HGST Ultrastar SSD800/1000/1600 TCG Enterprise SSDs FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Protection of Data at Rest

Version: 6.6

2018-02-20

Contents

Tables

Figures

1 Module Overview

HGST Ultrastar SSD800/1000/1600 TCG Enterprise SSDs, hereafter referred to as "Ultrastar SSD800/1000/1600" or "the Cryptographic Module" are multi-chip embedded Cryptographic Modules. They comply with FIPS 140-2 *Level 2* security. They also comply with the *Trusted Computing Group (TCG) SSC: Enterprise Specification*. The drive enclosure is the cryptographic boundary.

Figure 1 - Cryptographic Boundary Hardware Version (0001)

Figure 2 - Cryptographic Boundary Hardware Version (0002)

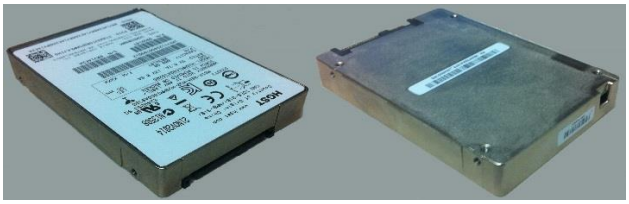

Figure 3 - Cryptographic Boundary Hardware Version (0003)

1.1 Models

The Ultrastar SSD800/1000/1600 is available in several models that vary in performance and storage capacities. Table 1 enumerates the models and characteristics, which include the hardware and firmware versions.

Model Number (Hardware Version)	Capacity (GB)	Firmware Version	Description
HUSMH8080ASS205 (0001)	800	R210,R230,R232,R252	2.5" 12 Gb/s SAS High Endurance
HUSMH8080ASS205 (0002)	800	R252,R254	2.5" 12 Gb/s SAS High Endurance
HUSMH8080BSS205 (0003)	800	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS High Endurance
HUSMH8040ASS205 (0001)	400	R210,R230, R232, R252	2.5" 12 Gb/s SAS High Endurance
HUSMH8040ASS205 (0002)	400	R252, R254	2.5" 12 Gb/s SAS High Endurance

Model Number (Hardware Version)	Capacity (GB)	Firmware Version	Description
HUSMH8040BSS205 (0003)	400	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS High Endurance
HUSMH8020ASS205 (0001)	200	R210,R230, R232, R252	2.5" 12 Gb/s SAS High Endurance
HUSMH8020ASS205 (0002)	200	R252, R254	2.5" 12 Gb/s SAS High Endurance
HUSMH8020BSS205 (0003)	200	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS High Endurance
HUSMH8010BSS205 (0003)	100	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS High Endurance
HUSMM1616ASS205 (0003)	1600	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300,K2CC,P302, D302	2.5" 12 Gb/s SAS Mainstream
HUSMM8080ASS205 (0001)	800	R210,R230, R232, R252	2.5" 12 Gb/s SAS Mainstream
HUSMM8080ASS205 (0002)	800	R252, R254	2.5" 12 Gb/s SAS Mainstream
HUSMM1680ASS205 (0003)	800	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300,K2CC,P302, D302	2.5" 12 Gb/s SAS Mainstream
HUSMM8040ASS205 (0001)	400	R210,R230, R232, R252	2.5" 12 Gb/s SAS Mainstream
HUSMM8040ASS205 (0002)	400	R252, R254	2.5" 12 Gb/s SAS Mainstream
HUSMM1640ASS205 (0003)	400	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS Mainstream
HUSMM8020ASS205 (0001)	200	R210,R230, R232, R252	2.5" 12 Gb/s SAS Mainstream
HUSMM8020ASS205 (0002)	200	R252, R254	2.5" 12 Gb/s SAS Mainstream
HUSMM1620ASS205 (0003)	200	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS Mainstream
HUSMR1619ASS235 (0003)	1920	R130	2.5" 12 Gb/s SAS Read Intensive 3DW/D

Model Number (Hardware Version)	Capacity (GB)	Firmware Version	Description
HUSMR1619ASS205 (0003)	1920	R104,R106,R108,R120,R130, R154, G155	2.5" 12 Gb/s SAS Read Intensive 1DW/D
HUSMR1616ASS205 (0003)	1600	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS Read Intensive
HUSMR1010ASS205 (0001)	1000	R210,R230, R232, R252	2.5" 12 Gb/s SAS Read Intensive
HUSMR1010ASS205 (0002)	1000	R252, R254	2.5" 12 Gb/s SAS Read Intensive
HUSMR1610ASS205 (0003)	1000	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS Read Intensive
HUSMR1680ASS205 (0003)	800	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS Read Intensive
HUSMR1050ASS205 (0001)	500	R210,R230, R232, R252	2.5" 12 Gb/s SAS Read Intensive
HUSMR1050ASS205 (0002)	500	R252, R254	2.5" 12 Gb/s SAS Read Intensive
HUSMR1650ASS205 (0003)	500	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS Read Intensive
HUSMR1640ASS205 (0003)	400	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS Read Intensive
HUSMR1025ASS205 (0001)	250	R210,R230, R232, R252	2.5" 12 Gb/s SAS Read Intensive
HUSMR1025ASS205 (0002)	250	R252, R254	2.5" 12 Gb/s SAS Read Intensive
HUSMR1625ASS205 (0003)	250	P216,P217,P218,P21J,P250, P252,P292,P298,P29A,P29C, P29E,P2C0,P2CA,P2CC,P2E0, P2F0, P300	2.5" 12 Gb/s SAS Read Intensive

Table 1 - Ultrastar SSD800/1000/1600 Product 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	3
Module Ports and Interfaces	2
Roles, Services and Authentication	3
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 Modules enters FIPS Approved Mode after successful completion of the Initialize Cryptographic Module service. Once configured to run in FIPS Approved mode, the module will always run in FIPS Approved mode as long as all self-tests complete successfully. A FIPS mode indicator is available from the Get FIPS Mode service. A value of “1” is returned when the Cryptographic Module is in FIPS mode. If the module is not configured correctly the module will run in the Non-FIPS Approved mode of operation, and the Get FIPS Mode service will return a ”0” value.

2.2 Approved Algorithms

The cryptographic module supports the following FIPS Approved algorithms. All algorithms and key lengths are in compliance with NIST SP 800-131A.

FIPS Approved Algorithm	CAVP Certificate
SP800-90A CTR-DRBG	302
Hardware AES ECB-128,256, XTS-128, 256 Encryption and Decryption * Note: The length of data unit for XTS-AES does not exceed 2^20 blocks.	2067
AES ECB-256, KW-256[1] Encryption, Decryption and Key Wrap	2365
RSA 2048 PSS Verify	1220

FIPS Approved Algorithm	CAVP Certificate
SHA-256	2037
HMAC-SHA-256 Used in SP 800-132 KDF	1468
SP800-132 KDF	Vendor Affirmed

Table 3 - FIPS Approved Algorithms

[1] AES-KW is only used for key storage to protect keys/CSPs in accordance with IG 7.16

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

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

3 Ports and Interfaces

Table 4 below identifies its ports and interfaces of the cryptographic module. A maintenance access interface is not provided.

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

Table 4 - Ultrastar SSD800/1000/1600 Pins and FIPS 140-2 Ports and Interfaces

The SAS (Serial Attached SCSI) connector is an industry defined standard [SAS], and the Serial connector is a two wire port, signal and ground. The Serial Connector is enabled only at HGST facilities; it is disabled before the Cryptographic Module is delivered to customers.

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. TCG SSC: Enterprise Section 11.3.1 defines this role.

4.1.2 EraseMaster Authority

This TCG authority zeroizes the cryptographic module. TCG SSC: Enterprise Section 11.4.1 defines this role. It may also disable User roles and erase LBA bands (user data regions).

4.2 User

User roles correspond to Bandmaster Authorities; they are defined in TCG SSC: Enterprise Section 11.4.1. They are authorized to lock/unlock and configure LBA bands (user data regions) and to issue read/write commands to the SED. The TCG EraseMaster authority can disable Users.

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

Out-of-scope services are provided for the vendor to configure and perform failure analysis within the vendor's facilities. Maker authentication data shall not leave the vendor's facilities. Maker is disabled when the Cryptographic Officer invokes the Initialize Cryptographic Module service.

The following table maps TCG authorities to FIPS140-2 roles.

TCG Authority	Description	Authentication Type	Authentication Data
SID Authority	A Cryptographic Officer role that initializes the Cryptographic Module and authorizes Firmware download.	Identity-based	CO Identity (TCG *SID Authority*) and PIN (TCG *SID Authority PIN*)
EraseMaster	A Cryptographic Officer role that zeroizes Media Encryption keys and disables Users.	Identity-based	CO Identity (TCG *EraseMaster Authority*) and PIN (TCG *EraseMaster PIN*)
BandMasterN (N = 0 to 3)	A User role that controls read/write access to LBA Bands.	Identity-based	User Identity (TCG *BandMaster Authority*) and PIN (TCG *BandMaster PIN*)
Anybody	A role that does not require authentication.	Unauthenticated	N/A
Maker (Disabled)	A TCG Authority which is not available upon completion of the	Identity-based	User Identity (TCG Maker Authority) and PIN (HGST Maker PIN)

TCG Authority	Description	Authentication Type	Authentication Data
	Initialize Cryptographic Module service		

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^{256} possible values. The probability that a random attempt succeeds is 1 chance in 2^{256} (approximately 8.64×10^{-78}) which is significantly less than 1/1,000,000 (1×10^{-6}). Multiple, successive authentication attempts can only occur sequentially (one at a time) and only when the failed authentication *Tries* count value does not exceed the associated *TriesLimit* 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 6.91×10^{-73} which is significantly less than 1 chance in 100,000 (1×10^{-5}).

Table 6 - Authentication Mechanism Strengths

5 Access Control Policy

5.1 Roles and Services

Service	Description	Role(s)
Initialize Cryptographic Module	Cryptographic Officer provisions the Cryptographic Module from organizational policies	CO (SID Authority)

Service	Description	Role(s)
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 verify by RSA2048 an entire firmware image. If the new self-tests complete successfully, the SED executes the new code. The Firmware Download Control shall be unlocked before Firmware can be downloaded.	CO (SID Authority)
Disable Zeroize	Disable TCG Revert method	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 TCG Credential	Inputs authentication data and replaces stored hashed PIN data.	CO, Users (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)

Service	Description	Role(s)
Erase LBA Band	Band cryptographic-erasure by changing LBA band encryption keys to new values. When the EraseMaster erases a LBA band, the TCG Credential is set to the default value.	CO (EraseMaster)
Set Vendor Data	A Non-Approved service that is unavailable after the Initialize Cryptographic Module service completes	Maker

Table 7 - Authenticated CM Services

5.2 Unauthenticated Services

The cryptographic module provides these unauthenticated services:

Service	Description
Reset Module	Power on Reset
Self-Test	The CM performs self-tests when the module 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 a data structure
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.

Table 8 - Unauthenticated Services

5.3 Definition of Critical Security Parameters (CSPs)

The Cryptographic Module contains the following CSPs. Zeroization of CSPs complies with [SP800-88] media sanitization.

Key Name	Type	Description
PIN - TCG Credential (6 total)	256-bit authentication data	Authenticates the Cryptographic Officer and User roles
MEK - Media Encryption Key (4 total - 1 per LBA band)	XTS-AES-256 (512 bits)	Encrypts and decrypts LBA Bands. Note: This key only associated with one key scope.
KEK – Key Encrypting Key (4 total)	SP 800-132 PBKDF (256 bits)	Keys derived from BandMaster PINs which wrap the MEKs Note: Keys protected by this SP 800-132 PBKDF derived key shall not leave the module
NDRNG	Entropy output	Entropy source for DRBG
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 Sensitive Security Parameters

The module contains the following public keys:

Key Name	Type	Description
RSAFW	RSA 2048 public key	Verify firmware download

Table 10 - Sensitive Security Parameters

5.5 SP800-132 Key Derivation Function Affirmations

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

- The KEKs (SP800-132 Master Keys) are derived from the User PINs (SP800-132 Password) with SP800-132 Option 1a.
- The length of the operator PIN is 256 bits and the stored security strength is 128 bits.
- The upper bound for the probability of guessing the User PIN is $2^{-128.}$
- The difficulty of guessing the User PIN is equivalent to a brute force attack.
- The KEKs (SP800-132 Master Keys) are only used to wrap 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 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 and User PIN and DRBG and KEK and MEK	E,W E,W E G G,W
Authenticate	CO PIN or User PIN	E E
Lock/Unlock Firmware Download Control	CO PIN	E
Firmware Download	CO PIN and RSAFW	E E
Disable Zeroize	CO PIN	E
Set	CO PIN or User PIN or Maker PIN	E E E
Set TCG Credential	CO PIN or User PIN	W W
Set LBA Band	User PIN	E
Lock/Unlock LBA Band	User PIN and KEK and MEK	E G E
Write Data	User PIN and MEK	E E
Read Data	User PIN and MEK	E E
Set Data Store	User PIN	E

Service	CSPs and Keys	Type of CSP Access
Erase LBA Band	CO PIN and KEK and MEK	E G Z,G,W
Self-Test	NDRNG and DRBG	E W
Reset Module	None	
Status Output	None	
Get FIPS mode	None	
Start Session	None	
End Session	None	
Generate Random	DRBG	E
Get Data Store	None	
Set Vendor Data	None	
Zeroize	PSID and CO PIN and User PIN and DRBG and KEK and MEK	E W W G G Z,G,W
SCSI	None	

Table 11 - CSP Access Rights within Roles & Services

6 Operational Environment

The Cryptographic Module operating environment is non-modifiable. While the Cryptographic Module is operational, the environment cannot be modified; the code working set cannot be added, deleted or modified. Firmware can be upgraded (replaced in entirety) with an authenticated download service. If the download operation is successfully authorized and verified, then the Cryptographic Module will begin operating with the new code working set.

7 Security Rules

The Ultrastar SSD800/1000/1600 enforces applicable *FIPS 140-2 Level 2 security* requirements. This section documents the security rules that the Cryptographic Module enforces.

7.1 Invariant Rules

- The Cryptographic Module supports two distinct types of operator roles: Cryptographic Officer and User.
- Cryptographic Module power cycles clear all existing authentications.
- When the Cryptographic Module has successfully completed self-tests and has been initialized, it is in FIPS mode, and the FIPS mode indicator is set to 1.
- When the module is unable to authenticate TCG Credentials, operators do not have access to any cryptographic service other than the unauthenticated Generate Random service.
- The cryptographic module performs the following tests
- Power up Self-Tests
    - Firmware Integrity16-bit CRC
    - Hardware AES Encrypt/Decrypt KAT (Known Answer Test)
    - Firmware AES Encrypt/Decrypt KAT
    - RSA Verify KAT
    - SHA-256 KAT
    - DRBG KAT
    - HMAC-SHA-256 KAT
- Conditional Tests
    - Continuous Random Number Generator test is performed on the DRBG and the hardware NDRNG entropy source.
    - Firmware Download Check
- An operator can command the module to perform the power-up self-test by power cycling the device.
- Power-up self-tests do not require operator action.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- Status information does not contain CSPs or sensitive data that if misused, could compromise the module.
- There are no restrictions on which plaintext keys or CSPs the zeroization service deletes.
- The module does not support a maintenance interface or maintenance role.
- The module does not support manual key entry.
- The module does not have any external input/output devices used for entry/output of data.
- The module does not output plaintext CSPs.
- The module does not output intermediate key values.
- The module does not support concurrent operators.

- The End Session service deletes the current operator authentication. The Cryptographic Module requires operators to re-authenticate upon execution of the End Session service.

7.2 Initialization Rules

The Cryptographic Officer shall follow the instructions in the Delivery & Operation (Cryptographic Officer's) Manual for acceptance and end of life procedures. Acceptance instructions include:

- Establish authentication data for the TCG Authorities
- 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

Zeroization is performed by the Cryptographic Officer with the TCG Revert Method. Revert includes zeroization of all Critical Security Parameters:

- Operator authentication data
- 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.

8.1.1 Hardware versions (0001) and (0002)

- All components are production-grade materials with standard passivation.
- The enclosure is opaque.
- Engineering design satisfies opacity requirements.
- Tamper-evident security labels are applied by HGST during manufacturing.
- The tamper-evident security labels cannot be penetrated or removed and reapplied without evidence of tampering.
- The tamper-evident security labels cannot be easily replicated.

Figure 4 - Large Tamper-Evident Label on Top Surface

Figure 5 - Smaller Tamper-Evident Label Underneath Large Label Wrapping Down Sides, Hardware Revision (0001) only

8.1.2 Hardware version (0003)

- All components are production-grade materials with standard passivation.
- The enclosure is opaque.
- Engineering design satisfies opacity requirements.
- Tamper-evident sealant is applied to screw heads by HGST during manufacturing.
- The tamper-evident sealant cannot be penetrated or removed and reapplied without evidence

of tampering.

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.

If signs of tamper are detected, the module should be returned to HGST, Inc.

8.2.1 Hardware versions (0001) and (0002)

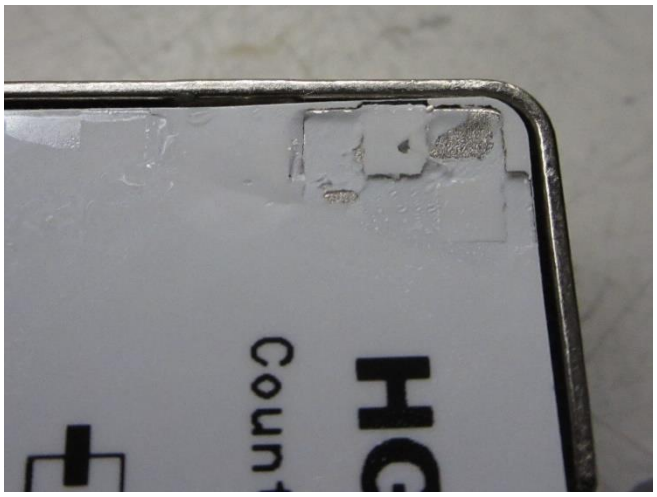

Figure 6 - Tamper Evidence on Large Tamper-Evident Label. Hardware Revision (0001) and (0002)

Figure 7 - Tamper Evidence on Smaller Tamper-Evident Label, Hardware Revision (0001) only

8.2.2 Hardware version (0003)

To inspect tamper evidence, the Cryptographic Officer and/or User shall:

1. Lift the top label as shown Figure 8.
2. Inspect the 4 screws for evidence of tampering as shown in Figure 9. Inspection includes both visual and mechanical methods. In the absence of tampering, the sealant shall show no visible disturbance and shall adhere to the screw when touched.

Figure 8 - Lift top label

Figure 9 - Left side shows tamper. Right side shows no tamper.

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 a role that is not authenticated. [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 that is 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 that an implement Approved security functions and is 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 where 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; it is typically 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 that is used to authenticate an identity. [TCG Core]
- **Plaintext**: Data that is not encrypted.
- **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 that is 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]
- **DRBG**: Deterministic Random Bit Generator
- **DRAM**: Dynamic Random Access Memory
- **HDD**: Hard Disk Drive
- **EMI**: Electromagnetic Interference
- **FIPS**: Federal Information Processing Standard
- **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
- **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 186-3, NIST, 2006, March
- [FIPS140] Security Requirements for Cryptographic Modules, FIPS PUB 140-2, NIST, 2002 December
- [HMAC] The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, 2007 June
- [SHA] Secure Hash Standard (SHS), FIPS PUB 180-3, NIST, 2007 June
- [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 3), NIST, 2012 July
- [SP800-88] Guidelines for Media Sanitization (Revision 1), NIST, 2014 December
- [SP800-90A] Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST, 2012 Jan
- [SP800-131A] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST, 2011 Jan
- [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)

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
READ (16)	88h
READ (32)	7Fh/09h
READ BUFFER	3Ch
READ CAPACITY (10)	25h

Description	Code
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

Description	Code
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
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

12.4 HGST Documents

- [Product Specification] HGST Ultrastar SSD800/1000/1600 SSD Product Specification, (October 22, 2014)
- [D&O] Delivery & Operation (Cryptographic Officer) Manual, version 0.6 (Nov, 31 2014)