SanDisk Technologies Inc

Ultrastar® DC SN650 BiCS5 NVMe® TCG Opal SSD, SED

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1
Date: 04/17/2026

Protection of Data at Rest

Table of Contents

1 – General 5
1.1 Overview 5
1.2 Security Levels 5
2 – Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 10
2.7 Algorithm Specific Information 14
2.8 RBG and Entropy 14
2.9 Key Generation 15
2.10 Key Establishment 16
2.11 Industry Protocols 16
3 Cryptographic Module Interfaces 17
3.1 Ports and Interfaces 17
4 Roles, Services, and Authentication 18
4.1 Authentication Methods 18
4.2 Roles 18
4.3 Approved Services 20
4.4 Non-Approved Services 60
4.5 External Software/Firmware Loaded 60
5 Software/Firmware Security 61
5.1 Integrity Techniques 61
5.2 Initiate on Demand 61
6 Operational Environment 62
6.1 Operational Environment Type and Requirements 62
6.2 Configuration Settings and Restrictions 62
7 Physical Security 63
7.1 Mechanisms and Actions Required 63
8 Non-Invasive Security 64
8.1 Mitigation Techniques 64
9 Sensitive Security Parameters Management 65

9.1 Storage Areas 65
9.2 SSP Input-Output Methods 65
9.3 SSP Zeroization Methods 65
9.4 SSPs 67
10 Self-Tests 88
10.1 Pre-Operational Self-Tests 88
10.2 Conditional Self-Tests 88
10.3 Periodic Self-Test Information 90
10.4 Error States 90
10.5 Operator Initiation of Self-Tests 91
11 Life-Cycle Assurance 92
11.1 Installation, Initialization, and Startup Procedures 92
11.2 Administrator Guidance 93
11.3 Non-Administrator Guidance 93
11.4 Design and Rules 93
11.5 Maintenance Requirements 94
11.6 End of Life 95
12 Mitigation of Other Attacks 96
References and Definitions 97
NIST Specifications 97
Trusted Computing Group Specifications 97
NVMe and PCIe Specifications 98
Corporate References 98
Other References 98
Definitions 99
Acronyms 102

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 7
Table 3: Modes List and Description 8
Table 4: Approved Algorithms 9
Table 5: Vendor-Affirmed Algorithms 10
Table 6: Security Function Implementations 13
Table 7: Entropy Certificates 14
Table 8: Entropy Sources 14
Table 9: Ports and Interfaces 17
Table 10: Authentication Methods 18
Table 11: Roles 19
Table 12: Approved Services 60
Table 13: Mechanisms and Actions Required 63
Table 14: Storage Areas 65
Table 15: SSP Input-Output Methods 65
Table 16: SSP Zeroization Methods 67
Table 17: SSP Table 1 75
Table 18: SSP Table 2 87
Table 19: Pre-Operational Self-Tests 88
Table 20: Conditional Self-Tests 89
Table 21: Pre-Operational Periodic Information 90
Table 22: Conditional Periodic Information 90
Table 23: Error States 91

List of Figures

Figure 1 - Security Subsystem Components 6
Figure 2 - Ultrastar® DC SN650, EDSFF-L-9.5mm 7
Figure 3 - Symmetric Key Tree 15
Figure 4 - Asymmetric Key Tree 61

1 – General

The Security Policy is non-proprietary.

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Ultrastar® DC SN650 BiCS5, NVMe® TCG Opal SSD, SED. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

1.2 Security Levels

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

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

Table 1: Security Levels

2 – Cryptographic Module Specification

2.1 Description

Module Type: Hardware

Description - The Ultrastar® DC SN650BiCS5 NVMe® TCG Opal SDD, SED, hereafter referred to as Ultrastar® DC SN650, Cryptographic Module, cryptographic module, or CM is a self-encrypting drive (SED) that complies in general with the specifications listed in 13.2 Trusted Computing Group Specifications and specifically with the TCG Storage Architecture Core Specification [TCG Core] and Trusted Computing Group) Storage Security Subsystem Class: Opal Specification (TCG Storage SSC: Opal) [TCG Opal].

The TCG Storage SSC: Opal specification defines a management interface for a host application to activate, provision, and manage encryption of user data. The specification includes data structures, 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.

Figure 1 illustrates a logical view of the top-level firmware components that constitute the security subsystem. The Security Core is the most secure portion of the security subsystem. It forms a security boundary that provides assurances for firmware integrity, SSP integrity, and data-at-rest security within the CM. The Security Protocol and Services ring contains the TCG Storage SSC: Opal security protocol. Components in this ring communicate to the security core using a Security Core API. The rest of the Cryptographic Module's firmware resides in the Security Application Client ring. The security application client firmware, collectively known as the "Base FW", interfaces with the Security Protocol and Services Layer. The Host system communicates with the Cryptographic Module through the Security Application Client layer.

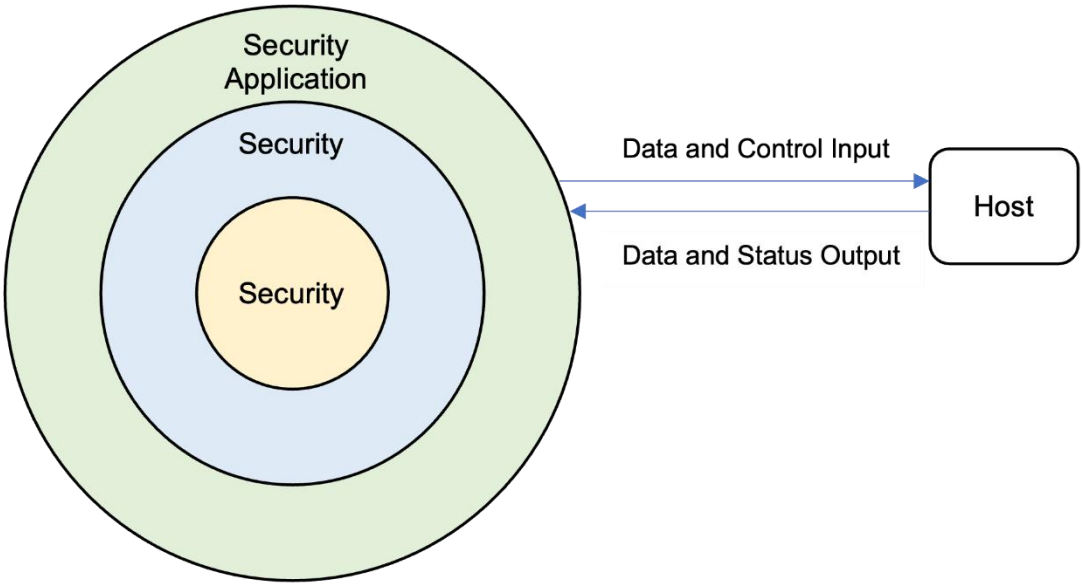

Figure 1 - Security Subsystem Components

Purpose - 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 within solid-state memory devices within the CM. The operator of the Cryptographic Module interfaces with the Cryptographic Module through applications that reside within a host system.

- Module Type - Hardware
- Module Embodiment - Multi-chip embedded.
- 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 FE2-PG4 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.
- Diagram, Schematic, or Photograph - Figure 2 below is representative of all Cryptographic Modules within the scope of this validation. The hard opaque surface of the enclosure defines the cryptographic boundary. All components within this boundary satisfy FIPS 140-3 requirements.

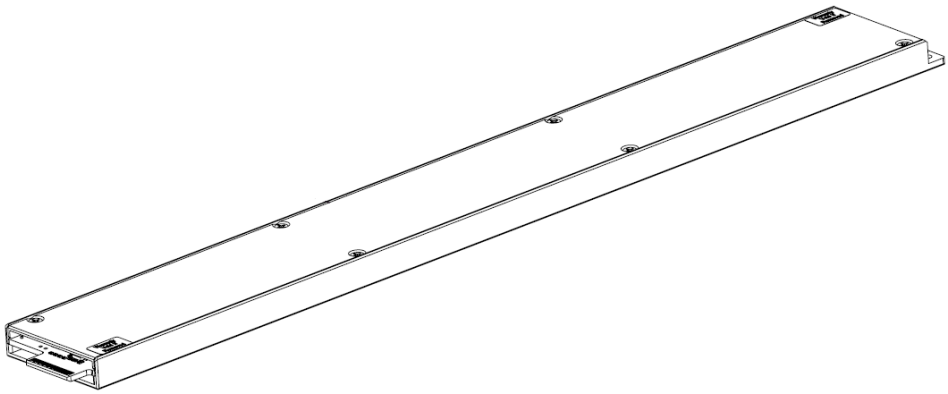

Figure 2 - Ultrastar® DC SN650, EDSFF-L-9.5mm

Module Embodiment: Multi-Chip Embedded

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

The Ultrastar® DC SN650 cryptographic module was tested on the following operational environment.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
WUS5BB1A1E9ELE8	0TS2411	RA210003	ARM Cortex-M3, ARM Cortex-A53, ARM Cortex-R5	N/A

Table 2: Tested Module Identification – Hardware

The Cryptographic Module operates within a limited operational environment. When 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 non-modifiable. If the download operation is successful, authorized, and verified, the Cryptographic Module begins operating with the new code working set after successfully executed all required pre-operational self-tests that comply with ISO 19790 7.10.2.2. 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 CM only supports CMVP 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 the Security Application Client firmware (aka Base 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 secured by a root key stored in HW RoT OTP bits.
4. Support for HW based Symmetric Key Generation
5. Cryptographic Algorithm Acceleration
6. End-to-End Protect between ACM & Key Server

2.3 Excluded Components

The Cryptographic Module does not have excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
isFIPS	The cryptographic module is operating as a FIPS 140-3 compliant module	Approved	1. The Level 0 Discovery service returns a value of 1 from the in FIPS global indicator data field and 2. The Firmware Download Control LockOnReset field is set to PowerCycle and 3. The LockOnReset attribute for each configured Locking SP User is set to PowerCycle .

Table 3: Modes List and Description

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 SL1 compliant module. The Crypto Officer is responsible for assuring that the mandatory configuration requirements remain unchanged. When correctly configured, the Cryptographic Module always powers up isFIPS mode.

The Cryptographic Module does not support non-approved or non-allowed security functions.

Mode Change Instructions and Status :

The table above specifies the conditions that must be true for the Cryptographic Module to operate in isFIPS mode. Any action by the operator that results in the negation of the Firmware Download Control's lock on PowerCycle setting transitions the CM to a noncompliant state. Any action by the operator that negates the Locking SP User attribute settings, specified the "Modes List and Description" Table above for LockOnReset, ReadLockEnabled, or WriteLockEnabled transitions the CM to a noncompliant state.

2.5 Algorithms

Approved Algorithms

The Module implements the FIPS Approved cryptographic algorithms listed the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	AES 3580	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A3410	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	AES 3580	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-KWP	A3374	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
AES-XTS Testing Revision 2.0	A3410	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38E
Counter DRBG	A3374	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
HMAC-SHA2-256	HMAC 2280	-	FIPS 198-1
PBKDF	A3374	Iteration Count - Iteration Count: 2-1024 Increment 1 Password Length - Password Length: 32	SP 800-132
RSA SigVer (FIPS186-4)	A3374	Signature Type - PKCS 1.5 Modulo - 2048	FIPS 186-4
RSA SigVer (FIPS186-4)	A3375	Signature Type - PKCS 1.5 Modulo - 2048	FIPS 186-4
SHA2-256	SHS 2942	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms

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

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

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed

N/A for this module.

Non-Approved, Not Allowed Algorithms

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Authority_Digest_Generation	MAC SHA	Generates an HMAC message digest of an Authentication Credential PIN	Publication:[FIPS 198-1] [IG10.3.A]	HMAC-SHA2-256: (HMAC 2280)
Authority_Digest_Verification	MAC SHA	Verifies the HMAC digest of an Authentication Credential PIN.	Publication:[FIPS 198-1] [IG 10.3.A]	HMAC-SHA2-256: (HMAC 2280)
Decryption	BC-UnAuth	Decrypts objects	Publication:[FIPS 197] [SP 800-38A] [IG 10.3.A]	AES-CBC: (AES 3580) Key Size: : 256 Key Strength:: 256 bits
Derived_Key_Generation	PBKDF	Generates derived	Publication:[SP 800-132] [IG 10.3.A] [IG D.N]	PBKDF: (A3374) HMAC-

Name	Type	Description	Properties	Algorithms
		authority keys Ka and Ku	[FIPS 198-1] [IG 10.3.A]	SHA2-256: (HMAC 2280)
Digest_Generation	SHA	Generates message digest	Publication:[FIPS 180-4] [IG 10.3.A] [IG C.B]	SHA2-256: (SHS 2942)
Digest_Verification	SHA	Verifies a message digest	Publication:[FIPS 180-4] [IG 10.3.A] [IG C.B]	SHA2-256: (SHS 2942)
Encryption	BC-UnAuth	Encrypts objects	Publication:[FIPS 197] [SP 800-38A] [IG 10.3.A]	AES-CBC: (AES 3580) Key Size: 256 Key Strength: 256 bits
FW_Authenticity	DigSig-SigVer SHA	Verifies the authenticity of a firmware image	Publication:[FIPS 186-4] [IG C.F] [FIPS 180-4] [IG 10.3.A] [IG C.B]	RSA SigVer (FIPS186-4): (A3374) SHA2-256: (SHS 2942)
FW_Integrity	DigSig-SigVer SHA	Verifies the integrity of a firmware image	Publication:[FIPS 186-4] [IG C.F] [FIPS 180-4] [IG 10.3.A] [IG C.B]	RSA SigVer (FIPS186-4): (A3375) SHA2-256: (SHS 2942)
Key Wrap	BC-Auth	Key Wrapping Key Unwrapping	Publication:[SP 800-38F] [IG D.G] [FIPS 197] [IG 10.3.A]	AES-KWP: (A3374) AES-ECB: (AES 3580) Key Size:: 256 Key Strength:: 256 bits
Keyed_Digest_Generation	MAC SHA	Generates an HMAC message digest to sign encrypted SSPs	Publication:[FIPS 198-1] [IG 10.3.A]	HMAC-SHA2-256: (HMAC 2280)
Keyed_Digest_Verification	MAC SHA	Verifies the HMAC message digest signature of	Publications:[FIPS 198-1] [IG 10.3.A]	HMAC-SHA2-256: (HMAC 2280)

Name	Type	Description	Properties	Algorithms
		an encrypted SSPs		
MEK Generation	BC-Auth	XOR of LRK and NSK	Publication:[IG C.I]	AES-XTS Testing Revision 2.0: (A3410) Payload Length:: 4096 - 32768 Increment: : 128 Tweak mode: Number Key Size: 256 Key Strength: 256 bits AES-ECB: (A3410) Key Size: : 256 Key Strength: 256 bits
RBG	DRBG	Random number generator	Publication:[SP 800-90A] [IG 10.3.A] [IG D.L] [IG D.R]	Counter DRBG: (A3374)
RBG Seeding	DRBG ENT-ESV	Seeds DRBG with entropy data	Publication:[SP 800-90B] [IG 9.3.A] [IG 10.3.A] [IG D.J] [IG D.K]	Counter DRBG: (A3374)
SecureLoader _ Integrity	DigSig-SigVer SHA	Verifies the integrity of the Secure Loader firmware image	Publication:[FIPS 186-4] [IG C.F] [FIPS 180-4] [IG 10.3.A] [IG C.B]	RSA SigVer (FIPS186-4): (A3374) SHA2-256: (SHS 2942)
User_Data_Decryption	BC-UnAuth	LBA data decryption	Publication:[FIPS 197] [SP 800-38E] [IG 10.3.A] [IG C.I]	AES-XTS Testing Revision 2.0: (A3410) Payload

Name	Type	Description	Properties	Algorithms
				Length:: 4096 - 32768 Increment:: 128 Tweak Mode:: Number Key Size: 256 Key Strength:: 256 bits AES-ECB: (A3410) Key Size: 256 Key Strength: 256 bits
User_Data_Encryption	BC-UnAuth	LBA data encryption	Publication:[FIPS 197] [SP 800-38E] [IG 10.3.A] [IG C.I]	AES-XTS Testing Revision 2.0: (A3410) Payload Length: 4096 - 32768 Increment:: 128 Tweak Mode:: Number Key Size:: 256 Key Strength:: 256 bits AES-ECB: (A3410) Key Size: 256 Key Strength: 256 bits

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES-XTS Key Pair Generation

The Cryptographic Module performs a key comparison test on each LRK.AESKey/LRK.XTS 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 using AES-KWP (Cert. #A3374).
The PBKDF2 password 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. The paragraphs titled Entropy Information and RBG Information summarize the characteristics of the entropy noise source that resides within the cryptographic boundary and seeds the CTR_DRBG.

Cert Number	Vendor Name
E5	Western Digital Corporation

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
ESV, E5	Physical	20-82-10047-A1, Tested Assy, IC, Thunderbird FE2-PG4, Rev A1, ARM Cortex M3, ARM Cortex-R5	32 bits	2.69	None

Table 8: Entropy Sources

Entropy Information

The hardware-based ring oscillator noise source referenced in the "Entropy Sources" Table consists 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 FE2-PG4 ASIC. No configuration steps are necessary to operate the entropy source in a compliant manner. As stated in the Public Use Document for E5, on power up the Cryptographic Module executes an entropy source initialization sequence that collects sufficient samples of raw noise to verify the health of the entropy noise source prior to seeding the RBG. 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 in the "Entropy Sources" Table consists of the raw data generate from thirty-two (32) free running ring oscillators. Eight (8) identical groups of four (4) variable length inverter chains define the implementation. Each 32-bit sample produces at least 2.69 bits of entropy. Each time the CTR_DRBG is instantiated or reseeded, one hundred sixty (160) 32-bit samples are concatenated to seed the CTR_DRBG. This equates to 5120 bits of entropy data and translates to at least 430 bits of min-entropy. This seeds the CTR_DRBG with approximately 287 bits of security strength (~287 bits of entropy input and ~143 bits of nonce). Seeding the DRBG with at least 287 bits of security strength exceeds the requirement to seed the CTR_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 key 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

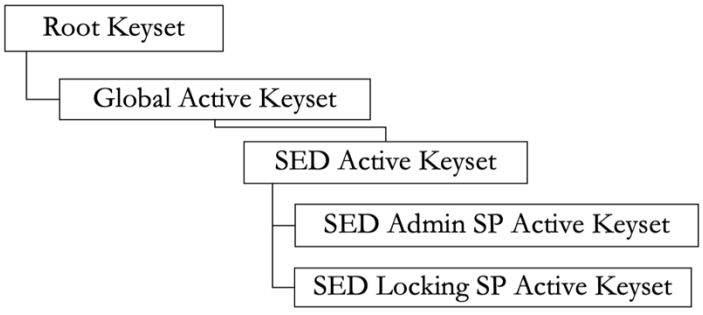

Figure 3 - Symmetric Key Tree

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: Opal [TCG Opal] security protocol.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

As a hardware module, the Cryptographic Module uses the EDSFF connector that conforms to the mechanical requirements within SFF-TA-1002 [SFF-8639]. The following table identifies the Cryptographic Module's ports and interfaces. The three-wire UART serial port connector consists of UART_TX, UART_RX, and ground.

The NVMe protocol provides the primary communication channel between the Cryptographic Module and the Host. The NVM Express® NVM Command Set Specification [NVMe Command] defines the format of input data and control information sent from the Host to the CM. Services provided by the Cryptographic Module that require the processing of Host issued commands include TCG Storage SSC: Opal 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 the operator.

Physical Port	Logical Interface(s)	Data That Passes
EDSFF connector	Control Input	Operator issued NVMe commands [12]
UART Connector	Control Input	Operator issued NVMe commands [12]
EDSFF connector	Data Input	User data and firmware update images are transmitted from the operator to the Cryptographic Module.
UART Connector	Data Input	User data and firmware update images are transmitted from the operator to the Cryptographic Module.
EDSFF connector	Data Output	User data is transmitted from the Cryptographic Module to the operator
UART Connector	Data Output	User data is transmitted from the Cryptographic Module to the operator
EDSFF connector	Status Output	Status data is transmitted from the CM to the operator
UART Connector	Status Output	Status data is transmitted from the CM to the operator
EDSFF connector	Power	Power connector

Table 9: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

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

Table 10: Authentication Methods

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

4.2 Roles

The 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 does not support concurrent operators. The Cryptographic Module enforces role dependent service access rules. Section 4.3 maps services to Crypto Officer and User roles. Access Control is implemented 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. When an authority is authenticated, its associated ACE boolean expression is set to be True. If the authority has not been authenticated, its 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 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.

Name	Type	Operator Type	Authentication Methods
Admin SP Admin1	Role	CO	Role-based Authentication - Credential PIN Authentication
Admin SP Maintenance	Role	Maintenance	Role-based Authentication - Credential PIN Authentication
SID	Role	CO	Role-based Authentication - Credential PIN Authentication
Anybody	Role	User	None
Locking SP Admin	Role	CO	Role-based Authentication - Credential PIN Authentication
Locking SP User	Role	CO	Role-based Authentication - Credential PIN Authentication
NVMe User	Role	User	Role-based Authentication - Credential PIN Authentication

Table 11: Roles

The CM supports both Crypto Officer (CO) and User roles. Except for the Anybody Authority, operators must authenticate to the corresponding TCG Authority to assume a Crypto Officer, User or Maintenance role.

- Crypto Officer Roles
  - Secure ID (SID)
    - This Crypto Officer role corresponds to the TPer owner within the Admin SP Authority as defined in the TCG Storage Security Subsystem Class: Opal Specification [TCG Opal].
  - Admin SP Admin1
    - This Crypto Officer role corresponds to the Admin SP Admin1 authority defined in the TCG Storage Security Subsystem Class: Opal Specification [TCG Opal].
  - Locking SP Admin

        - This Crypto Officer role corresponds to the Locking SP Admin Authority as defined in the TCG Storage Security Subsystem Class: Opal Specification [TCG Opal]. The Cryptographic Mode supports up to four (4) Locking SP Admin authorities.
    - Locking SP User
        - This Crypto Officer role corresponds to the Locking SP User Authority as defined in the TCG Storage Security Subsystem Class: Opal Specification [TCG Opal]. The Cryptographic Mode supports up to ten (10) Locking SP User authorities.
- User Roles
    - NVMe User
        - This Crypto Officer role utilizes the NVM Express™ (NVMe™) interface protocols, which are designed to provide an efficient peer-to-peer communication link, for a Host to send commands to the Cryptographic Module and receive responses. Authentication to the SID authenticates the Drive Owner to the Crypto Officer role. The NVMe User may execute services that were previously enabled by another authenticated role.
    - Anybody
        - This user role corresponds to the Locking SP Anybody Authority as defined in the TCG Storage Security Subsystem Class: Opal Specification [TCG Opal]. As specified in the TCG Storage Architecture Core Specification [TCG Core], the Anybody authority is always considered "authenticated" within a session, even if the Anybody authority was not specifically called out during session startup. The Anybody authority executes services that do not require authentication or were previously enabled by an authenticated role.
- Maintenance Role
    - Admin SP Maintenance

For error injection purposes, the SID authenticates to the Admin SP Maintenance authority, enables the error injection service, and issues Vendor Unique Commands to determine if the CM report the correct Device Panic status data. Prior to authenticating to the Admin SP Maintenance role, the Crypto Officer shall execute Revert to zeroize all SSPs. After disabling the error injection service, the Crypto Officer shall execute Revert to zeroize all SSPs. Power cycling the Cryptographic Module automatically negates authentication to Admin SP Maintenance authority and disables the error injection service. While authenticated to the Admin SP Maintenance authority, modification of the operational environment is blocked.

4.3 Approved Services

The following table lists approved services implemented by the Cryptographic Module.

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

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W =Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.

- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Activate	Activate, is an Opal SSC [2] specific method that allows the TPer owner to "turn on" a Security Provider created in manufacturing.	isFIPS mode is true	5.1.1 Activate - Admin Template SP Object Method [2] 3.1.1 Activate [8]	Success or UEC failure code	Authority_Digest_Generation Derived_Key_Generation Encryption Key Wrap Keyed_Digest_Generation MEK Generation RBG RBG Seeding User_Data_Decryption	SID - Admin SP Admin1 PIN Digest: G,E - DRBG.Key: G,E - DRBG.V: G,W,E - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): G - Admin Authority Key (Ka): G,E - Non-Admin Authority Key (Ku) (Locking SP User unique): G,E - Locking Range Keyset (LRK) LRK.AES Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						LRK.XTS Key (Locking SP User unique): G,E - Range Access Key (RAK) (Locking SP User unique): G,E - User Access Key (UAK) (Locking SP User unique): G,E - User Management Key (UMK): G,E - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique): G,E - SED Volatile Encryption Key: G,W,E - SED Volatile Signing

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,W,E - Locking SP User [1-10] PIN: Z - Admin SP Admin1 PIN: E - SED AdminSP Encryption Key: E - SED AdminSP Signing Key: E - DRBG.Seed: E - Anybody User Access Key (UAKa): G
Activate, Single User Mode [5]	Activate, is an Opal SSC [2] specific method that allows the TPer owner to "turn on" a Security Provider created in manufacturing.	isFIPS mode is true	See 3.1.2.1 Activate [5]	Success or UEC failure code	None	SID - Admin SP Admin1 PIN Digest: G,W,E - DRBG.Key: G,E - DRBG.V: G,E - DRBG.Seed: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authenticate PSID	PSID character string authentication	isFIPS mode is true	PSID	Success or UEC failure code	Decryption Keyed_Digest_Verification	SID - PSID: E,W - SED Active Encryption Key: E - SED Active Signing Key: E - PSID Digest: E Anybody - PSID: E,W - SED Active Encryption Key: E - SED Active Signing Key: E - PSID Digest: E
Authenticate TCG Authority	Authentication Credential authentication	isFIPS mode is true	Authentication Credential PIN	Success or UEC failure code	Authority_Digest_Verification	SID - Admin SP Admin1 PIN: W,E - Admin SP Admin1 PIN Digest: E - Admin SP Maintenance PIN: W,E - Admin SP Maintenance PIN Digest: E - Locking SP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Admin [1-4] PIN: W,E - Locking SP Admin [1-4] PIN Digest: E - Locking SP User [1-10] PIN: W,E - Locking SP User [1-10] PIN Digest: E - SED Active Signing Key: E Admin SP Admin1 - SID PIN: W,E - SID PIN Digest: E - Locking SP Admin [1-4] PIN: W,E - Locking SP Admin [1-4] PIN Digest: E - Locking SP User [1-10] PIN: W,E - Locking SP User [1-10] PIN Digest: E - SED

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Active Signing Key: E Admin SP Maintenance - SID PIN: W,E - SID PIN Digest: E - Admin SP Admin1 PIN: W,E - Admin SP Admin1 PIN Digest: E - Locking SP Admin [1-4] PIN: W,E - Locking SP Admin [1-4] PIN Digest: E - Locking SP User [1-10] PIN: W,E - Locking SP User [1-10] PIN Digest: E - SED Active Signing Key: E Locking SP Admin - SID PIN: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SID PIN Digest: E - Admin SP Admin1 PIN: W,E - Admin SP Admin1 PIN Digest: E - Locking SP Admin [1-4] PIN: W,E - Locking SP Admin [1-4] PIN Digest: E - Locking SP User [1-10] PIN: W,E - Locking SP User [1-10] PIN Digest: E - SED Active Signing Key: E Locking SP User - SID PIN: W,E - SID PIN Digest: E - Admin SP Admin1 PIN: W,E - Admin SP Admin1 PIN

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Digest: E - Locking SP Admin [1-4] PIN: W,E - Locking SP Admin [1-4] PIN Digest: E - Locking SP User [1-10] PIN: W,E - Locking SP User [1-10] PIN Digest: E - SED Active Signing Key: E Anybody - SID PIN: W,E - SID PIN Digest: E - Admin SP Admin1 PIN: W,E - Admin SP Admin1 PIN Digest: E - Locking SP Admin [1-4] PIN: W,E - Locking SP Admin [1-4] PIN Digest: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Locking SP User [1-10] PIN: W,E - Locking SP User [1-10] PIN Digest: E - SED Active Signing Key: E
BootFlashIntegrity	An RSA digital signature verifies the authenticity of a binary firmware image.	isFIPS mode is true	RSA 2048 PKCS1 v1.5 signed firmware image	Success or UEC failure code	SecureLoader _ Integrity	Unauthenticated - Storage Device Certification Authority Key (SD_CA Key): E
Error Injection	This service allows the operator to test the CM's adverse condition response by injected an error condition.	isFIPS mode is true	See §4.11 [17]	See §4.11 [17]	Authority_Digest _Verification	SID - SID PIN: E,W - SID PIN Digest: E - SED Active Signing Key: E Admin SP Maintenance - Admin SP Maintenance PIN: E,W - Admin SP Maintenance PIN Digest: E - SED Active

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Key: E
FIPS 140 Compliance Descriptor (Show Version)	This service reports the FIPS 140 revision as well as the Cryptographic Module's overall security level, hardware revision, firmware revision and module name.	isFIPS mode is true	Security Protocol IN (0x0, 0x2, 0x2)	FIPS 140 Compliance Descriptor table data or UEC failure code	None	NVMe User
Firmware Download	ADigital signature verification of a binary firmware image.	isFIPS mode is true	RSA 2048 PKCS1 v1.5 signed firmware image	Success or UEC failure code	FW_Authenticity	SID - OEM Firmware Key (OEM FW Key): E - Product Group Key (PROD GROUP Key): E
Firmware Download Control	Enable or disable access to the Firmware Download service	isFIPS mode is true	FW_DOWNLOAD_PORT bit within the AdminSP Logical Port Table	Success or UEC failure code	None	SID
Firmware Integrity	An RSA digital signature verifies	isFIPS mod	RSA 2048 PKCS1 v1.5 signed	Success or UEC	FW_Integrity	Unauthenticated - OEM Firmware

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the authenticity of a binary firmware image.	e is true	firmware image	failure code		Key (OEM FW Key): E - Security Core Firmware Key (SC_FW Key): E - Security Protocol Firmware Key (SP_FW Key): E - OEM Original Factory State Key (OEM_OFS Key): E - Storage Device Boot FW Key (SD_BFW Key): E - Storage Device Certification Authority Key (SD_CA Key): E
Format_NVM_SecureErase	Cryptographic zeroization of user data..	isFIPS mode is true	See §5.23, §5.24 [10], §4.1.2 [12]	Success or UEC failure code	Keyed_Digest_Generation MEK Generation RBG RBG Seeding User_Data_Encryption	NVMe User - DRBG.Key: G,E - DRBG.V: G,E -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique): G,E,Z - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): G,Z - Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique): E - Global Active Encryption Key (AEK): E - Global Active

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Key: E
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	Anybody - DRBG.Key: G,E - DRBG.V: G,E
Get	Reads data structure; access control enforcement occurs per data structure field	IsFIPS global indicator =1	See §5.3.3.6 Basic Table Method Group - Get (Table and Object Method) [1]	Get method table data	Decryption Keyed_Digest_Verification	Anybody - MSID: R
Get DataStore	Read a stream of bytes from unstructured storage	isFIPS mode is true	See §3.2.13.9 Read data from the DataStore table [7]	DataStore plaintext data or UEC failure code	None	Anybody
Get Range Attributes	Returns the data stored in the Locking SP table for an LBA Range	isFIPS mode is true	Band_UID [12]	Range attribute data	None	Anybody Locking SP User
Level 0 Discovery	TCG 'Level 0 Discovery' discloses	isFIPS mode is true	See §3.3.6 Level 0 Discovery, §3.3.6.2 IF-	Level 0 Discovery Response	None	Anybody

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	basic configuration data about the Cryptographic Module, both current and potential		RECV Command [1]	data See §3.3.6 Level 0 Discovery [1]		
Locking SP User Password Update	Allows Locking SP Admins to update the PIN of a user that in not in Single User Mode	isFIPS mode is true	Locking SP UserPIN	Success or UEC failure code	Authority_Digest _Generation Decryption Derived_Key_Generation Encryption Keyed_Digest_Generation RBG	Locking SP Admin - DRBG.Key: G,E - DRBG.V: G,E - KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User): G - Locking SP User [1-10] PIN: W - User Access Key (UAK) (Locking SP User unique): E - User Manage

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ment Key (UMK): E - Non-Admin Authority Key (Ku) (Locking SP User unique): E
Reactivate	In Single User Mode, the reactivate service allows the hostoperator 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.	isFIPS mode is true	See §3.1.1.1 Reactivate [5] and §3.1.1 Reactivate [8]	Success or UEC failure code	None	Locking SP Admin - Admin Authority Key (Ka): G,E - Non-Admin Authority Key (Ku) (Locking SP User unique): G,E - Locking SP Admin [1-4] PIN Digest: G - SED Active Encryption Key: E - SED Active Signing Key: E - SED LockingSP Signing Key: E - SED Volatile Encryption Key: E - SED

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Volatile Signing Key: E - Range Access Key (RAK) (Locking SP User unique): E - User Access Key (UAK) (Locking SP User unique): E - User Management Key (UMK): E - Locking SP Admin [1-4] PIN: W
Read User Data	Reads ciphertext from a specified LBA range and outputs the user data as plaintext.	isFIPS mode is true	See §3.2.4 Read Command [12]	Plaintext user data or UEC failure code	User_Data_Decryption	NVMe User - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): E
Reset Module	Power on Reset	isFIPS	None	Drive Ready	Derived_Key_Generation	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		mode is true		Indicator or UEC failure code	Encryption Key Wrap RBG RBG Seeding	- DRBG.Key: G,E - DRBG.V: G,E - ESV: G - SED Volatile Encryption Key: G - SED Volatile Signing Key: G - User Access Key (UAK) (Locking SP User unique): G - User Management Key (UMK): G
Revert	The TCG 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 Key Wrap Keyed_Digest_Generation MEK Generation RBG	SID - SID PIN Digest: G,Z - Admin SP Admin1 PIN Digest: G,Z - DRBG.Key: G,E - DRBG.V: G,E - Global Active Signing Key: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SED Active Encryption Key: G,Z - SED Active Signing Key: G,Z - SED AdminSP Encryption Key: G,Z - SED AdminSP Signing Key: G,Z - SED LockingSP Encryption Key: G,Z - SED LockingSP Signing Key: G,Z - SED Volatile Encryption Key: G,Z - SED Volatile Signing Key: G,Z - PSID: W - Locking SP Admin [1-4] PIN Digest: G,Z - Global Active

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key (AEK): G,E,Z - Locking SP User [1-10] PIN Digest: G,E,Z - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): G,E,Z - Admin Authority Key (Ka): G,E,Z - Non-Admin Authority Key (Ku) (Locking SP User unique): G,E,Z - Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						SP User unique): G,E,Z - Range Access Key (RAK) (Locking SP User unique): G,E,Z - User Access Key (UAK) (Locking SP User unique): G,E,Z - User Management Key (UMK): G,E,Z - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique): G,E,Z - Root Encryption Key: G,E,Z - Root Signing Key: G,E,Z - MSID: E - MSID

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Digest: E Anybody - SID PIN Digest: G,Z - Admin SP Admin1 PIN Digest: G,Z - Locking SP Admin [1-4] PIN Digest: G,Z - Locking SP User [1-10] PIN Digest: G,Z - DRBG.Key: G,E - DRBG.V: G,E - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): G,Z - Admin Authority

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key (Ka): G,E,Z - Non-Admin Authority Key (Ku) (Locking SP User unique): G,E,Z - Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique): G,E,Z - Range Access Key (RAK) (Locking SP User unique): G,E,Z - User Access Key (UAK) (Locking SP User unique): G,E,Z - User Management Key (UMK): G,E,Z - Namespace Keyset (NSK)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						NSK.AES Key NSK.XTS Key (Locking SP User unique): G,E,Z - Root Encryption Key: G,E,Z - Root Signing Key: G,E,Z - Global Active Encryption Key (AEK): G,E,Z - Global Active Signing Key: G,E,Z - SED Active Encryption Key: G,Z - SED Active Signing Key: G,E,Z - SED AdminSP Encryption Key: G,E,Z - SED LockingSP Encryption Key: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SED LockingSP Signing Key: G,E,Z - SED Volatile Encryption Key: G,E,Z - SED Volatile Signing Key: G,E,Z - PSID: W - MSID: E - MSID Digest: E
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 [2]	Drive Ready Indicator or UEC failure code	Encryption Key Wrap Keyed_Digest_ Generation MEK Generation RBG	Anybody - SID PIN Digest: G,Z - Admin SP Admin1 PIN Digest: G,Z - Locking SP Admin [1-4] PIN Digest: G,Z - Locking SP User [1-10] PIN Digest: G,Z - DRBG.Key: G,E -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG.Seed: G,E - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): G,E,Z - Non-Admin Authority Key (Ku) (Locking SP User unique): G,E,Z - Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique): G,E,Z - Range Access Key (RAK) (Locking SP User unique): G,E,Z - User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Access Key (UAK) (Locking SP User unique): G,E,Z - User Management Key (UMK): G,E,Z - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique): G,E,Z - Root Encryption Key: G,E,Z - Root Signing Key: G,E,Z - Global Active Encryption Key (AEK): G,E,Z - Global Active Signing Key: G,E,Z - SED Active Encryption Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E - SED Active Signing Key: G,E,Z - SED AdminSP Encryption Key: G,E,Z - SED AdminSP Signing Key: G,E,Z - SED LockingSP Encryption Key: G,E,Z - SED LockingSP Signing Key: G,E,Z - SED Volatile Encryption Key: G,E,Z - SED Volatile Signing Key: G,E,Z - SID PIN: E - Admin SP Admin1 PIN: E - Locking SP Admin [1-4] PIN:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - Locking SP User [1-10] PIN: E - MSID: E - MSID Digest: E SID - SID PIN Digest: G,Z - Admin SP Admin1 PIN Digest: G,Z - Locking SP Admin [1-4] PIN Digest: G,Z - Locking SP User [1-10] PIN Digest: G,Z - DRBG.Key: G - DRBG.Seed: G - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XT

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						S Tweak Key (16 total - 1 per LBA range): G,Z - Admin Authority Key (Ka): G,E,Z - Non-Admin Authority Key (Ku) (Locking SP User unique): G,E,Z - Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique): G,E,Z - Range Access Key (RAK) (Locking SP User unique): G,E,Z - User Access Key (UAK) (Locking SP User unique): G,E,Z - User Manage

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ment Key (UMK): G,E,Z - Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique): G,E,Z - Root Encryption Key: G,E,Z - Root Signing Key: G,E,Z - Global Active Encryption Key (AEK): G,E,Z - Global Active Signing Key: G,E,Z - SED Active Encryption Key: G,E,Z - SED Active Signing Key: G,E,Z - SED AdminSP Encryptio

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						n Key: G,E,Z - SED AdminSP Signing Key: G,E,Z - SED LockingSP Encryption Key: G,E,Z - SED LockingSP Signing Key: G,E,Z - SED Volatile Encryption Key: G,E,Z - SED Volatile Signing Key: G,E,Z - MSID: E
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 Encryption FW_Integrity Key Wrap Keyed_Digest_Generation Keyed_Digest_Verification RBG	Unauthenticated - DRBG.Key: G,E - DRBG.V: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Set	Write data structures; access control enforcement occurs per data structure field. This service can change Authentication Credential PINs	isFIPS mode is true	See §5.3.3.7 Basic Table Method Group - Set [1]	Success or UEC failure code	Encryption Keyed_Digest_ Generation	SID - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - SED AdminSP Encryption Key: E - SED AdminSP Signing Key: E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - SID PIN: W - SED Active Encryption Key: E - SED Active Signing Key: E Anybody - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - SED Active

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key: E - SED Active Signing Key: E - SED Volatile Encryption Key: E - MSID: E Admin SP Admin1 - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - SED AdminSP Encryption Key: E - SED AdminSP Signing Key: E - SED Volatile Signing Key: E - SED Volatile Encryption Key: E - SED Active Encryption Key: E - SED Active Signing Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Locking SP Admin - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - SED Active Encryption Key: E - SED Active Signing Key: E - SED LockingSP Encryption Key: E - SED LockingSP Signing Key: E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - Admin Authority Key (Ka): E - Locking SP Admin [1-4] PIN: W Locking

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						SP User - Global Active Encryption Key (AEK): E - Global Active Signing Key: E - SED Active Encryption Key: E - SED Active Signing Key: E - SED LockingSP Encryption Key: E - SED LockingSP Signing Key: E - SED Volatile Encryption Key: E - SED Volatile Signing Key: E - Non-Admin Authority Key (Ku) (Locking SP User unique): E - Locking SP User [1-10] PIN: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Set Range Attributes	Writes configuration data to a Locking SP table for an LBA Range	isFIPS mode is true	LBA range configuration data [2]	Success or UEC failure code	Encryption Keyed_Digest_ Generation	Locking SP User
Set DataStore	Write a stream of bytes to unstructured storage.	isFIPS mode is true	See §3.2.13.6 Write data to the DataStore table [7]	Success or UEC failure code	None	Anybody Locking SP User
Show Status	The NVMe Controller Health status poll command requests NVMe storage device (e.g., Cryptographic Module) status information	N/A	Input parameters are defined within NVM Express® Management Interface [11]	Output data is defined within NVM Express® Management Interface [11]	None	NVMe User
TCG Erase, Single User Mode	TCG Erase cryptographically erases user data within a defined data range.	isFIPS mode is true	[NVMe Command] defines the input parameters.	Return requested module data or UEC failure code.	Encryption Keyed_Digest_ Generation MEK Generation RBG	Locking SP Admin - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XT

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						S Tweak Key (16 total - 1 per LBA range): G,Z - Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique): Z - DRBG.Key: E - DRBG.V: E - Range Access Key (RAK) (Locking SP User unique): E - User Access Key (UAK) (Locking SP User unique): E Locking SP User - MEK - Media Encryption Keyset MEK.AESEnc

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): G,E,Z - Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique): G,Z - DRBG.Key: E - DRBG.V: E - Range Access Key (RAK) (Locking SP User unique): E - User Access Key (UAK) (Locking SP User unique): E - User Manage

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ment Key (UMK): E
TCG GenKey	TCG GenKey cryptographically erases user data within a defined data range.	isFIPS mode is true	See §5.3.3.16 Key Related Method Group - GenKey [1]	Success or UEC failure code	Encryption Keyed_Digest_Generation MEK Generation RBG	Locking SP User - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): G,E,Z - Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique): G,Z - DRBG.Key: E - DRBG.V: E - User Access Key (UAK) (Locking SP User unique): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Write User Data	Transforms plaintext user data into ciphertext and writes the data to a specified LBA band.	isFIPS mode is true	Operation Code, LBA, Transfer Length, Data-Out Buffer [NVMe Command]	Success or UEC failure code	User_Data_Encryption	NVMe User - MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range): E

Table 12: Approved Services

4.4 Non-Approved Services

The Cryptographic does not support non-approved services.
N/A for this module.

4.5 External Software/Firmware Loaded

The Cryptographic Module utilizes RSA public key cryptography to verify that the firmware downloaded to the module is authentic. The Cryptographic Module uses RSA 2048 PKCS1 v1.5 with SHA2-256 to verify the digital signature of all downloaded firmware binary image. RSA Public/Private key pairs used in the firmware signing process are generated and stored within a Hardware Security Module (HSM), which resides in a secure Western Digital facility. The Cryptographic Module rejects a downloaded firmware binary image if the FW_Authenticity security function 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.
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 secure loader, which is signed by the SD_CA Key, enables the boot process to use other keys besides the SD_CA Key for boot time RSA digital signature check (i.e., SD_BFW Key). For example, the secure loader loads the SD_BFW public key certificate and verifies the SD_CA Key RSA digital 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.

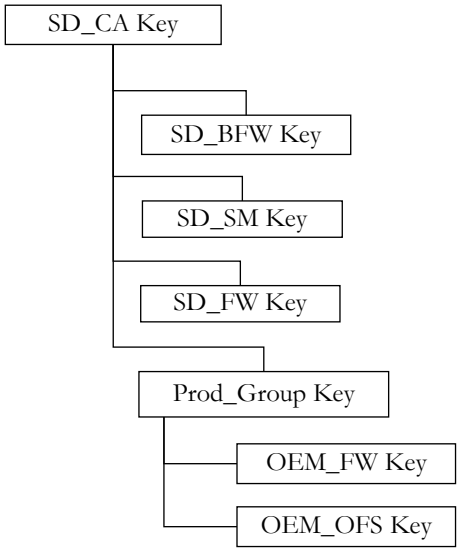

Figure 4 - Asymmetric Key Tree

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational 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 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 ASIC, hardware interface type (e.g., SAS, SATA, PCIe, etc.) 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 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 SN650 Specification [Product Manual] for guidance.

The Crypto Officer is responsible for assuring that the Locking SP User Authentication PIN Credential for all configured Locking SP Users does not equal the MSID value. LBA ranges associated with a Locking SP User with a default authentication PIN values are considered plaintext.

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

The Crypto Officer is responsible for assuring that the ReadLockEnabled and WriteLockEnabled attribute for any configured Locking SP User is set to True. The Cryptographic Module is in a noncompliant state when the state of the ReadLockEnabled or WriteLockEnabled attribute of any configured Locking SP User is set to False.
Consult the TCG Storage SSC: Opal Specification [TCG Opal] for guidance.

7 Physical Security

The Cryptographic Module is a multiple-chip embedded module that complies with FIPS 140-3 Level 1 security. An ambient temperature from 0° to 70°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 1 security. Therefore, the CM does not employ any fault induction mitigation techniques or an EFP feature that immediately zeroise all unprotected SSPs if the temperature or voltage falls outside of the Cryptographic Module's normal operating range. The CM will institute a thermal safety shutdown to preserve data integrity if the operating temperature reaches 83°C. The thermal safety shutdown process does not zeroize SSPs.

- All components are production-grade materials with standard passivation.
- The enclosure is opaque.
- Engineering design supports opacity requirements.

Mechanism	Inspection Frequency	Inspection Guidance
N/A	N/A	N/A

Table 13: Mechanisms and Actions Required

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 1.

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 cryptographically erase SSPs.

Storage Area Name	Description	Persistence Type
DRAM	General purpose system memory	Dynamic
IRAM	Memory internal to the ACM	Dynamic
NOR Flash	SSP and boot code storage	Static
NAND Flash	SSP storage and firmware image storage	Static
One-time Programable (OTP)	Root Key and Certificate Authority Key storage	Static

Table 14: Storage Areas

9.2 SSP Input-Output Methods

The CM limits the input of SSPs to plaintext Authentication Credential PINs and RSA-2048 public keys. RSA-2048 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.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Authentication Credential PIN	Operator	Cryptographic Module	Plaintext	Automated	Electronic	FW_Authenticity
Public Key	HSM	Cryptographic Module	Plaintext	Automated	Electronic	RSA SigVer (FIPS186-4) (A3374)

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

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

Zeroization Method	Description	Rationale	Operator Initiation
Format_NVM_SecureErase	Format_NVM_SecureErase cryptographically erases user data regardless of location (e.g., within an exposed LBA, within a cache, within deallocated LBAs, etc.) by regenerating the Namespace Keyset (NSK) and Media Encryption Keyset (MEK)	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	The operator issues a Format NVM command as specified in [12].
Power Cycle	Power cycling involves disconnecting and reconnecting the CM to its source of power.	Plaintext SSPs stored in IRAM memory within the ACM are destroyed instantaneously when power is removed.	The operator physically or remotely disconnects the CM from its source of power.
Revert	The Revert method cryptographically erases CSPs. Revert removes the owner's Authentication Credentials and returns the Cryptographic Module to its original manufactured state	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	The operator transmits a TCG IF-SEND command to the CM as to instruct the TPer to initiate a zeroization 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. Global Range data is preserved if the KeepGlobalRangeKey parameter is set to True.	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	The operator transmits a TCG IF-SEND command to the CM as to instruct the TPer to initiate a zeroisation process.
TCG Erase	In Single User Data mode, executing the TCG Erase method cryptographically	All SSPs within the scope of this zeroization	The operator transmits a command to

Zeroization Method	Description	Rationale	Operator Initiation
	erases user data by regenerating and replacing the Locking Range Key (LRK) and Media Encryption Key (MEK) associated with a data range.	method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	the CM as to instruct the TPer to initiate a user data erasure process.
TCG GenKey	In Single User Data mode and non-Single User Mode, executing the TCG GenKey method cryptographically erases user data by regenerating and replacing the Locking Range Key (LRK) and Media Encryption Key (MEK) associated with a data range	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	The operator transmits a command to the CM as to instruct the TPer to initiate a key generation 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.	All SSPs within the scope of this zeroization method are encrypted and signed. Therefore, the rationale specified under item e of VE09.30.01 is not applicable.	The operator transmits proprietary commands to the CM to initiate a rebuild process that zeroizes and regenerates the symmetric and asymmetric key trees

Table 16: SSP Zeroization Methods

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Admin Authority Key (Ka)	The Ka key encrypts and decrypts UAKs and the UMK.	256 bits - 256 bits	Derived Symmetric Key - CSP	PBKDF (A3374)		AES-CBC (AES 3580)
Admin SP Admin1 PIN	Authentication Credential PIN for the Admin SP Admin1 Authority.	12 to 32 bytes - 96 to 256 bits	Plaintext - CSP			
Admin SP Admin1 PIN Digest	Authenticates the Admin SP Admin1 Authority.	256 bits - 256 bits	Message Digest - CSP	HMAC-SHA2-256 (HMAC 2280)		
Admin SP Maintenance PIN	Authentication Credential PIN for the Admin SP Admin1 Authority.	12 to 32 bytes - 96 to 256 bits	Plaintext - CSP			Authority_Digest_Generation Derived_Key_Generation
Admin SP Maintenance PIN Digest	Authenticates the Admin SP Admin1 Authority.	256 bits - 256 bits	Message Digest - CSP	HMAC-SHA2-256 (HMAC 2280)		Authority_Digest_Verification
Anybody User Access Key (UAKa)	The Anybody Authority uses UAKa to decrypt the RAK of unlocked LBA bands.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)
DRBG.Key	Internal state associated with the [SP 800-90A] CTR_DRBG using AES-256	256 bits - 256 bits	Entropy - CSP	Counter DRBG (A3374)		Counter DRBG (A3374)
DRBG.Seed	Internal state associated with the [SP 800-90A] CTR_DRBG using AES-256.	128 bits - 128 bits	Entropy - CSP	RBG Seeding		Counter DRBG (A3374)
DRBG.V	Internal state associated with the [SP 800-90A]	128 bits -	Entropy - CSP	Counter DRBG (A3374)		Counter DRBG (A3374)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	CTR_DRBG using AES-256.	128 bits				
ESV	Entropy source input to the [SP 800-90A] CTR_DRBG	32-bit sample - 2.69 bits per 32-bit sample	Entropy - CSP	Counter DRBG (A3374)		Counter DRBG (A3374)
Global Active Encryption Key (AEK)	The Global Active Encryption Key encrypts and decrypts the SED Active Encryption Key, SED Active Signing Key, NSK and the UAKa key.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)
Global Active Signing Key	Signs the encrypted SED Active Encryption Key and SED Active Signing Key.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		HMAC-SHA2-256 (HMAC 2280)
KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User)	KDF Salts are integral to the PBKDF2 generation of each Ka and Ku derived authority key.	256 bits - 256 bits	Symmetric Key - PSP	Counter DRBG (A3374)		HMAC-SHA2-256 (HMAC 2280)
Locking Range Keyset (LRK) LRK.AES Key LRK.XTS	LRKs in combination with the NSKs derive MEKs, which encrypt LBA bands	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		MEK Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Key (Locking SP User unique)						
Locking SP Admin [1-4] PIN	Authentication Credential PIN for a Locking SP Admin Authority	12 to 32 bytes - 96 to 256 bits	Plaintext - CSP			Authority_Digest_Generation Derived_Key_Generation
Locking SP Admin [1-4] PIN Digest	Authenticates the associated Locking SP Admin Authority	256 bits - 256 bits	Message Digest - CSP	HMAC-SHA2-256 (HMAC 2280)		Authority_Digest_Verification
Locking SP User [1-10] PIN	Authentication Credential PIN for a Locking SP User Authority	12 to 32 bytes - 96 to 256 bits	Plaintext - CSP			Authority_Digest_Generation Derived_Key_Generation
Locking SP User [1-10] PIN Digest	Authenticates the associated for Locking SP User Authority	256 bits - 256 bits	Message Digest - CSP	HMAC-SHA2-256 (HMAC 2280)		Authority_Digest_Verification
MEK - Media Encryption Keyset MEK.AES Enc Key MEK.AES Dec Key MEK.XTS Tweak Key (16 total - 1 per LBA range)	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 - CSP	MEK Generation		User_Data_Encryption
MSID	The MSID string is the default password for the SID and Admin SP Admin1 authorities.	32 bytes - 162.8 bits	Plaintext - CSP	Counter DRBG (A3374)		Digest_Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Inserted during the manufacturing process, this thirty-two-character value is generated by the CM by processing a CTR-DRBG generated random number through an Alphanumeric Character Conversion algorithm. The algorithm's output is limited to a thirty-four-element character set.					
MSID Digest	Authenticates the MSID PIN	256 bits - 256 bits	Message Digest - CSP	HMAC-SHA2-256 (HMAC 2280)		Derived_Key_Generation
Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique)	NSKs in combination with the LRKs derive MEKs, which encrypt LBA bands	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		MEK Generation
Non-Admin Authority Key (Ku) (Locking SP User unique)	Ku keys encrypt and decrypt all UAKs except UAKa.	256 bits - 256 bits	Derived Symmetric Key - CSP	PBKDF (A3374)		AES-CBC (AES 3580)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
OEM Firmware Key (OEM FW Key)	The OEM FW Key verifies the overall download firmware image.	2048-bits - 112 bits	Public Key - Neither			RSA SigVer (FIPS186-4) (A3374)
OEM Original Factory State Key (OEM_OFS Key)	The OEM_OFS Key verifies the OEM Original Factory Settings files.	2048-bits - 112 bits	Public Key - Neither			RSA SigVer (FIPS186-4) (A3374)
Product Group Key (PROD GROUP Key)	The PROD GROUP Key verifies OEM FW Key certificates.	2048-bits - 112 bits	Public Key - PSP			RSA SigVer (FIPS186-4) (A3374)
PSID	The PSID string serves as authentication data and proof of physical presence for the Zeroise Service. Inserted during the manufacturing process, this thirty-two-character value is generated by the CM by processing a CTR-DRBG generated random number through an Alphanumeric Character Conversion algorithm. The algorithm's output is limited to a thirty-four-element character set.	32 bytes - 162.8 bits	Plaintext - PSP	Counter DRBG (A3374)		Digest_Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PSID Digest	HMAC-SHA2-256 digest of PSID	256 bits - 256 bits	Message Digest - CSP	HMAC-SHA2-256 (HMAC 2280)		Digest_Verification
Range Access Key (RAK) (Locking SP User unique)	RAKs encrypt and decrypt LRKs.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)
Root Encryption Key	The Root Encryption Key encrypts the Global Active Encryption Key, Global Active Signing Key.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580) AES-ECB (AES 3580) AES-KWP (A3374) AES-ECB (A3410)
Root Signing Key	Signs the encrypted Global Active Encryption Key, Global Active Signing Key.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		HMAC-SHA2-256 (HMAC 2280)
Security Core Firmware Key (SC_FW Key)	The SC_FW Key verifies ACM security core firmware.	2048-bits - 112 bits	Public Key - Neither			RSA SigVer (FIPS186-4) (A3374)
Security Protocol Firmware Key (SP_FW Key)	The SP_FW Key verifies ACM security protocol and services firmware.	2048-bits - 112 bits	Public Key - Neither			RSA SigVer (FIPS186-4) (A3374)
SED Active Encryption Key	The SED Active Encryption Key encrypts and decrypts the SED AdminSP Encryption Key, SED AdminSP Signing Key, SED LockingSP	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Encryption Key, and SED LockingSP Signing Key.					
SED Active Signing Key	Signs the encrypted SED AdminSP Encryption Key and SED AdminSP Signing Key. Signs the encrypted SED LockingSP Encryption Key and SED LockingSP Signing Key.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		HMAC-SHA2-256 (HMAC 2280)
SED AdminSP Encryption Key	Encrypts and decrypts an Admin SP Object Tables.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)
SED AdminSP Signing Key	Signs an encrypted Admin SP Object Table.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		HMAC-SHA2-256 (HMAC 2280)
SED LockingSP Encryption Key	Encrypts and decrypts a Locking SP Object Tables.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)
SED LockingSP Signing Key	Signs an encrypted Locking SP Object Table.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		SHA2-256 (SHS 2942)
SED Volatile Encryption Key	Encrypts, and decrypts LRKs and MEKs.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)
SED Volatile Signing Key	Signs encrypted LRKs and MEKs.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		HMAC-SHA2-256 (HMAC 2280)
SID PIN	Authentication Credential PIN for the Admin SP	12 to 32 bytes	Plaintext - CSP			Authority_Digest_Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	SID Authority.Authentication Credential	- 96 to 256 bits				
SID PIN Digest	Authenticates the SID Authority.	256 bits - 256 bits	Message Digest - CSP	HMAC-SHA2-256 (HMAC 2280)		Authority_Digest_Verification
Storage Device Boot FW Key (SD_BFW Key)	The SD_BFW Key is public key used to verify all boot flash images.	2048-bits - 112 bits	Public Key - Neither			RSA SigVer (FIPS186-4) (A3374)
Storage Device Certification Authority Key (SD_CA Key)	The SD_CA Key is the Master RSA 2048 public key. It verifies the authenticity of the other key certificates and the Secure Loader image	2048-bits - 112 bits	Public Key - Neither			RSA SigVer (FIPS186-4) (A3374)
User Access Key (UAK) (Locking SP User unique)	Encrypts and decrypts RAKs associated with a Locking SP User.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)
User Management Key (UMK)	Encrypts and decrypts UAKs. All enabled Locking SP Admins and the Admin SP Admin1 share the UMK.	256 bits - 256 bits	Symmetric Key - CSP	Counter DRBG (A3374)		AES-CBC (AES 3580)

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Admin Authority Key (Ka)		IRAM:Plaintext	Ephemeral Destroyed after use.	Power Cycle	User Access Key (UAK) (Locking SP User unique):Encrypts User Management Key (UMK):Encrypts Admin SP Admin1 PIN:Derived From KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User):Derived From Locking SP Admin [1-4] PIN:Derived From
Admin SP Admin1 PIN	Authentication Credential PIN		Ephemeral Destroyed after use.	Power Cycle	Admin SP Admin1 PIN Digest:Paired With KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User):Paired With Admin Authority Key

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					(Ka):Paired With
Admin SP Admin1 PIN Digest		NAND Flash:Encrypted		Revert RevertSP	Admin SP Admin1 PIN:Generated from SED AdminSP Signing Key:Generated from
Admin SP Maintenance PIN	Authentication Credential PIN	DRAM:Plaintext	Ephemeral, destroyed after use	Power Cycle	Admin SP Maintenance PIN Digest:Paired With Admin Authority Key (Ka):Paired With KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User):Paired With
Admin SP Maintenance PIN Digest		NAND Flash:Encrypted		Revert RevertSP	Admin SP Maintenance PIN:Generated from SED AdminSP Signing Key:Generated from
Anybody User Access Key (UAKa)		NAND Flash:Encrypted IRAM:Plaintext	Power up to power down	Power Cycle Revert RevertSP	Range Access Key (RAK) (Locking SP User unique):Decrypts
DRBG.Key		IRAM:Plaintext	Power up to	Power Cycle	DRBG.Seed:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			power down		DRBG.V:Paired With
DRBG.Seed		IRAM:Plaintext	Power up to power down	Power Cycle	DRBG.V:Paired With DRBG.Key:Paired With
DRBG.V		IRAM:Plaintext	Power up to power down	Power Cycle	DRBG.Seed:Paired With DRBG.Key:Paired With
ESV		IRAM:Plaintext	Power up to power down	Power Cycle	DRBG.Seed:Paired With
Global Active Encryption Key (AEK)		NOR Flash:Encrypted		Secure Manufacturing Reconfiguration Process	SED Active Signing Key:Encrypts SED Active Signing Key:Decrypts Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique):Encrypts Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique):Decrypts User Access Key (UAK) (Locking SP User unique):Encrypts User Access Key (UAK) (Locking SP User

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					unique):Decrypts SED Active Encryption Key:Encrypts SED Active Encryption Key:Decrypts
Global Active Signing Key		NOR Flash:Encrypted		Secure Manufacturing Reconfiguration Process	Global Active Encryption Key (AEK):Derived From SED Active Encryption Key:Derived From SED Active Signing Key:Derived From
KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User)		NAND Flash:Encrypted		Revert RevertSP	Admin SP Admin1 PIN:Paired With Locking SP Admin [1-4] PIN:Paired With Locking SP User [1-10] PIN:Paired With Admin Authority Key (Ka):Paired With
Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique)		DRAM:Encrypted NAND Flash:Encrypted	Generation to power down	Power Cycle Revert RevertSP TCG Erase TCG GenKey	Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique):Paired With MEK - Media Encryption Keyset

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range):Paired With SED Volatile Encryption Key:Encrypts Range Access Key (RAK) (Locking SP User unique):Encrypts
Locking SP Admin [1-4] PIN	Authentication Credential PIN	DRAM:Plaintext	Ephemeral Destroyed after use.	Power Cycle	Locking SP Admin [1-4] PIN Digest:Paired With KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User):Paired With
Locking SP Admin [1-4] PIN Digest		NAND Flash:Encrypted		Revert RevertSP	Locking SP Admin [1-4] PIN:Generated from
Locking SP User [1-10] PIN	Authentication Credential PIN	DRAM:Plaintext	Ephemeral Destroyed after use.	Power Cycle	Locking SP User [1-10] PIN Digest:Paired With Non-Admin Authority Key (Ku) (Locking SP User unique):Paired

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					With KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User):Paired With
Locking SP User [1-10] PIN Digest		NAND Flash:Encrypted		Revert RevertSP	Locking SP User [1-10] PIN:Generated from SED LockingSP Signing Key:Derived From
MEK - Media Encryption Keyset MEK.AES Enc Key MEK.AES Dec Key MEK.XTS Tweak Key (16 total - 1 per LBA range)		DRAM:Encrypted	Generation to power down	Power Cycle Revert RevertSP	Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique):Generated from Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique):Generated from SED Volatile Encryption Key:Encrypts
MSID		IRAM:Plaintext NOR Flash:Encrypted	Ephemeral Destroyed after use.	Power Cycle	SED Active Signing Key:Derived From MSID Digest:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
MSID Digest		IRAM:Plaintext NOR Flash:Encrypted	Ephemeral Destroyed after use	Power Cycle	MSID:Generated from SED Active Signing Key:Generated from
Namespace Keyset (NSK) NSK.AES Key NSK.XTS Key (Locking SP User unique)		DRAM:Encrypted NAND Flash:Encrypted	Generation to power down.	Format_NVM_Secure Erase Power Cycle Revert RevertSP	Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique):Paired With MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range):Paired With Global Active Encryption Key (AEK):Encrypts
Non-Admin Authority Key (Ku) (Locking SP User unique)			Ephemeral Destroyed after use	Power Cycle	Locking SP User [1-10] PIN:Derived From KDF Salt (Unique to Admin SP Admin1, each Locking SP Admin and each Locking SP User):Derived From Anybody User Access Key (UAKa):Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
OEM Firmware Key (OEM FW Key)	Public Key	NOR Flash:Encrypted		N/A	Product Group Key (PROD GROUP Key):Verified by
OEM Original Factory State Key (OEM_OFS Key)	Public Key	NOR Flash:Encrypted		N/A	Product Group Key (PROD GROUP Key):Verified by
Product Group Key (PROD GROUP Key)	Public Key	NOR Flash:Encrypted		N/A	Storage Device Certification Authority Key (SD_CA Key):Verified by
PSID		IRAM:Plaintext	Ephemeral Destroyed after use.	Power Cycle	PSID Digest:Paired With SED Active Encryption Key:Encrypts SED Active Signing Key:Signed by
PSID Digest		IRAM:Plaintext NAND Flash:Encrypted	Ephemeral Destroyed after use.	Power Cycle Revert RevertSP	PSID:Generated from SED Active Signing Key:Generated from
Range Access Key (RAK) (Locking SP User unique)		NAND Flash:Encrypted		Revert RevertSP	Anybody User Access Key (UAKa):Encrypted by Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique):Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Root Encryption Key		One-time Programable (OTP):Encrypted		Secure Manufacturing Reconfiguration Process	Global Active Encryption Key (AEK):Encrypts Global Active Signing Key:Encrypts Root Signing Key:Wraps
Root Signing Key		NOR Flash:Encrypted		Secure Manufacturing Reconfiguration Process	Global Active Encryption Key (AEK):Signs Root Encryption Key:Wraps
Security Core Firmware Key (SC_FW Key)	Public Key	NOR Flash:Encrypted		N/A	Storage Device Certification Authority Key (SD_CA Key):Verified by
Security Protocol Firmware Key (SP_FW Key)	Public Key	NOR Flash:Encrypted		N/A	Storage Device Certification Authority Key (SD_CA Key):Verified by
SED Active Encryption Key		NOR Flash:Encrypted		Revert RevertSP	SED AdminSP Encryption Key:Encrypts SED AdminSP Signing Key:Encrypts SED LockingSP Encryption Key:Encrypts SED LockingSP Signing Key:Encrypts
SED Active Signing Key		NOR Flash:Encrypted		Revert RevertSP	SED AdminSP Encryption Key:Signs SED AdminSP Signing Key:Signs

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					SED LockingSP Encryption Key:Signs SED LockingSP Signing Key:Signs
SED AdminSP Encryption Key		NOR Flash:Encrypted		Revert RevertSP	Admin SP Admin1 PIN:Encrypts Admin SP Admin1 PIN Digest:Encrypts
SED AdminSP Signing Key		NOR Flash:Encrypted		Revert RevertSP	Admin SP Admin1 PIN:Signs Admin SP Admin1 PIN Digest:Signs
SED LockingSP Encryption Key		NOR Flash:Encrypted		Revert RevertSP	Locking SP Admin [1-4] PIN:Encrypts Locking SP Admin [1-4] PIN Digest:Encrypts Locking SP User [1-10] PIN:Encrypts
SED LockingSP Signing Key		NOR Flash:Encrypted		Revert RevertSP	Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique):Signs
SED Volatile Encryption Key		IRAM:Plaintext	Power up to power down	Power Cycle Revert RevertSP	Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique):Encryp

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					ts MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range):Encrypts
SED Volatile Signing Key		IRAM:Plaintext	Power up to power down	Power Cycle Revert RevertSP	Locking Range Keyset (LRK) LRK.AES Key LRK.XTS Key (Locking SP User unique):Signs MEK - Media Encryption Keyset MEK.AESEnc Key MEK.AESDec Key MEK.XTS Tweak Key (16 total - 1 per LBA range):Signs
SID PIN	Authentication Credential PIN	IRAM:Plaintext	Ephemeral Destroyed after use.	Power Cycle	SID PIN Digest:Paired With
SID PIN Digest		NAND Flash:Encrypted		Revert RevertSP	SID PIN:Generated from SED AdminSP Signing Key:Generated from AdminSP Signing Key:Signed by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Storage Device Boot FW Key (SD_BFW Key)	Public Key	NOR Flash:Encrypted		N/A	Storage Device Certification Authority Key (SD_CA Key):Verified
Storage Device Certification Authority Key (SD_CA Key)	Public Key	NOR Flash:Plaintext One-time Programable (OTP):Encrypted		N/A	Storage Device Boot FW Key (SD_BFW Key):Signs Security Core Firmware Key (SC_FW Key):Signs Security Protocol Firmware Key (SP_FW Key):Signs
User Access Key (UAK) (Locking SP User unique)		NAND Flash:Encrypted		Revert RevertSP	Range Access Key (RAK) (Locking SP User unique):Encrypts
User Management Key (UMK)		NAND Flash:Encrypted		Revert RevertSP	Anybody User Access Key (UAKa):Encrypts

Table 18: SSP Table 2

10 Self-Tests

The Cryptographic Module performs pre-operational and conditional self-tests automatically at powered up. Pre-operational self-tests tests ensure that the Cryptographic Module is not corrupted. The conditional self-tests assure that the cryptographic algorithms comply with their associated certificate. 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

The Cryptographic Module 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 Cryptographic Module transitions to a Device Unavailable Error state.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ESV	Sequential data collection	Adaptive Proportion Test	Critical Function	Pass: Next test Fail: Device Unavailable Error	APT Threshold
RSA SigVer (FIPS186-4)	A3374, A3375, SHS 2942	2048-bit, PKCS1 v1.5w/SHA2-256	SW/FW Integrity	Pass: Next test Fail: Device Unavailable Error	Verify Digital Signature

Table 19: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES CBC Encrypt	256-bit key	KAT	CAST	Pass: Next test Fail: Degraded Error	Encrypt, verify	Power up
AEs CBC Decrypt	256-bit key	KAT	CAST	Pass: Next test Fail: Degraded Error	Decrypt, verify	Power up
AES ECB Encrypt	256-bit key	KAT	CAST	Pass: Next test Fail: Degraded Error	Encrypt, verify	Power up
AES ECB Decrypt	256-bit key	KAT	CAST	Pass: Next test Fail: Degraded Error	Decrypt, verify	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A3374)	5120-bit seed	KAT	CAST	Pass: Next test Fail: Device Unavailable Error	SP 800-90ARev1 section 11.3 health test (Instantiate, generate and reseed)	Power up
HMAC-SHA2-256 (HMAC 2280)	Message, 256-bit key, 256-bit hash digest	KAT	CAST	Pass: Next test Fail: Degraded Error	Verify	Power up
PBKDF (A3374)	256-bit Salt Iteration Count: 1024	KAT	CAST	Pass: Next test Fail: Degraded Error	Verify	Power up
RSA SigVer KAT	2048- bit public key, 256-bit hash digest	KAT	CAST	Pass: Next test Fail: Degraded Error	Verify	Power up
RSA SigVer for Load Test	2048- bit public key, 256-bit hash digest	Digital Signature Verification	SW/FW Load	Pass: Next test Fail: Degraded Error	Verify	Power up
SHA2-256 (SHS 2942)	Message, 256-bit hash digest	KAT	CAST	Pass: Next test Fail: Degraded Error	Verify	Power up
AES KWP Encrypt	256-bit KEK	KAT	CAST	Pass: Next test Fail: Degraded Error	Encrypt, Verify	Power up
AES KWP Decrypt	256-bit KEK	KAT	CAST	Pass: Next test Fail: Degraded Error	Decrypt, Verify	Power up
ESV APT	RCT threshold	Health Test	CAST	Pass: Next test Fail: Degraded Error	Verify	Power-up or after 2^32 CTR_DRBG reseeds.
ESV RCT	APT threshold	Health Test	CAST	Pass: Next test Fail: Degraded Error	Verify	Power-up or after 2^32 CTR_DRBG reseeds.

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ESV	Adaptive Proportion Test	Critical Function	N/A	Power cycle
RSA SigVer (FIPS186-4)	2048-bit, PKCS1 v1.5w/SHA2-256	SW/FW Integrity	N/A	Power cycle

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES CBC Encrypt	KAT	CAST	N/A	Power cycle
AEs CBC Decrypt	KAT	CAST	N/A	Power cycle
AES ECB Encrypt	KAT	CAST	N/A	Power cycle
AES ECB Decrypt	KAT	CAST	N/A	Power cycle
Counter DRBG (A3374)	KAT	CAST	N/A	Power cycle
HMAC-SHA2-256 (HMAC 2280)	KAT	CAST	N/A	Power cycle
PBKDF (A3374)	KAT	CAST	N/A	Power cycle
RSA SigVer KAT	KAT	CAST	N/A	Power cycle
RSA SigVer for Load Test	Digital Signature Verification	SW/FW Load	N/A	Power cycle
SHA2-256 (SHS 2942)	KAT	CAST	N/A	Power cycle
AES KWP Encrypt	KAT	CAST	N/A	Power cycle
AES KWP Decrypt	KAT	CAST	N/A	Power cycle
ESV APT	Health Test	CAST	N/A	Power cycle
ESV RCT	Health Test	CAST	N/A	Power cycle

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Degraded Error	This error indicates that a fatal failure occurred from which the CM could not recover itself.	Conditional test failure	Power cycle	UEC failure code

Name	Description	Conditions	Recovery Method	Indicator
Device Unavailable Error	This error indicates that a boot initialization, security subsystem initialization or firmware integrity failure event occurred. In this state, the CM does not respond to any command received via the data input port.	Pre-operational test failure	Power cycle	Device is unresponsive

Table 23: Error States

10.5 Operator Initiation of 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: Opal Specification [TCG Opal].

Installation and Initialization:

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 SL1

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 and replace 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 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 zeroization requirements (7.9.7)."

Take-Ownership Scenario Example

1. Authenticate to the SID.
    a. If the default MSID was used to authenticate to the SID, 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 Admin SP Admin1.
    a. If the Crypto Officer authenticated to Admin SP Admin1 with the default MSID value, change the Admin SP Admin1 PIN to a random value between 12 and 32 bytes in length.
4. Authenticate to each Locking SP Admin that is within the scope of the operator site requirements.
    a. If the Crypto Officer authenticated to a Locking SP Admin with the default MSID value, change the Locking SP Admin PIN to a random value between 12 and 32 bytes in length.
5. Authenticate to each Locking SP User that is within the scope of the operator site requirements.
    a. If the default MSID was used to authenticate to a Locking SP User, change the Locking SP User PIN to a random value between 12 and 32 bytes in length.

b. Utilize the Get Range Attributes service to determine the state of the Locking SP User's LockOnReset attribute. If the LockOnReset attribute is not set to PowerCycle, use the Set Range Attribute service to set the LockOnReset attribute to Power Cycle.
c. Utilize the Get Range Attributes service to determine the state of the Locking SP User's ReadLockEnabled attribute. If the ReadLockEnabled attribute is not set to True, use the Set Range Attribute service to set the ReadLockEnabled attribute to True.
d. Utilize the Get Range Attributes service to determine the state of the Locking SP User's WriteLockEnabled attribute. If the WriteLockEnabled attribute is not set to True, use the Set Range Attribute service to set the WriteLockEnabled attribute to True.

11.2 Administrator Guidance

Solid-state drives can be fragile. Do not drop or jar the drive. Handle the drive only by the enclosure.

SSD 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. Handle the drive only by the metal case surrounding the drive. Avoid contacting with the EDSFF connector.
To assure proper installation and operation, verify all cooling requirements are met prior to initiating the installation instructions within the Ultrastar® DC SN650 Product Manual [Product Manual].

The Ultrastar® DC SN650 Product Manual [Product Manual] provides administrator guidance.

11.3 Non-Administrator Guidance

Inspect the CM for damage to the case or EDSFF connector. Return the CM for warranty replacement service if any damage is detected.
The Ultrastar® DC SN650 Product Manual [Product Manual] provides 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 isFIPS 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 Cryptographic Module provides three distinct operator roles: User, Maintenance and Cryptographic Officer.
2. The Cryptographic Module provides role-based authentication.
3. On power cycle the Module clears previous authentications.
4. The Cryptographic 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 Cryptographic 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. Data output is inhibited 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 Cryptographic Module.
10. The Cryptographic Module implements multiple zeroization service that vary in scope. The scope of each zeroization service is defined in Section 9.3 SSP Zeroization Methods.
11. The Cryptographic Module does not support concurrent operators.
12. The Cryptographic Module supports a maintenance role.
13. The Cryptographic Module does not support manual SSP establishment method.
14. The Cryptographic Module does not have any proprietary external input/output devices used for entry/output of data.
15. The Cryptographic Module does not enter or output plaintext CSPs.
16. The Cryptographic Module does not store any plaintext CSPs.
17. The Cryptographic Module does not output intermediate key values.
18. The Cryptographic 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 SL1.

References and Definitions

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

NIST Specifications

Abbreviation	Specification Name
[FIPS 140 IG]	Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program, August 2024
[FIPS 140]	Security Requirements for Cryptographic Modules, FIPS PUB 140-3, NIST, March 2019
[FIPS 180]	Secure Hash Standard (SHS), FIPS PUB 180-4, NIST, August 2015
[FIPS 186]	Digital Signature Standard, FIPS PUB 186-5, NIST, February 2023
[FIPS 197]	Advanced Encryption Standard, FIPS PUB 197, NIST, May 2023
[FIPS 198]	The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, July 2008
[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
[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

Trusted Computing Group Specifications

Abbreviation	Specification Name
[TCG Core]	TCG Storage Architecture Core Specification, Version 2.01 Revision 1.00 (August 5, 2015)
[TCG Namespace]	TCG Storage Opal SSC Feature Set: Configurable Namespace Locking, Specification Version 1.00, Final Revision 1.33 (February 22, 2019)

Abbreviation	Specification Name
[TCG Opal Guideline]	TCG Storage Opal Integration Guidelines, Version 1.00, Final Revision 1.00 (March 16, 2016)
[TCG Opal]	TCG Storage Security Subsystem Class: Opal Specification, Version 2.01, Final Revision 1.00 (August 5, 2015)
[TCG PSID]	TCG Storage Opal SSC Feature Set: PSID, Specification Version 1.00, Final Revision 1.00 (August 5, 2015)
[TCG SIIS]	TCG Storage Interface Interactions Specification (SIIS), Version 1.07, (January 30, 2018)
[TCG Opal Single User]	TCG Storage Opal SSC Feature Set: Single User Mode Specification, Version 1.00, Final Revision 1.00 (February 24, 2012)
[TCG Opal Datastore]	TCG Storage Opal SSC Feature Set: Additional DataStore Tables, Specification Version 1.00

NVMe and PCIe Specifications

Abbreviation	Specification Name
[NVMe Base]	NVM Express® Base Specification, Revision 1.3.c, May 24, 2018
[NVMe Command]	NVM Express® NVM Command Set Specification, Revision 1.0, May 18, 2021
[NVMe Management]]	NVM Express® Management Interface, Revision 1.1, April 29, 2019
[PCIe Base]	PCI Express® Base Specification, Revision 3.0, November 10 ,2010

Corporate References

Abbreviation	Specification Name
[Product Manual]	Ultrastar® DC SN650 NVMe Solid-State Drive Product Manual, https://www.westerndigital.com/support
[Datasheet]	Ultrastar® DC SN650 Datasheet, https://www.westerndigital.com/support

Other References

Abbreviation	Reference Name
[IETF]	IETF RFC 2119, 1997, “Key words for use in RFCs to Indicate Requirement Levels.”
[ISO 19790]	ISO/IEC 19790, Information technology - Security techniques - Security requirements for cryptographic modules, International Organization for Standardization (ISO), December 2015
[OCP Datacenter]	Open Computing Project, Datacenter NVMe® SSD Specification, Version 2.0, July 30, 2021
[OCP NVMe Cloud]	Open Compute Project, NVMe Cloud SSD Specification, Version 1.0, March 18, 2020
[PW]	Calculating Password Entropy: https://www.pleacher.com/mp/mlessons/algebra/entropy.html
[SFF-8639]	SFF-8639, SFF-TA-1001 Specification for Universal x4 Link Definition for SFF-8639, Rev 1.1 May 28, 2018
[SFSC]	Security Features for SCSI Commands, Revision 2, September 2015

Definitions

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

Name	Definition
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].
Integrity	A cryptographic property that blocks the modification or deletion of sensitive in an unauthorized and undetected manner.
Interface	A logical entry or exit point of a Cryptographic Module that provides access to the Cryptographic Module for logical information flows. [FIPS 140]
Key Derivation Function (KDF)	An Approved cryptographic algorithm that derives one or more keys from a secret value and other information.
Key Encrypting Key (KEK)	A cryptographic key used to encrypt or decrypt other keys.
Key Management	The activities involving the handling of cryptographic keys and other related security parameters during the entire life cycle of the Cryptographic Module. The handling of authentication data is representative of a key management activity.
Key Wrap	An Approved cryptographic algorithm that uses a KEK to provide Confidentiality and Integrity.
LBA Range	A formal term that defines a contiguous logical block range (sequential LBAs) to store encrypted User Data; ramgess 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.

Name	Definition
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.
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
Security Identifier (SID)	The authority that represents the TPer owner. Crypto Officer serves in this role. [TCG Core]
Security Provider (SP)	A TCG term used to define a collection of Tables and Methods with access control.
SED Active Keyset	A set of 256-bit keys that consists of the SED Active Encryption Key and the SED Active Signing Key.
SED AdminSP Active Keyset	A set of 256-bit keys that consists of the SED AdminSP Active Encryption Key and the SED AdminSP Active Signing Key.
SED Global Active Keyset	A set of 256-bit keys that consists of the Global Active Encryption Key (AEK) and the Global Active Signing Key.
SED LockingSP Active Keyset	A set of 256-bit keys that consists of the SED LockingSP Active Encryption Key and the SED LockingSP Active Signing Key. The keyset protects TCG protocol LockingSP CSPs.
SED Volatile Keyset	A set of 256-bit keys that consists of the SED Volatile Key and the SED Volatile Signing Key.
Self-Encrypting Drive (SED)	A storage device that provides data storage services, which automatically encrypts all user data written to the device and automatically decrypts all user data read from the device.
Session	A formal TCG term that envelops the lifetime of an Operator's authentication. [TCG Core]
Small Form Factor (SFF)	Small form factor is a computer form factor designed to minimize the volume and footprint of a desktop computer.
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 NVMe Read and Write commands.
User	An Operator that consumes cryptographic services. [FIPS 140]
Write Data	An external request to transfer User Data to a SED.

Name	Definition
Zeroise	Invalidate a Critical Security Parameter. [FIPS 140]

Acronyms

Acronym	Definition
AEK	Active Encryption Key
AEN	Asynchronous Event Notification
AES	Advanced Encryption Standard (FIPS 197)
ACE	Access Control Entry
ACL	Access Control List
CBC	Cipher Block Chaining, an operational mode of AES
CM	Cryptographic Module
CO	Crypto Officer [FIPS 140]
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter [FIPS 140]
DEE	Data Encryption Engine
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
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

Acronym	Definition
PSID	Physical Security Identifier
PSP	Public Security Parameter
RID	Reserved Area Internal Data
SAS	Serial Attached SCSI
SD_CA	Storage Device Certification Authority
SECD	Security Data
SED	Self-Encrypting Drive
SFF	Small Form Factor
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