



Long Live Data™

HGST Ultrastar C10K1800 TCG Enterprise HDDs  
FIPS 140-2 Cryptographic Module  
Non-Proprietary Security Policy

*Protection of Data at Rest*

Version: 2.4  
2016-03-10

# CONTENTS

|       |   |    |
|-------|---|----|
| 1     | Cryptographic Module Overview .....   | 4  |
| 1.1   | Models .....  | 4  |
| 1.2   | Security Level .....  | 6  |
| 2     | Modes of Operation .....  | 7  |
| 2.1   | FIPS Approved Mode of Operation .....   | 7  |
| 2.2   | Approved Algorithms .....   | 7  |
| 3     | Ports and Interfaces .....  | 7  |
| 4     | Identification and Authentication Policy .....  | 8  |
| 4.1   | Cryptographic Officer .....   | 8  |
| 4.1.1 | Secure ID (SID) Authority .....   | 8  |
| 4.1.2 | EraseMaster Authority .....   | 8  |
| 4.2   | User .....  | 8  |
| 4.3   | Anybody .....   | 8  |
| 4.4   | Maker .....   | 8  |
| 5     | Access Control Policy .....   | 9  |
| 5.1   | Roles and Services .....  | 9  |
| 5.2   | Unauthenticated Services .....  | 10 |
| 5.3   | Definition of Critical Security Parameters (CSPs) .....   | 11 |
| 5.4   | Definition of Public Security Parameters .....  | 11 |
| 5.5   | SP800-132 Key Derivation Function Affirmations .....  | 11 |
| 5.6   | Definition of CSP Modes of Access .....   | 12 |
| 6     | Operational Environment .....   | 13 |
| 7     | Security Rules .....  | 13 |
| 7.1   | Invariant Rules .....   | 13 |
| 7.2   | Initialization Rules .....  | 14 |
| 7.3   | Zeroization Rules .....   | 15 |
| 8     | Physical Security Policy .....  | 15 |
| 8.1   | Mechanisms .....  | 15 |
| 8.2   | Operator Responsibility .....   | 17 |
| 9     | Mitigation of Other Attacks Policy .....  | 17 |
| 10    | Definitions .....   | 17 |
| 11    | Acronyms .....  | 19 |
| 12    | References .....  | 19 |
| 12.1  | NIST Specifications .....   | 19 |
| 12.2  | Trusted Computing Group Specifications .....  | 20 |
| 12.3  | International Committee on Information Technology Standards T10 Technical Committee Standards ..... | 20 |
| 12.4  | HGST Documents .....  | 22 |

## Tables

|   |    |
|---|----|
| Table 1 - Ultrastar C10K1800 Product Models .....                           | 6  |
| Table 2 - Module Security Level Specification .....                         | 6  |
| Table 3 - FIPS Approved Algorithms .....                                    | 7  |
| Table 4 - Ultrastar C10K1800 Pins and FIPS 140-2 Ports and Interfaces ..... | 8  |
| Table 5 - Roles and Required Identification and Authentication.....         | 9  |
| Table 6 - Authentication Mechanism Strengths.....                           | 9  |
| Table 7 - Authenticated CM Services .....                                   | 10 |
| Table 8 - Unauthenticated Services.....                                     | 11 |
| Table 9 - CSPs and Private Keys.....  | 11 |
| Table 10 - Sensitive Security Parameters.....                               | 11 |
| Table 11 - CSP Access Rights within Roles & Services.....                   | 13 |
| Table 12 - SCSI Commands .....  | 22 |

## Figures

|   |    |
|---|----|
| Figure 1: Cryptographic Boundary.....                             | 4  |
| Figure 2: Large Tamper-Evident Label Hardware Version (1).....    | 15 |
| Figure 3: Smaller Tamper Evident Label Hardware Version (1).....  | 15 |
| Figure 4: Large Tamper-Evident Label Hardware Version (2).....    | 16 |
| Figure 5: Smaller Tamper Evident Label Hardware Version (2).....  | 16 |
| Figure 6: Large Tamper-Evident Label Hardware Version (3).....    | 16 |
| Figure 7: Smaller Tamper-Evident Label Hardware Version (3) ..... | 16 |
| Figure 8: Tamper Evidence on Large Tamper Label.....              | 17 |
| Figure 9: Tamper Evidence on Metal Surface.....                   | 17 |

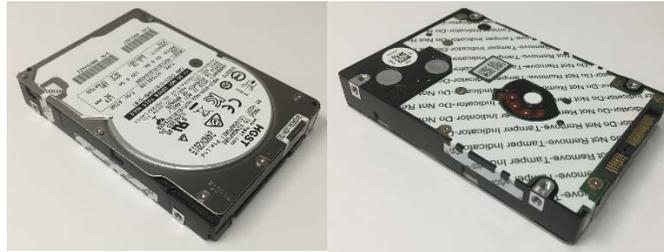
# 1 Cryptographic Module Overview

HGST Ultrastar C10K1800 TCG Enterprise HDDs, hereafter referred to as “Ultrastar C10K1800” or “the Cryptographic Module” are multi-chip embedded modules that 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 (see Figure 1). All components within this boundary are tested against the FIPS 140-2 requirements except for the Actuator Assembly. This part has been excluded from the boundary since it is not security relevant.



Hardware Version (1)

Hardware Version (2)



Hardware Version (3)

Figure 1: Cryptographic Boundary

## 1.1 Models

The Ultrastar C10K1800 is available in several models that vary by storage capacity and block size. Table 1 enumerates the models and characteristics and includes the hardware and firmware versions.

| Model Number (Hardware Version)            | Firmware Version   | Capacity (GB) | Block Size (bytes)         | Description                   |
|--|--|---------------|----------------------------|-------------------------------|
| HUC101818CS4205 (1)                        | R1A0, R3B0, R3F0, R3R0, R3R2, R3T0, R3X0, R3X2   | 1,800         | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101818CS4205 (2)<br>HUC101818CS4205 (3) | R1A0, R3B0, R3F0, R3R0, R3R2, R3T0, R3X0, R3X2, R703, R770, R7R1, R801, NA00, NE00, NE02, R7G2, R904, R920, R940, R990 | 1,800         | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101812CS4205 (1)                        | R1A0, R3B0, R3F0, R3R0, R3R2, R3T0, R3X0, R3X2   | 1,200         | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |

HGST Ultrastar C10K1800 TCG Enterprise HDDs

| Model Number<br>(Hardware Version)         | Firmware Version   | Capacity<br>(GB) | Block Size<br>(bytes)      | Description                   |
|--|--|------------------|----------------------------|-------------------------------|
| HUC101812CS4205 (2)<br>HUC101818CS4205 (3) | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2, R703<br>R770, R7R1, R7G2,<br>R904, R920, R940,<br>R990       | 1,200            | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101890CS4205 (1)                        | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2   | 900              | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101890CS4205 (2)<br>HUC101890CS4205 (3) | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2, R703<br>R770, R7R1, NA00,<br>R7G2, R904, R920,<br>R940, R990 | 900              | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101860CS4205 (1)                        | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2   | 600              | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101860CS4205 (2)<br>HUC101860CS4205 (3) | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2, R703<br>R770, R7R1, R7G2,<br>R904, R920, R940,<br>R990       | 600              | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101845CS4205 (1)                        | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2   | 450              | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101845CS4205 (2)<br>HUC101845CS4205 (3) | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2, R703<br>R770, R7R1, R7G2,<br>R904, R920, R940,<br>R990       | 450              | 4K Native<br>512 emulation | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101812CSS205 (1)                        | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2   | 1,200            | 512 Native                 | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101812CSS205 (2)<br>HUC101812CSS205 (3) | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2, R703<br>R770, R7R1, R7G2,<br>R904, R920, R940,<br>R990       | 1,200            | 512 Native                 | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101890CSS205 (1)                        | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2   | 900              | 512 Native                 | SAS 12 Gb/s, 10,000RPM, 2.5in |

| Model Number<br>(Hardware Version)         | Firmware Version   | Capacity<br>(GB) | Block Size<br>(bytes) | Description                   |
|--|--|------------------|-----------------------|-------------------------------|
| HUC101890CSS205 (2)<br>HUC101890CSS205 (3) | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2, R703<br>R770, R7R1, R7G2,<br>R904, R920, R940,<br>R990 | 900              | 512 Native            | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101860CSS205 (1)                        | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2   | 600              | 512 Native            | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101860CSS205 (2)<br>HUC101860CSS205 (3) | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2, R703<br>R770, R7R1, R7G2,<br>R904, R920, R940,<br>R990 | 600              | 512 Native            | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101830CSS205 (1)                        | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2   | 300              | 512 Native            | SAS 12 Gb/s, 10,000RPM, 2.5in |
| HUC101830CSS205 (2)<br>HUC101830CSS205 (3) | R1A0, R3B0, R3F0,<br>R3R0, R3R2, R3T0,<br>R3X0, R3X2, R703<br>R770, R7R1, R7G2,<br>R904, R920, R940,<br>R990 | 300              | 512 Native            | SAS 12 Gb/s, 10,000RPM, 2.5in |

Table 1 - Ultrastar C10K1800 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 that is entered after successful completion of the Initialize Cryptographic Module service. Once configured to run in FIPS Approved mode, the Cryptographic Module will always run in FIPS-Approved mode as long as all of the self-tests complete successfully. 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. The Get FIPS Mode service will return a value of ”0”.

### 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<br>Encryption and Decryption<br>* Note: The length of data unit for AES-XTS does not exceed 2 <sup>20</sup> blocks. | 2067             |
| AES ECB-256<br>Encryption, Decryption and Key Wrap  | 2365             |
| RSA 2048 PSS Verify   | 1220             |
| SHA-256   | 2037             |
| HMAC-SHA-256<br>Used in SP 800-132 KDF  | 1468             |
| SP800-132 KDF   | Vendor Affirmed  |

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 3 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 [SAS]      |
| Control Input        | SAS connector [SAS]        |
| Status Output        | SAS connector [SAS]        |
| Data Input           | SAS connector [SAS]        |
| Data Output          | SAS connector [SAS]        |

Table 4 - Ultrastar C10K1800 Pins and 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. 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 FIPS 140-2 roles.

| TCG Authority               | Description   | Authentication Type | Authentication Data   |
|-----------------------------|---|---------------------|---|
| SID Authority               | A Cryptographic Officer role which initializes the Cryptographic Module and authorizes Firmware download. | Identity-based      | CO Identity (TCG <i>SID Authority</i> ) and PIN (TCG <i>SID Authority PIN</i> )       |
| EraseMaster                 | A Cryptographic Officer role which zeroizes Media Encryption keys and disables Users.                     | Identity-based      | CO Identity (TCG <i>EraseMaster Authority</i> ) and PIN (TCG <i>EraseMaster PIN</i> ) |
| BandMasterN<br>(N = 0 to 5) | A User role which controls read/write access to LBA Bands.  | Identity-based      | User Identity (TCG <i>BandMaster Authority</i> ) and PIN (TCG <i>BandMaster PIN</i> ) |

| TCG Authority | Description   | Authentication Type | Authentication Data  |
|---------------|---|---------------------|--|
| Anybody       | A role that does not require authentication.  | Unauthenticated     | N/A  |
| Maker         | A TCG Authority which is not available upon completion of the Initialize Cryptographic Module service | Identity-based      | User Identity (TCG Maker Authority) and PIN (HGST Maker PIN) |

**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)     | <p>TCG Credentials are 256 bits, which provides <math>2^{256}</math> possible values. The probability that a random attempt succeeds is 1 chance in <math>2^{256}</math> (approximately <math>8.64 \times 10^{-78}</math>) which is significantly less than 1/1,000,000 (<math>1 \times 10^{-6}</math>).</p> <p>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 <math>6.91 \times 10^{-73}</math> which is significantly less than 1 chance in 100,000 (<math>1 \times 10^{-5}</math>).</p> |

**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)   |
| 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)   |

| Service              | Description   | Role(s)  |
|----------------------|---|--|
| 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<br>(SID Authority)  |
| Disable Zeroize      | Disable TCG Revert method   | CO<br>(SID Authority)  |
| Set                  | Write data structures; access control enforcement occurs per data structure field. PINs can be changed using this service.  | CO, Users,<br>Maker<br>(SID Authority,<br>EraseMaster,<br>BandMasters) |
| Set TCG Credential   | Inputs authentication data and replaces stored hashed PIN data.   | CO, Users<br>(SID Authority,<br>EraseMaster),<br>(BandMasters)         |
| Set LBA Band         | Set the starting location, size, and attributes of a set of contiguous Logical Blocks   | Users<br>(BandMasters)   |
| Lock/Unlock LBA Band | Deny/Permit access to a LBA Band  | Users<br>(BandMasters)   |
| Write Data           | Transform plaintext user data to ciphertext and write in a LBA band   | Users<br>(BandMasters)   |
| Read Data            | Read ciphertext from a LBA band and output user plaintext data  | Users<br>(BandMasters)   |
| Set Data Store       | Write a stream of bytes to unstructured storage   | Users<br>(BandMasters)   |
| 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<br>(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 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                                   |

| Service         | Description  |
|-----------------|--|
| 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.                                    |

**Table 8 - Unauthenticated Services**

### 5.3 Definition of Critical Security Parameters (CSPs)

The Cryptographic Module contains the following CSPs:

| Key Name   | Type                        | Description  |
|--|-----------------------------|--|
| PIN - TCG Credential<br>(8 total)                        | 256-bit authentication data | Authenticates the Cryptographic Officer and User roles   |
| MEK - Media Encryption Key<br>(6 total - 1 per LBA band) | XTS-AES-256 (512 bits)      | Encrypts and decrypts LBA Bands<br>Note: This key is only associated with one key scope.   |
| KEK – Key Encrypting Key<br>(6 total)                    | SP 800-132 PBKDF (256 bits) | Keys derived from BandMaster PINs which wrap the MEKs<br>Note: Keys protected by this SP 800-132 PBKDF derived key shall not leave the module. |
| NDRNG  | Entropy data                | Entropy source for DRBG  |
| DRBG   | Internal CTR_DRBG state     | All properties and state associated with the SP800-90A Deterministic Random Bit Generator which include the values V and the Key.              |

**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              |
|----------|---------------------|--------------------------|
| 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 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          | 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                  |
|                                       | Maker PIN     | E                  |
| Set TCG Credential                    | CO PIN        | W                  |
|                                       | User PIN      | W                  |
| 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                  |

| Service         | CSPs and Keys | Type of CSP Access |
|-----------------|---------------|--------------------|
|                 | MEK           | E                  |
| Set Data Store  | User PIN      | E                  |
| Erase LBA Band  | CO PIN        | E                  |
|                 | KEK           | G                  |
|                 | MEK           | Z, G, W            |
| Self-Test       | NDRNG         | E                  |
|                 | DRBG          | 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          | E                  |
|                 | CO PIN        | W                  |
|                 | User PIN      | W                  |
|                 | DRBG          | G                  |
|                 | KEK           | G                  |
|                 | MEK           | 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

Ultrastar C10K1800 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 Cryptographic 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 Integrity 16-bit CRC
- Hardware AES Encrypt KAT (Known Answer Test)
- Hardware AES Decrypt KAT
- Firmware AES Encrypt KAT
- Firmware AES 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 Cryptographic 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 Cryptographic Module.
- There are no restrictions on which plaintext keys or CSPs the zeroization service deletes.
- The Cryptographic Module does not support a maintenance interface or maintenance role.
- The Cryptographic Module does not support manual key entry.
- The Cryptographic Module does not have any external input/output devices used for entry/output of data.
- The Cryptographic Module does not output plaintext CSPs.
- The Cryptographic Module does not output intermediate key values.
- The Cryptographic 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) 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:

- All components are production-grade materials with standard passivation.
- The enclosure is opaque.
- Engineering design supports 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 2: Large Tamper-Evident Label Hardware Version (1)



Figure 3: Smaller Tamper Evident Label Hardware Version (1)



## 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 8: Tamper Evidence on Large Tamper Label



Figure 9: Tamper Evidence on Metal Surface

## 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

- [SP800-90A] 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  |

| 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     |

| Description           | Code    |
|-----------------------|---------|
| 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 |
| 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 C10K1800 Hard Disk Drive Specification, version 1.2 (Nov 17, 2014)
- [D&O] Delivery & Operation (Cryptographic Officer) Manual, version 0.6 (Nov, 31 2014)