HGST

a Western Digital brand

# HGST Ultrastar SS200 TCG Enterprise SSD
# FIPS 140-2 Cryptographic Module
# Non-Proprietary Security Policy

*Protection of Data at Rest*

Version: 1.5
Date: 9/27/2017

# Table of Contents

# List of Tables

# List of Figures

# 1 Introduction

This document defines the Security Policy for the HGST Ultrastar SS200 TCG Enterprise SSD cryptographic modules, hereafter denoted as the Module. It is compliant with FIPS 140-2 overall Level 2 requirements and is a multi-chip embedded embodiment. The Module is a 12Gbps Solid State Drive (SSD)-Self-Encrypting Drive (SED). The Module is constructed and compliant with the following standards and specifications:

- FIPS PUB 140-2 [FIPS140]
- NIST [SP800 88] Guidelines for Media Sanitization
- Trusted Computing Group Storage Architecture Core Specification [TCG Core]
- Trusted Computing Group Enterprise Specification [TCG Enterprise]
- Trusted Computing Group Storage Interface Interaction Specification [TCG SIIS]
- Small Computer System Interface Block Commands [SCSI SBC]
- Small Computer System Interface Primary Commands [SCSI SPC]
- Serial Attached SCSI [SAS]
- Small Form Factor 8200 2.5" Enclosure Specification [SFF Enclosure]
- Small Form Factor 8639 Connector Specification [SFF Connector]

More information on the Module is available from the following sources:

- http://www.hgst.com/products/solid-state-solutions/ultrastar-ss200 has information on HGST products
- http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm has contact information for individuals that can answer technical and sales questions

There shall be no discrepancies with the product model numbers, the hardware version numbers and the firmware version numbers from the three following sources:

- This Security Policy
- The NIST/CMVP website
- The output information provided by the 'FIPS Info' service

Table 1 – Product Models and Versions

| Model Number, HW Version | FW Version | Capacity | Description |
|---|---|---|---|
| SDLL1HLR-076T Version 1 | XC00 | 7680 GB | 12Gbs SAS, 2.5in, 15mm |
| SDLL1MLR-038T Version 1 | XC00 | 3840 GB | 12Gbs SAS, 2.5in, 15mm |
| SDLL1CLR-020T Version 1 | XC00 | 1920 GB | 12Gbs SAS, 2.5in, 15mm |
| SDLL1DLR-920G Version 1 | XC00 | 920 GB | 12Gbs SAS, 2.5in, 15mm |

The FIPS 140-2 security levels for the Module are:

Table 2 – Security Level of Security Requirements

| Security Requirement | Security Level |
|---|---|
| Cryptographic Module Specification | 2 |
| Cryptographic Module Ports and Interfaces | 2 |
| Roles, Services, and Authentication | 2 |
| Finite State Model | 2 |
| Physical Security | 2 |

| Security Requirement | Security Level |
|---|---|
| Operational Environment | N/A |
| Cryptographic Key Management | 2 |
| EMI/EMC | 3 |
| Self-Tests | 2 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | N/A |

## 1.1 Hardware and Physical Cryptographic Boundary

Figure 1 depicts the front and rear views of the Module. The drive enclosure defines the cryptographic boundary.

Figure 1 – SDLL1HLR-076T and SDLL1MLR-038T Cryptographic Module Definition

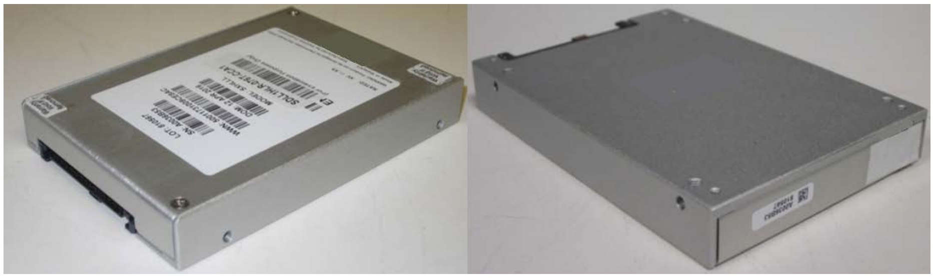


Figure 2 - SDLL1CLR-020T and SDLL1DLR-920G Cryptographic Module Definition

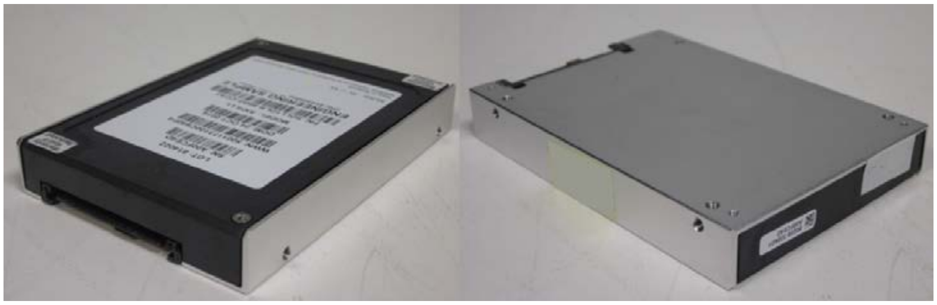


Table 3 – Ports and Interfaces

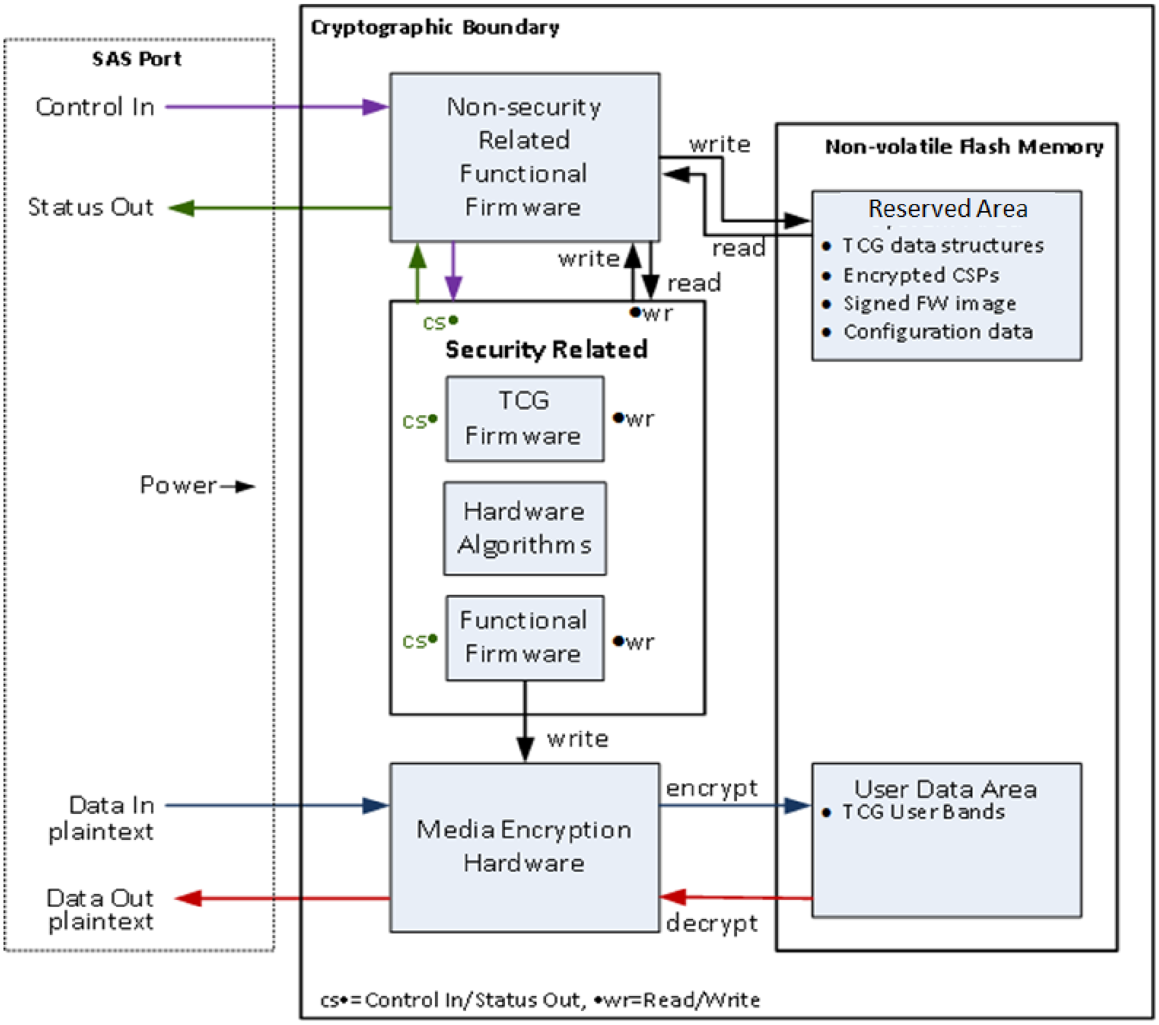
| FIPS140 Logical Interface | Module Physical Ports |
|---|---|
| Power | Power connector |
| Control Input | Dual Port SAS connector, Micro-HDMI connector is disabled with a tamper evidence seal |
| Status Output | Dual Port SAS connector, Micro-HDMI connector is disabled with a tamper evidence seal |
| Data Input | Dual Port SAS connector, Micro-HDMI connector is disabled with a tamper evidence seal |
| Data Output | Dual Port SAS connector, Micro-HDMI connector is disabled with a tamper evidence seal |

The SAS (Serial Attached SCSI) connector is defined by the storage industry [SFF]. Two independent SAS ports are implemented. The Data Input interface is active only during the data phase of a SCSI Write command, and the Data Output interface is active only during the data phase of a SCSI Read Command. The Micro-HDMI connector is enabled only at HGST facilities; it is disabled with a tamper evidence seal before the Module is delivered.

## 1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module's operational environment.

Figure 3 – Module Block Diagram



## 1.3 Mode of Operation

The Module operates in a FIPS Approved mode unless any self-test fails, in which case the Module enters a TCG Shutdown error state. To verify that the Module is in the Approved mode of operation, invoke the FIPS Info service. This service provides the model number, hardware version number and firmware version number. Failure of the FIPS Info service indicates the Module is in an error state that can only be cleared by the Reset service.

# 2 Cryptographic Features

The Module implements FIPS Approved and Allowed cryptographic functions. All algorithms and key lengths comply with [SP800 131A].

Table 4 – Approved and CAVP Validated Cryptographic Functions

| Algorithm | Description | Cert # |
|---|---|---|
| AES Firmware | [FIPS 197, SP800 38A]<br>Functions: Encryption and Decryption<br>Modes: ECB<br>Key sizes: 256 bits | 4343 |
| AES XTS Hardware | [FIPS 197, SP800 38A, SP800 38E]<br>Functions: Encryption of Data In, Decryption of Data Out<br>Modes: XTS<br>Key sizes: 256 bits<br>• XTS Key 1 is not equal to XTS Key 2<br>XTS data unit length is less than $2^{20}$ blocks<br>Modes: ECB<br>Key sizes: 256 bits | 4463 |
| DRBG Firmware | [SP800 90A]<br>Functions: HMAC_DRBG Deterministic Random Bit Generator<br>Security Strength: 256 bits | 1385 |
| HMAC Firmware | [FIPS 198-1]<br>Functions: SP800 132 KDF and SP800 90A DRBG<br>SHA sizes: SHA-256 | 2881 |
| RSA Hardware | [FIPS 186-4, PKCS#1 v1.5]<br>Functions: Signature Verification with SHA-256<br>Key sizes: 2048 bits | 2439 |
| SHA Firmware | [FIPS 180-4]<br>Functions: non-Digital Signature Applications<br>SHA sizes: SHA-256 | 3578 |
| SHA-256 Hardware | [FIPS 180-4]<br>Functions: Digital Signature Verification and Integrity<br>SHA sizes: SHA-256 | 3675 |

Table 5 – Approved Cryptographic Functions Tested with Vendor Affirmation

| Algorithm | Description | Rationale |
|---|---|---|
| CKG | [SP800 133] Cryptographic Key Generation<br>Functions: Generated from the DRBG without further modification or post processing | Vendor Affirmed [FIPS140] IG D.12.<br>See Section 2.1. |

| Algorithm | Description | Rationale |
|---|---|---|
| PBKDF | [SP800 132] Password Based Key Derivation Function<br>Functions: Key Encrypting Key<br>Modes: HMAC/SHA-256<br>Key Sizes: 256 bits | Vendor Affirmed<br>[FIPS140 IG] D.6.<br>See Section 2.3. |

Table 6 – Non-Approved but Allowed Cryptographic Functions

| Algorithm | Description |
|---|---|
| NDRNG | [FIPS140 IG] 7.11<br>Hardware Non-Deterministic Random Number Generator with 16-bits per access. The output seeds the SP800 90A Deterministic Random Bit Generator. |

There are no Non-Approved Cryptographic Functions.

## 2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 7 – Critical Security Parameters (CSPs)

| CSP | Type | Description |
|---|---|---|
| CO TCG PIN: 2<br>User TCG PIN: 16 | 256-bit value | Authentication data of TCG Authorities (Roles) is a binary value with no encoding; industry practice is a 256-bit random number or a SHA-256 digest [TCG App] |
| Drive AUTH: 16 | 256-bit value | Private KEKs that wrap MEKs when Bands are set to ‘Unlock on Reset’ with the Set Band service; generated from the DRBG without modification |
| MEKs<br>(Media Encryption Keys)<br>16 total | AES256-XTS<br>(512 bits) | Encrypts User data for the Data In interface and decrypts User data for the Data Out interface; generated from the DRBG without modification |
| KEKs<br>(Key Encrypting Keys)<br>16 total | 256 bits | SP800 132 KDF output; ephemeral, calculated keys that wrap MEKs |
| DRBG | HMAC_DRBG state<br>(256-bit output) | State associated with the SP800 90A Deterministic Random Bit Generator; the internal state includes values “V” and “Key” |
| NDRNG | entropy source | 2048-bit seed and 1024-bit nonce for DRBG |

### 2.2 Public Keys

Table 8 – Public Security Parameters (PSPs)

| Key | Description |
|---|---|
| Download Key | Public key of a 2048-bit RSA key pair used to verify downloaded firmware |
| **Value [qty]** | **Description** |
| MSID [1] | Initial authentication data for all operators |
| PSID [1] | Crypto-Officer authentication data for TCG Revert |
| AUTH Salt [18] | Concatenated with CO TCG PIN, User TCG PIN or Drive AUTH, hashed with SHA256 and digest stored within the Module |
| MEK Salt [16] | Input to SP800 132 PBKDF |

### 2.3 SP800 132 Key Derivation Function Affirmations

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

- The KEKs (SP800 132 Master Keys) are derived from the User TCG PINs and the CO TCG PINs (SP800 132 Password) with SP800-132 Option 1a
- The length of the User TCG PINs and the CO TCG PINs is 256 bits and the stored security strength is 256 bits
- The upper bound for the probability of guessing the User TCG PINs and the CO TCG PINs is $2^{-256.}$
- The difficulty of guessing the User TCG PINs and the CO TCG PINs is equivalent to a brute force attack
- The KEKs (SP800 132 Master Keys) are only used to wrap the Media Encryption Keys (MEKs).
- The CSPs derived using [SP800 132] are only used within storage applications.

## 3 Roles, Authentication and Services

### 3.1 Assumption of Roles

The Module supports three (3) distinct authenticated operator roles: Cryptographic Officer (CO), User and one HGST role. The Module enforces the separation of roles with Identity based authentication and fixed entity to key relationships. The relationship between Users (BandMasters), Bands and MEKs (Media Encryption Keys) is 1:1:1. Each CO and User role is associated with a 64-bit public Unique ID (UID) that is defined in [TCG Core]. The HGST role uses RSA2048 PKCS#1 v1.5 signature verification.

Table 9 lists all of the operator roles supported by the Module. The Module does not support a maintenance role or a bypass mode. The Module protects authentication data from unauthorized disclosure on the Data Out and Status Out interfaces by not storing plaintext authentication data within the Module and by the constraints imposed by the TCG/SCSI protocol stack.

Table 9 – Roles Description

| Role Name | Description | Authentication Type | Credentials |
|---|---|---|---|
| Crypto-Officer (CO) | TCG SID Authority. initializes the Module | Identity-based | 64-bit UID and 256-bit authentication data (TCG PIN) |
| | TCG EraseMaster Authority is authorized to generate new Band keys | Identity-based | 64-bit UID and 256-bit authentication data (TCG PIN) |

| Role Name | Description | Authentication Type | Credentials |
|---|---|---|---|
| User | TCG BandMasters [0-15] Authorities set Band location and size and lock/unlock a band;<br>Module maintains Drive authentication data when a User has not locked a band | Role-based | TCG BandMasters 64-bit UID and 256-bit authentication data (TCG PIN);<br>Drive AUTH: 256-bit authentication data |
| Drive AUTH | The Module authenticates itself when Band [0-15] are not configured to lock on Reset. It is required because a KEK cannot be generated without successful User Authentication | Role-based | 256-bit plaintext secret that is generated at the HGST factory and re-generated at Zeroize |
| HGST | The Module verifies FW Images with a RSA2048 public key | Identity-based | A RSA2048 private key signs FW images at a HGST facility |

Table 10 – Unauthenticated Roles

| Role Name | Description | Authentication Type | Rationale |
|---|---|---|---|
| Anybody | TCG Anybody Authority is permitted to access unauthenticated services | None | Public 64-bit UID; no TCG PIN is required |
| CO.MSID | A Module unique default TCG PIN is installed during manufacturing | Public value | Obtained with the Get service and used by the CO as authentication data for the Initialize service |
| CO.PSID | A Module unique TCG PIN is installed during manufacturing | Public value | Printed on the Module’s label and used by the CO as authentication data for the Zeroize service |
| MakerSymK | A TCG Authority that may obtain a random number from the [SP800 90A] DRBG | None | Equivalent to the Random service but uses the Authenticate service |
| User.MSID | A Module unique default TCG PIN is installed during manufacturing | Public value | Obtained with the Get service and provided by the User as authentication data |

## 3.2 Authentication Methods

The Authenticate service for User TCG PINs and the CO TCG PINs has two input parameters: a 64-bit public Unique ID (UID) defined in [TCG Core] and 256-bit authentication data. The authentication data is binary, i.e., there are no restrictions on values such as character or digit encoding. The [TCG Core] term for authentication data is a PIN. The difficulty of guessing a TCG PIN is equivalent to a brute force attack.

Firmware downloads are signed at an HGST facility with RSA2048 PKCS#1 v1.5 and verified by the Module before they are stored within the module.

Table 11 – Authentication Description

| Authentication Method | Probability | Rationale |
|---|---|---|
| 256-bit authentication data | 1 chance in $2^{256}$ | A TCG PIN is 256 non-coded bits, which provides $2^{256}$ possible values. The probability that a random attempt succeeds is ~8.6 x $10^{-78}$, which is significantly less than 1/1,000,000 (1 x $10^{-6}$).<br>Multiple, successive authentication attempts can only occur sequentially. Any authentication attempt consumes at least 10 microseconds, and at most, 6,000,000 authentication attempts are possible in one minute. Thus, the probability that a false acceptance occurs over a one-minute interval is ~5 x $10^{-71}$, which is significantly less than 1 chance in 100,000 (1 x $10^{-5}$). |
| RSA2048 PKCS#1 v1.5 | 1 chance in $2^{112}$ | Given the $2^{112}$ strength of security from [SP800 131A], the probability that a random attempt succeeds is ~1.9 x $10^{-34}$, which is significantly less than 1/1,000,000 (1 x $10^{-6}$).<br>Multiple, successive authentication attempts can only occur sequentially. Any authentication attempt consumes at least four (4) seconds, and at most, 15 authentication attempts are possible in one minute. Thus, the probability that a false acceptance occurs over a one-minute interval is ~3 x $10^{-33}$, which is significantly less than 1 chance in 100,000 (1 x $10^{-5}$). |

## 3.3 Services

All services implemented by the Module are listed in Table 12 and Table 13. Table 14 declares all usage of CSPs by service.

Table 12 – Authenticated Services

| Service | Description | CO.SID Authority | CO.EraseMaster | User | Drive AUTH | HGST |
|---|---|---|---|---|---|---|
| Authenticate | TCG method to input a UID and PIN for authentication | X | X | X | | |
| Set | A polymorphic TCG method that writes structured data subject to operator authorization | X | X | X | | |
| Set TCG PIN | A specific TCG Set method that modifies a PIN. An operator can only change its own PIN | X | X | X | | |
| Set Band | A specific TCG Set method that creates and modifies a Band's location, capacity and properties | | | X | | |
| Lock/Unlock Band | A specific TCG Set method that denies/permits access to a Band | | | X | | |
| Erase Band | A TCG method that generates a new Band Media Encryption Key | | X | | | |
| Read User Data | SCSI READ command reads from a Band, transforms ciphertext to plaintext and outputs User data to the Data Out interface | | | X | X | |
| Write User Data | SCSI WRITE command Inputs from the Data In interface, transforms plaintext User Data to ciphertext and writes to a Band | | | X | X | |
| Set Data Store | A specific TCG Set method to write a stream of bytes to unstructured storage | | | X | | |
| Download Firmware | The SCSI WRITE BUFFER command loads and verifies a firmware image by RSA2048. If the new self-tests complete successfully, the Module executes the new code | | | | | X |
| Enable/Disable Vendor Access | CO may disable the Download Firmware service and vendor log access | X | | | | |

Table 13 – Unauthenticated Services

| Service | Description | Anybody | CO.MSID | CO.PSID | MakerSymK | User.MSID |
|---|---|---|---|---|---|---|
| **Module Services** | | | | | | |
| Initialize | The Crypto-Officer takes ownership of the Module with organizational policies. re: 'Section 8.2 Crypto-Officer Initialization | | X | | | |
| Reset | The Module is reset by a power cycle | X | | | | |
| Self-test | The Module executes self-tests without operator intervention at power on | X | | | | |
| Show Status | Module Status Out is a compound type constructed with the TCG, SCSI and SAS protocol stack. Status elements are the TCG IF-SEND and IF-RECV payloads, SCSI SENSE DATA and SAS status | X | | | | |
| Zeroize | Invoke the TCG Revert service | | | X | | |
| **TCG Services** | | | | | | |
| Authenticate (at Initialize) | TCG method to input a UID and PIN for authentication | | X | X | X | X |
| Get | A polymorphic TCG method that reads structured data | X | | | | |
| Random | The TCG Random method outputs a random number from the [SP800 90A] DRBG | X | | | X | |
| Get Data Store | A specific TCG Get method to read a stream of bytes from unstructured storage | X | | | | |
| StartSession | A TCG method that connects to a TCG Security Provider object | X | | | | |
| End Session | A TCG protocol token from the Module to the operator that disconnects a TCG Security Provider object | X | | | | |
| Revert | A TCG method that restores authentication data to MSID, the original factory default, and generates new Media Encryption Keys | | | X | | |
| **SCSI Services** | | | | | | |
| FIPS Info | Outputs the [SCSI Core] FIPS 140 compliance descriptor, which provides a model number, hardware version, firmware version | X | | | | |

| Service | Description | Anybody | CO.MSID | CO.PSID | MakerSymK | User.MSID |
|---|---|---|---|---|---|---|
| IF-RECV | SCSI SECURITY IN command which provides a tunnel for the TCG protocol | X | | | | |
| IF-SEND | SCSI SECURITY OUT command which provides a tunnel for the TCG protocol | X | | | | |
| Sanitize | SCSI SANITIZE command that generates and establishes a new Media Encryption Key | X | | | | |
| **Non-security Related Services** | | | | | | |
| TCG methods/messages | re: Section 9.1 Non-security Related TCG requests | X | | | | |
| SCSI Commands | re: Section 9.2 Non-security Related SCSI Commands | X | | | | |

Table 14 defines the relationship between access to SSPs (i.e., the union of CSPs and PSPs) and the different Module services. The modes of access shown in the table are defined as:

- G = Generate: The Module generates the SSP.
- R = Read: The Module reads the SSP. The read access is typically performed before the Module uses the SSP.
- E = Execute: The Module executes using the SSP.
- W = Write: The Module writes the SSP. The write access is typically performed after a SSP is imported into the Module, when the Module generates a SSP, or when the Module overwrites an existing SSP.
- Z = Zeroize: The Module zeroizes the SSP.

Table 14 –Access Rights within Services

| Service | CSP | | | | | | | PSP | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | CO TCG PIN | User TCG PIN | Drive AUTH | MEKs | KEKs | DRBG | NDRNG | Download Key | MSID | PSID | AUTH Salt | MEK Salt |
| Authenticate | R | R | | | | | | | | | R | |
| Set | W | RW | E | | GEZ | R | R | | | | GW | GWR |
| Set TCG PIN | W | W | | W | GEZ | R | R | | | | GW | GW |
| Set Band | | R | E | W | GEZ | | | | | | | R |
| Lock/Unlock Band | | R | | R | GEZ | | | | | | | R |

| Service | CSP | | | | | | | PSP | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | CO TCG PIN | User TCG PIN | Drive AUTH | MEKs | KEKs | DRBG | NDRNG | Download Key | MSID | PSID | AUTH Salt | MEK Salt |
| Erase Band | R | | E | ZGW | | R | R | | | | | GW |
| Read User Data | | | E | E | | | | | | | | |
| Write User Data | | | E | E | | | | | | | | |
| Set Data Store | | R | | | | | | | | | R | |
| Download Firmware | | | | | | | | E | | | | |
| Enable/Disable Vendor Access | R | | | | | | | | | | R | |
| Initialize | W | W | | W | GEZ | R | R | | R | | GW | GW |
| Reset | | | G[1]E | | | ZG | ZR | | | | | |
| Self-test | | | | | | | | | | | | |
| Show Status | | | | | | | | | | | | |
| Zeroize | ZW | ZW | ZGWE | ZGW | | ZG | ZR | | R | R | GW | GW |
| Authenticate (at Initialize) | R | R | | | | | | | | | R | |
| Get | | | | | | | | | R | | | |
| Random | | | | | | R | R | | | | | |
| Get Data Store | | | | | | | | | | | | |
| StartSession | | | | | | | | | | | | |
| End Session | | | | | | | | | | | | |
| Revert | ZW | ZW | ZGWE | ZGW | | ZG | ZR | | R | R | GW | GW |
| FIPS Info | | | | | | | | | | | | |
| IF-RECV | | | | | | | | | | | | |
| IF-SEND | | | | | | | | | | | | |
| Sanitize | | | E | ZGW | | R | R | | | | | GW |
| TCG methods/messages | | | | | | | | | | | | |
| SCSI Commands | | | | | | | | | | | | |

[1] - Drive AUTH is initially generated at the first Power On Reset during Vendor manufacturing. A User may choose to override Drive AUTH with authentication data or to grant access to a Band at Reset. The latter is useful for clients that must load Master Boot Records and operating system software before User authentication can be executed.

# 4 Self-tests

Each time the Module is powered on, it tests that the cryptographic algorithms operate correctly and that sensitive data has not been damaged. Power on self–tests are available on demand by power cycling the Module. Table 15 describes the power-on self-tests. All KATs are completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the TCG Shutdown error state. Table 16 describes the conditional self-tests that are performed during certain conditions after power-on.

The module outputs an error indicator. The error indicator is x04440019 for each self-test that fails. The only exceptions are the following:

- the error indicator is 0x05269A00 for FW Download failure and
- the error indicator is "*** No firmware images could be loaded ***" for FW integrity failure.

Table 15 – Power Up Self-tests

| Test Target | Description |
|---|---|
| Firmware Integrity | 32-bit checksum of firmware by parts; all parts are checked. |
| AES Firmware | KATs: Encryption, Decryption<br>Modes: ECB<br>Key sizes: 256 bits |
| DRBG Firmware | Performed within SP800 90A section 11.3 health checks below |
| HMAC Firmware | KATs: Generation<br>SHA sizes: SHA-256 |
| KDF Firmware | KATs: None during SP800 132 vendor affirmation period per [FIPS140 IG] D.6 |
| SHA Firmware | KATs: SHA-256 |
| AES-XTS Hardware | KATs: Encryption, Decryption<br>Modes: XTS<br>Key sizes: 256 bits |
| RSA Hardware | KATs: Signature Verification<br>Key sizes: 2048 bits |
| SHA Hardware | KATs: SHA-256 |

Table 16 – Conditional Self-tests

| Test Target | Description |
|---|---|
| NDRNG | Continuous Test performed when a random value is requested from the NDRNG. |
| DRBG | Continuous Test performed when a random value is requested from the DRBG. |
| DRBG Health Checks | KAT, Instantiate, Generate and Reseed tests are performed per [SP800 90A] ⍰11.3 |
| Firmware Image | RSA 2048 with SHA-256 signature verification performed when firmware is loaded. |

# 5 Physical Security

## 5.1 Mechanisms

The Module has the following physical security properties:

- Production-grade components with standard passivation are used
- The drive enclosure is opaque
- The tamper-evident seals are comprised of two (2) different sizes, one is smaller at 12mm x 7mm; the other is larger at 20mm x 10mm
- Three (3) tamper-evident seals are applied at HGST manufacturing:
    - Two (2) small seals to prevent removal of the top cover in order to gain access or visibility
    - One (1) large seal to prevent access to the Micro-HDMI connector
- The tamper-evident seals cannot be penetrated or removed and reapplied without showing tamper-evidence
- The tamper-evident seals cannot be replicated during a low attack time

## 5.2 Tamper-Evident Seals and Locations

Figure 4 - Tamper-Evident Seal Over Screws (12mm x 7mm)

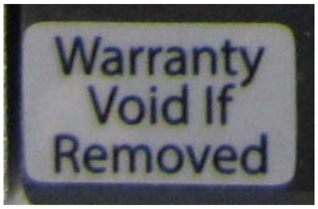


Figure 5 - Tamper-Evident Seal Over HDMI Port (20mm x 10mm)

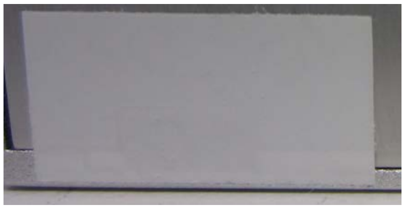


Figure 6 – Tamper-Evident Seal Locations on Top SDLL1HLR-076T Version 1 and SDLL1MLR-038T Version 1

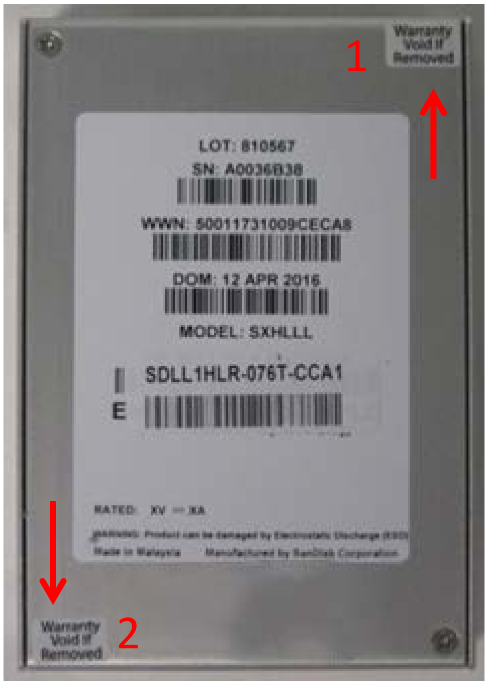


Figure 7. - Tamper-Evident Seal Locations on Top SDLL1CLR-020T Version 1 and SDLL1DLR-920G Version 1

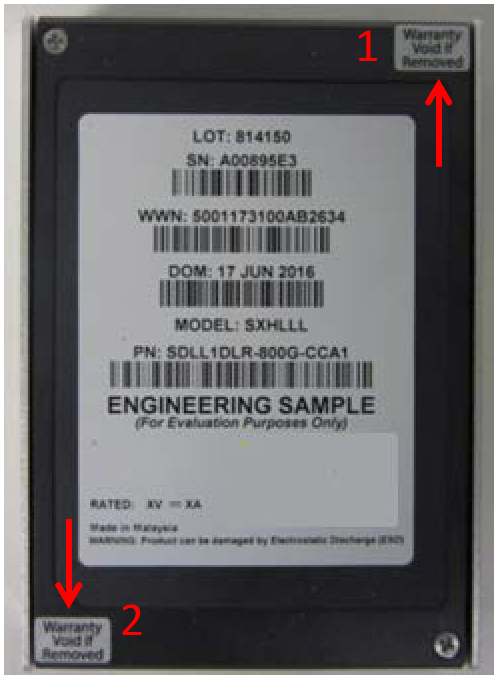


Figure 8. - Tamper-Evident Seal Location on Back Covering HDMI Port

SDLL1HLR-076T Version 1 and SDLL1MLR-038T Version 1

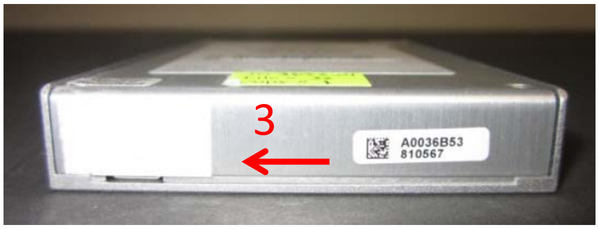
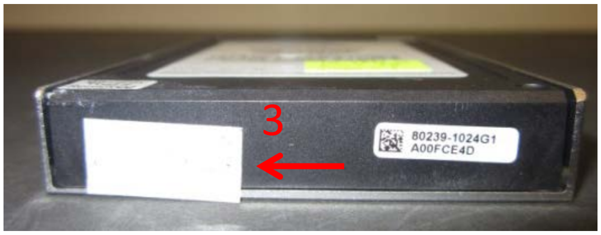


Figure 9 - Tamper-Evident Seal Location on Back Covering HDMI Port

SDLL1CLR-020T Version 1 and SDLL1DLR-920G Version 1



### 5.3 Operator Inspection

The Operator should inspect the Module for evidence of tampering upon receipt of the Module and once per year thereafter. If tampering is detected, the module should be removed from service and returned to HGST.

A tamper-evident seal that is intact will look smooth and uniform. Its edges will be firmly adhered to the surface of the drive. Careful scrutiny of the seal should reveal whether or not the seal has been tampered with. Attempts to remove the seal may be manifested by one or more of the following indicators:

- The adhesive layer is separated or non-uniform, leaving a visible pattern
- The seal’s surface has blistered, bubbled up, or has bumps beneath it, and is no longer smooth or flat. Surface irregularities can be highlighted by tilting the seal back and forth in the light.
- Edges of seal are lifted, or will not stay adhered. The seal will lift very easily by gently sliding a pick or fingernail under its edge.
- Residue of adhesive is visible around edges of seal indicating the seal has been removed and replaced.

Figure 10 – Small Seal Before Tamper

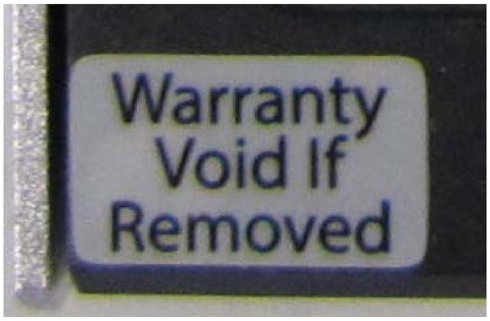


Figure 11 – Small Seal with Tamper Evidence

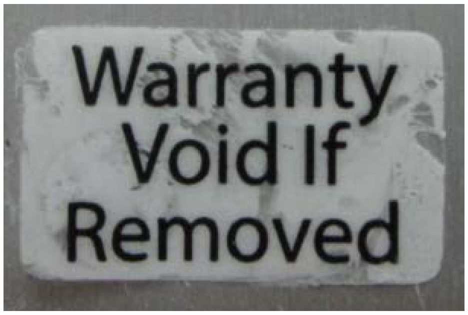


Figure 12 – Large Seal Before Tamper

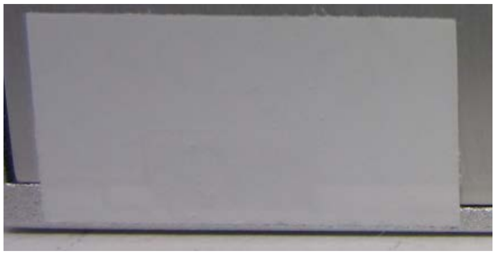
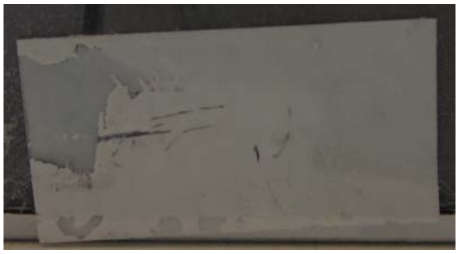


Figure 13 – Large Seal with Tamper Evidence



## 6 Operational Environment

The operating environment is non-modifiable. While the Module is operational, the environment cannot be modified; the code working set cannot be added, deleted or modified. Parts of the Firmware can be upgraded with an authenticated download service. If the download operation is successfully authorized and verified, then the Module will begin operating with the new code working set after successful completion of the Reset service.

## 7 Mitigation of Other Attacks Policy

None

## 8 Security Rules and Guidance

The Module design corresponds to these Module security rules. This section documents the security rules enforced by the Module and the Cryptographic Officer instructions that are necessary to implement the security requirements of FIPS 140-2 Level 2.

## 8.1 Invariant Rules

1. The Module provides two distinct authenticated operator roles: User and Cryptographic Officer.
2. The Module provides role-based authentication.
3. The Module clears previous operator authentications on power cycle.
4. When operators have initialized the Module with a valid configuration , operators do not have access to cryptographic services without successful authentication.
5. The operator is capable of commanding the Module to perform the self-tests by cycling power.
6. Power on self-tests do not require any operator action.
7. Data output is inhibited during self-tests and error states.
8. Data output is logically disconnected during key generation and zeroization.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The Module supports concurrent operators.
12. The Module does not support a maintenance interface or role.
13. The Module does not support manual key entry.
14. The Module does not have any external input/output devices used for entry/output of data.
15. The Module does not enter or output plaintext CSPs.
16. The Module does not output intermediate key values.
17. When the Module has successfully completed self-tests, FIPS mode is always available.
18. The End Session service deletes all ephemeral operator authentications. The Module requires operators to re-authenticate upon execution of the End Session service.
19. The Module enforces fixed entity to key relationships

## 8.2 Crypto-Officer Initialization

The Crypto-Officer shall follow the instructions in the Delivery & Operation (Cryptographic Officer) Manual for incoming inspection and end of life procedures. The instructions include:

- Establish authentication data for the TCG Authorities
- Establish the User Data Bands

## 8.3 Crypto-Officer Zeroization

The Crypto-Officer shall zeroize the Module by following the below instructions:

- Authenticate the CO.SID Authority with the PSID that is printed on the Module's label
- Execute the TCG Revert method

After successful completion of this procedure, the Module is reverted to the state in which it was delivered from HGST manufacturing, except new Media Encryption Keys are generated. Crypto-Officer Initialization shall be performed to re-enter TCG Policy mode.

# 9 Non-security Related Services

## 9.1 Non-security Related TCG Methods and Protocol

Table 17 – TCG Methods/Messages

| | | |
|---|---|---|
| Discovery | Get | GetACL |
| Next | Properties | Protocol Stack Reset |
| Set | StartSession | CloseSession |

## 9.2 Non-security Related SCSI Commands

Table 18 – SCSI Commands

| | | |
|---|---|---|
| FORMAT UNIT | INQUIRY | LOG SELECT |
| LOG SENSE | MODE SELECT | MODE SENSE |
| PERSISTENT RESERVE IN | PERSISTENT RESERVE OUT | READ |
| READ BUFFER | READ CAPACITY | READ DEFECT DATA |
| READ LONG | REASSIGN BLOCKS | RECEIVE DIAGNOSTICS RESULTS |
| REPORT LUNS | REPORT SUPPORTED OP CODES | RESERVE |
| REQUEST SENSE | SECURITY IN | SECURITY OUT |
| SEND DIAGNOSTIC | START STOP UNIT | SYNCHRONIZE CACHE |
| TEST UNIT READY | UNMAP | VERIFY |
| WRITE | WRITE AND VERIFY | WRITE BUFFER |
| WRITE LONG | WRITE SAME | |

# 10 References

The following standards are referred to in this Security Policy.

Table 19 – References

| **Abbreviation** | **Document Reference** |
|---|---|
| **NIST Standards** | |
| [AES] | Advanced Encryption Standard, FIPS PUB 197, NIST, 2001-Nov |
| [DSS] | Digital Signature Standard, FIPS PUB 186-4, NIST, 2013-Jul |
| [FIPS140] | Security Requirements for Cryptographic Modules, FIPS PUB 140-2, NIST, 2002-Dec |
| [FIPS140 DTR] | Derived Test Requirements for FIPS PUB 140-2, NIST, 2011-Jan |
| [FIPS140 IG] | Implementation Guidance for FIPS PUB 140-2, NIST, 2017-Aug |
| [HMAC] | The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, 2008-July |
| [SHA] | Secure Hash Standard (SHS), FIPS PUB 180-4, NIST, 2015-Aug |
| SP 800-38A | SP 800-38A |
| [SP800 38E] | Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, SP800 38E, NIST, 2010-Jan |
| [SP800 57] | Recommendation for Key Management – Part I General (Revision 4), NIST, 2016-Jan |
| [SP800 88] | Guidelines for Media Sanitization (Revision 1), NIST, 2014-Dec |
| [SP800 90A] | Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Revision 1, NIST, 2015 Jun |

| Abbreviation | Document Reference |
|---|---|
| [SP800 131A] | Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 1, NIST, 2015-Nov |
| [SP800 132] | Recommendation for Password-Based Key Derivation, NIST, 2010-Dec |
| [SP800 133] | Recommendation for Cryptographic Key Generation, NIST, 2012-Dec |
| **Trusted Computing Group (TCG) Specifications** | |
| [TCG Core] | TCG Storage Architecture Core Specification, Specification Version 2.01, Revision 1.00, 2015-Aug |
| [TCG Enterprise] | TCG Storage Security Subsystem Class: Enterprise Specification Version 1.01 Revision 1.00, 2015-Aug |
| [TCG SIIS] | TCG Storage Interface Interactions Specification (SIIS), Version 1.04, Revision 1.00, 2015-Aug |
| [TCG App] | TCG Storage Application Note: Encrypting Storage Devices Compliant with SSC: Enterprise, Version 1.00 Revision 1.00, 2009-Dec |
| **International Committee on Information Technology Standards T10 Technical Committee Standards** | |
| [SCSI Core] | SCSI Primary Commands-4 Rev 33 (SPC-4) |
| [SCSI Block] | SCSI Block Commands Rev15 (SBC-3) |
| [SAS] | Serial Attached SCSI-2 Rev 13 (SAS-2) |
| **Small Form Factor (SFF) Committee Specification** | |
| [SFF Enclosure] | SFF-8200 Specification for Suite of 2.5" Form Factor Drives Rev 3.3, SFF Committee, 2016-Jan |
| [SFF Connector] | SFF-8639 Specification for Multifunction 6X Unshielded Connector<br>Rev 2.0, SFF Committee, 2015-Jan |
| **HGST Specifications** | |
| [D&O] | Delivery & Operation (Cryptographic Officer) Manual |
| [Product Spec] | Ultrastar SS200 Series Product Specification |

## 11 Glossary

Table 20 – Acronyms and Definitions

| Term | Definition |
|---|---|
| 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. See [SP800 131A] for terms. |
| Anybody | A TCG Authority that is unauthenticated. [TCG Core] |
| Approved | [FIPS140] approved or recommended in a NIST Special Publication [SP800 57] |
| Approved mode of operation | A mode of a cryptographic Module that employs only Approved security functions. [FIPS140] |
| Authenticate | Prove the identity of an Operator or the integrity of an object [SP800 57] |
| Authorize | Grant an authenticated Operator access to a service or an object [SP800 57] |
| Band | A contiguous range of non-volatile memory that stores encrypted data. Bands shall not overlap and each has an individual encryption key, settable properties and authentication [TCG Core] |
| CO<br>Cryptographic Officer | An Operator performing cryptographic initialization and management functions [FIPS140] |

| Term | Definition |
|---|---|
| Confidentiality | A cryptographic property that sensitive information is not disclosed to unauthorized parties [SP800 57] |
| Ciphertext | Encrypted data transformed by an Approved security function [SP800 57] |
| 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] |
| CSP<br>Critical Security Parameter | Security-related information (e.g., secret and private cryptographic keys, and authentication data whose disclosure or modification can compromise the security of a cryptographic module [FIPS140] |
| DRBG | Deterministic Random Bit Generator [SP800 90A] |
| Ephemeral | Existing a short time |
| FIPS | Federal Information Processing Standard |
| Integrity | A cryptographic property that sensitive data has not been modified or deleted in an unauthorized and undetected manner [SP800 57] |
| Interface | A logical entry or exit point of a cryptographic module that provides access to the cryptographic module for logical information flows [FIPS140] |
| KAT | Known Answer Test |
| KDF<br>Key Derivation Function | An Approved cryptographic algorithm by which one or more keys are derived from a shared secret and other information [SP800 57] |
| KEK<br>Key Encrypting Key | A cryptographic key that is used to encrypt or decrypt other keys [SP800 57] |
| Key<br>Cryptographic Key | An input parameter to an Approved cryptographic algorithm [SP800 57] |
| Key Wrap | An Approved cryptographic algorithm that uses a KEK to provide Confidentiality and Integrity [SP800 57] |
| Logical Block | The smallest addressable unit of reading and writing on a standardized storage unit [SCSI Block] |
| MEK | Media Encryption Key [TCG Core] |
| Method | A TCG operation identified by a UID [TCG Core] |
| Module<br>Cryptographic Module | The set of hardware, software, and/or firmware that implement Approved security functions and is contained within the cryptographic boundary [FIPS140] |
| MSID<br>Manufactured SID | A SED unique value that vendors generate during manufacturing; it is readable with the TCG protocol and is the default value for TCG PINs [TCG Core] |
| NDRNG | Non-deterministic Random Number Generator: is the source of entropy for the DRBG [SP800 57] |
| Operator | A consumer, either human or automation, of Module services that is external to the Cryptographic Module [FIPS140] |
| Plaintext | Data that is not encrypted [SP800 57] |
| Port | A physical entry or exit point of a cryptographic module that provides access to the Cryptographic Module for physical signals [FIPS140] |
| PSP<br>Public Security Parameter | Information that is not secret but whose modification can compromise the security of the cryptographic module (e.g., a public key of a keypair) [ISO19790:2012] |
| PSID<br>Physical SID | A unique value that vendors print on an external label; it is used as authentication data for the Zeroize service [TCG Core] |

| Term | Definition |
|---|---|
| Session | An ephemeral exchange between a Security Provider and Operator that envelops the lifetime of an Operator's authentication. It acquires/releases a Security Provider and enables protocol synchronization<br>[TCG Core] |
| SAS | Serial Attached SCSI |
| SCSI | Small Computer System Interface |
| SID<br>Security Identifier | A TCG Authority that represents the Cryptographic Officer [TCG Core] |
| SED<br>Self-Encrypting Drive | A standardized storage unit that provides data storage services and supports cryptographic erase media sanitization |
| SP<br>Security Provider | A collection of data structures and methods with access control that is identified by a UID [TCG Core] |
| SSP<br>Sensitive Security Parameter | The union of CSPs and PSPs [ISO19790:2012] |
| Storage Medium | The non-volatile, persistent memory of a SED that is partitioned into two disjoint sets, a User Data area and a Reserved Area [SCSI Block] |
| Reserved Area | Private data on the Storage Medium that is not accessible outside the Cryptographic Boundary [Product Spec] |
| TCG | Trusted Computing Group |
| TCG Authority | Associates a TCG credential with an authentication operation, equivalent to a FIPS140 role [TCG CORE] |
| TCG Credential | UID, TCG PIN and other non-security related properties [TCG Core] |
| TCG PIN | Personal Identification Number: a string of 32 un-encoded octets that is used to authenticate a TCG Authority [TCG Core] |
| UID | 64-bit Unique Identifier of objects, methods and Authorities [TCG Core] |
| 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 services [SCSI Block] |
| Zeroize | Invalidate a Critical Security Parameter. [FIPS140] |