



Long Live Data™

HGST Ultrastar He<sup>10</sup> TCG Enterprise HDD  
FIPS 140-2 Cryptographic Module  
Non-Proprietary Security Policy

*Protection of Data at Rest*

Version: 1.6  
2016-11-21

Copyright 2016, HGST, a Western Digital company. Public Material - May be reproduced only in its original entirety [without revision].

## CONTENTS

1. Cryptographic Module Overview .....	4
1.1 Models .....	4
1.2 Security Level .....	5
2. Modes of Operation .....	5
2.1 FIPS Approved Mode of Operation .....	5
2.2 Approved Algorithms .....	5
3. Ports and Interfaces .....	6
4. Identification and Authentication Policy .....	6
4.1 Cryptographic Officer .....	6
4.1.1 Secure ID (SID) Authority .....	6
4.1.2 EraseMaster Authority .....	6
4.2 BandMaster (User) .....	6
4.3 Anybody .....	7
4.4 Maker .....	7
5. Access Control Policy .....	8
5.1 Roles and Services .....	8
5.2 Unauthenticated Services .....	9
5.3 Definition of Critical Security Parameters (CSPs) .....	9
5.4 Definition of Public Security Parameters .....	10
5.5 SP800-132 Key Derivation Function Affirmations .....	10
5.6 Definition of CSP Modes of Access .....	11
6. Operational Environment .....	12
7. Security Rules .....	12
7.1 Invariant Rules .....	12
7.2 Initialization Rules .....	13
7.3 Zeroization Rules .....	13
8. Physical Security Policy .....	14
8.1 Mechanisms .....	14
8.2 Operator Responsibility .....	14
9. Mitigation of Other Attacks Policy .....	15
10. Definitions .....	15
11. Acronyms .....	16
12. References .....	17
12.1 NIST Specifications .....	17
12.2 Trusted Computing Group Specifications .....	18
12.3 International Committee on Information Technology Standards T10 Technical Committee Standards .....	18
12.4 HGST Documents .....	18
12.5 SCSI Commands .....	18

**Tables**

Table 1 Ultrastar He<sup>10</sup> TCG Enterprise HDD Models .....4  
Table 2 - Module Security Level Specification .....5  
Table 3 - FIPS Approved Algorithms.....6  
Table 4 - Ultrastar He<sup>10</sup> FIPS 140-2 Ports and Interfaces .....6  
Table 5 - Roles and Required Identification and Authentication .....7  
Table 6 - Authentication Mechanism Strengths .....7  
Table 7 - Authenticated CM Services .....8  
Table 8 - Unauthenticated Services .....9  
Table 9 - CSPs and Private Keys .....10  
Table 10 - Public Security Parameters .....10  
Table 11 - CSP Access Rights within Roles & Services .....12  
Table 12 - SCSI Commands .....20

**Figures**

Figure 1: Ultrastar He<sup>10</sup> Cryptographic Boundary.....4  
Figure 2: Tamper-Evident Label .....14  
Figure 3: Tamper Evidence on Tamper Label.....14

## 1. Cryptographic Module Overview

The self-encrypting *HGST Ultrastar He<sup>10</sup> TCG Enterprise HDD*, hereafter referred to as “Ultrastar He<sup>10</sup>” or “the Cryptographic Module” is a multi-chip embedded module that complies with FIPS 140-2 *Level 2* security. The Ultrastar He<sup>10</sup> complies with the *Trusted Computing Group (TCG) SSC: Enterprise Specification*. The drive enclosure defines the cryptographic boundary. See Figure 1: Ultrastar He<sup>10</sup> Cryptographic Boundary. All components within this boundary are tested against the FIPS 140-2 requirements except for the four-conductor motor control cable. This part was excluded from the FIPS 140-2 requirements because it is not security relevant.



**Figure 1: Ultrastar He<sup>10</sup> Cryptographic Boundary**

### 1.1 Models

The Ultrastar He<sup>10</sup> is available in several models that vary by storage capacity and block size. The validated models listed below utilize the listed base version of Ultrastar He<sup>10</sup> firmware and associated security library. The hardware version of each model is enclosed in the parenthesis that follow each part number.

Part Number (Hardware Version)	Firmware	Description
HUH721010AL5205 (0001)	R308, R328, R32A, NA00, NE00	10TB, 512e, 3.5 inch HDD, 7200 RPM, 12 Gb/s, SAS
HUH721010AL4205 (0001)	R308, R328, R32A, NA00, NE00	10TB, 4Kn, 3.5 inch HDD, 7200 RPM, 12 Gb/s, SAS
HUH721008AL5205 (0001)	R308, R328, R32A, NA00, NE00	8TB, 512e, 3.5 inch HDD, 7200 RPM, 12 Gb/s, SAS
HUH721008AL4205 (0001)	R308, R328, R32A, NA00, NE00	8TB, 4Kn, 3.5 inch HDD, 7200 RPM, 12 Gb/s, SAS

**Table 1 Ultrastar He<sup>10</sup> 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	2
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. The Cryptographic Module enters FIPS Approved Mode after successful completion of the Initialize Cryptographic service instructions. The FIPS mode bit is set to 1 after the Cryptographic Officer executes the Set Makers.Enabled = FALSE instruction. The Cryptographic Officer shall not enable the Maker Authority after the Cryptographic Module enters FIPS Approved mode. If the Cryptographic Officer enables the Maker Authority after the module enters FIPS Approved mode the Cryptographic Officer must also zeroize the module by executing the TCG Revert Method. The Cryptographic Officer shall not exercise the Disable Zeroize service after the cryptographic module enters FIPS Approved mode.

### 2.2 Approved Algorithms

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

FIPS Approved Algorithm	CAVP Certificate
ASIC AES ECB-128, AES ECB-256	3881
ASIC AES XTS-128, AES XTS-256 <sup>1</sup> Note: XTS is only used for storage applications. AES XTS-128 was tested but not used.	3881
AES ECB-256 (Firmware)	3880

<sup>1</sup> The length of the XTS-AES data unit does not exceed 2<sup>20</sup> blocks.

FIPS Approved Algorithm	CAVP Certificate
RSA 2048 PSS Verify using SHA-256 (Cert. #3203 or Cert. #3204)	1978
SHA-256 (Firmware)	3203
SHA-256 (Hardware & Firmware)	3204
HMAC-SHA-256 Used in SP 800-132 PBKDF	2522
SP 800-132 PBKDF	Vendor Affirmed
SP 800-38F AES-256 Key Wrap	3880
SP 800-90A CTR DRBG	1108

**Table 3 - FIPS Approved Algorithms**

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

- Hardware NDRNG for seeding the Approved SP800-90A DRBG

### 3. Ports and Interfaces

Table 4 below identifies the Cryptographic Module’s ports and interfaces. The Cryptographic Module does not provide a maintenance access interface.

FIPS 140-2 Interface	Cryptographic Module Ports
Power	Power connector [SAS]
Control Input	SAS connector [SAS]
Status Output	SAS connector [SAS]
Data Input	SAS connector [SAS]
Data Output	SAS connector [SAS]

**Table 4 - Ultrastar He<sup>10</sup> FIPS 140-2 Ports and Interfaces**

### 4. Identification and Authentication Policy

The Cryptographic Module enforces the following FIPS140-2 operator roles.

#### 4.1 Cryptographic Officer

##### 4.1.1 Secure ID (SID) Authority

This TCG authority initializes the Cryptographic Module. Section 11.3.1 of the [TCG Storage Security Subsystem Class: Enterprise Specification](#) defines this role.

##### 4.1.2 EraseMaster Authority

This TCG authority can selectively zeroize bands within the Cryptographic Module. Section 11.4.1 of the [TCG Storage Security Subsystem Class: Enterprise Specification](#) defines this role. The TCG EraseMaster authority can disable Users and erase LBA bands (user data regions).

#### 4.2 BandMaster (User)

User roles correspond to Bandmaster Authorities. Section 11.4.1 of the [TCG Storage Security Subsystem Class: Enterprise Specification](#) provides a definition. Users have the authority to lock, unlock, and configure LBA bands (user data regions) and to issue read and write commands to the SED.

### 4.3 Anybody

Services are provided that do not require authentication. With one exception, these do not disclose, modify, or substitute Critical Security Parameters, use an Approved security function, or otherwise affect the security of the Cryptographic Module. The excepted service is the Generate Random service, which provides output from an instance of the SP800-90A DRBG.

### 4.4 Maker

For failure analysis purposes, out of scope services are available to the vendor to configure and perform failure analysis within the vendor’s facilities after the cryptographic module exits FIPS Approved mode. The Maker authority is disabled when the Cryptographic Officer invokes the Initialize Cryptographic Module service.

The following table maps TCG authorities to FIPS 140-2 roles.

TCG Authority	Description	Authentication Type	Authentication Data
SID Authority	The SID Authority is a Cryptographic Officer role that initializes the Cryptographic Module and authorizes Firmware download.	Role-based	CO Identity (TCG <i>SID Authority</i> ) and PIN (TCG <i>SID Authority PIN</i> )
EraseMaster Authority	The EraseMaster Authority is a Cryptographic Officer role that zeroizes Media Encryption keys and disables Users.	Role-based	CO Identity (TCG <i>EraseMaster Authority</i> ) and PIN (TCG <i>EraseMaster PIN</i> )
BandMaster N (N = 0 to 15)	BandMaster is User role that controls read/write access to LBA Bands.	Role-based	User Identity (TCG <i>BandMaster Authority</i> ) and PIN (TCG <i>BandMaster PIN</i> )
Anybody	Anybody is a role that does not require authentication.	Unauthenticated	N/A
Maker (Disabled)	Maker is a TCG Authority that is not available upon completion of the Initialize Cryptographic Module service	Role-based	User Identity (TCG <i>Maker Authority</i> ) and PIN (HGST <i>Maker PIN</i> )

**Table 5 - Roles and Required Identification and Authentication**

The Cryptographic Module enforces role separation by requiring a role identifier and an authentication credential (Personal Identification Number or PIN).

Authentication Mechanism	Mechanism Strength
TCG Credential (PIN)	TCG Credentials are 256 bits, which provides 2 <sup>256</sup> possible values. The probability that a random attempt succeeds is 1 chance in 2 <sup>256</sup> (approximately (8.64 x 10 <sup>-78</sup> ) which is significantly less than 1/1,000,000 (1x 10 <sup>-6</sup> ).  Multiple, successive authentication attempts can only occur sequentially (one at a time) and only when the failed authentication <i>Tries</i> count value does not exceed the associated <i>TriesLimit</i> value. Any authentication attempt consumes at least approximately 750 microseconds. Hence, at most, approximately 80,000 authentication attempts are possible in one minute. Thus, the probability that a false acceptance occurs a one minute interval is approximately 6.91 x 10 <sup>-73</sup> which is significantly less than 1 chance in 100,000 (1 x 10 <sup>-5</sup> ).

**Table 6 - Authentication Mechanism Strengths**

## 5. Access Control Policy

### 5.1 Roles and Services

Service	Description	Role(s)
Initialize Cryptographic Module <sup>2</sup>	Cryptographic Officer provisions the Cryptographic Module from organizational policies	CO (SID Authority)
Authenticate	Input a TCG Credential for authentication	CO, Users, Maker (SID Authority, EraseMaster, BandMasters)
Lock/Unlock Firmware Download Control	Deny/Permit access to Firmware Download service	CO (SID Authority)
Firmware Download	Load and utilize RSA2048 PSS and SHA-256 to verify the entire firmware image. If the new self-tests complete successfully, the SED executes the new code. Unlocking the Firmware Download Control enables the downloading of firmware.	CO (SID Authority)
Disable Zeroize	Disable TCG Revert method (Not allowed in the FIPS Approved mode)	CO (SID Authority)
Set	Write data structures; access control enforcement occurs per data structure field. PINs can be changed using this service.	CO, Users, Maker (SID Authority, EraseMaster, BandMasters)
Set LBA Band	Set the starting location, size, and attributes of a set of contiguous Logical Blocks	Users (BandMasters)
Lock/Unlock LBA Band	Deny/Permit access to a LBA Band	Users (BandMasters)
Write Data	Transform plaintext user data to ciphertext and write in a LBA band	Users (BandMasters)
Read Data	Read ciphertext from a LBA band and output user plaintext data	Users (BandMasters)
Set Data Store	Write a stream of bytes to unstructured storage	Users (BandMasters)
Erase LBA Band	Band cryptographic-erasure by changing LBA band encryption keys to new values. Erasing an LBA band with EraseMaster sets the TCG Credential to the default value.	CO (EraseMaster)

**Table 7 - Authenticated CM Services**

<sup>2</sup> See Cryptographic Module Acceptance and Provisioning within the HGST Ultrastar He10 SAS OEM Specification

## 5.2 Unauthenticated Services

The Cryptographic Module provides these unauthenticated services via the Anybody role:

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
Get FIPS Mode	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
Zeroize	TCG Revert method to return the Cryptographic Module to its original manufactured state; authentication data (PSID) is printed on the external label
SCSI	[SCSI Core] and [SCSI Block] commands to function as a standardized storage device. See Table 12 - SCSI Commands
FIPS 140 Compliance Descriptor <sup>3</sup>	This service reports the FIPS 140 revision as well as the cryptographic module's overall security level, hardware revision, firmware revision and module name.

**Table 8 - Unauthenticated Services**

## 5.3 Definition of Critical Security Parameters (CSPs)

The Cryptographic Module contains the following CSPs:

Key Name	Type	Description
Cryptographic Officer PIN - TCG Credential (2 total)	256-bit authentication data	Authenticates the Cryptographic Officer roles
User PIN –TCG Credential (16 total)	256-bit authentication data	Authenticates the User roles
MEK - Media Encryption Key (16 total - 1 per LBA band)	XTS-AES-256 (512 bits)	Encrypts and decrypts LBA Bands. This key is only associated with one key scope.
KEK – Key Encrypting Key (16 total)	SP 800-132 PBKDF (256 bits)	Keys derived from User PINs that wrap the MEKs. Keys protected by this SP 800-132 PBKDF derived key shall not leave the module.
NDRNG	256-byte Entropy output	Entropy source for DRBG

<sup>3</sup> See Compliance Descriptor Overview within the HGST Ultrastar He<sup>10</sup> SAS OEM Specification

Key Name	Type	Description
DRBG	Internal CTR_DRBG state	All properties and state associated with the SP800-90A Deterministic Random Bit Generator

**Table 9 - CSPs and Private Keys**

## 5.4 Definition of Public Security Parameters

The Cryptographic Module contains the following public key:

Key Name	Type	Description
RSAPublicKey[0]	RSA 2048 public key	Primary key used to verify firmware downloads
RSAPublicKey[1]	RSA 2048 public key	Secondary key used to verify firmware downloads

**Table 10 - Public Security Parameters**

## 5.5 SP800-132 Key Derivation Function Affirmations

The Cryptographic Module deploys a [SP800-132] Password Based Key Derivation Function (PBKDF).

- The Cryptographic Module deploys a [SP800-132] Key Derivation Function (KDF). The Cryptographic Module tracks TCG Credentials (PINs) by hashing a 256-bit salt and User PIN and storing the SHA256 digest in the Reserved Area. The digest is the CSP labeled AUTH.
- The cryptographic module complies with SP800-132 Option 2a.
- KEKs (SP800-132 Master Keys) derive from passing a User PIN (SP800-132 Password) and 256-bit salt through an SP800-132 KDF. The cryptographic module creates a unique KEK for each LBA Band.
- Security policy rules set the minimum User PIN length at 32 bytes. The cryptographic module allows values from 0x00 to 0xFF for each byte of the User PIN.
- Each salt is a random number generated using the [SP800-90A] DRBG.
- The KEK generation process utilizes the HMAC-SHA-256 algorithm to generate the keys.
- Each KEK has a security strength of 128-bits against a collision attack.
- The upper bound for the probability of guessing a User PIN is  $1/2^{256}$ .
- The difficulty of guessing the User PIN is equivalent to a brute force attack.
- The sole use of the KEKs is to wrap and unwrap the Media Encryption Keys (MEKs).

## 5.6 Definition of CSP Modes of Access

Table 11 defines the relationship between access to Critical Security Parameters (CSPs) and the different Cryptographic Module services. The modes of access shown in the table are defined as:

- **G = Generate:** The Cryptographic Module generates a CSP from the SP800-90A DRBG, derives a CSP with the Key Derivation Function or hashes authentication data with SHA-256.
- **E = Execute:** The module executes using the CSP.
- **W = Write:** The Cryptographic Module writes a CSP. The write access is performed after the Cryptographic Module generates a CSP.
- **Z = Zeroize:** The Cryptographic Module zeroizes a CSP.

Service	CSPs and Keys	Type of CSP Access
Initialize Cryptographic Module	CO PIN	E,W
	User PIN	E,W
	DRBG, NDRNG	E
	KEK	G
	MEK	G,W
Authenticate	CO PIN	E
	User PIN	E
Lock/Unlock Firmware Download Control	CO PIN	E
Firmware Download	CO PIN	E
	RSAFW	E
Disable Zeroize	CO PIN	E
Set	CO PIN	E
	User PIN	E
Set LBA Band	User PIN	E
Lock/Unlock LBA Band	User PIN	E
	KEK	G
	MEK	E
Write Data	User PIN	E
	MEK	E
Read Data	User PIN	E
	MEK	E
Set Data Store	User PIN	E
Erase LBA Band	CO PIN	E
	User PIN	Z
	KEK	G
	MEK	Z,G,W
Self-Test	NDRNG	E
	DRBG	W
Reset Module	None	None
Status Output	None	None
Get FIPS mode	None	None
Start Session	None	None
End Session	None	None
Generate Random	DRBG	E
Get	None	None

Service	CSPs and Keys	Type of CSP Access
Get Data Store	None	None
Zeroize	CO PIN	W
	User PIN	W
	DRBG	G
	KEK	G
	MEK	Z,G,W
SCSI	None	None
FIPS 140 Compliance Descriptor	None	None

Table 11 - CSP Access Rights within Roles & Services

## 6. Operational Environment

When the Cryptographic Module is operational, the environment cannot be modified. Therefore, the FIPS 140-2 operational environment requirements are not applicable to this module. While operational, the code working set cannot be added, deleted or modified; however, firmware can be upgraded (replaced in entirety) with an authenticated download service. If the download operation is successfully authorized and verified, the Cryptographic Module will begin operating with the new code working set.

## 7. Security Rules

Ultrastar He<sup>10</sup> 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: Cryptographic Officer and User. The module also supports an additional role, the Maker role. Initialization disables the Maker role.
2. Cryptographic Module power cycles clear all existing authentications.
3. 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.
4. The Cryptographic Module performs the following tests. Upon failure of any test, the Cryptographic Module enters a soft error state; the error condition is reported via the [SCSI] protocol. Functional commands are not permitted until a reset or power on reset occurs.
  - A. Power up Self-Tests
    - 1) Firmware Integrity 32-bit EDC
    - 2) AES Encrypt KAT, Cert #3880
    - 3) AES Decrypt KAT, Cert #3880
    - 4) RSA 2048 PSS Verify KAT
    - 5) DRBG KAT
    - 6) DRBG Health Test
    - 7) SHA-256 KAT, Cert #3203
    - 8) HMAC-SHA-256 KAT
    - 9) ASIC AES Encrypt KAT, Cert #3881
    - 10) ASIC AES Decrypt KAT, Cert #3881
    - 11) HW/FW SHA-256 KAT, Cert #3204
  - B. Conditional Tests

- 1) Continuous Random Number Generator test is performed on the DRBG and the hardware NDRNG entropy source.
- 2) Firmware Download Test, RSA 2048 PSS (Cert#1978), SHA-256 (Cert#3204 or Cert#3203)
5. An operator can command the Cryptographic Module to perform the power-up self-test by power cycling the device.
6. If a power-up self-tests fails, the drive will report a UEC that shows which test failed. After reporting the failure data, the drive will transition to a soft error state.
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 zeroization service can delete any plaintext key or CSP.
11. The Cryptographic Module does not support a maintenance interface or maintenance role.
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 End Session service deletes the current operator authentication. The Cryptographic Module requires operators to re-authenticate upon execution of the End Session service.
18. The Cryptographic Officer shall not enable the Maker Authority after the cryptographic module enters FIPS Approved mode.
19. The Cryptographic Officer shall not exercise the Disable Zeroize service after the cryptographic module enters FIPS Approved mode.
20. The Crypto Officer shall assure that all host issued User PINs are 32-bytes in length.
21. The host shall authenticate to LBA Bands after a power cycle.

## 7.2 Initialization Rules

The Cryptographic Officer shall follow the instructions in Section 11.17.4 Cryptographic Module Acceptance and Provisioning of the [Ultrastar He<sup>10</sup> Product Specification](#) for acceptance and provisioning procedures. Instructions include:

- Establish authentication data for the TCG Authorities replacing the MSID (default PIN values).
- Establish the LBA Bands, which causes the Cryptographic Module to generate Media Encryption Keys
- Disable Maker Authority
- Lock the Firmware Download service control

## 7.3 Zeroization Rules

The Cryptographic Officer uses the TCG Revert Method to perform the zeroization function. Revert includes zeroization of all Critical Security Parameters:

- Operator authentication data (CO PIN, User PIN)
- Key Encryption Key
- Media Encryption Keys

- NDRNG state
- DRBG state

## 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.
- HGST applies one (1) Tamper-evident security label during manufacturing.
- The tamper-evident security label cannot be penetrated or removed and reapplied without evidence of tampering.
- The tamper-evident security label cannot be easily replicated.



Figure 2: Tamper-Evident Label

### 8.2 Operator Responsibility

The Cryptographic Officer and/or User shall inspect the Cryptographic Module enclosure for evidence of tampering a minimum of once a year.

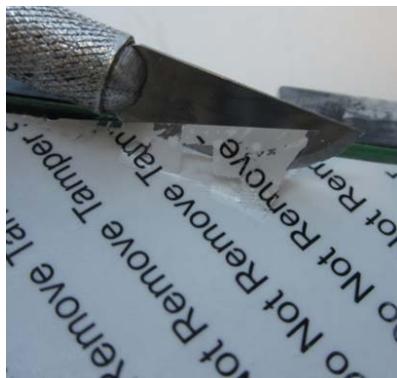


Figure 3: Tamper Evidence on Tamper Label

## 9. Mitigation of Other Attacks Policy

The Cryptographic Module is not designed to mitigate any attacks beyond FIPS 140-2 Security Level 2 requirements.

## 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] for terms
- Anybody: A formal TCG term for an unauthenticated role. [TCG Core]
- Approved: [FIPS140] approved or recommended in a NIST Special Publication.
- Approved mode of operation: A mode of the cryptographic module that employs only approved security functions. [FIPS140]
- 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.
- 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 Boundary: An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module. [FIPS140]
- Cryptographic key (Key): An input parameter to an Approved cryptographic algorithm
- Cryptographic Module: The set of hardware, software, and/or firmware used to implement approved security functions contained within the cryptographic boundary. [FIPS140]
- Cryptographic Officer: An Operator performing cryptographic initialization and management functions. [FIPS140]
- Ciphertext: Encrypted data transformed by an Approved security function.
- 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]
- Integrity: A cryptographic property that 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 that is used to encrypt or decrypt other keys.
- Key management: The activities involving the handling of cryptographic keys and other related security parameters (e.g., authentication data) during the entire life cycle of the Cryptographic Module.
- 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.
- Method: A TCG command or message. [TCG Core]
- Manufactured SID (MSID): A unique default value that vendors assign to each SED during manufacturing. Typically, it is printed on an external label and is readable with the TCG protocol. It is the initial and default value for all TCG credentials. [TCG Core]
- 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 provides access to the Cryptographic Module for physical signals. [FIPS140]
- Public Security Parameters (PSP): Public information whose modification can compromise the security of the cryptographic module (e.g., a public key of a key pair).
- 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.
- Session: A formal TCG term that envelops the lifetime of an Operator's authentication. [TCG Core]
- Security Identifier (SID): A TCG authority used by the Cryptographic Officer. [TCG Core]
- Self-Encrypting Drive (SED): A storage device that provides data storage services.
- 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.
- User: An Operator that consumes cryptographic services. [FIPS140]
- User Data: Data transferred from/to a SED using the Read Data and Write Data commands. [SCSI Block]
- Write Data: An external request to transfer User Data to a SED. [SCSI Block]
- Zeroize: Invalidate a Critical Security Parameter. [FIPS140]

## 11. Acronyms

- CO: Cryptographic Office [FIPS140]
- CSP: Critical Security Parameter [FIPS140]
- CRC: Cyclic Redundancy Check
- DRBG: Deterministic Random Bit Generator
- DRAM: Dynamic Random Access Memory
- HDD: Hard Disk Drive
- EMI: Electromagnetic Interference
- FIPS: Federal Information Processing Standard
- KDF: Key Derivation Function
- KAT: Known Answer Test

- LBA: Logical Block Address
- MEK: Media Encryption Key
- MSID (Manufactured Security Identifier): a public, drive-unique value that is created during manufacturing and is used as default PIN credential values
- NDRNG: Non-deterministic Random Number Generator that is the source of entropy for the DRBG
- NIST: National Institute of Standards and Technology
- PIN: Personal Identification Number
- PSID (Physical Security Identifier): a SED unique value that is printed on the Cryptographic Module's label and is used as authentication data and proof of physical presence for the Zeroize service
- PSP: Public Security Parameter
- SAS: Serial Attached SCSI
- SCSI: Small Computer System Interface
- SED: Self encrypting Drive
- SID: TCG Security Identifier, the authority representing the Cryptographic Module owner
- TCG: Trusted Computing Group
- UEC: Universal Error Code
- XTS: A mode of AES

## 12. References

### 12.1 NIST Specifications

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

- [SP800-131A] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (Revision 1), NIST, 2015 November
- [SP800-132] Recommendation for Password-Based Key Derivation, NIST, 2010 December

## 12.2 Trusted Computing Group Specifications

- [TCG Core] *TCG Storage Architecture Core Specification*, Version 2.0 Revision 1.0 (April 20, 2009)
- [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)

## 12.3 International Committee on Information Technology Standards T10 Technical Committee Standards

- [SCSI Core] SCSI Primary Commands-4 Rev 15 (SPC-4)
- [SCSI Block] SCSI Block Commands Rev15 (SBC-3)
- [SAS] Serial Attached SCSI-2 Rev 13 (SAS-2)

## 12.4 HGST Documents

- [Product Specification] HGST Ultrastar He<sup>10</sup> SAS OEM Specification, Version 1.6 (October 20, 2016), [www.hgst.com/sites/default/files/resources/HGST-Ultrastar-He10-SAS-OEM-Spec](http://www.hgst.com/sites/default/files/resources/HGST-Ultrastar-He10-SAS-OEM-Spec)
- [D&O] Delivery & Operation (Cryptographic Officer) Manual, Version: 0.8 (February 26 2016)

## 12.5 SCSI Commands

Description	Code
FORMAT UNIT	04h
INQUIRY	12h
LOG SELECT	4Ch
LOG SENSE	4Dh
MODE SELECT	15h
MODE SELECT	55h
MODE SENSE	1Ah
MODE SENSE	5Ah
PERSISTENT RESERVE IN	5Eh
PERSISTENT RESERVE OUT	5Fh
PRE-FETCH (16)	90h
PRE-FETCH (10)	34h
READ (6)	08h
READ (10)	28h
READ (12)	A8h

Description	Code
READ (16)	88h
READ (32)	7Fh/09h
READ BUFFER	3Ch
READ CAPACITY (10)	25h
READ CAPACITY (16)	9Eh/10h
READ DEFECT DATA	37h
READ DEFECT DATA	B7h
READ LONG (16)	9Eh/11h
READ LONG	3Eh
REASSIGN BLOCKS	07h
RECEIVE DIAGNOSTICS RESULTS	1Ch
RELEASE	17h
RELEASE	57h
REPORT DEVICE IDENTIFIER	A3h/05h
REPORT LUNS	A0h
REPORT SUPPORTED OPERATION CODES	A3h/0Ch
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS	A3h/0Dh
REQUEST SENSE	03h
RESERVE	16h
RESERVE	56h
REZERO UNIT	01h
SANITIZE	48h
SEEK (6)	0Bh
SEEK (10)	2Bh
SEND DIAGNOSTIC	1Dh
SET DEVICE IDENTIFIER	A4h/06h
START STOP UNIT	1Bh
SYNCHRONIZE CACHE (10)	35h
SYNCHRONIZE CACHE (16)	91h
TEST UNIT READY	00h
UNMAP	42h
VERIFY (10)	2Fh
VERIFY (12)	AFh
VERIFY (16)	8Fh
VERIFY (32)	7Fh/0Ah
WRITE (6)	0Ah
WRITE (10)	2Ah
WRITE (12)	AAh
WRITE (16)	8Ah
WRITE (32)	7Fh/0Bh

Description	Code
WRITE AND VERIFY (10)	2Eh
WRITE AND VERIFY (12)	AEh
WRITE AND VERIFY (16)	8Eh
WRITE AND VERIFY (32)	7Fh/0Ch
WRITE BUFFER	3Bh
WRITE LONG (10)	3Fh
WRITE LONG (16)	9Fh/11h
WRITE SAME (10)	41h
WRITE SAME (16)	93h
WRITE SAME (32)	7Fh/0Dh

Table 12 - SCSI Commands