Ultrastar DC HC550 TCG Enterprise HDD
FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Protection of Data at Rest

Document Version: 1.6
2023-07-26

Contents

Tables

Figures

1. Cryptographic Module Overview

The self-encrypting Ultrastar DC HC550 TCG Enterprise HDD, hereafter referred to as Ultrastar DC HC550, Cryptographic Module, or CM is a multi-chip embedded module that complies with FIPS 140-2 Level 2 security. The Cryptographic Module complies with the Trusted Computing Group (TCG) SSC: Enterprise Specification. The drive enclosure defines the cryptographic boundary. See Figure 1: Ultrastar DC HC550 Cryptographic Module. All components within this boundary satisfy FIPS 140-2 requirements. The physical interface to the Cryptographic Module is the SAS connector and SIO port pins. In FIPS Approved mode and non-Approve mode, the Cryptographic Module disables the SIO port pins (red box in Figure 1) to the right of the SAS connector. The logical interface is the industry standard TCG SWG [TCG Core] and [TCG Enterprise] protocols, which uses the SAS transport interface [SAS]. The primary function of the Cryptographic Module is to provide data encryption, access control, and cryptographic erase of 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. Except for the four-conductor motor control cable, all components within the cryptographic boundary tested as compliant with FIPS 140-2 requirements. The control cable is not security relevant and therefore excluded from FIPS 140-2 requirements.

Figure 1: Ultrastar DC HC550 Cryptographic Module

1.1 Models

Multiple models define the scope of the Cryptographic Module. The different models vary in storage capacity and disk format type. Table 1 provides the model numbers, characteristics, and firmware versions associated with each validated model.

Model Number	Firmware	Description
WUH721814AL5205	R6A0, R6D2, R6D3	14 TB, 512e, 3.5-inch HDD, 7200 RPM, 12 Gb/s SAS
WUH721816AL5205	R290, R650, R680, R684, R6A0, R6D2, R6D3, UM05, UM06, UM08	16 TB, 512e, 3.5-inch HDD, 7200 RPM, 12 Gb/s SAS
WUH721818AL5205	R290, R650, R680, R684, R6A0, R6D2, R6D3, UM05, UM06, UM08	18 TB, 512e, 3.5-inch HDD, 7200 RPM, 12 Gb/s SAS
WUH721814AL4205	R6A0, R6D2, R6D3	14 TB, 4Kn, 3.5-inch HDD, 7200 RPM, 12 Gb/s SAS
WUH721816AL4205	R290, R650, R680, R684, R6A0, R6D2, R6D3, UM05, UM06, UM08	16 TB, 4Kn, 3.5-inch HDD, 7200 RPM, 12 Gb/s SAS
WUH721818AL4205	R290, R650, R680, R684, R690, R6A0, R6D2, R6D3, UM05, UM06, UM08	18 TB, 4Kn, 3.5-inch HDD, 7200 RPM, 12 Gb/s SAS

Table 1 Ultrastar DC HC550 TCG Enterprise HDD Models

1.2 Security Level

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

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

Table 2 - Module Security Level Specification

2. 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. The Cryptographic Module 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. An operator can determine if the Cryptographic Module is operating in a FIPS Approved mode by invoking the Level 0 Discovery service[1]. The Cryptographic Module disables authentication to the Makers Authority after the Cryptographic Module enters FIPS Approved mode. After initialization, setting any Authority PIN to MSID and power cycling the Cryptographic Module causes the Cryptographic Module to transition to non-Approved mode. After the Cryptographic Module transitions to non-Approved mode, the Crypto Officer shall execute the Zeroize service. If the Crypto Officer, subsequently, executes the Initialize Cryptographic service instructions provided in Section 7.2 with the intent of placing the Cryptographic Module in FIPS Approved mode, the Crypto Officer shall first execute the Zeroize service.

The chapter titled FIPS 140 Crypto Officer Instructions within the Ultrastar DC HC550 Product Manual provides information on how to execute the Initialize Cryptographic service as well as the TCG Revert Method.

2.2 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 Function: AES-CBC-256 encrypts and decrypts CSPs. Mode: ECB, CBC, XTS Key Size: 128[2], 256 Key Strength: 128 bits and 256 bits

[1] The InFIPS bit is set to one when FIPS Approved mode has been configured.

[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.

CAVP Cert	Algorithm Standards and Function
AES A670	[FIPS 197, SP 800-38A, SP 800-38E] AES 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 Key Size: 128[3], 256 Key Strength: 128 bits and 256 bits
DRBG A1389[4], 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: 384 Key Strength: 256 bits Prerequisite: AES Cert. #3580
HMAC 2280	[FIPS 198-1] HMAC Function: Used to sign and verify CSPs and derive keys in PBKDF2. Mode: SHA-1[5], SHA2-224, and SHA2-256 Key Size: 256 Key Strength: 256 bits Prerequisite: SHS Cert. #2942
PBKDF A1389, A1390[6]	[SP 800-132] PBKDF2 Function: PBKDF2 utilizes a 32-character PIN (password) and 256-bit KDF Salt to generate 256-bit Derived Authority Keys. Mode: HMAC-SHA2-256 Key Size: 256 Key Strength: 256 bits Prerequisite: SHS Cert. #2942, HMAC Cert. #2280
RSA A1389, A1390	[FIPS 186-4] RSA Function: Digital signature verification with SHA2-256 Mode: PKCS#1 v1.5 Key size: 2048 Key Strength: 256 bits Prerequisite: SHS Cert. #2942
SHS 2942	[FIPS 180-4] SHS Functions: Digital signature verification and in used in the HMAC function Mode: SHA-1[7], SHA2-224 SHA2-256 Key Size: 160, 224, and 256 Key Strength: 256 bits

Table 3 - FIPS Approved Algorithms

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

Table 4 – Approved Cryptographic Functions Tested with Vendor Affirmation

[3] Tested AES ECB-128 and AES-XTS-128. However, the cryptographic module does not use these algorithms.
[4] A1389 is only applicable to firmware release R290 and later in the R200 code brand
[5] Tested HMAC-SHA1 and HMAC-SHA2-224. However, the cryptographic module does not use these algorithms.
[6] A1390 is only applicable to firmware release R650 and later in the R600 code branch
[7] Tested SHA-1 and SHA2-224. However, the cryptographic module does not use these algorithms.

The Cryptographic Module supports the following non-Approved but allowed algorithm:

- A hardware NDRNG seeds the Approved [SP800-90A] DRBG. Available entropy does not modify the security strength of the cryptographic keys generated by the module. Each 32-bit sample block contains at least 2.9277 bits of min-entropy. Each time the DRBG is instantiated or reseeded, one hundred sixty (160) 32-bit samples seed the DRBG. This equates to 5120 bits of entropy data and translates to at least 468.432 bits of min-entropy. The nonce consumes approximately 156 bits. Therefore, approximately 312 bits of entropy remain to determine the bit strength of the keys generated by the DRBG. The bit security strength of an AES based CTR-DRBG implementation limits the bit strength to 256 bits. A security strength of 256 bits exceeds the minimum requirement of 256 bits of security strength established by NIST.

3. Ports and Interfaces

The drive uses the standard 29-pin Serial Attached SCSI (SAS) connector that conforms to the mechanical requirements of SFF 8680. Table 5 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 prior to shipment of the Cryptographic Module. The Cryptographic Module does not provide a maintenance access interface.

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 5 - Ultrastar DC HC550 Pins and FIPS 140-2 Ports and Interfaces

4. Identification and Authentication Policy

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

4.1 Crypto Officer Roles

4.1.1 Secure ID (SID)

This Crypto Officer role corresponds to the Admin SP Secure ID (SID) Authority as defined in the TCG Storage Security Subsystem Class: Enterprise Specification [TCG Enterprise].

4.1.2 EraseMaster

This Crypto Officer role corresponds to the Locking SP EraseMaster Authority as defined in the TCG Storage Security Subsystem Class: Enterprise Specification [TCG Enterprise]. The EraseMaster is a single dedicated authority used to reset one or more LBA Ranges by invoking the Erase method on the Locking object representing that Range. It can disable User roles.

4.2 User Roles

4.2.1 BandMaster

This user role corresponds to the Locking SP Bandmaster Authority as defined in the TCG Storage Security Subsystem Class: Enterprise Specification [TCG Enterprise]. BandMasters lock and unlock LBA ranges and configure LBA bands (user data regions) to control the ability of an operator to read and write data to the Cryptographic Module. The EraseMaster Authority can disable a BandMaster. The Cryptographic Module supports a maximum of sixteen (16) active BandMaster Authorities.

4.2.2 Anybody

The Anybody role executes services that do not require authentication. With two exceptions, these services do not disclose, modify, or substitute Critical Security Parameters when using an Approved security function, or otherwise affect the security of the Cryptographic Module. The Generate Random service provides an output from the SP 800-90A DRBG. The Zeroize service utilizes the TCG Revert method to cryptographically erase CSPs and return the Cryptographic Module to its original manufactured state.

4.3 Makers

For failure analysis purposes, authorized Western Digital personnel can enable a logical diagnostic port to perform diagnostics and gather data on the failure within a Western Digital facility. A power cycle automatically disables the logical diagnostic port. An operator must authenticate to the SID authority and the Makers authority to enable the logical diagnostic port. Authentication to the Makers authority is blocked in FIPS Approved mode. Authenticating to the Makers authority requires access to secure server controlled by Western Digital. A signed secure message, which includes a unique ID, issued by the secure server is necessary to authenticate to the Makers authority.

TCG Authority	Description	Authentication Type	Authentication Data
SID	The SID Authority is a Crypto Officer role that initializes the Cryptographic Module and authorizes Firmware downloads.	Role-based	CO Identity (SID Authority) and PIN (SID Authority PIN)
EraseMaster	The EraseMaster Authority is a Crypto Officer role that zeroizes Media Encryption keys and disables Users.	Role-based	CO Identity (EraseMaster Authority) and PIN (EraseMaster PIN)
BandMasterN (N = 0 to 15)	The BandMaster Authority is a User role that controls read/write access to LBA Bands.	Role-based	User Identity (BandMaster Authority) and PIN (BandMaster PIN)
Anybody	Anybody is a role that does not require authentication.	Unauthenticated	N/A
Makers	Completion of the Initialize Cryptographic Module service blocks authentication to the Makers Authority	Role-based	CO Identity (SID Authority) and PIN (Makers PIN)

Table 6 - 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 service 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 the Crypto Officer, User or Makers role. Authority PINs are 32-byte TCG credentials. For any Authority PIN, there are 2^{256} possible values. Values from 0x00 to 0xFF are allowed at each byte position. Assuming all possible values have an equal chance of use, the probability of guessing the correct value is one chance in 2^{256} or approximately 8.64×10^{-78}, which is significantly less than 1/1,000,000.

The TCG Enterprise security model includes a TryLimit attribute, which if exceeded, locks out further Admin SP or Locking SP authentication attempts. Assuming the TryLimit is not set to zero[8], 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 848 microseconds. Hence, at most, approximately 70,720 (TryLimit = 0) authentication attempts are possible in one minute. Thus, the probability that a false acceptance occurs within a

[8] When TryLimit is set to zero the module places no limit on the number of authentication attempts.

one-minute interval is approximately 6.1 x 10^{-73} (8.64 x 10^{-78} x 70,720), which is significantly less than 1 chance in 100,000.

5. Access Control Policy

5.1 Roles and Services

Service	Description	Role(s)	Approved Mode	Non-Approved
Initialize Cryptographic Module[9]	Crypto Officer provisions the Cryptographic Module from the organizational policies	CO (SID)	X	X
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 on the Cryptographic Module. Access control is configured for LBA range unlocking.	CO (SID)	X	X
Authenticate	Input a TCG Credential for authentication	CO (SID, EraseMaster), Users (BandMasters), Makers	X	X
Lock/Unlock Firmware Download Control	Deny/Permit access to Firmware Download service	CO (SID)	X	X
Firmware Download	RSA2048 PKCS#1 v1.5 and SHA-256 verify the entire firmware image. After a successful download, the SED executes the new firmware object code.	CO (SID)	X	X
Set	Write data structures; access control enforcement occurs per data structure field. This service can change PINs.	CO (SID, EraseMaster) Users (BandMasters)	X	X
Set Band Attributes	Set the starting location, size, and attributes of an LBA band.	Users (BandMasters)	X	X
Lock/Unlock LBA Band	Deny/Permit access to a LBA Band	Users (BandMasters)	X	X
Write Data	Transform plaintext user data into ciphertext and write in a LBA band.	Users (BandMasters)	X	X
Read Data	Read ciphertext from a LBA band and output user plaintext data.	Users (BandMasters)	X	X
Set Data Store	Write a stream of bytes to unstructured storage.	Users (BandMasters)	X	X
Erase LBA Band	This service cryptographically erases user data within a specific LBA Range and resets the access control of that LBA Range	CO (EraseMaster)	X	X

[9] See the Cryptographic Module Acceptance and Provisioning section within the Ultrastar DC HC550 Product Manual.

Service	Description	Role(s)	Approved Mode	Non-Approved
Field FA	This service provides basic drive health analysis testing and media verification. The service does not leak any clear text user data to the host interface. This service is limited to performing the following functions: • Basic health tests • Media verification. • All Host Read/Write Commands are inhibited.	CO (SID) Users (BandMasters)	X	X
Diagnostics	A non-Approved service that is unavailable after the Initialize Cryptographic Module service completes. For failure analysis purposes, the vendor can enable a logical diagnostic port to perform diagnostics and gather data on the failure.	Makers		X

Table 7 - Authenticated CM Services

5.2 Unauthenticated Services

Table 8 - Unauthenticated Services lists the unauthenticated services the *C*ryptographic Module provides.

Service	Description
Reset Module	Power on Reset
Self-Test	The Cryptographic Module performs self-tests when it powers up
Status Output	TCG (IF-RECV) protocol
Level 0 Discovery	TCG 'Level 0 Discovery' method outputs the FIPS mode of the Cryptographic Module
Start Session	Start TCG session
End Session	End a TCG session by clearing all session state
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
SCSI	[SCSI Core] and [SCSI Block] commands to function as a standardized storage device. See Table 13 - SCSI Commands
FIPS 140 Compliance Descriptor[10]	This service reports the FIPS 140 revision as well as the Cryptographic Module's overall security level, hardware revision, firmware revision and module name.
Zeroize (TCG Revert)	The TCG Revert method cryptographically erases CSPs and returns the Cryptographic Module to its original manufactured state.
SecureDrive Command	The SAS native protocol IF-SEND and IF-RCV transport secure commands to and from the Cryptographic Module. The SD SM Key verifies secure commands.
SoC Rebuild	The SoC Rebuild service utilizes the SecureDrive Command service to zeroize and regenerate the Root Keyset and the Global Active Keyset

Table 8 - Unauthenticated Services

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

5.3 Definition of Critical Security Parameters (CSPs)

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

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 AdminSP Active key or SED LockingSP Active 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 the credential of a TCG Authority.
BandMaster PIN (16 total - 1 per LBA band)	Authority PIN	A 256-bit data used to authenticate the TCG Authority credential of a BandMaster.
Crypto Officer PIN	Authority PIN	A 256-bit data used to authenticate the TCG Authority credentials of the SID.
EraseMaster PIN	Authority PIN	A 256-bit data used to authenticate the TCG Authority credential of the EraseMaster.
Root Keyset	Set of 256-bit keys: Root Encryption Key Root Signing Key	The Root Encryption Key encrypts the Global Active Keyset. The HMAC-SHA256 Root Signing Key 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 the SED Active Keyset and the Namespace Keys. The HMAC-SHA256 Global Active Signing Key signs the SED Active Keyset. The Cryptographic Module's DRBG generates each key without modification
SED Active Keyset	Set of 256-bit keys: SED Active Key SED Active Signing Key	The SED Active Key encrypts/decrypts the SED Admin SP Active Keyset and the SED Locking SP Active Keyset. The HMAC-SHA256 SED Active Signing Key signs the SED Admin SP Active Keyset and the SED Locking SP Active 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/decrypts CSPs that belong to the Admin SP. The HMAC-SHA256 SED Admin SP Signing Key signs CSPs that belong to the Admin SP. The Cryptographic Module's DRBG generates each key without modification

Name	Type	Description
SED Locking SP Keyset	Set of 256-bit keys: SED Locking SP Key SED Locking SP Signing Key	The SED Locking SP Key encrypts/decrypts CSPs that belong to the Locking SP. The HMAC-SHA256 SED Locking SP Signing Key signs CSPs that belong to the Locking SP. 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/decrypts keys stored in IRAM. The HMAC-SHA256 SED Volatile Signing Key signs keys that are stored in IRAM. The Cryptographic Module's DRBG generates each key without modification.
Admin Authority Key (K_a)	256-bit key	This PBKDF2 derived key encrypts and decrypts UAKs and the UMK. The K_a key is destroyed after use.
Non-Admin Authority Key (K_u) (16 total - 1 per LBA band)	256-bit key	These PBKDF2 derived keys encrypt and decrypt all UAKs except UAK_a. K_u keys are destroyed after use.
User Access Key (UAK) (16 total - 1 per LBA band)	256-bit key	UAKs encrypt and decrypt RAKs. The Cryptographic Module's DRBG generates each key without modification.
Anybody User Access Key[11] (UAK_a)	256-bit key	The Anybody Authority uses UAK_a to decrypt the RAK of unlocked LBA bands. The Cryptographic Module's DRBG generates each key without modification.
User Management Key (UMK)	256-bit key	The CM uses the UMK to decrypt UAKs. The Cryptographic Module's DRBG generates each key without modification.
Range Access Key (RAK)	256-bit key	RAKs encrypt/decrypt LRKs. The Cryptographic Module's DRBG generates each key without modification.
Locking Range Key (LRK) (16 total - 1 per LBA band)	Set of 256-bit keys: LRK.AES Key, LRK.XTS Key	An LRK is used in combination with an NSK to create 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 band)	Set of 256-bit keys: NSK.AES Key, NSK.XTS Key	An NSK is used in combination with an LRK to create 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 band)	Derived set of 256-bit keys: MEK.AESEnc Key, MEK.AESDec Key MEK.XTS Tweak Key	The MEK encrypts and decrypts LBA bands. 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 9 - CSPs

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 is used to generate the RSA Public/Private key pairs. The Cryptographic Module rejects the downloaded firmware image if the digital signature verification process fails.

[11] The AEK encrypts the UAK_a.

Key Name	Type	Description
PSID[12]	32-character alphanumeric string	The PSID is derived from a 32-byte value generated by the Cryptographic Module's DRBG, without modification. The alphanumeric string is derived by passing the 32-byte value through an Alphanumeric Character Conversion process. The value is displayed on the module's product label. The PSID provides authentication data and proof of physical presence for the Zeroize service.
MSID[13]	32-character alphanumeric string	The MSID is derived from a 32-byte value generated by the Cryptographic Module's DRBG, without modification. The alphanumeric string is derived by passing the 32-byte value through an Alphanumeric Character Conversion process.
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 OEM.x 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 10 - Public Security Parameters

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.

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

- 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 though an PBKDF2 algorithm [SP800 132]. The Cryptographic Module creates a K_a key to protect the EraseMaster UMK and unique K_u keys to protect each BandMaster 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 11 and Table 12 define the relationship between access to Critical Security Parameters (CSPs) and the listed Cryptographic Module services. The definitions shown below define the access modes listed in Table 11 and Table 12.

- **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	Authority PIN (BandMaster PIN, Crypto Officer PIN, EraseMaster PIN)	DRBG	NDRNG	MEK	K_a	K_u	LRK	RAK
Initialize Cryptographic Module	GS	IE	GE	GE	GS	GS	GS	GS	GS
Activate			GE		GS	GS	GS	GS	GS
Authenticate	E	IE				E	E		
Lock/Unlock Firmware Download Control									
Firmware Download									
Set		I							
Set Band Attributes									
Lock/Unlock LBA Band									
Write Data					E			E	E
Read Data					E			E	E
Set Data Store					E			E	E
Field FA									
Erase LBA Band					GSZ			GSZ	GSZ
Self-Test (KATs)									

Service	Authority Digest	Authority PIN (BandMaster PIN, Crypto Officer PIN, EraseMaster PIN)	DRBG	NDRNG	MEK	K_a	K_u	LRK	RAK
Reset Module (Power on Reset)			GE	GE	S			S	S
Status Output									
Level 0 Discovery									
Start Session									
End Session									
Generate Random			GE						
Get Data Store					E		E	E	E
Get									
Zeroize (TCG Revert)	GZ	Z	GE		GSZ	Z	Z	GSZ	GSZ
SoC Rebuild									
SCSI									
SecureDrive Command									
Diagnostics									
FIPS 140 Compliance Descriptor									

Table 11 - CSP Access Rights within Roles & Services

Service	UAK	UMK	NSK	Root Keyset	Global Active Keyset (AEK)	SED Active Keyset	SED Admin SP Keyset	SED Locking SP Keyset	SED Volatile Keyset
Initialize Cryptographic Module	GS	GS	GS						
Activate	GS	GS	GS						
Authenticate									
Lock/Unlock Firmware Download Control									
Firmware Download									
Set									
Set Band Attributes									
Lock/Unlock LBA Band									
Write Data	E	E	E	E	E	E	E	E	E
Read Data	E	E	E	E	E	E	E	E	E

Service	UAK	UMK	NSK	Root Keyset	Global Active Keyset (AEK)	SED Active Keyset	SED Admin SP Keyset	SED Locking SP Keyset	SED Volatile Keyset
Set Data Store	E	E	E	E	E	E	E	E	E
Field FA									
Erase LBA Band		E	GSZ						
Self-Test (KATs)									
Reset Module (Power on Reset)	S	S							GS
Status Output									
Level 0 Discovery									
Start Session									
End Session									
Generate Random									
Get Data Store	E	E	E	E	E	E	E	E	E
Get									
Zeroize (TCG Revert)	GSZ	GSZ	GSZ			GSZ	GSZ	GSZ	GSZ
SoC Rebuild				GSZ	GSZ				
SCSI									
SecureDrive Command									
Diagnostics									
FIPS 140 Compliance Descriptor									

Table 12 - CSP Access Rights within Roles & Services

5.7 Definition of PSP Modes of Access

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

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

Service	MSID	PSID	KDF Salt	SD_CA Key	SD_BFW Key	SD_SM Key	SC_FW Key	SP_FW Key	PROD_GROUP Key	OEM_FW Key	OEM_Release Key	OEM_OFS Key
Initialize Cryptographic Module	OE		GS									
Activate												
Authenticate			E									
Lock/Unlock Firmware Download Control												
Firmware Download									E	ES	ES	E
Set												
Set Band Attributes												
Lock/Unlock LBA Band												
Write Data												
Read Data												
Set Data Store												
Field FA						E						
Erase LBA Band												
Self-Test (KATs)												
Reset Module (Power on Reset)				E	E		E	E	E	E		
Status Output												
Level 0 Discovery												
Start Session												
End Session												
Generate Random												
Get Data Store												
Get												
Zeroize (TCG Revert)		I	GSZ									
SoC Rebuild												
SCSI												
SecureDrive Command						E						
Diagnostics												
FIPS 140 Compliance Descriptor												

Table 13 - PSP Access Rights within Roles & Services

6. Operational Environment

The Cryptographic Module's operating environment is non-modifiable. Therefore, the FIPS 140-2 operational environment requirements are not applicable to this module. 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. If the download operation is successful, authorized, and verified, the Cryptographic Module will begin operating with the new code working set. Firmware loaded into the module that is not on the FIPS 140-2 certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

7. Security Rules

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

7.1 Invariant Rules

1. The Cryptographic Module supports two distinct types of operator roles: Crypto Officer and User. The module also supports an additional role, the Makers role. Initialization blocks authentication to the Makers role.
2. Cryptographic Module power cycles clear 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 Generate Random service.
5. The Cryptographic Module performs the following tests. Upon failure of any test, the Cryptographic Module enters a soft error state. The Cryptographic module reports the error condition by transmitting an UEC via the [SCSI] protocol. After entering the soft error state, the Cryptographic Module does not process functional commands unless a power cycle occurs.
    a. Power up Self-Tests
        i. SHA-256 KAT, Cert. #SHS 2942
        ii. HMAC-SHA-256 KAT, Cert. #HMAC 2280
        iii. AES Encrypt ECB KAT, Cert. #AES 3580
        iv. AES Decrypt ECB KAT, Cert. #AES 3580
        v. RSA 2048 PKCS#1 v1.5 Verify KAT, Certs. #A1389 and #A1390
        vi. SP 800-90B Entropy Source Health Test
        vii. Firmware Integrity, RSAPKCS#1 v1.5 2048 Digital Signature, Certs. #A1389 and #A1390
        viii. DRBG KAT[14], Certs. #A1389 and #A1390
        ix. PBKDF2 KAT, Certs. #A1389, and #A1390
        x. AES Encrypt ECB KAT, DEE, Cert. #A670
        xi. AES Decrypt ECB KAT, DEE, Cert. #A670
    b. Conditional Tests
        i. The Cryptographic Module performs a Repetition Count Test and Adaptive Proportion Test on the hardware NDRNG entropy source.

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

   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 (Certs #A1389 and #A1390), SHA-256 (Cert. #SHS 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.
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. The SoC Rebuild service deletes the Root Keyset and Global Active Keyset.
12. The Cryptographic Module does not support a maintenance role.
13. The Cryptographic Module does not support manual key entry.
14. The Cryptographic Module does not have any external input/output devices used for entry/output of data.
15. The Cryptographic Module does not output plaintext CSPs.
16. The Cryptographic Module does not output intermediate key values.
17. The Cryptographic Module does not support concurrent operators.
18. The Cryptographic Module requires operators to re-authenticate to TCG Authorities after power cycling the module or upon execution of the End Session service.
19. The Crypto Officer shall assure that all host issued Authority PINs are 32-bytes in length.
20. After a Firmware Download, the Crypto Officer shall execute "Set Firmware_Dload_Port.PortLocked = True".

7.2 Initialization Rules

The Crypto Officer shall initialize the modules cryptographic services by executing the TCG methods listed below. The FIPS 140 Crypto Officer Instructions section of the Ultrastar DC HC550 Product Manual provides the same instructions. 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. StartSession and SyncSession using the 'Admin SP'
   a. Get MSID
   b. Use the MSID to authenticate to the SID.
      i. An authentication failure indicates that a tamper event has occurred for the Cryptographic Module
   c. Set 'SID PIN' to a new 32-byte value
   d. Set 'Makers.Enabled = FALSE'
   e. Set 'Firmware_Dload_Port.PortLocked = True'
   f. Set 'Firmware_Dload_Port.LockOnReset = PowerCycle'
2. EndSession
3. StartSession and SyncSession using the 'Locking SP'
   a. Use the MSID to authenticate to the EraseMaster
      i. An authentication failure indicates that a tamper event has occurred for the Cryptographic Module
   b. Set 'EraseMaster PIN' to a new 32-byte value
   c. Erase Band0
   d. Use the MSID to authenticate to BandMaster0.
      i. An authentication failure indicates that a tamper event has occurred for the Cryptographic Module.

e. Set 'BandMaster0 PIN' to a new 32-byte
f. Repeat steps 3.d and 3.e for BandMaster1 to BandMaster15.

4. EndSession
5. Power cycle or reset the Cryptographic Module.

At the end of the initialization process, the Cryptographic Module will be in a FIPS Approved Mode of operation. While in FIPS Approved mode, only an authenticated Crypto Officer can change the state of the firmware download service.

7.3 Zeroization Rules

The Crypto Officer shall use the Zeroize service to zeroize all CSP, apart from the Root Keyset and the Global Active Set. After successfully executing the Zeroize service, the Crypto Officer shall power cycle the module. Power cycling the module assures the erasure of all CSPs stored in volatile memory.

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

8. Physical Security Policy

8.1 Mechanisms

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

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

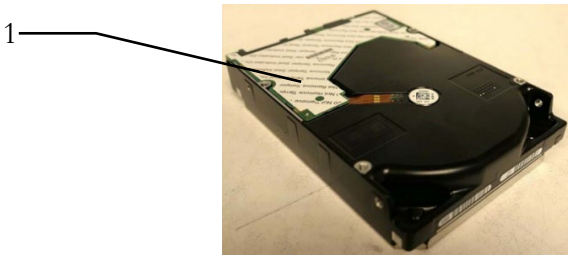

Figure 2: Tamper-Evident Seal

8.2 Operator Responsibility

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

Figure 3: Tamper Evidence on Tamper Seal

9. Mitigation of Other Attacks Policy

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

10. Definitions

- **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. [TCG Core]

- **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. [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. [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]
- **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 Band**: A formal [TCG Core] term that defines a contiguous logical block range (sequential LBAs) to store encrypted User Data; bands do not overlap, and each has its own unique encryption key and other settable properties.

- **Manufactured SID (MSID)**: A unique default value assigned to each SED during manufacturing. An externally visible MSID value is not required if the user can derive the MSID from other information printed on the drive. The MSID is readable with the TCG protocol. It is the initial and default value for all TCG credentials. [TCG Core]
- **Method**: A remote procedure call to an SP that initiates an action on the SP. [TCG Core]
- **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. [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. [FIPS140]
- **PSID (Physical Security Identifier)**: A SED unique value printed on the Cryptographic Module's label used as authentication data and proof of physical presence for the Zeroize service.
- **Public Security Parameters (PSP)**: Public information, that if modified can compromise the security of the Cryptographic Module (e.g., a public key).
- **Read Data**: An external request to transfer User Data from the SED. [SCSI Block]
- **Reserved Area**: Private data on the Storage Medium that is not accessible outside the Cryptographic Boundary.
- **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. 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.
- **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 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 Core specification. [TCG Core]
- **TPer:** A Trusted Peripheral. [TCG Core]
- **Triple Level Cell (TLC)**: Triple level cells refer to NAND flash devices that store three bits of information per cell, with eight total voltage states.
- **User Data**: Data transferred from/to a SED using the Read Data and Write Data commands. [SCSI Block]
- **User**: An Operator that consumes cryptographic services. [FIPS140]

- **Write Data**: An external request to transfer User Data to a SED. [SCSI Block]
- **Zeroize**: Invalidate a Critical Security Parameter. [FIPS140]

11. Acronyms

- **AEK:** Active Encryption Key
- **AES:** Advanced Encryption Standard (FIPS 197)
- **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
- **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
- **OFS:** Original Factory Setting
- **PBKDF2**: Password Base Key Derivation Function
- **PIN**: Personal Identification Number
- **POR**: Power on Reset
- **PSID**: Physical Security Identifier
- **PSP**: Public Security Parameter
- **RID:** Reserved Area Internal Data
- **SAS**: Serial Attached SCSI
- **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

- [TCG Core] *TCG Storage Architecture Core Specification,* Version 2.0 Revision 1.0 (April 20, 2009)
- [TCG Enterprise] *TCG Storage Security Subsystem Class: Enterprise Specification,* Version 1.00 Revision 3.00 (January 10, 2011)
- [TCG App Note] *TCG Storage Application Note: Encrypting Storage Devices Compliant with SSC: Enterprise,* Version 1.00 Revision 1.00 Final
- [TCG Opal] *TCG Storage Security Subsystem Class: Opal Specification,* Version 2.00 Final Revision 1.00 (February 24, 2012)
- TCG Storage Interface Interactions Specification (SIIS), Version 1.02, (2011)

12.3 International Standards

- [SCSI Core] SCSI Primary Commands (SPC-5)
- [SCSI Block] SCSI Block Commands (SBC-3)
- [SAS] Serial Attached SCSI (SAS-4)
- [SFSC] Security Features for SCSI Commands

12.4 Corporate Documents

- [Product Manual] Ultrastar DC HC550 2.5-inch Serial Attached SCSI (SAS) Solid-State Drive Product Manual, Version 1.0 (March 2020), https://www.westerndigital.com/support
- [Datasheet] Ultrastar DC HC550 Product Brief, (November 2019), https://www.westerndigital.com/products/data-center-drives/ultrastar-sas-series-HDD

12.5 SCSI Commands

Table 14 - SCSI Commands

Description	Code	Description	Code
FORMAT UNIT	04h	RESERVE	16h
INQUIRY	12h	RESERVE	56h
LOG SELECT	4Ch	REZERO UNIT	01h
LOG SENSE	4Dh	SANITIZE	48h
MODE SELECT	15h	SEEK (6)	0Bh
MODE SELECT	55h	SEEK (10)	2Bh
MODE SENSE	1Ah	SEND DIAGNOSTIC	1Dh
MODE SENSE	5Ah	SET DEVICE IDENTIFIER	A4h/06h
PERSISTENT RESERVE IN	5Eh	START STOP UNIT	1Bh
PERSISTENT RESERVE OUT	5Fh	SYNCHRONIZE CACHE (10)	35h
PRE-FETCH (16)	90h	SYNCHRONIZE CACHE (16)	91h
PRE-FETCH (10)	34h	TEST UNIT READY	00h
READ (6)	08h	UNMAP	42h
READ (10)	28h	VERIFY (10)	2Fh
READ (12)	A8h	VERIFY (12)	AFh
READ (16)	88h	VERIFY (16)	8Fh
READ (32)	7Fh/09h	VERIFY (32)	7Fh/0Ah
READ BUFFER	3Ch	WRITE (6)	0Ah
READ CAPACITY (10)	25h	WRITE (10)	2Ah
READ CAPACITY (16)	9Eh/10h	WRITE (12)	AAh
READ DEFECT DATA	37h	WRITE (16)	8Ah
READ DEFECT DATA	B7h	WRITE (32)	7Fh/0Bh
READ LONG (16)	9Eh/11h	WRITE AND VERIFY (10)	2Eh
READ LONG	3Eh	WRITE AND VERIFY (12)	AEh
REASSIGN BLOCKS	07h	WRITE AND VERIFY (16)	8Eh
RECEIVE DIAGNOSTICS RESULTS	1Ch	WRITE AND VERIFY (32)	7Fh/0Ch
RELEASE	17h	WRITE BUFFER	3Bh
RELEASE	57h	WRITE LONG (10)	3Fh
REPORT DEVICE IDENTIFIER	A3h/05h	WRITE LONG (16)	9Fh/11h
REPORT LUNS	A0h	WRITE SAME (10)	41h

Description	Code		Description	Code
REPORT SUPPORTED OPERATION CODES	A3h/0Ch		WRITE SAME (16)	93h
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS	A3h/0Dh		WRITE SAME (32)	7Fh/0Dh
REQUEST SENSE	03h			