Ultrastar® DC HC550 TCG Opal Self-Encrypting Drive
Ultrastar® DC HC650 TCG Opal Self-Encrypting Drive
FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Protection of Data at Rest

Document Version: 1.2
2022-05-25

Table of Contents

Tables

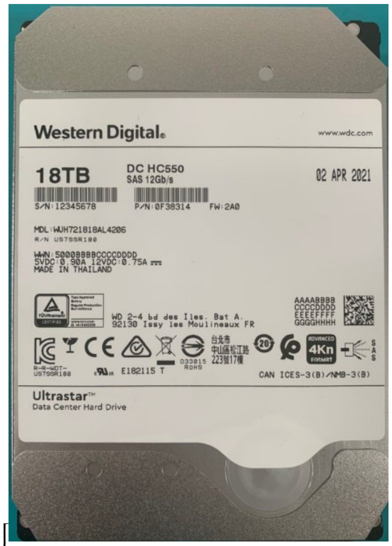
Figures

1 Cryptographic Module Overview

The Ultrastar DC HC550 TCG Opal Self-Encrypting Drive and Ultrastar DC HC650 TCG Opal Self-Encrypting Drive are hard disk drives. These modules hereafter referred to as Ultrastar DC HC550, Ultrastar DC HC650 or Cryptographic Module (CM) are multiple-chip embedded modules that comply with FIPS 140-2 Level 1 security. The drive enclosure defines the cryptographic boundary. See Figure 1: Ultrastar DC HC550 Cryptographic Module and Figure 2: Ultrastar DC HC650 Cryptographic Module. The physical interface for the Ultrastar DC HC550 consists of either a SAS or SATA interface connector and two SIO port pins. The physical interface for the Ultrastar DC HC650 consists of a SAS interface connector and two SIO port pins. In FIPS Approved and non-Approve modes, the Cryptographic Module disables the SIO port pins, outlined by the red box in Figure 3. All components within this boundary satisfy FIPS 140-2 requirements.

The logical interface is the industry standard TCG Storage Work Group (SWG) [TCG Core] and [TCG Opal] protocols. The primary function of the Cryptographic Module is to provide data encryption, access control, and cryptographic erase of the data stored on the hard drive media. The operator of the Cryptographic Module interfaces with the Cryptographic Module through a “host” application on a host system.

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



[

Figure 1: Ultrastar DC HC550

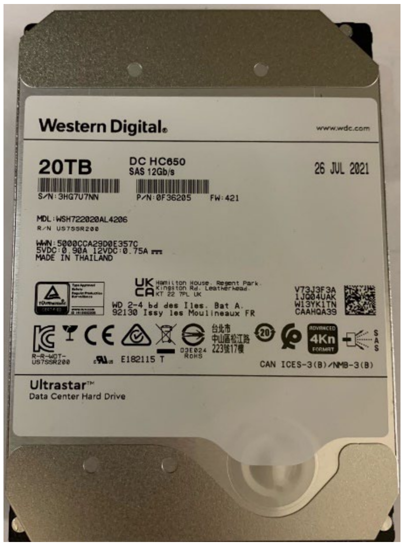


Figure 2: Ultrastar DC HC650

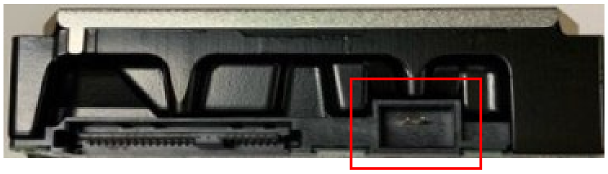


Figure 3: Ultrastar DC HC550/HC650 Interface Connector

1.1 Models

Multiple hardware versions define the scope of the Cryptographic Module. Storage capacity, write endurance, and overprovisioning define the differences.

Table 1 and Table 2 provide the model numbers, characteristics, and firmware version associated with each validated model.

Model Number	Firmware	Description
WUH721818AL4206	R670	18 TB, 4Kn, 3.5-inch HDD, 7200 RPM, 12 Gb/s SAS, SED, CMR
WUH721816ALN6L6	R670	18 TB, 4Kn, 3.5-inch HDD, 7200 RPM, 6 Gb/s SATA, SED, CMR

Table 1 - Ultrastar DC HC550 Models

Model Number	Firmware	Description
WSH722020AL4206	R463	20 TB, 4Kn, 3.5-inch HDD, 7200 RPM, 12 Gb/s SAS, SED, SMR

Table 2 - Ultrastar DC HC650 Models

1.2 Security Level

The Cryptographic Module meets all requirements applicable to FIPS 140-2 Level 1 Security.

FIPS 140-2 Security Requirements Section	FIPS 140-2 Security Level Achieved
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	3
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 3 - Module Security Level Specification

2 FIPS 140 Modes of Operation

2.1 FIPS Approved Mode of Operation

The Cryptographic Module has a single FIPS Approved mode of operation. Configuration and policy determine the Cryptographic Module's FIPS mode of operation. Prior to initialization, the CM operates in FIPS non-Approved mode. The CM enters FIPS Approved Mode after successful completion of the Initialize Cryptographic service instructions. See Section 7.2 for information on the Cryptographic Module's initialization rules. The operator can determine if the Cryptographic Module is operating in a FIPS approved mode by invoking the Level 0 Discovery service[1].

2.2 TCG Opal Security Mode

The TCG Storage Opal security mode utilizes TCG commands that address the TCG Admin SP and TCG Locking SP to provide services. The Crypto Officer must execute the Activate service to enable the TCG Storage Opal security mode. The TCG Storage Opal security mode allows multiple users with individualized access control to read, write, and erase data within independent data areas, which are referred to as LBA ranges. The TCG Storage Opal security mode supports administrator functions within the Crypto Officer role to,

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

2.3 Single User Data Ranges

The Crypto Officer may elect to define one or more data ranges as Single User Data Ranges (SUDR) when invoking the Activate service. The TCG Opal Feature Set: Single User Mode [5] defines Single User Data Ranges. As specified, the associated User role solely manages its assigned SUDR. Executing the Reactivation service allows the operator to reclassify user data ranges.

2.4 Approved Algorithms

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

CAVP Cert	Algorithm Standards and Function
AES 3580	[FIPS 197, SP 800-38A, SP 800-38E] AES[2] Function: AES-CBC-256 encrypts and decrypts CSPs. Mode: CBC Key Size: 256 Security Strength: 256 bits
AES A670	[FIPS 197, SP 800-38A, SP 800-38E] AES[3] Function: Used to encrypt and decrypt data-at-rest in a storage application Mode: ECB, XTS • 256-bit XTS Tweak Key does not equal to the 256-bit AES Encryption Key per IG A.9 Key Size: 256 Security Strength: 256 bits
DRBG A1390	[SP 800-90A, SP 800-38A, SP 800-38D] DRBG Function: Deterministic random number generator (DRBG). Uses an AES-256 block cipher derivation function to generate encryption keys. Mode: CTR AES-256 Key Size: 256 Seed Length: 384 Security Strength: 256 bits Prerequisite: AES Cert. #3580

[1] The CM sets the In FIPS bit to one after the operator successfully completes the Initialize Cryptographic service instructions.

[2] Tested AES ECB-128, AES ECB-256, AES-CBC-128, AES-XTS-128, and AES-XTS-256. However, the cryptographic module does not use these algorithms.

[3] Tested AES ECB-128 and AES-XTS-128. However, the cryptographic module does not use these algorithms.

CAVP Cert	Algorithm Standards and Function
ENT (P)	[SP800-90B] Function: Hardware entropy noise source seeds the Approved [SP800-90A] DRBG Type: Ring Oscillator DRBG Seed Length: 5120 bits DRBG Seed Entropy: 477.296 bits (2.9831 bits per 32 bits)
HMAC 2280	[FIPS 198-1] HMAC[4] Function: Used to sign and verify CSPs and derive keys in PBKDF2. Mode: SHA2-256 Key Size: 256 Security Strength: 256 bits Prerequisite: SHS Cert. #2942
PBKDF A1390	[SP 800-132] PBKDF2 Function: Utilizes a Password and KDF Salt to generate 256-bit Derived Authority Keys. Mode: HMAC-SHA2-256 Password Size: 32-character PIN Salt Size: 256 Security Strength: 256 bits Prerequisite: SHS Cert. #2942, HMAC Cert. #2280
RSA A1390	[FIPS 186-4] RSA Function: Digital signature verification with SHA2-256 Mode: PKCS#1 v1.5 Key size: 2048 Security Strength: 112 bits Prerequisite: SHS Cert. #2942
SHS 2942	[FIPS 180-4] SHS[5], Functions: Digital signature verification and in used in the HMAC function Mode: SHA2-256 Security Strength: 128 bits

Table 4 - FIPS Approved Algorithms

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

Table 5 – Approved Cryptographic Functions Tested with Vendor Affirmation

2.5 Approved Random Number Generator

A hardware NDRNG seeds the Approved [SP800-90A] DRBG. Available entropy does not modify the bit strength of the cryptographic keys generated by the module. The IG 7.15 assessment concluded that the noise source provides least 2.9831 bits of min entropy per 32-bit sample. Each time the DRBG is instantiated or reseeded, one hundred sixty (160) 32-bit samples seed the DRBG. This equates to 5120 bits of entropy data and translates to 477.296 bits of min-entropy. Therefore, 160 32-bit samples of entropy data provide at least 477 bits of min entropy, which is greater than the 384 bits of entropy required to instantiate the DRBG at a security strength of 256 bits. A security strength of 256 bits exceeds the minimum requirement of 112 bits of security strength established by NIST

[4] Tested HMAC-SHA1 and HMAC-SHA2-224. However, the cryptographic module does not use these algorithms.

[5] Tested SHA-1 and SHA2-224. However, the cryptographic module does not use these algorithms.

3 Ports and Interfaces

The Ultrastar DC HC550 uses a 29-pin Serial Attached SCSI (SAS) connector that conforms to the mechanical requirements of SFF-8680 or 68-pin Serial ATA connector that conforms to the mechanical requirements of SFF-8639. The Ultrastar DC HC650 uses a 29-pin Serial Attached SCSI (SAS) connector that conforms to the mechanical requirements of SFF-8680 Table 6 and Table 7 identifies the Cryptographic Module's ports and interfaces. The serial connector is a two-wire port that consists of signal and ground. Western Digital disables the serial connector (SIO) at its manufacturing facility before delivering the Cryptographic Module to customers. The Cryptographic Module does not provide a physical maintenance access interface.

FIPS 140-2 Interface	Cryptographic Module Port Connector Pins
Power	Power connector
Control Input	SAS or SATA connector, Serial connector(disabled)
Status Output	SAS or SATA connector, Serial connector (disabled)
Data Input	SAS or SATA connector, Serial connector (disabled)
Data Output	SAS or SATA connector, Serial connector (disabled)

Table 6 - Ultrastar DC HC550 Ports and Interfaces

FIPS 140-2 Interface	Cryptographic Module Port Connector Pins
Power	Power connector
Control Input	SAS connector, Serial connector(disabled)
Status Output	SAS connector, Serial connector (disabled)
Data Input	SAS connector, Serial connector (disabled)
Data Output	SAS connector, Serial connector (disabled)

Table 7 - Ultrastar DC HC650 Ports and Interfaces

4 Identification and Authentication Policy

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

4.1 Crypto Officer Roles

4.1.1 Secure ID (SID)

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

4.1.2 Admin SP Admin

This Crypto Officer role corresponds to the Admin SP Admin authority defined in the TCG Storage Opal SSC [2]. The Admin SP Admin authority can enable a Locking SP Admin.

4.1.3 Locking SP Admins (1-4)

This Crypto Officer role corresponds to the Locking SP Admin Authority as defined in the TCG Storage Opal SSC [2]. The CM enables Locking SP Admin1 by default. The CM disables Locking SP Admin 2, Admin 3, and Admin 4 by default. The Admin SP Admin authority can enable a Locking SP Admin. When the Single User Data Range (SUDR) feature is disabled, a Locking SP Admin can enable and disable Users, create and delete data ranges, set data range attributes, lock, unlock, and erase data ranges. A Locking SP Admin executes the Erase service to cryptographically erase a SUDR, a by invoking TCG Erase. A Locking SP Admin executes the Erase service to cryptographically erase a non-SUDR, a by invoking TCG GenKey. Both methods accomplish the same end by replacing the Media Encryption Key (MEK) assigned to the data range.

4.2 User Roles

4.2.1 Locking SP Users (1-9)

This user role corresponds to the Locking SP User Authorities as defined in the TCG Storage Opal SSC [2]. This role can lock and unlock LBA ranges to control the ability of an operator to read and write data to and from the CM. The CM enables at most nine (9) separate Users when operating in TCG Storage Opal Security Mode. Enabled Locking SP Admins enable Locking SP Users and assign them read/write/erase access to LBA data ranges. A Locking SP User cryptographically erases a SUDR by invoking TCG Erase or TCG GenKey within the Erase service. A Locking SP User cryptographically erases a non-SUDR by invoking TCG GenKey within the Erase service. Both methods accomplish the same end by replacing the Media Encryption Key (MEK) assigned to the data range.

4.3 Anybody

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

TCG Authority	Description	Authentication Type	Authentication Data
Admin SP SID	Crypto Officer role includes the Admin SP SID authority. The SID authority is defined in the TCG Storage Opal SSC [2]	Role-based	Admin SP SID PIN
Admin SP Admin	The Crypto Officer role includes the Admin SP Admin authority. The TCG Storage Opal SSC [2] defines the Admin SP Admin authority.	Role-based	Admin SP Admin PIN
Locking SP Admin [1-4]	The Crypto Officer role includes the Locking SP Admin authority. The TCG Storage Opal SSC [2] defines Locking SP Admin authority.	Role-based	Locking SP Admin [1-4] PIN
Locking SP User [1-9]	The User role includes the Locking SP User authority. The TCG Storage Opal SSC [2] defines the Locking SP User authority.	Role-based	Locking SP User [1-9] PIN
Anybody	Anybody is a role that does not require authentication. The TCG Storage Opal SSC [2] defines the Anybody authority.	Unauthenticated	N/A

Table 8 - Roles and Required Identification and Authentication

4.4 Authentication Method and Strength

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

Operators utilize an Authority PIN to authenticate to a Crypto Officer or User role. Authority PINs are 32-byte TCG credentials. For a 32-byte PIN, there are 2^{256} possible values. Each byte position contains a value from 0x00 to 0xFF. However, the module operates in FIPS non-Approved mode if any PIN equals all zeros or the MSID value. Assuming all possible values have an equal chance of use, the probability of guessing the correct PIN is one chance in 2^{256} or approximately 8.64×10^{-78}, which is significantly less than 1/1,000,000.

The TCG Opal security model includes a TryLimit attribute, which if exceeded, locks out further Admin SP or Locking SP authentication attempts. Assuming the TryLimit is non-zero[6], an Authority_Locked_Out state exists if the Tries count value exceeds the TryLimit value associated with either the Admin SP or Locking SP. Each authentication attempt consumes approximately 198 microseconds. Hence, at most, approximately 30,287 authentication attempts can occur within one minute when the TryLimit equals zero (0). Thus, the probability that a false acceptance occurs within a one-minute interval is approximately 2.62×10^{-73} ($8.64 \times 10^{-78} \times 30{,}287$), which is significantly less than 1/100,000.

5 Access Control Policy

5.1 Roles and Authenticated Services

Service	Description	Role(s)	Approved Mode	Non-Approved Mode
Activate	The Activate method allows the TPer owner to "turn on" a Security Provider (SP) that was created in manufacturing. LBA ranges are configured, and data encryption and access control credentials (re)generated and/or set within the Cryptographic Module. Access control is configured for LBA range unlocking.	CO (Admin SP SID, Admin SP Admin)	X	X
Authenticate	Input a TCG Credential for authentication	CO (Admin SP SID, Admin SP Admin, Locking SP Admins), Users (Locking SP Users),	X	X
Disable User Set PIN	This service disables the ability of a non-SUDR User to modify its own PIN.	CO (Locking SP Admins)	X	X
Enable/Disable Admin SP Admin	This service enables and disables an Admin SP Admin authority.	CO (Admin SP SID)	X	X
Enable/Disable Locking SP Admin or User (non-SUDR)	This service enables and disables a Locking SP Admin or non-SUDR User authority.	CO (Locking SP Admin)	X	X
Enable/Disable SUDR	This service enables and disables the classification of a data range as a SUDR.	CO (Locking SP Admins)	X	X

[6] When TryLimit is set to zero (0), the CM places no limit on the number of authentication attempts.

Service	Description	Role(s)	Approved Mode	Non-Approved Mode
Erase non-SUDR	A cryptographic erasure service that utilizes the TCG GenKey method to generate and replace the MEK assigned to an LBA data range	CO (Locking SP Admins) Users (Locking SP Users)	X	X
Erase SUDR	A cryptographic erasure service that utilizes the TCG GenKey or TCG Erase method to generate and replace the MEK assigned to an LBA data range	CO (Locking SP Admins)[7] Users (Locking SP Users)[8]	X	X
Field FA	This service provides basic drive health analysis testing and media verification. The service does not leak any clear text user data to the host interface. This service is limited to performing the following functions: • Basic health tests • Media verification All Host Read/Write Commands are inhibited.	CO (Admin SP SID, Admin SP Admin, Locking SP Admins) Users (Locking SP Users)	X	X
Initialize Cryptographic Module[9]	Crypto Officer provisions the Cryptographic Module from the organizational policies	CO (Admin SP SID, Admin SP Admin)	X	X
Lock/Unlock Data Range	This service denies or permits read and write access to an LBA range	CO (Locking SP Admins)[10], Users (Locking SP Users)	X	X
Lock/Unlock Firmware Download Control	Deny/Permit access to Firmware Download service	CO (Admin SP SID)	X	X
Set	Write data structures; access control enforcement occurs per data structure field. This service can change PINs.	CO (Admin SP SID, Admin SP Admin, Locking SP Admins) Users (Locking SP Users)	X	X
Set Data Range Attributes for a non-SUDR	This service sets the starting location, size, and locking attributes for a SUDR.	CO (Locking SP Admins) Users (Locking SP Users)	X	X
Set Data Range Attributes for a SUDR	This service sets the starting location, size, and locking attributes as well as the User access rights for a non-SUDR.	CO (Locking SP Admins) Users (Locking SP Users)	X	X
Set Data Store	Write a stream of bytes to unstructured storage.	Users (Locking SP Users)	X	X
Zeroize (TCG Revert)	This service utilizes the TCG Revert method to zeroize the CM and return the CM to its original manufactured state. Execution of this service requires knowledge of the Cryptographic Module's unique PSID[11].	CO (Admin SP SID, Admin SP Admin, Locking SP Admins) Users (Locking SP Users), Anybody	X	X

[7] TCG Erase

[8] TCG GenKey or TCG Erase

[9] See the Cryptographic Module Acceptance and Provisioning section within 7.2 Initialization Rules.

[10] Applies only to non-SUDRs

[11] See TCG Storage Opal SSC Feature Set: PSID [3]

Table 9 - Authenticated CM Services

5.2 Unauthenticated Services

Table 10 - Unauthenticated Services lists the unauthenticated services the *C*ryptographic Module provides.

Service	Description
End Session	End a TCG session by clearing all session state
FIPS 140 Compliance Descriptor[12]	This service reports the FIPS 140 revision as well as the Cryptographic Module's overall security level, hardware revision, firmware revision and module name.
Firmware Download	RSA2048 PKCS#1 v1.5 and SHA-256 verify the entire firmware image.
Generate Random	TCG Random method generates a random number from the SP800-90A DRBG
Get	Reads data structure; access control enforcement occurs per data structure field
Get Data Store	Read a stream of bytes from unstructured storage
Level 0 Discovery	TCG 'Level 0 Discovery' method outputs the FIPS mode of the Cryptographic Module
Read Data	This service decrypts user data when reading the data from a data range. The data range must be unlocked to enable reads from the data range.
Reset Module	Power on Reset
SecureDrive Command	TCG IF-SEND and IF-RECV transport secure commands to and from the Cryptographic Module. The SD SM Key verifies secure commands.
Security Receive	The Security Receive command transfers the status and data result of one or more Security Send commands that were previously submitted to the Cryptographic Module.
Security Send	The Security Send command is used to transfer security protocol data to the Cryptographic Module.
Self-Test	The Cryptographic Module performs self-tests when it powers up
SoC Rebuild	The SoC Rebuild service utilizes the SecureDrive Command service to zeroize and regenerate the Root Keyset and the Global Active Keyset
Start Session	Start TCG session
Status Output	TCG (IF-RECV) protocol
Write Data	This service encrypts user data when writing the data from a data range. The data range must be unlocked to enable writes to the data range.
Zeroize (TCG Revert)	This service utilizes the TCG Revert method to zeroize the CM and return the CM to its original manufactured state.

Table 10 - Unauthenticated Services

5.3 Definition of Critical Security Parameters (CSPs)

The Cryptographic Module contains the CSPs listed in Table 11 - Critical Security Parameters. Zeroization of CSPs complies with the purge requirements for SCSI Hard Disk drives within [SP800-88], Guidelines for Media Sanitization.

[12] See §5.1.5.3 FIPS 140 Compliance Descriptor within the Security Features for SCSI Commands [SFSC]

Name	Type	Description
NDRNG	5120-bit Entropy output	Entropy source for DRBG
DRBG.Seed	256-byte Entropy input	Internal state associated with the [SP800-90A] CTR_DRBG using AES-256 Sourced from NDRNG
DRBG.Key	256-bit value	Internal state associated with the [SP800-90A] CTR_DRBG using AES-256
DRBG.V	128-bit value	Internal state associated with the [SP800-90A] CTR_DRBG using AES-256.
Authority Digest	256-bit digest	An HMAC-SHA2-256 digest of an Authority PIN and its associated SED Admin SP key or SED Locking SP key.
Authority PIN	32-byte value	Values from 0x00 to 0xFF are allowed for each byte position. A PBKDF2 algorithm uses an Authority PIN to authenticate to the credential of a TCG Authority.
Admin SP SID PIN	Authority PIN	A 32-byte data value used to authenticate the TCG credential of the Admin SP SID Authority.
Admin SP Admin PIN	Authority PIN	A 32-byte data value used to authenticate the TCG credential of the Admin SP Admin Authority.
Locking SP Admin PIN (4 total)	Authority PIN	A 32-byte data value used to authenticate the TCG credential of each Locking SP Admin Authority.
Locking SP User PIN (9 total)	Authority PIN	A 32-byte data value used to authenticate the TCG credential of each Locking SP User Authority.
Root Keyset	256-bit keys Root Encryption Key Root Signing Key	The Root Encryption Key encrypts, and decrypts the Global Active Keyset. An HMAC-SHA-256 digest of the Root Signing Key and encrypted Global Active Keyset signs the Global Active Keyset. The Cryptographic Module's DRBG generates each key without modification.
Global Active Keyset (AEK)	Set of 256-bit keys: Global Active Key, Global Active Signing Key	The Global Active Key encrypts, and decrypts the SED Active Keyset, UAKa, and the Namespace Keys. An HMAC-SHA-256 digest of the Global Active Signing Key and the encrypted SED Active Keyset, UAKa or Namespace Key signs the respective CSP. The Cryptographic Module's DRBG generates each key without modification

Name	Type	Description
SED Active Keyset	Set of 256-bit keys: SED Active Key SED Active Signing Key	The SED Active Key encrypts and decrypts the SED Admin SP Keyset and the SED Locking SP Keyset. An HMAC-SHA-256 digest of the SED Active Signing Key and the encrypted SED Admin SP Keyset or encrypted SED Locking SP Keyset signs the respective keyset. The Cryptographic Module's DRBG generates each key without modification
SED Admin SP Keyset	Set of 256-bit keys: SED Admin SP Key SED Admin SP Signing Key	The SED Admin SP Key encrypts, and decrypts TCG table data associated with an Admin SP. An HMAC-SHA-256 digest of the SED Admin SP Signing Key and an Admin SP authority's table data signs the associated table. The Cryptographic Module's DRBG generates each key without modification
SED Locking SP Keyset	Set of 256-bit keys: SED Locking SP Key SED Locking SP Signing Key	The SED Locking SP Key encrypts, and decrypts table data associated with a Locking SP authority. An HMAC-SHA-256 digest of the SED Locking SP Signing Key and a Locking SP authority's table data signs the associated table. The Cryptographic Module's DRBG generates each key without modification
SED Volatile Keyset	Set of 256-bit keys: SED Volatile Key SED Volatile Signing Key	The SED Volatile Key encrypts, and decrypts keys stored in IRAM. An HMAC-SHA-256 digest of the SED Volatile Signing Key and an encrypted key stored in IRAM signs the key. The Cryptographic Module's DRBG generates each key without modification.
Admin Authority Key (K_a) (4 total)	256-bit key	PBKDF2 derived Ka keys encrypt and decrypt UAK_0 and the UMK. The Cryptographic Module derives a unique K_a for each Admin SP Admin. K_a keys are destroyed after use.
Non-Admin Authority Key (K_u) (9 total)	256-bit key	PBKDF2 derived Ku keys encrypt and decrypt their associated UAK. The Cryptographic Module derives a unique K_u for each Locking SP User. K_u keys are destroyed after use.
User Access Key (UAK) (9 total)	256-bit key	UAKs encrypt and decrypt RAKs. The Cryptographic Module generates a unique UAK for each Locking SP User. The Cryptographic Module's DRBG generates each key without modification.
Admin User Access Key (UAK_0)	256-bit key	UAK_0 encrypts and decrypts RAKs. All Admin SP Admins share UAK_0. The Cryptographic Module's DRBG generates the key without modification.

Name	Type	Description
Anybody User Access Key (UAK$_a$)	256-bit key	The Anybody Authority uses UAK$_a$ to encrypt and decrypt RAKs. The Cryptographic Module's DRBG generates the key without modification.
User Management Key (UMK)	256-bit key	The UMK encrypts and decrypts UAKs. All Admin SP Admins share the UMK. The Cryptographic Module's DRBG generates each key without modification.
Range Access Key (RAK) (16 total – 1 per LBA range)	256-bit key	RAKs encrypt and decrypt their associated LRK. The Cryptographic Module's DRBG generates each key without modification.
Locking Range Key (LRK) (16 total - 1 per LBA range)	Set of 256-bit keys: LRK.AES Key LRK.XTS Key	An LRK in combination with its associated NSK creates an MEK. The Cryptographic Module's DRBG generates each LRK.AES Key and LRK.XTS Key without modification.
Namespace Key (NSK) (16 total - 1 per LBA range)	Set of 256-bit keys: NSK.AES Key NSK.XTS Key	An NSK in combination with its associated LRK creates an MEK. The Cryptographic Module's DRBG generates each NSK.AES Key and NSK.XTS Key without modification.
MEK - Media Encryption Keyset (16 total - 1 per LBA range)	Derived set of 256-bit keys: MEK.AESEnc Key, MEK.AESDec Key MEK.XTS Tweak Key	The MEK encrypts and decrypts LBA ranges. The MEK.AESEnc Key is an XOR of an LRK.AES Key and an NSK.AES Key. The MEK.XTS.Tweak Key is an XOR of an LRK.XTS Key and an NSK.XTS Key. The MEK.AESDec key is the last entry of key schedule for an MEK.AESEnc key.

Table 11 - Critical Security Parameters

5.4 Definition of Public Security Parameters

The Cryptographic Module utilizes RSA public key cryptography to verify that firmware downloaded to the module is authentic and to verify specific steps in the secure boot process. The Cryptographic Module uses RSA 2048 PKCS#1 v1.5 to verify each signature within the asymmetric key tree to establish a chain of trust. The private key used in this process is stored within a Hardware Security Module (HSM), which generated the RSA Public/Private key pairs. The Cryptographic Module rejects the downloaded firmware image if the digital signature verification process fails.

Key Name	Type	Description
PSID[13]	32-character alphanumeric string	The PSID derives from a 32-byte value generated by the Cryptographic Module's DRBG, without modification. Passing the 32-byte value through an Alphanumeric Character Conversion process derives the alphanumeric string. The module's product label displays the PSID. The PSID provides authentication data and proof of physical presence for the Zeroize service.
MSID[14]	32-character alphanumeric string	The MSID derives from a 32-byte value generated by the Cryptographic Module's DRBG, without modification. Passing the 32-byte value through an Alphanumeric Character Conversion process derives the alphanumeric string.
KDF Salt	256-bit key	The PBKDF2 implementation utilizes unique KDF Salts to derive each UAK and the UMK. The Cryptographic Module's DRBG generates KDF Salts without modification.
Storage Device Certification Authority Key (SD_CA Key)	RSA 2048 PKCS#1 v1.5 public key	The SD_CA Key is the Master RSA Public Key used to verify the Secure Loader image.
Storage Device Boot FW Key (SD_BFW Key)	RSA 2048 PKCS#1 v1.5 public key	The SD_BFW Key is public key used to verify all boot flash images.
Storage Device Secure Message Key (SD_SM Key)	RSA 2048 PKCS#1 v1.5 public key	The SD_SM Key verifies secure messages used for manufacturing, development, and failure analysis
Security Core Firmware Key (SC_FW Key)	RSA 2048 PKCS#1 v1.5 public key	The SC_FW Key verifies the Access Control Module (ACM) images containing security core firmware.
Security Protocol Firmware Key (SP_FW Key)	RSA 2048 PKCS#1 v1.5 public key	The SP_FW Key verifies ACM firmware images that contain security protocol and services,
Product Group Key (PROD GROUP Key)	RSA 2048 PKCS#1 v1.5 public key	The PROD GROUP Key verifies an OEM's Key certificates.
OEM Firmware Key (OEM FW Key)	RSA 2048 PKCS#1 v1.5 public key	The OEM FW Key verifies OEM firmware images and packages.
OEM_Release Key (OEM_Release Key)	RSA 2048 PKCS#1 v1.5 public key	The OEM Release Key verifies the outer signature of an OEM firmware package.
OEM Original Factory State Key (OEM_OFS Key)	RSA 2048 PKCS#1 v1.5 public key	The OEM_OFS Key verifies the OEM Original Factory Settings files.

Table 12 - Public Security Parameters

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

[14] An HMAC SHA2-256 digest of the MSID is store in the Reserved Area. The TCG Revert method regenerates the digest.

5.5 SP800-132 Key Derivation Function Affirmations

- The Cryptographic Module utilizes an HMAC-SHA-256 based [SP800 132] Password Based Key Derivation Function (PBKDF2) that complies with Option 2a of SP800-132.
- Security Policy rules set the minimum Authority PIN length at 32-bytes. The Cryptographic Module allows values from 0x00 to 0xFF for each byte of the Authority PIN.
- The upper bound for the probability of guessing an Authority PIN is 2^{-256}. The difficulty of guessing the Authority PIN is equivalent to a brute force attack.
- Derived Authority Keys, K_a and K_u ([SP800 132] Master Keys) are derive by processing a clear-text 32-character Authority PIN ([SP800 132] Password) and a 256-bit KDF Salt through a PBKDF2 algorithm [SP800 132]. The Cryptographic Module derives unique K_a keys to protect UAK_0 and the UMK. The Cryptographic Module derives unique K_u keys to protect each Locking SP User UAK.
  - Each K_a and K_u has a security strength of 256-bits against a collision attack.
- Each 256-bit KDF Salt is a random number generated using the [SP800 90A] DRBG.

5.6 Definition of CSP Modes of Access

Table 13 and Table 14 define the relationship between access to Critical Security Parameters (CSPs) and the listed Cryptographic Module services. The definitions shown below define the access modes listed in each table.

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

Service	Authority Digest	Admin SP SID PIN Admin SP Admin PIN	Locking SP Admin PINs Locking SP User PINs	DRBG.Seed	DRBG.Key	DRBG.V	NDRNG	MEK	Ka	Ku	LRK	RAK
Activate				E	GE	GE		GS	GS	GS	GS	GS
Authenticate	E	IE	IE						E	E		
Diagnostics												
Disable User Set PIN												
Enable/Disable Admin SP Admin												

Service	**Authority Digest**	**Admin SP SID PIN** **Admin SP Admin PIN**	**Locking SP Admin PINs** **Locking SP User PINs**	**DRBG.Seed**	**DRBG.Key**	**DRBG.V**	**NDRNG**	**MEK**	**Ka**	**Ku**	**LRK**	**RAK**
Enable/Disable Locking SP Admin or User (non-SUDR)												
Enable/Disable SUDR												
Erase non-SUDR								GSZ			GSZ	E
Erase SUDR								GSZ			GSZ	E
End Session												
Field FA												
FIPS 140 Compliance Descriptor												
Firmware Download												
Generate Random				E	GE	GE						
Get												
Get Data Store								E		E	E	E
Initialize Cryptographic Module	GS	IE	IE	GE	GE	GE	GE	GS	GS	GS	GS	EGS
Level 0 Discovery												
Lock/Unlock Data Range												
Lock/Unlock Firmware Download Control												
Read Data								E			E	E
Reset Module				GEZ	GEZ	GEZ	GE	S			S	S
SecureDrive Command												
Security Receive												
Security Send												
Self-Test (KATs)												
Set		I	I									
Set Data Range Attributes for a non-SUDR												

Service	Authority Digest	Admin SP SID PIN Admin SP Admin PIN	Locking SP Admin PINs Locking SP User PINs	DRBG.Seed	DRBG.Key	DRBG.V	NDRNG	MEK	Ka	Ku	LRK	RAK
Set Data Range Attributes for a SUDR												
Set Data Store								E			E	E
SoC Rebuild												
Start Session												
Status Output												
Write Data								E			E	E
Zeroize (TCG Revert)	GZ	Z	Z	GE	GE	GE		GSZ	Z	Z	GSZ	EGSZ

Table 13 - CSP Access Rights within Roles & Services

Service	UAK	UAK_0	UAKa	UMK	NSK	Root Keyset	Global Active Keyset (AEK)	SED Active Keyset	SED Admin SP Keyset	SED Locking SP Keyset	SED Volatile Keyset
Activate	GS	GS	GS	GS	GS						
Authenticate											
Diagnostics											
Disable User Set PIN											
Enable/Disable Admin SP Admin											
Enable/Disable Locking SP Admin or User (non-SUDR)											
Enable/Disable SUDR											
Erase non-SUDR				E	GSZ						
Erase SUDR				E	GSZ						

Service	UAK	UAK$_0$	UAKa	UMK	NSK	Root Keyset	Global Active Keyset (AEK)	SED Active Keyset	SED Admin SP Keyset	SED Locking SP Keyset	SED Volatile Keyset
End Session											
Field FA											
FIPS 140 Compliance Descriptor											
Firmware Download											
Generate Random											
Get											
Get Data Store	E	E	E	E	E	E	E	E	E	E	E
Initialize Cryptographic Module	GS	GS	GS	GS	GS						
Level 0 Discovery											
Lock/Unlock Data Range											
Lock/Unlock Firmware Download Control											
Read Data	E	E	E	E	E	E	E	E	E	E	E
Reset Module	S	S	S	S							GS
SecureDrive Command											
Self-Test (KATs)											
Security Receive											
Security Send											
Set											
Set Data Range Attributes for a non-SUDR											
Set Data Range Attributes for a SUDR											
Set Data Store	E	E	E	E	E	E	E	E	E	E	E
SoC Rebuild						GSZ	GSZ				
Start Session											
Status Output											
Write Data	E	E	E	E	E	E	E	E	E	E	E

Service	**UAK**	**UAK$_0$**	**UAKa**	**UMK**	**NSK**	**Root Keyset**	**Global Active Keyset (AEK)**	**SED Active Keyset**	**SED Admin SP Keyset**	**SED Locking SP Keyset**	**SED Volatile Keyset**
Zeroize (TCG Revert)	GSZ	GSZ	GSZ	GSZ	GSZ			GSZ	GSZ	GSZ	GSZ

Table 14 - CSP Access Rights within Roles & Services

5.7 Definition of PSP Modes of Access

Table 15 defines the relationship between access to Public Security Parameters (PSP) and the listed Cryptographic Module services. The definitions shown below define the access modes listed in the table.

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

Service	**MSID**	**PSID**	**KDF Salt**	**SD_CA Key**	**SD_BFW Key**	**SD_SM Key**	**SC_FW Key**	**SP_FW Key**	**PROD_GROUP Key**	**OEM_FW Key**	**OEM_Release Key**	**OEM_OFS Key**
Activate												
Authenticate			E									
Diagnostics												
Disable User Set PIN												
Enable/Disable Admin SP Admin												
Enable/Disable Locking SP Admin or User (non-SUDR)												
Enable/Disable SUDR												
Erase non-SUDR												
Erase SUDR												
End Session												

Service	MSID	PSID	KDF Salt	SD_CA Key	SD_BFW Key	SD_SM Key	SC_FW Key	SP_FW Key	PROD_GROUP Key	OEM_FW Key	OEM_Release Key	OEM_OFS Key
Field FA						E						
FIPS 140 Compliance Descriptor												
Firmware Download										IS	ES	IS
Generate Random												
Get												
Get Data Store												
Initialize Cryptographic Module	OE		GS									
Level 0 Discovery												
Lock/Unlock Data Range												
Lock/Unlock Firmware Download Control												
Read Data												
Reset Module				E	E		E	E	E	E		
SecureDrive Command						E						
Security Receive												
Security Send												
Self-Test (KATs)												
Set												
Set Data Range Attributes for a non-SUDR												
Set Data Range Attributes for a SUDR												
Set Data Store												
SoC Rebuild												
Start Session												
Status Output												
Write Data												
Zeroize (TCG Revert)		I	GSZ									

Table 15 - PSP Access Rights within Roles & Services

6 Operational Environment

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

7 Security Rules

The Cryptographic Module enforces applicable FIPS 140-2 Level 1 security requirements. This section documents the security rules that the Cryptographic Module enforces.

7.1 Invariant Rules

1. The Cryptographic Module supports three distinct types of operator roles: Crypto Officer and User. The module does not support the Makers authority or a Maintenance Role.
2. Power cycling the Cryptographic Module clears all existing authentications.
3. After the Cryptographic Module has successfully completed all self-tests and initialized according to the instructions provided in Section 7.2, it is in FIPS Approved mode.
4. When the Cryptographic Module is unable to authenticate TCG Credentials, operators do not have access to any cryptographic service other than the unauthenticated services.
5. The Cryptographic Module performs the following tests. Upon failure of any test, the Cryptographic Module enters a soft error state. A failing Cryptographic Module reports the error condition by transmitting a UEC to the host over its logical interface. After entering the soft error state, a failing Cryptographic Module does not process functional commands unless a power cycle occurs.
   a. Power up Self-Tests
      i. SHA-256 KAT, SHS Cert. #2942
      ii. HMAC-SHA-256 KAT, HMAC Cert. #2280
      iii. AES ECB Encrypt KAT, AES Cert. #3580
      iv. AES ECB Decrypt KAT, AES Cert. #3580
      v. RSA 2048 PKCS#1 v1.5 Verify KAT, Cert. #A1390
      vi. SP 800-90B Entropy Source Health Test
      vii. Firmware Integrity, RSA 2048 PKCS#1 v1.5 Digital Signature, Cert. #A1390
      viii. DRBG KAT[15], Cert. #A1390
      ix. PBKDF2 KAT, Cert. #A1390
      x. AES ECB Encrypt KAT, DEE, Cert. #A670
      xi. AES ECB Decrypt KAT, DEE, Cert. #A670
   b. Conditional Tests
      i. The Cryptographic Module performs an SP 800-90B compliant Repetition Count Test (RCT) and an Adaptive Proportion Test (APT) heath test on the hardware NDRNG entropy source after seeding the [SP 800 90A] CTR-DRBG 2^{32} times. The same RCT and APT health tests run during the Power up Self-Test.
      ii. The Cryptographic Module performs a key comparison test on each LRK.AESKey/LRK.XTS and NSK.AESKey/NSK.XTS keyset to assure compliance with IG A.9 XTS-AES Key Generation Requirements.
      iii. Firmware Download Test, RSA 2048 PKCS#1 v1.5 (Cert. #1390), SHA-256 (SHS Cert. #2942)
6. An operator can command the Cryptographic Module to perform the power-up self-test by power cycling the device.
7. Power-up self-tests do not require operator action.

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

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 compromise the Cryptographic Module.
10. The Zeroize service deletes all plaintext keys and CSPs.
11. Thebuild service deletes the Root Keyset and Global Active Keyset.
12. The Cryptographic Module does not support manual key entry.
13. The Cryptographic Module does not have any external input/output devices used for entry/output of data.
14. The Cryptographic Module does not output plaintext CSPs.
15. The Cryptographic Module does not output intermediate key values.
16. The Cryptographic Module does not support concurrent operators.
17. The Cryptographic Module requires operators to re-authenticate to TCG Authorities after power cycling the module or upon execution of the End Session service.
18. The Crypto Officer shall assure that all host issued Authority PINs are 32-bytes in length and not equal to all zeros.

7.2 Initialization Rules

The Crypto Officer can determine if the Cryptographic Module is operating in a FIPS approved mode by invoking the Level 0 Discovery service. If the Cryptographic Module is operating non-Approve mode, the Crypto Officer shall initialize the modules cryptographic services by executing the mandatory instructions listed below. The Crypto Officer shall follow the delivery and operational instructions within the Delivery & Operation (Crypto Officer's) Manual for acceptance and end of life procedures.

1. Mandatory Initialization Instructions
   a. Invoke StartSession and SyncSession for the 'Admin SP'
   b. Get MSID
   c. Use the MSID to authenticate to the Admin SP SID
      i. An authentication failure indicates that a tamper event has occurred for the Cryptographic Module
   d. Set the Admin SP SID PIN to a new 32-byte value
   e. Set Enabled to True within the Admin SP Admin SPInfo [1] table
   f. Set the Admin SP Admin PIN to a new 32-byte value
   g. Set 'Makers.Enabled = FALSE'
   h. Call TCG Activate command
   i. EndSession
2. Optional Highly Recommended Initialization Instructions
   a. Invoke StartSession and SyncSession for the 'Locking SP'
   b. Use the Admin SP SID PIN to authenticate to Locking SP Admin1
   c. Set the Locking SP Admin1 PIN for the to a new 32-byte value.
   d. Set Enabled to True within the Locking SP Admin2 SPInfo table.
   e. Set the PIN for Locking SP Admin2 to a new 32-byte value.
   f. Repeat steps 3.d and 3.d for Locking SP Admin3 and Locking SP Admin4
   g. Set Enabled to True within the Locking SP User1 SPInfo table.
   h. Set the PIN for Locking SP User1 to a new 32-byte value.
   i. Repeat steps 3.g and 3.h for Locking SP User2 through Locking SP User9

   j. EndSession

3. Power cycle or reset the Cryptographic Module. (This step is mandatory)

At the end of the initialization process, the Cryptographic Module will be in a FIPS Approved Mode of operation.

7.3 Zeroization Rules

The Crypto Officer shall use the TCG Revert Method to zeroize all CSPs, apart from the Root Keyset and the Global Active Set. After successfully executing TCG Revert, the Crypto Officer shall power cycle the module. Power cycling the module assures the erasure of all CSPs stored in volatile memory. Reverting and power cycling the Cryptographic Module zeroizes all Critical Security Parameters within the scope of the TCG Revert Method.

The Crypto Officer may execute the SoC Rebuild service to protect the integrity of the Cryptographic Module. The SoC Rebuild service zeroizes and regenerates the Root Keyset and the Global Active Keyset. Executing this service exhausts an SoC life. The module is inoperable when the SoC life count equals zero.

8 Physical Security Policy

8.1 Mechanisms

The Cryptographic Module does not make claims in the Physical Security area beyond FIPS 140-2 Security Level 1.

- All components are production-grade materials with standard passivation.
- The enclosure is opaque

9 Mitigation of Other Attacks Policy

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

10 Definitions

- **Allowed**: NIST approved, i.e., recommended in a NIST Special Publication, or acceptable, i.e., no known security risk as opposed to deprecated, restricted and legacy-use. [SP800-131A]
- **Anybody**: A formal TCG term for an unauthenticated role [1].
- **Approved mode of operation**: A mode of the Cryptographic Module that employs only approved security functions. [FIPS140]
- **Approved**: [FIPS140] approved or recommended in a NIST Special Publication.
- **Authenticate**: Prove the identity of an Operator or the integrity of an object.
- **Authorize**: Grant an authenticated Operator access to a service or an object.
- **Ciphertext**: Encrypted data transformed by an Approved security function.
- **Confidentiality**: A cryptographic property that sensitive information is not disclosed to unauthorized parties.
- **Credential**: A formal TCG term for data used to authenticate an Operator [1].
- **Critical Security Parameter (CSP)**: Security-related information (e.g., secret, and private cryptographic keys, and authentication data such as credentials and PINs) whose disclosure or modification can compromise the security of a Cryptographic Module. [FIPS140]
- **Cryptographic Boundar**y: An explicitly defined continuous perimeter that establishes the physical bounds of a Cryptographic Module and contains all the hardware, software, and/or firmware components of a Cryptographic Module. [FIPS140]

- **Cryptographic key (Key)**: An input parameter to an Approved cryptographic algorithm
- **Cryptographic Module**: The set of hardware, software, and/or firmware used to implement approved security functions contained within the cryptographic boundary. [FIPS140]
- **Crypto Officer**: An Operator performing cryptographic initialization and management functions. [FIPS140]
- **Data at Rest**: User data residing on the storage device media when the storage device is powered off.
- **Discovery**: A TCG method that provides the properties of the TCG device. [TCG Enterprise]
- **Drive Writes per Day (DWPD):** Drive Writes per Day defines how many times the entire capacity of the HDD can be overwrite every single day of its usable life without failure during the warranty period.
- **Hardware Security Module (HSM):** A hardware security module is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication, and other cryptographic functions.
- **Integrity**: A cryptographic property to assure sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **Interface**: A logical entry or exit point of a Cryptographic Module that provides access to the Cryptographic Module for logical information flows. [FIPS140]
- **Intelligent RAM (IRAM): IRAM**: Intelligent RAM contains 1024 memory blocks each 1kb wide. The advantages of IRAM include lower memory latency, higher memory bandwidth, lower system power, adjustable memory width and size, and less board space.
- **Key Derivation Function (KDF)**: An Approved cryptographic algorithm by which one or more keys are derived from a shared secret and other information.
- **Key Encrypting Key (KEK)**: A cryptographic key used to encrypt or decrypt other keys.
- **Key management**: The activities involving the handling of cryptographic keys and other related security parameters during the entire life cycle of the Cryptographic Module. The handling of authentication data is representative of a key management activity.
- **Key Wrap**: An Approved cryptographic algorithm that uses a KEK to provide Confidentiality and Integrity.
- **LBA Range**: A formal TCG SWG [1] term that defines a contiguous logical block range (sequential LBAs) to store encrypted User Data; ranges do not overlap, and each has its own unique encryption key and other settable properties.
- **Manufactured SID (MSID)**: A unique default value assigned to each SED during manufacturing. An externally visible MSID value is not required if the user can derive the MSID from other information printed on the drive. The MSID is readable with the TCG protocol. It is the initial and default value for all TCG credentials [1].
- **Method**: A remote procedure call to an SP that initiates an action on the SP [1].
- **Namespace:** A namespace is a collection of logical blocks that range from zero (0) to the capacity of the namespace.
- **Namespace Identifier (NSID):** A namespace identifier is an identifier used by a controller to provide access to a namespace.
- **OFS file**: OFS files are used to reset the Cryptographic Module's configuration back to its original factory setting during the Revert operations (e.g., TCG Revert).
- **Operator**: A consumer, either human or automation, of cryptographic services that is external to the Cryptographic Module. [FIPS140]

- **Personal Identification Number (PIN)**: A formal TCG term designating a string of octets used to authenticate an identity [1].
- **Plaintext**: Unencrypted data.
- **Port**: A physical entry or exit point of a Cryptographic Module that. A port provides access to the Cryptographic Module's physical signals. [FIPS140]
- **PSID (Physical Security Identifier)**: A SED unique value printed on the Cryptographic Module's label used as authentication data and proof of physical presence for the Zeroize service.
- **Public Security Parameters (PSP)**: Public information, that if modified can compromise the security of the Cryptographic Module (e.g., a public key).
- **Read Data**: An external request to transfer User Data from the SED. [SBC-3]
- **Reserved Area**: Private data on the Storage Medium that is not accessible outside the Cryptographic Boundary.
- **Sanitize:** Sanitization cryptographically erases all user data in the NVM subsystem such that recovery of any previous user data from any cache, non-volatile media, or any controller memory buffer is not possible.
- **SD_CA Key**: Storage Device Certification Authority Key (X509v3). This key serves as the Cryptographic Module's Master RSA Public Key and is the root source of verification for all other key certificates. The SD_CA Key signs the SecureLoader. This key is injected at manufacturing time and a hash of this key is stored as OTP bits.
- **Security Identifier (SID)**: The authority that represents the TPer owner [1]. Crypto Officer serves in this role.
- **Security Provider (SP):** A TCG term used to define a collection of Tables and Methods with access control.
- **Self-Encrypting Drive (SED)**: A storage device that provides data storage services, which automatically encrypts all user data written to the device and automatically decrypts all user data read from the device.
- **Session**: A formal TCG term that envelops the lifetime of an Operator's authentication [1].
- **Small Form Factor (SFF):** Small form factor is a computer form factor designed to minimize the volume and footprint of a desktop computer
- **Storage Medium**: The non-volatile, persistent storage location of a SED; it is partitioned into two disjoint sets, a User Data area, and a Reserved Area.
- **Table**: The basic data structures within a Security Provider (SP). The tables store persistent SP state data defined in TCG Storage Core specification [1].
- **TPer:** A Trusted Peripheral [1].
- **Triple Level Cell (TLC)**: Triple level cells refer to NAND flash devices that store three bits of information per cell, with eight total voltage states.
- **User Data**: Data transferred from/to a SED using the Read Data and Write Data commands. [SBC-3]
- **User**: An Operator that consumes cryptographic services. [FIPS140]
- **Write Data**: An external request to transfer User Data to a SED. [SBC-3]
- **Zeroize**: Invalidate a Critical Security Parameter. [FIPS140]

11 Acronyms

- **AEK:** Active Encryption Key
- **AES:** Advanced Encryption Standard (FIPS 197)

- **BLRE:** Boot Loader (Engine?)
- **CAC:** Cryptographic Assist Controller
- **CBC:** Cipher Block Chaining, an operational mode of AES
- **CM:** Cryptographic Module
- **CO**: Crypto Officer [FIPS140]
- **CRC**: Cyclic Redundancy Check
- **CSP**: Critical Security Parameter [FIPS140]
- **DEE:** Data Encryption Engine
- **DRAM**: Dynamic Random Access Memory
- **DRBG**: Deterministic Random Bit Generator
- **DW/D:** Drive Writes per Day
- **EDC:** Error Detection Code
- **EMI**: Electromagnetic Interference
- **FSEC:** Flash Security Data
- **FID:** Flash Internal Data
- **FIPS**: Federal Information Processing Standard
- **HDD**: Hard Disk Drive
- **IRAM: Intelligent RAM**
- **IV**: Initialization Vector
- **KAT**: Known Answer Test
- **KDF**: Key Derivation Function
- **LBA**: Logical Block Address
- **MEK**: Media Encryption Key
- **MSID**: Manufactured Security Identifier
- **NAND: N**egative AND, Flash Memory technology
- **NOR: N**egative OR, Flash Memory technology
- **NDRNG**: Non-deterministic Random Number Generator
- **NIST**: National Institute of Standards and Technology
- **NSID:** Namespace Identifier
- **NVM:** Non-volatile Memory
- **NVMe:** NVM Express
- **OFS:** Original Factory Setting
- **PBKDF2**: Password Base Key Derivation Function
- **PCIe:** Peripheral Component Interconnect Express
- **PIN**: Personal Identification Number
- **POR**: Power on Reset
- **PSID**: Physical Security Identifier
- **PSP**: Public Security Parameter
- **RID:** Reserved Area Internal Data
- **SAS**: Serial Attached SCSI
- **SECD:** Security Data
- **SED:** Self-Encrypting Drive
- **SCSI**: Small Computer System Interface
- **SD_CA**: Storage Device Certification Authority
- **SED**: Self Encrypting Drive
- **SFF:** HDD Form Factor or Small Form Factor
- **SID**: Security Identifier, The TCG authority representing the Cryptographic Module owner
- **SIO**: Serial Input/Output
- **SOC**: System-on-a-Chip
- **SP**: Security Provider or Security Partition (TCG), also Security Policy (FIPS 140)
- **SSC**: Subsystem Class
- **SSD**: Solid-state Drive
- **SWG**: Storage Work Group
- **TCG**: Trusted Computing Group
- **TLC:** Triple Level Cell
- **UEC:** Universal Error Code
- **XTS**: A mode of AES that utilizes "Tweakable" block ciphers

12 References

12.1 NIST Specifications

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

12.2 Trusted Computing Group Specifications

- [1] TCG Storage Architecture Core Specification, Specification Version 2.01 Revision 1.00 (August 5, 2015)
- [2] TCG Storage Security Subsystem Class: Opal, Specification Version 2.01, Final Revision 1.00 (August 5, 2015)
- [3] TCG Storage Opal SSC Feature Set: PSID, Specification Version 1.00, Final Revision 1.00 (August 5, 2015)
- [4] TCG Storage Opal SSC Feature Set: Configurable Namespace Locking, Specification Version 1.00, Final Revision 1.33 (February 22, 2019)
- [5] TCG Storage Opal SSC Feature Set: Single User Mode, Specification Version 1.00, Final Revision 1.00 (February 24, 2012)
- [6] TCG Storage Opal Integration Guidelines, Version 1.00, Final Revision 1.00 (March 16, 2016)
- [7] TCG Storage Interface Interactions Specification (SIIS), Version 1.02, (2011)

12.3 International Standards

- [SBC-3] SBC-3 Commands - 3, Revision 22, March 29, 2010
- [SFSC] Security Features for SCSI Commands, Revision 2, September 25, 2015

- [SPC-5] SCSI Primary Commands - 5, Revision 22, April 19, 2019
- [SFF-TA-1002] Protocol Agnostic Multi-Lane High Speed Connector, Revision 1.3, February 19, 2020

12.4 Corporate Documents

- [Product Manual] Ultrastar DC HC550 3.5-inch Serial Attached SCSI (SAS) Product Manual, Version 1.5 (January 2021), https://www.westerndigital.com/support
- [Product Manual] Ultrastar DC HC550 3.5-inch Serial ATA (SATA) Product Manual, Version 1.3 (January 2021), https://www.westerndigital.com/support
- [Product Manual] Ultrastar DC HC650 3.5-inch Serial Attached SCSI (SAS) Product Manual, Version 1.4 (November 2020), https://www.westerndigital.com/support
- [Datasheet] Ultrastar DC HC550 Datasheet, (September 2020), https://www.westerndigital.com/support
- [Datasheet] Ultrastar DC HC650 Datasheet, (July 2020), https://www.westerndigital.com/support