DRBG
Get	Reads data structure; access control enforcement occurs per data structure field
Get Data Store[15]	Read a stream of bytes from unstructured storage
Level 0 Discovery	TCG 'Level 0 Discovery' method outputs the FIPS mode of the Cryptographic Module
NVMe Admin Commands	The NVMe admin commands are defined in the NVM Express v1.3.c [10] and NVM Express™ Management Interface [11] specifications
NVMe I/O Commands	The NVMe admin commands are defined in the NVM Express v1.3.c [10] and NVM Express™ Management Interface [11] specifications
Read Data	This service decrypts user data when reading the data from a data range. The data range must be unlocked to enable reads from the data range.
Reset Module	Power on Reset
SecureDrive Command	TCG IF-SEND and IF-RECV transport secure commands to and from the Cryptographic Module.
Security Receive	The Security Receive command transfers the status and data result of one or more Security Send commands that were previously submitted to the controller.
Security Send	The Security Send command is used to transfer security protocol data to the controller.
Self-Test	The Cryptographic Module performs self-tests when it powers up
Set Data Store[16]	Write a stream of bytes to unstructured storage.
SoC Rebuild	The SoC Rebuild service utilizes the SecureDrive Command service to zeroize and regenerate the Root Keyset and the Global Active Keyset
Start Session	Start TCG session
Status Output	TCG (IF-RECV) protocol
Write Data	This service encrypts user data when writing the data from a data range. The data range must be unlocked to enable writes to the data range.

Table 8 - Unauthenticated CM Services

[14] See §5.1.5.3 FIPS 140 Compliance Descriptor section within the Security Features for SCSI Commands [14].
[15] The access control for the retrieval of data in the DataStore initially requires Admin SP Admin1 or an Locking SP Admin to enable access
[16] The access control for the modification of data in the DataStore initially requires the Admin SP Admin1 or an Locking SP Admin to enable access.

5.3 Critical Security Parameters (CSPs)

The Cryptographic Module contains the CSPs listed in Table 9. Zeroization of CSPs complies with the purge requirements for SCSI Hard Disk drives within [SP800-88], Guidelines for Media Sanitization.

Name	Type	Description
ENT (P)	5120-bit Entropy output	Entropy source for DRBG
DRBG.Seed	256-byte Entropy input	Internal state associated with the [SP800-90A] CTR_DRBG using AES-256 Sourced from ENT (P)
DRBG.Key	256-bit value	Internal state associated with the [SP800-90A] CTR_DRBG using AES-256
DRBG.V	128-bit value	Internal state associated with the [SP800-90A] CTR_DRBG using AES-256.
Authority Digest	256-bit digest	An HMAC-SHA2-256 digest of an Authority PIN and its associated SED Admin SP key or SED Locking SP key.
Authority PIN	32-byte value	Values from 0x00 to 0xFF are allowed for each byte position. A PBKDF2 algorithm uses an Authority PIN to authenticate to the credential of a TCG Authority.
SID PIN	Authority PIN	A 32-byte data value used to authenticate to the TCG credentials of the SID Authority.
Admin SP Admin1 PIN	Authority PIN	A 32-byte data value used to authenticate to the TCG credentials of the Admin SP Admin1 Authority.
Locking SP Admin PIN (Maximum of 4)	Authority PIN	A 32-byte data value used to authenticate to the TCG credential of each Locking SP Admin Authority.
Locking SP User PIN (Maximum of 9)	Authority PIN	A 32-byte data value used to authenticate to the TCG credential of each Locking SP User Authority.
Root Encryption Key	256-bit keys	The CM utilizes AES-CBC-256 and the Root Encryption Key to encrypt and decrypt the Global Active Keyset. The [SP 800-38F] KWP algorithm uses the Root Encryption Key to wrap and unwrap the Root Signing Key. The Cryptographic Module's DRBG generates this key without modification. The CM stores this key in OTP memory.
Root Signing Key	256-bit key	An HMAC-SHA2-256 digest of the concatenated Root Signing Key and encrypted Global Active Keyset signs the Global Active Keyset. The Cryptographic Module's DRBG generates this key without modification. The CM stores the Key Wrapped value within the Reserved Area of NOR flash.

Name	Type	Description
Global Active Keyset (AEK)	Set of 256-bit keys: Global Active Key, Global Active Signing Key	The CM utilizes AES-CBC-256 and the Global Active Key to encrypt and decrypt the SED Active Keyset, UAKa and Namespace Keys. An HMAC-SHA2-256 digest of the Global Active Signing Key and the SED Active Keyset signs the SED Active Keyset. An HMAC-SHA2-256 digest of the Global Active Signing Key and the UAKa signs the UAKa. An HMAC-SHA2-256 digest of the Global Active Signing Key and a Namespace Key, signs a Namespace Key. The Cryptographic Module's DRBG generates these keys without modification. The CM stores the encrypted keyset within the Reserved Area of NOR flash.
SED Active Keyset	Set of 256-bit keys: SED Active Key SED Active Signing Key	The CM utilizes AES-CBC-256 and the SED Active Key to encrypt and decrypt the SED Admin SP Keyset and the SED Locking SP Keyset. An HMAC-SHA2-256 digest of the SED Active Signing Key and the SED Admin SP Keyset signs the SED Admin SP Keyset. An HMAC-SHA2-256 digest of the SED Active Signing Key and the SED Locking SP Keyset signs the SED Locking SP Keyset. The Cryptographic Module's DRBG generates these keys without modification. The CM stores the encrypted keyset within the Reserved Area of NOR flash.
SED Admin SP Keyset	Set of 256-bit keys: SED Admin SP Key SED Admin SP Signing Key	The CM utilizes AES-CBC-256 and the SED Admin SP Key to encrypt and decrypt TCG table data associated with an Admin SP. An HMAC-SHA2-256 digest of the SED Admin SP Signing Key and the entire contents of an Admin SP table, signs the associated table. The Cryptographic Module's DRBG generates these keys without modification. The CM stores the encrypted keyset within the Reserved Area of NOR flash.
SED Locking SP Keyset	Set of 256-bit keys: SED Locking SP Key SED Locking SP Signing Key	The CM utilizes AES-CBC-256 and the SED Locking SP Key to encrypt and decrypt table data associated with a Locking SP authority. An HMAC-SHA2-256 digest of the SED Locking SP Signing Key and the entire contents of a Locking SP table signs the associated table. The Cryptographic Module's DRBG generates these keys without modification. The CM stores the encrypted keyset within the Reserved Area of NOR flash.

Name	Type	Description
SED Volatile Keyset	Set of 256-bit keys: SED Volatile Key SED Volatile Signing Key	The CM utilizes AES-CBC-256 and the SED Volatile Key to encrypt and decrypt keys stored in IRAM. An HMAC-SHA2-256 digest of the SED Volatile Signing Key and the encrypted key stored in IRAM, signs the encrypted key. The Cryptographic Module's DRBG generates these keys without modification. The CM stores the keyset in IRAM.
Admin Authority Key (K_a) (Maximum of 5)	256-bit key	The CM utilizes AES-CBC-256 and a PBKDF2 derived K_a key to encrypt and decrypt UAK_0 and the UMK. The Cryptographic Module derives a unique K_a for Admin SP Admin1 and each enabled Locking SP Admin. K_a keys are destroyed after use.
Non-Admin Authority Key (K_u) (Maximum of 9)	256-bit key	The CM utilizes AES-CBC-256 and a PBKDF2 derived K_u keys to encrypt and decrypt an associated UAK. The Cryptographic Module derives a unique K_u for each enabled Locking SP User. Ku keys are destroyed after use.
User Access Key (UAK) (Maximum of 9)	256-bit key	The CM utilizes AES-CBC-256 and a UAK to encrypt and decrypt an associated RAK. The Cryptographic Module generates a unique UAK for each enabled Locking SP User. The Cryptographic Module's DRBG generates these keys without modification. The CM stores each encrypted key within the Reserved Area of NAND flash.
Admin User Access Key (UAK_0)	256-bit key	The CM utilizes AES-CBC-256 and UAK_0 key to encrypt and decrypt RAKs. All Locking SP Admins share UAK_0. The Cryptographic Module's DRBG generates this key without modification. The CM stores its encrypted value within the Reserved Area of NAND flash.
Anybody User Access Key (UAK_a)	256-bit key	The CM utilizes AES-CBC-256 and UAKa to encrypt and decrypt RAKs. The Cryptographic Module's DRBG generates this key without modification. The CM stores its encrypted value within the Reserved Area of NAND flash.
User Management Key (UMK)	256-bit key	The CM utilizes AES-CBC-256 and the UMK to encrypt and decrypt UAKs. All enabled Locking SP Admins and Admin SP Admin1 share the UMK. The Cryptographic Module's DRBG generates this key without modification. The CM stores its encrypted value within the Reserved Area of NAND flash.
Range Access Key (RAK) (16 total – 1 per LBA range)	256-bit key	The CM utilizes AES-CBC-256 and an RAK to encrypt and decrypt associated LRKs. The Cryptographic Module's DRBG generates these keys without modification. The CM stores their encrypted value within the Reserved Area of NAND flash.

Name	Type	Description
Locking Range Key (LRK) (16 total - 1 per LBA range)	Set of 256-bit keys: AES Key, XTS Key	An LRK in combination with its associated NSK creates an MEK. The Cryptographic Module's DRBG generates each LRK.AES Key and LRK.XTS Key without modification. The CM stores their encrypted value within the Reserved Area of NAND flash.
Namespace Key (NSK) (16 total - 1 per LBA range)	Set of 256-bit keys: AES Key, XTS Key	An NSK in combination with its associated LRK creates an MEK. The Cryptographic Module's DRBG generates each NSK.AES Key and NSK.XTS Key without modification. The CM stores their encrypted value within the Reserved Area of NAND flash.
MEK - Media Encryption Keyset (16 total - 1 per LBA range)	Derived set of 256-bit keys: AES Encryption Key, AES Decryption Key XTS Tweak Key	The MEK encrypts and decrypts LBA ranges. The MEK.AESEnc Key is an XOR of an LRK.AES Key and an NSK.AES Key. The MEK.XTS.Tweak Key is an XOR of an LRK.XTS Key and an NSK.XTS Key. The CM stores each encrypted MEK in IRAM.

Table 9 - Critical Security Parameters

5.4 Public Security Parameters

The Cryptographic Module utilizes RSA public key cryptography to verify that firmware downloaded to the module is authentic and to verify specific steps in the secure boot process. The Cryptographic Module uses RSA 2048 PKCS#1 v1.5 to verify each signature within the asymmetric key tree to establish a chain of trust. The RSA Public/Private key pairs used in this process are generated and stored within a Western Digital controlled Hardware Security Module (HSM). The SD_CA Key, SD_BFW Key, SD_SM Key, PROD GROUP Key, OEM FW Key, and OEM_OFS Key public keys are injected during the manufacturing process and stored within the Reserved Area of NOR flash memory. The Cryptographic Module rejects downloaded firmware image if the digital signature verification process fails.

Key Name	Type	Description
PSID[17]	32-character alphanumeric string	The PSID is derived from a 32-byte value generated by the Cryptographic Module's DRBG, without modification. An Alphanumeric Character Conversion process derives the alphanumeric string from the 32-byte value. The value is displayed on the module's product label. The PSID provides authentication data and proof of physical presence for the Zeroize service.
MSID[18]	32-character alphanumeric string	The MSID derives from a 32-byte value generated by the Cryptographic Module's DRBG. An Alphanumeric Character Conversion process derives the alphanumeric string from the 32-byte value.
KDF Salt	256-bit key	The PBKDF2 implementation, using HMAC-SHA2-256, utilizes unique KDF Salts to derive each K_a and K_u key. The Cryptographic Module's DRBG generates KDF Salts without modification.

[17] The SED Active Key encrypts the PSID. An HMAC-SHA2-256 digest of the PSID is store in the Reserved Area. The TCG Revert method regenerates the digest.
[18] An HMAC-SHA2-256 digest of the MSID is store in the Reserved Area. The TCG Revert method regenerates the digest.

Key Name	Type	Description
Storage Device Certification Authority Key (SD_CA Key)	RSA 2048 PKCS#1 v1.5 public key	The SD_CA Key is the Master RSA Public Key used to verify the Secure Loader image.
Storage Device Boot FW Key (SD_BFW Key)	RSA 2048 PKCS#1 v1.5 public key	The SD_BFW Key is public key used to verify all boot flash images.
Storage Device Secure Message Key (SD_SM Key)	RSA 2048 PKCS#1 v1.5 public key	The SD_SM Key verifies secure messages used for manufacturing, development, and failure analysis
Product Group Key (PROD GROUP Key)	RSA 2048 PKCS#1 v1.5 public key	The PROD GROUP Key verifies an OEM's Key certificates.
OEM Firmware Key (OEM FW Key)	RSA 2048 PKCS#1 v1.5 public key	The OEM FW Key verifies OEM firmware images and packages.
OEM Original Factory State Key (OEM_OFS Key)	RSA 2048 PKCS#1 v1.5 public key	The OEM_OFS Key verifies the OEM Original Factory Settings files.

Table 10 - Public Security Parameters

5.5 SP800-132 Key Derivation Function Affirmations

- The Cryptographic Module utilizes an HMAC-SHA2-256 based [SP800 132] Password Based Key Derivation Function (PBKDF2) that complies with Option 2a of SP800-132.
- Security Policy rules set the minimum Authority PIN length at 32-bytes. The Cryptographic Module allows values from 0x00 to 0xFF for each byte of the Authority PIN.
- The upper bound for the probability of guessing an Authority PIN is 2^{-256}. The difficulty of guessing the Authority PIN is equivalent to a brute force attack.
- Derived Authority Keys, K_a, and K_u ([SP800 132] Master Keys) are derive by processing a 32-byte Authority PIN ([SP800 132] Password) and a 256-bit KDF Salt though an PBKDF2 algorithm [SP800 132], using HMAC-SHA2-256. Each KDF Salt associated with a K_a or K_u key is unique. Therefore, each K_a and K_u key is unique. Each K_a and K_u has a security strength of 256 bits.
- Each 256-bit KDF Salt is a random number generated using the [SP800 90A] DRBG.

5.6 Critical Security Parameter Modes of Access

Table 11 and Table 12 define the relationship between access to Critical Security Parameters (CSPs) and the listed Cryptographic Module services. The definitions shown below define the access modes listed in both tables.

- **G** = Generate: The Cryptographic Module generates a CSP from the [SP800-90A] DRBG, derives a CSP with the PBKDF2 Key Derivation Function or generates an HMAC-SHA2-256 hash to sign a CSP.
- **I =** Input**:** The Cryptographic Module imports a CSP from outside the cryptographic boundary.
- **O =** Output: The Cryptographic Module does not support the output of CSPs outside the cryptographic boundary.
- **E** = Execute: The module executes a service that uses the CSP.
- **S** = Store: The Cryptographic Module stores a CSP persistently on media within the Cryptographic Module.
- **Z** = Zeroize: The Cryptographic Module zeroizes a CSP that is stored in volatile or non-volatile memory.

Service	Authority Digest	SID PIN Admin SP Admin1 PIN	Locking SP Admin PINs	Locking SP User PINs	DRBG.Seed	DRBG.Key	DRBG.V	ENT (P)	MEK	K_a	K_u	LRK
Activate	GS			Z	E	GE	GE		GS	GS	GS	GS
Authenticate	E	IE	IE	IE						E	E	
Disable User Set PIN												
Enable/Disable Admin SP Admin												
Enable/Disable Locking SP Admin or User (non-SUDR)												
Enable/Disable SUDR												
Erase non-SUDR									GSZ			GSZ
Erase SUDR									GSZ			GSZ
End Session												
Field FA												
FIPS 140 Compliance Descriptor												
Firmware Download												
Format NVM[19]									GSZ			E
Generate Random					E	GE	GE					
Get												
Get Data Store									E		E	E
Initialize Cryptographic Module	GS	IE	IE	IE	GE	GE	GE	GE	GS	GS	GS	GS
Level 0 Discovery												
Lock/Unlock Data Range												
NVMe Admin Commands												
NVMe I/O Commands												
Reactivate	GS			Z	E	GE	GE				GS	
Read Data									E			E
Reset Module					GEZ	GEZ	GEZ	GE	S			S
SecureDrive Command												
Security Receive												
Security Send												
Self-Test (KATs)												

[19] [19] If a range is write locked the execution of Format NVM is blocked.

Service	Authority Digest	SID PIN Admin SP Admin1 PIN	Locking SP Admin PINs	Locking SP User PINs	DRBG.Seed	DRBG.Key	DRBG.V	ENT (P)	MEK	K_a	K_u	LRK
Set		I	I	I								
Set Data Range Attributes for a non-SUDR												
Set Data Range Attributes for a SUDR												
Set Data Store									E			E
SoC Rebuild												
Start Session												
Status Output												
Write Data									E			E
Zeroize	GZ	Z	Z	Z	GE	GE	GE		GSZ	Z	Z	GSZ

Table 11 - CSP Access Rights within Roles & Services

Service	RAK	UAK	UAK_0	UAKa	UMK	NSK	Root Keyset	Global Active Keyset (AEK)	SED Active Keyset	SED Admin SP Keyset	SED Locking SP Keyset	SED Volatile Keyset
Activate	GS	GS	GS	GS	GS	GS			E	E	E	GE
Authenticate												
Disable User Set PIN												
Enable/Disable Admin SP Admin												
Enable/Disable Locking SP Admin or User (non-SUDR)												
Enable/Disable SUDR												
Erase non-SUDR	E				E	GSZ						
Erase SUDR	E				E	GSZ						
End Session												
Field FA												
FIPS 140 Compliance Descriptor												

Service	RAK	UAK	UAK_0	UAKa	UMK	NSK	Root Keyset	Global Active Keyset (AEK)	SED Active Keyset	SED Admin SP Keyset	SED Locking SP Keyset	SED Volatile Keyset
Firmware Download												
Format NVM						EGSZ		E				
Generate Random												
Get												
Get Data Store	E	E	E	E	E	E	E	E	E	E	E	E
Initialize Cryptographic Module	EGS	GS	GS	GS	GS	GS						
Level 0 Discovery												
Lock/Unlock Data Range												
NVMe Admin Commands												
NVMe I/O Commands												
Reactivate	GS	GS							E	E	E	GE
Read Data	E	E	E	E	E	E	E	E	E	E	E	E
Reset Module	S	S	S	S	S							G
SecureDrive Command												
Self-Test (KATs)												
Security Receive												
Security Send												
Set												
Set Data Range Attributes for a non-SUDR												
Set Data Range Attributes for a SUDR												
Set Data Store	E	E	E	E	E	E	E	E	E	E	E	E
SoC Rebuild							GSZ	GSZ				
Start Session												
Status Output												
Write Data	E	E	E	E	E	E	E	E	E	E	E	E
Zeroize	EGSZ	GSZ	GSZ	GSZ	GSZ	GSZ			GSZ	GSZ	GSZ	GZ

Table 12 - CSP Access Rights within Roles & Services

5.7 Public Security Parameter Modes of Access

Table 13 defines the relationship between access to Public Security Parameters (PSP) and the listed Cryptographic Module services. The definitions shown below define the access modes listed in Table 13.

- **G** = Generate: The Cryptographic Module generates a PSP from the [SP800-90A] DRBG, derives a PSP with the Key Derivation Function or hashes authentication data with SHA-256 or HMAC-SHA-256.
- **I =** Input**:** The Cryptographic Module imports a PSP from outside the cryptographic boundary.
- **O =** Output: The Cryptographic module outputs the value of selective PSPs.
- **E** = Execute: The module executes a service that uses the PSP.
- **S** = Store: The Cryptographic Module stores a PSP persistently on media within the Cryptographic Module.
- **Z** = Zeroize: The Cryptographic Module zeroizes a PSP that is stored in volatile or non-volatile memory.

Service	MSID	PSID	KDF Salt	SD_CA Key	SD_BFW Key	SD_SM Key	PROD_GROUP Key	OEM_FW Key	OEM_OFS Key
Activate			EGS						
Authenticate		E	E						
Disable User Set PIN									
Enable/Disable Admin SP Admin									
Enable/Disable Locking SP Admin or User (non-SUDR)									
Enable/Disable SUDR									
Erase non-SUDR									
Erase SUDR									
End Session									
Field FA						E			
FIPS 140 Compliance Descriptor									
Firmware Download								IS	IS
Format NVM									
Generate Random									
Get									
Get Data Store									
Initialize Cryptographic Module	OE		GS						
Level 0 Discovery									
Lock/Unlock Data Range									
NVMe Admin Commands									
NVMe I/O Commands									
Reactivate			EGS						
Read Data									
Reset Module				E	E		E	E	
SecureDrive Command						E			
Security Receive									
Security Send									

Service	MSID	PSID	KDF Salt	SD_CA Key	SD_BFW Key	SD_SM Key	PROD_GROUP Key	OEM_FW Key	OEM_OFS Key
Self-Test (KATs)									
Set									
Set Data Range Attributes for a non-SUDR									
Set Data Range Attributes for a SUDR									
Set Data Store									
SoC Rebuild									
Start Session									
Status Output									
Write Data									
Zeroize		I	GSZ						

Table 13 - PSP Access Rights within Roles & Services

6. Operational Environment

The Cryptographic Module operating environment is non-modifiable. Therefore, the FIPS 140-2 operational environment requirements are not applicable to this module. When operational, the Cryptographic Module prohibits additions, deletions, or modification of the code working set. For firmware upgrades, the Cryptographic Module uses the Firmware Download service to verify the digital signature of the firmware image and save a complete firmware image. If the download operation is successful, authorized, and verified the Cryptographic Module may begin operating with the new code working set. Firmware loaded into the module that is not on the FIPS 140-2 certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

7. Security Rules

The Cryptographic Module enforces applicable FIPS 140-2 Level 2 security requirements. This section documents the security rules that the Cryptographic Module enforces.

7.1 Invariant Rules

1. The Cryptographic Module supports two distinct types of operator roles: Crypto Officer and User.
2. Power cycling the Cryptographic Module or exiting a TCG sessions clears active authentications.
3. The Cryptographic Module requires operators to re-authenticate to TCG Authorities after power cycling the module or upon execution of the End Session service.
4. The Cryptographic Module powers up in FIPS Approved mode.
5. When the Cryptographic Module is unable to authenticate TCG Credentials, operators do not have access to any cryptographic service other than the unauthenticated Generate Random service.

6. The Cryptographic Module performs the following tests. Upon failure of any test, the Cryptographic Module enters a soft error state. The Cryptographic module reports the error condition by transmitting an UEC to the host over the U.2 interface. After entering the soft error state, the Cryptographic Module cannot execute security services unless a power cycle clears the error state.
    a. Power up Self-Tests
        i. RSA 2048 PKCS#1 v1.5 Verify KAT, Cert# A1184
        ii. Firmware Integrity, RSAPKCS#1 v1.5 2048 Digital Signature, Cert# A1184
        iii. AES ECB Encrypt KAT, Cert# AES 3913
        iv. AES ECB Decrypt KAT, Cert# AES 3913
        v. SHA-256 KAT, Cert# SHS 2942
        vi. HMAC-SHA2-256 KAT, Cert# HMAC 2280
        vii. AES ECB Encrypt KAT, Cert# AES 3580
        viii. AES ECB Decrypt KAT, Cert# AES 3580
        ix. RSA 2048 PKCS#1 v1.5 Verify KAT, Cert# A1025
        x. Key Wrap KAT, KW-AE, Cert# A1025[20]
        xi. Key Wrap KAT, KW-AD, Cert# A1025[19]
        xii. DRBG KAT[21], Cert# A1025
        xiii. PBKDF2 KAT, Cert# A1025
        xiv. SP 800-90B Entropy Source Health Test
        xv. AES ECB Encrypt KAT, DEE, Cert# C1973
        xvi. AES ECB Decrypt KAT, DEE, Cert# C1973
    b. Conditional Tests
        i. The Cryptographic Module performs a Repetition Count Test and Adaptive Proportion Test on the ENT (P) entropy source. These entropy source health tests are executed each time the DRBG is reseeded at powered up and as the result of DRBG reseed event, which occurs after the DRBG consumes 2^{32} bits of seed data.
        ii. The Cryptographic Module performs a key comparison test on each LRK.AESKey/LRK.XTS keyset and its associated NSK.AESKey/NSK.XTS keyset to assure compliance with IG A.9 XTS-AES Key Generation Requirements.
        iii. Firmware Download Test, RSA 2048 PKCS#1 v1.5 (Cert# A1025), SHA-256 (Cert# SHS 2942)
7. An operator can command the Cryptographic Module to perform the power-up self-test by power cycling the module.
8. Power-up self-tests do not require operator action.
9. Data output is inhibited during key generation, self-tests, zeroization, and error states.
10. Status information does not contain CSPs or sensitive data that if misused, could compromise the Cryptographic Module.
11. The Zeroize service deletes all plaintext keys and CSPs.
12. The SoC Rebuild service deletes the Root Keyset and Global Active Keyset.
13. The Cryptographic Module does not support a maintenance role.
14. The Cryptographic Module does not support manual key entry.

[20] Utilizes AES-ECB-256 (Cert# AES 3913)

[21] The DRBG KAT is inclusive of the instantiate, generate and reseed function health tests required in [SP 800-90A]

15. The Cryptographic Module does not have any external input/output devices used for entry/output of data.
16. The Cryptographic Module does not output plaintext CSPs.
17. The Cryptographic Module does not output intermediate key values.
18. The Cryptographic Module does not support concurrent operators.
19. The Crypto Officer shall assure that all host issued Authority PINs are 32-bytes in length.

7.2 Initialization Instructions

The MSID value is set at manufacturing time by the storage device. It represents the default TCG Credential for the SID authority and the Locking SP Admin1 authority. This value is electronically readable, by the host, over the host interface.

During enrollment, the host reads the MSID value from the Cryptographic Module and uses it to authenticate and change TCG Credential values within the Cryptographic Module.

Having the MSID Credential value electronically available to the host constitutes a risk to the overall security of the Cryptographic Module. Therefore, as best practice, the host should execute a Take-Ownership scenario the first time the Cryptographic Module is inserted into a system.

Recommended Take-Ownership Scenario

1. StartSession to 'Admin SP'
    a. Get MSID
    b. Use the MSID to authenticate to the SID authority.
        i. An authentication failure indicates that a tamper event has occurred for the Cryptographic Module.
    c. Set the SID PIN to a new 32-byte value.
    d. Optional:
        i. Enable Admin SP Admin1.
        ii. Set the Admin SP Admin1 PIN to a non-MSID 32-byte value.
    e. Execute the TCG Activate command.
    f. EndSession
2. Optional:
    a. StartSession to 'Locking SP'
        i. Use the SID PIN established at step 1.c to authenticate to the Locking SP Admin1 authority.
        ii. Set the Locking SP Admin1 PIN to a new 32-byte value.
        iii. Enable Locking SP Admin2.
        iv. Set the Locking SP Admin2 PIN to a non-MSID 32-byte value.
        v. Repeat steps 2.a.iii and 2.a.iv for Locking SP Admin [3-4].
        vi. Enable Locking SP User1.
        vii. Set the Locking SP User1 PIN to a non-MSID 32-byte value.
        viii. Repeat steps 2.a.vi and 2.a.vii for Locking SP User [2-9].
    b. EndSession

If any of the above-mentioned steps fail, the Crypto Officer should remove the device from the system, as malicious behavior may have compromised the Cryptographic Module.

7.3 Zeroization Rules

The Crypto Officer shall use the Zeroize service, which utilizes the TCG Revert Method, to zeroize all CSPs, apart from the Root Keyset and the Global Active Keyset. After successfully executing the Zeroize service, the Crypto Officer should, as a best practice, power cycle the Cryptographic Module.

The SoC Rebuild service zeroizes and regenerates the Root Keyset and the Global Active Keyset. Executing this process exhausts an SoC life. The CM is inoperable when the life count reaches zero. The Crypto Officer shall assure that SoC Rebuild service is never execute unless necessary to protect the integrity of the Cryptographic Module.

8. Physical Security Policy

8.1 Mechanisms

The Cryptographic Module does not make claims in the Physical Security area beyond FIPS 140-2 Security Level 2.

- All components are production-grade materials with standard passivation.
- The Cryptographic Module enclosure is opaque and enclosed installed within the host system.
- Engineering design supports opacity requirements.
- Western Digital applies three (3) tamper-evident security seal during manufacturing. See Figure 2.
- The tamper-evident security seal cannot be penetrated or removed and reapplied without evidence of tampering. In addition, it is difficult to replicate the of tamper-evident security seal.

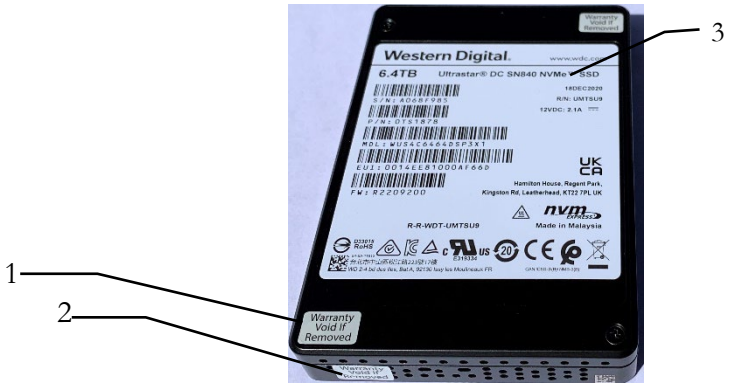

Figure 3: Tamper-Evident Seal

8.2 Operator Responsibility

The Crypto Officer and/or User shall inspect the Cryptographic Module enclosure at installation and at least once a year thereafter for evidence of tampering. See Figure 3: Tamper Evidence on Tamper Seal. If the inspection reveals evidence of tampering, the Crypto Officer should return the module to Western Digital.

Figure 4: Tamper Evidence on Tamper Seal

9. Mitigation of Other Attacks Policy

The Cryptographic Module lacks features to mitigate any specific attacks beyond the scope of the requirements within FIPS 140-2.

10. Definitions

- **Access Control Element:** A Boolean expression of authorities.
- **Access Control List**: A list of access control elements.
- **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. [SP800-131A]
- **Anybody**: A formal TCG term for an unauthenticated role [1].
- **Approved mode of operation**: A mode of the Cryptographic Module that employs only approved security functions. [FIPS140]
- **Approved**: [FIPS140] approved or recommended in a NIST Special Publication.
- **Authenticate**: Prove the identity of an Operator or the integrity of an object.
- **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 sensitive information is not disclosed to unauthorized parties.
- **Credential**: A formal TCG term for data used to authenticate an Operator [1].
- **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. [FIPS140]
- **Cryptographic Boundary**: An explicitly defined continuous perimeter that establishes the physical bounds of a Cryptographic Module and contains all the hardware, software, and/or firmware components of a Cryptographic Module. [FIPS140]
- **Cryptographic key (Key)**: An input parameter to an Approved cryptographic algorithm
- **Cryptographic Module**: The set of hardware, software, and/or firmware used to implement approved security functions contained within the cryptographic boundary. [FIPS140]
- **Crypto Officer**: An Operator performing cryptographic initialization and management functions. [FIPS140]
- **Data at Rest**: User data residing on the storage device media when the storage device is powered off.
- **Discovery**: A TCG method that provides the properties of the TCG device. [TCG Enterprise]
- **Drive Writes per Day (DWPD):** Drive Writes per Day defines how many times the entire capacity of the HDD can be overwrite every single day of its usable life without failure during the warranty period.
- **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.
- **Integrity**: A cryptographic property to assure sensitive data has not been modified or deleted 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. [FIPS140]
- **Internal RAM (IRAM): RAM memory that is internal to an SoC.**
- **Key Derivation Function (KDF)**: An Approved cryptographic algorithm by which one or more keys are derived from a shared secret and other information.

- **Key Encrypting Key (KEK)**: A cryptographic key used to encrypt or decrypt other keys.
- **Key management**: The activities involving the handling of cryptographic keys and other related security parameters during the entire life cycle of the Cryptographic Module. The handling of authentication data is representative of a key management activity.
- **Key Wrap**: An Approved cryptographic algorithm that uses a KEK to provide Confidentiality and Integrity.
- **LBA Range**: A formal TCG SWG [1] term that defines a contiguous logical block range (sequential LBAs) to store encrypted User Data; ranges 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 TCG credentials [1].
- **Method**: A remote procedure call to an SP that initiates an action on the SP [1].
- **Namespace:** A namespace is a collection of logical blocks that range from zero (0) to the capacity of the namespace.
- **Namespace Identifier (NSID):** A namespace identifier is an identifier used by a controller to provide access to a namespace.
- **OFS file**: OFS files are used to reset the Cryptographic Module's configuration back to its original factory setting during the Revert operations (e.g., TCG Revert).
- **Operator**: A consumer, either human or automation, of cryptographic services that is external to the Cryptographic Module. [FIPS140]
- **Personal Identification Number (PIN)**: A formal TCG term designating a string of octets used to authenticate an identity [1].
- **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. [FIPS140]
- **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 Zeroize 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**: Private data on the Storage Medium that is not accessible outside the Cryptographic Boundary.
- **Sanitize:** Sanitization cryptographically erases all user data in the NVM subsystem such that recovery of any previous user data from any cache, non-volatile media, or any controller memory buffer is not possible.
- **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. This key is injected at manufacturing time and a hash of this key is stored as OTP bits.
- **Security Identifier (SID)**: The authority that represents the TPer owner [1]. Crypto Officer serves in this role.
- **Security Provider (SP):** A TCG term used to define a collection of Tables and Methods with access control.
- **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 [1].
- **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 of a SED; it is partitioned into two disjoint sets, a User Data area, and a Reserved Area.
- **Table**: The basic data structures within a Security Provider (SP). The tables store persistent SP state data defined in TCG Storage Core specification [1].
- **TPer:** A Trusted Peripheral. The Trusted Peripheral (TPer) resides in a Storage Device. The TPer manages trusted storage-related functions and data structures as defined in TCG Storage Core specification [1].
- **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. [FIPS140]
- **Write Data**: An external request to transfer User Data to a SED. [SCSI Block]
- **Zeroize**: Invalidate a Critical Security Parameter. [FIPS140]

11. Key Words

The Key Words "SHALL", "SHALL NOT", "SHOULD," and "MAY" if used in this document are to be interpreted as described in [9].

12. Acronyms

- **ACL:** Access Control List
- **AEK:** Active Encryption Key
- **AES:** Advanced Encryption Standard (FIPS 197)
- **BLRE:** Boot Loader
- **CAC:** Cryptographic Assist Controller
- **CBC:** Cipher Block Chaining, an operational mode of AES
- **CM:** Cryptographic Module
- **CO**: Crypto Officer [FIPS140]
- **CRC**: Cyclic Redundancy Check
- **CSP**: Critical Security Parameter [FIPS140]
- **DEE:** Data Encryption Engine
- **DRAM**: Dynamic Random Access Memory
- **DRBG**: Deterministic Random Bit Generator
- **DW/D:** Drive Writes per Day
- **EDC:** Error Detection Code
- **EMI**: Electromagnetic Interference
- **FSEC:** Flash Security Data
- **FID:** Flash Internal Data
- **FIPS**: Federal Information Processing Standard
- **HDD**: Hard Disk Drive
- **IRAM: Internal RAM**
- **IV**: Initialization Vector
- **KAT**: Known Answer Test
- **KDF**: Key Derivation Function
- **LBA**: Logical Block Address
- **MEK**: Media Encryption Key
- **MSID**: Manufactured Security Identifier
- **NAND: N**egative AND, Flash Memory technology
- **NOR: N**egative OR, Flash Memory technology
- **NDRNG**: Non-deterministic Random Number Generator
- **NIST**: National Institute of Standards and Technology
- **NSID:** Namespace Identifier
- **NVM:** Non-volatile Memory
- **NVMe:** NVM Express

- **OFS:** Original Factory Setting
- **PBKDF2**: Password Base Key Derivation Function
- **PCIe:** Peripheral Component Interconnect Express
- **PIN**: Personal Identification Number
- **POR**: Power on Reset
- **PSID**: Physical Security Identifier
- **PSP**: Public Security Parameter
- **RID:** Reserved Area Internal Data
- **SAS**: Serial Attached SCSI
- **SECD:** Security Data
- **SED:** Self-Encrypting Drive
- **SCSI**: Small Computer System Interface
- **SD_CA**: Storage Device Certification Authority
- **SED**: Self Encrypting Drive
- **SFF:** HDD Form Factor or Small Form Factor
- **SID**: Security Identifier, The TCG authority representing the Cryptographic Module owner
- **SIO**: Serial Input/Output
- **SoC**: System-on-a-Chip
- **SP**: Security Provider or Security Partition (TCG), also Security Policy (FIPS 140)
- **SSC**: Subsystem Class
- **SSD**: Solid-state Drive
- **SWG**: Storage Work Group
- **TCG**: Trusted Computing Group
- **TLC:** Triple Level Cell
- **UEC:** Universal Error Code
- **XTS**: A mode of AES that utilizes "Tweakable" block ciphers

13. References

13.1 NIST Specifications

- [AES] Advanced Encryption Standard, FIPS PUB 197, NIST, November 2001
- [DSS] Digital Signature Standard, FIPS PUB 186-4, NIST, July 2013
- [FIPS140] Security Requirements for Cryptographic Modules, FIPS PUB 140-2, NIST, December 2002
- [HMAC] The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, July 2008
- [SHA] Secure Hash Standard (SHS), FIPS PUB 180-4, NIST, August 2015
- [SP800 38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST, December 2001
- [SP800 38E] Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, SP800-38E, NIST, January 2010
- [SP800 38F] Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, NIST, December 2012
- [SP800 57] Recommendation for Key Management – Part I General (Revision 4), NIST, January 2016
- [SP800 90A] Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revision 1), NIST, June 2015
- [SP800 90B] Recommendation for the Entropy Sources Used for Random Bit Generation, NIST, January 2018
- [SP800 131A] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (Revision 2), NIST, March 2019
- [SP800 132] Recommendation for Password-Based Key Derivation, NIST, December 2010
- [SP800 133] Recommendation for Cryptographic Key Generation (Revision 2), NIST, June 2020

13.2 Trusted Computing Group Specifications

- [1] TCG Storage Architecture Core Specification, Specification Version 2.01 Revision 1.00 (August 5, 2015)

- [2] TCG Storage Security Subsystem Class: Opal, Specification Version 2.01, Final Revision 1.00 (August 5, 2015)
- [3] TCG Storage Opal SSC Feature Set: PSID, Specification Version 1.00, Final Revision 1.00 (August 5, 2015)
- [4] TCG Storage Opal SSC Feature Set: Configurable Namespace Locking, Specification Version 1.00, Final Revision 1.33 (February 22, 2019)
- [5] TCG Storage Opal SSC Feature Set: Single User Mode, Specification Version 1.00, Final Revision 1.00 (February 24, 2012)
- [6] TCG Storage Opal Integration Guidelines, Version 1.00, Final Revision 1.00 (March 16, 2016)
- [7] TCG Storage Interface Interactions Specification (SIIS), Version 1.07, (January 30, 2018)
- [8] TCG Storage Security Subsystem Class: Ruby, Version 1.00, Revision 1.00 (January 7, 2020)

13.3 International Standards

- [9] IETF RFC 2119, 1997, "Key words for use in RFCs to Indicate Requirement Levels"
- [10] NVM Express™, Revision 1.3.c, May 24, 2018
- [11] NVM Express™ Management Interface, Revision 1.1, April 29, 2019
- [12] PCI Express® Base Specification, Revision 3.0, November 10 ,2010
- [13] SCSI Block Commands - 3, Revision 22, March 29, 2010
- [14] Security Features for SCSI Commands, Revision 2, September 25, 2015
- [15] SCSI Primary Commands - 5, Revision 22, April 19, 2019
- [16] Protocol Agnostic Multi-Lane High Speed Connector, Revision 1.3, February 19, 2020

13.4 Corporate Documents

- [Datasheet] Ultrastar DC SN840 Datasheet, 02-05-WW-04-00227-A05 (September 2020), https://www.westerndigital.com/support