Western Digital®

Ultrastar® DC SS530 TCG Enterprise SSD
FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Protection of Data at Rest

Document Version: 1.5
2020-06-25

CONTENTS

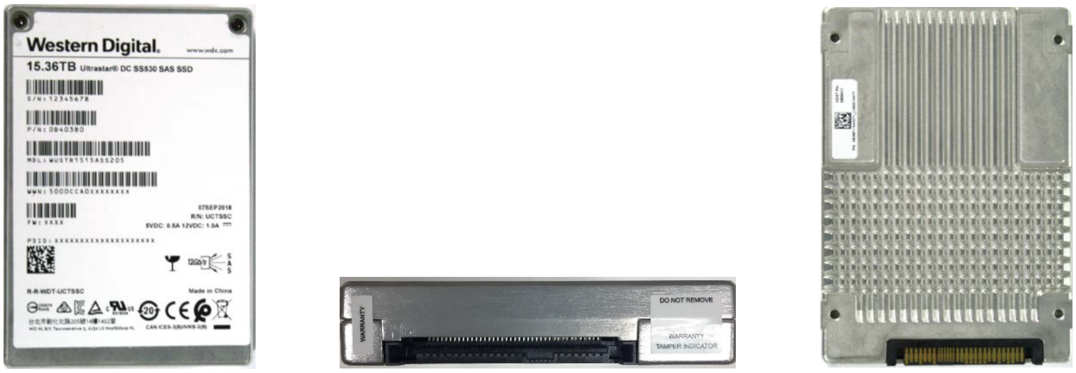
Tables

Figures

1. Cryptographic Module Overview

The self-encrypting Ultrastar® DC SS530 *TCG Enterprise SSD*, hereafter referred to as "Ultrastar DC SS530", or "the Cryptographic Module", is a multi-chip embedded module that comply with FIPS 140-2 *Level 2* security. The Cryptographic Module complies with the *Trusted Computing Group (TCG) SSC: Enterprise Specification.* The drive enclosure defines the cryptographic boundary. See Figure 1: Ultrastar DC SS530 Cryptographic Boundary. All components within this boundary satisfy FIPS 140-2 requirements.

Figure 1: Ultrastar DC SS530 Cryptographic Boundary


Western Digital.
15.36TB Ultrastar® DC SS530 SAS SSD
WARRANTY
DO NOT REMOVE
WARRANTY TAMPER INDICATOR

Top View SAS Connector View Bottom View

1.1 Models

The Cryptographic Module is available in several models that vary in write endurance and storage capacity. Data storage within the Cryptographic Module incorporates both NOR flash and NAND flash. All user data is stored in NAND flash. NOR flash stores all CSP data within the SECD FID and FSEC FID. The address range of all NOR flash is outside the address range of the NAND flash media. Therefore, NAND flash capacity and write endurance are not security relevant and excluded from FIPS 140-2 requirements.

The validated models listed below in Table 1 lists the models, characteristics, and firmware version associated with each model.

Table 1 Ultrastar DC SS530 TCG Enterprise SSD Models

Part Number	Firmware	Capacity (GB)	Description
WUSTM3240ASS205	R900, R901, R920, R925, R957, R960	400	2.5"-SFF, 12 Gb/s SAS, 3D TLC NAND, 10DW/D
WUSTM3280ASS205	R900, R901, R920, R925, R957, R960	800	2.5"-SFF, 12 Gb/s SAS, 3D TLC NAND, 10DW/D
WUSTM3216ASS205	R900, R901, R920, R925, R957, R960	1600	2.5"-SFF, 12 Gb/s SAS, 3D TLC NAND, 10DW/D
WUSTM3232ASS205	R900, R901, R920, R925, R92C, R957, R960	3200	2.5"-SFF, 12 Gb/s SAS, 3D TLC NAND, 10DW/D
WUSTR6440ASS205	R900, R901, R920, R925, R957, R95A, R960	400	2.5"-SFF, 12 Gb/s SAS, 3D TLC NAND, 3DW/D
WUSTR6480ASS205	R900, R901, R920, R925, R957, R95A, R960	800	2.5"-SFF, 12 Gb/s SAS, 3D TLC NAND, 3DW/D

Part Number	Firmware	Capacity (GB)	Description
WUSTR6416ASS205	R900, R901, R920, R925, R957, R95A, R960	1600	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 3DW/D
WUSTR6432ASS205	R900, R901, R920, R925, R92C, R957, R95A, R960	3200	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 3DW/D
WUSTR6464ASS205	R900, R901, R920, R925, R92C, R957, R960	6400	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 3DW/D
WUSTR1548ASS205	R900, R901, R920, R925, R92C, R957, R960	480	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 1DW/D
WUSTR1596ASS205	R900, R901, R920, R925, R957, R960	960	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 1DW/D
WUSTR1519ASS205	R900, R901, R920, R925, R92C, R957, R960	1920	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 1DW/D
WUSTR1538ASS205	R900, R901, R920, R925, R957, R95A, R960	3840	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 1DW/D
WUSTR1576ASS205	R900, R901, R920, R925, R957, R95A, R960	7680	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 1DW/D
WUSTR1515ASS205	R900, R901, R920, R925, R92C, R957, R95A, R95D, R960	15360	2.5”-SFF, 12 Gb/s SAS, 3D TLC NAND, 1DW/D

1.2 Security Level

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

Table 2 - Module Security Level Specification

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

2. Modes of Operation

2.1 FIPS Approved Mode of Operation

The Cryptographic Module has a single FIPS Approved mode of operation. Configuration and policy determine the Cryptographic Module's FIPS mode of operation. The Cryptographic Module enters FIPS Approved Mode after successful completion of the Initialize Cryptographic service instructions. See Section 7.2 for information on the Cryptographic Module's initialization rules. The operator can determine if the Cryptographic Module is operating in a FIPS approved mode by invoking the Get FIPS mode service[1]. The Crypto-Officer shall not enable the Maker Authority after the cryptographic module enters FIPS Approved mode. The cryptographic module is in FIPS non-Approved mode whenever a successful authentication to the Maker Authority occurs. If the Crypto-Officer enables the Maker Authority after the module enters FIPS Approved mode, the Crypto-Officer must also execute the TCG Revert Method to zeroize the cryptographic module. If the Crypto-Officer, subsequently, executes the Initialize Cryptographic service instructions provided in Section 7.2 with the intent of placing the cryptographic module in FIPS Approved mode, the Crypto-Officer must first execute the TCG Revert Method to zeroize the cryptographic module.

The chapter titled FIPS 140 Crypto-Officer Instructions within the Ultrastar DC SS530 Product Manual provides information on how to execute the Initialize Cryptographic service as well as the TCG Revert Method.

2.2 Approved Algorithms

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

Table 3 - FIPS Approved Algorithms

Algorithm	Description	Cert #
AES Firmware	[FIPS 197, SP800 38A, SP 800 38F] Functions: Encryption, decryption, and key wrapping to protect an associated MEK in data storage applications Modes: ECB, KW, CTR Key Size: 256	4281
AES ECB Hardware[2]	[FIPS 197, SP800 38A] Functions: Encryption and decryption Mode: ECB Key Sizes: 128, 256	4309
AES XTS Hardware[3]	[FIPS 197, SP800 38A, SP800 38E] Functions: Encryption and decryption in storage applications Mode: XTS • XTS-AES Key_1 does not equal XTS-AES Key_2 • The length of the XTS-AES data unit does not exceed 2^{20} blocks. Key Sizes: 128, 256	4309
DRBG Firmware	[SP800 90A] Function: Deterministic random number generator Mode: CTR Security Strength: 256 bits	1341

[1] A return value of 1 indicates that the cryptographic module is operating in FIPS Approved mode.
[2] Tested AES ECB-128. However, the cryptographic module does not use this algorithm.
[3] Tested AES XTS-128. However, the cryptographic module does not use this algorithm.

Algorithm	Description	Cert #
HMAC Firmware	[FIPS 198-1] Function: Key encrypting key (KEK) derivation used within the PBKDF SHA size: SHA-256	2817
RSA Firmware	[FIPS 186-4, PSS] Function: Digital signature verification with SHA-256[4] Key size: 2048	2302
SHA Hardware/Firmware	[FIPS 180-4] Functions: Digital Signature verification and KEK generation SHA size: SHA-256	3517
SHA Firmware	[FIPS 180-4] Functions: Digital Signature verification and KEK generation SHA size: SHA-256	3519

Table 4 – Approved Cryptographic Functions Tested with Vendor Affirmation

Algorithm	Description	Rationale
CKG	[SP800 133] Cryptographic Key Generation Function: Generated from the DRBG without further modification or post processing	Vendor Affirmed [FIPS140] IG D.12. See Section 5.3.
PBKDF	[SP 800-132] PBKDF	Vendor Affirmed

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

- A hardware NDRNG seeds the Approved [SP800-90A] DRBG. The NDRNG provides a minimum of 256 bits of entropy for key generation.

3. Ports and Interfaces

The drive uses the standard 29-pin Serial Attached SCSI (SAS) connector that conforms to the mechanical requirements of SFF 8680. Table 5 identifies the Cryptographic Module's ports and interfaces. The Serial connector is a two-wire port that consists of signal and ground. Western Digital disables the serial connector at its manufacturing facility before delivering the Cryptographic Module to customers. The Cryptographic Module does not provide a maintenance access interface.

Table 5 - Ultrastar DC SS530 Pins and FIPS 140-2 Ports and Interfaces

FIPS 140-2 Interface	Cryptographic Module Port Connector Pins
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

[4] SHA-256 Cert. #3519

4. Identification and Authentication Policy

The Cryptographic Module enforces role separation by requiring a role identifier and an authentication credential (Personal Identification Number or PIN). The Cryptographic Module enforces the following FIPS140-2 operator roles.

4.1 Crypto-Officer

4.1.1 Secure ID (SID) Authority

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

4.1.2 EraseMaster Authority

This TCG authority can selectively zeroize bands within the cryptographic module. Section 11.4.1 of the TCG Storage Security Subsystem Class: Enterprise Specification defines this role. It may also disable User roles and erase LBA bands (user data regions).

4.2 BandMaster Authority (User)

User roles correspond to Bandmaster Authorities. Section 11.4.1 of the TCG Storage Security Subsystem Class: Enterprise Specification provides a definition. Bandmaster authorities can lock/unlock and configure LBA bands (user data regions) and issue read/write commands to the SE Cryptographic Module. The TCG EraseMaster authority can disable a Bandmaster.

4.3 Anybody

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

4.4 Maker

For failure analysis purposes, the vendor can enable the serial port to perform diagnostics and gather data on the failure. A power cycle automatically locks the serial port. The vendor must authenticate to the SID and the Maker authorities to open the serial port. The cryptographic module is in FIPS non-Approved mode whenever the vendor authenticates to the Maker Authority. The vendor performs failure analysis within the vendor's facility. Maker authentication data shall not leave the vendor's facilities. During normal operation, the Crypto-Officer disables the Maker Authority when invoking the Initialize Cryptographic Module service.

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

Table 6 - Roles and Required Identification and Authentication

TCG Authority	Description	Authentication Type	Authentication Data
SID Authority	The SID Authority is a Crypto-Officer role that initializes the Cryptographic Module and authorizes Firmware download.	Role-based	CO Identity (TCG *SID Authority*) and PIN (TCG *SID Authority PIN*)
EraseMaster Authority	The EraseMaster Authority is a Crypto-Officer role that zeroizes Media Encryption keys and disables Users.	Role-based	CO Identity (TCG *EraseMaster Authority*) and PIN (TCG *EraseMaster PIN*)
BandMaster N (N = 0 to 15)	The BandMaster Authority is a User role that controls read/write access to LBA Bands.	Role-based	User Identity (TCG *BandMaster Authority*) and PIN (TCG *BandMaster PIN*)

TCG Authority	Description	Authentication Type	Authentication Data
Anybody	Anybody is a role that does not require authentication.	Unauthenticated	N/A
Maker (Disabled)	Completion of the Initialize Cryptographic Module service disables the Maker Authority	Role-based	User Identity (TCG Maker Authority) and PIN (Maker PIN)

Table 7 - Authentication Mechanism Strengths

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 x $10^{-78)}$ which is significantly less than 1/1,000,000 (1x 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 *TryLimit* value. Each authentication attempt consumes approximately 700 microseconds. Hence, at most, approximately 86,000 authentication attempts are possible in one minute. Thus, the probability that a false acceptance occurs within a one-minute interval is approximately 7.4 x 10^{-73}, which is significantly less than 1 chance in 100,000 (1 x 10^{-5}).
Maintenance Role	The maintenance role credential embedded within the VUC that enables the maintenance role is a 32-bit EDC, which provides 2^{32} possible values. The probability that a random attempt will succeed or a false acceptance will occur is at least 1 chance in 2^{32} (2.33 x10^{-10}), which is significantly less than 1/1,000,000 (1x 10^{-6}). Authentication attempts consume 74.5 milliseconds. Therefore, at most, 805 authentication attempts are possible within a one-minute interval. Thus, the probability that a false acceptance occurs within a one-minute interval is 1.88 x 10^{-7}, which is less than 1 chance in 100,000 (1 x 10^{-5}).

5. Access Control Policy

5.1 Roles and Services

Table 8 - Authenticated CM Services (Approved Mode)

Service	Description	Role(s)
Initialize Cryptographic Module[5]	Crypto-Officer provisions the Cryptographic Module from the organizational policies	CO (SID Authority)
Authenticate	Input a TCG Credential for authentication	CO, Users (SID Authority, EraseMaster, BandMasters)
Lock/Unlock Firmware Download Control	Deny/Permit access to Firmware Download service	CO (SID Authority)

[5] See the Cryptographic Module Acceptance and Provisioning section within the Ultrastar DC SS530 Product Manual.

Service	Description	Role(s)
Firmware Download	Unlocking the Firmware Download Control enables firmware downloads. RSA2048 PSS and SHA-256 verify the entire firmware image. If, after a successful download and the self-tests complete successfully the SED executes the new code.	CO (SID Authority)
Zeroize (TCG Revert)	The TCG Revert method zeroizes a drive and returns the Cryptographic Module to its original manufactured state.	CO, Users
Set	Write data structures; access control enforcement occurs per data structure field. This service can change PINs.	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 into ciphertext and write in a LBA band.	Users (BandMasters)
Read Data	Read ciphertext from a LBA band and output user plaintext data.	Users (BandMasters)
Set Data Store	Write a stream of bytes to unstructured storage.	Users (BandMasters)
Erase LBA Band	Band cryptographic-erasure by changing LBA band encryption keys to new values. Erasing an LBA band with EraseMaster sets the TCG Credential to the default value.	CO (EraseMaster)
Diagnostics (non-compliant)	Vendor Unique Commands (VUC) support diagnostic functions for testing the memory of the drive and the SCSI bus integrity. The VUCs do not alter the medium of the drive.	Maintenance

Table 9 - Authenticated CM Services (Non-Approved Mode)

Service	Description	Role(s)
Initialize Cryptographic Module[6] (non-compliant)	Crypto-Officer provisions the Cryptographic Module from the organizational policies	CO (SID Authority)
Authenticate (non-compliant)	Input a TCG Credential for authentication	CO, Users, Maker (SID Authority, EraseMaster, BandMasters)
Lock/Unlock Firmware Download Control (non-compliant)	Deny/Permit access to Firmware Download service	CO (SID Authority)

[6] See the Cryptographic Module Acceptance and Provisioning section within the Ultrastar DC SS530 Product Manual

Service	Description	Role(s)
Firmware Download (non-compliant)	Unlocking the Firmware Download Control enables firmware downloads. RSA2048 PSS and SHA-256 verify the entire firmware image. If, after a successful download, and all self-tests complete successfully, the SED executes the new code.	CO (SID Authority)
Zeroize (TCG Revert) (non-compliant)	The TCG Revert method zeroizes a drive and returns the Cryptographic Module to its original manufactured state.	CO, Users
Set (non-compliant)	Write data structures; access control enforcement occurs per data structure field. This service can change PINs.	CO, Users, Maker (SID Authority, EraseMaster, BandMasters)
Set LBA Band (non-compliant)	Set the starting location, size, and attributes of a set of contiguous Logical Blocks.	Users (BandMasters)
Lock/Unlock LBA Band (non-compliant)	Deny/Permit access to a LBA Band	Users (BandMasters)
Write Data (non-compliant)	Transform plaintext user data into ciphertext and write in a LBA band.	Users (BandMasters)
Read Data (non-compliant)	Read ciphertext from a LBA band and output user plaintext data.	Users (BandMasters)
Set Data Store (non-compliant)	Write a stream of bytes to unstructured storage.	Users (BandMasters)
Erase LBA Band (non-compliant)	Band cryptographic-erasure by changing LBA band encryption keys to new values. Erasing an LBA band with EraseMaster sets the TCG Credential to the default value.	CO (EraseMaster)
Set Vendor Data (non-compliant)	A Non-Approved service that is unavailable after the Initialize Cryptographic Module service completes.	Maker
Diagnostics (non-compliant)	Vendor Unique Commands (VUC) support diagnostic functions for testing the memory of the drive and the SCSI bus integrity. The VUCs do not alter the medium of the drive.	Maintenance

5.2 Unauthenticated Services

Table 10 - Unauthenticated Services lists the unauthenticated services the *C*ryptographic Module provides.

Table 10 - 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
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 14 - SCSI Commands
FIPS 140 Compliance Descriptor[7]	This service reports the FIPS 140 revision as well as the cryptographic module's overall security level, hardware revision, firmware revision and module name.

5.3 Definition of Critical Security Parameters (CSPs)

The Cryptographic Module contains the CSPs listed in

Table 11 - CSPs and Private Keys. Zeroization of CSPs complies with the purge requirements for SCSI solid state drives within [SP800-88], Guidelines for Media Sanitization.

Table 11 - CSPs and Private Keys

Key Name	Type	Description
Crypto-Officer PIN - TCG Credential (2 total)	256-bit authentication data	The PBKDF uses this PIN to authenticate the Crypto-Officer's credentials.
User PIN –TCG Credential (16 total)	256-bit authentication data	The PBKDF uses this PIN to authenticate the User's credentials

[7] See the FIPS 140 Compliance Descriptor section within the Ultrastar DC SS530 Product Manual

Key Name	Type	Description
MEK - Media Encryption Key[8] (16 total - 1 per LBA band)	XTS-AES-256 (512 bits)	Encrypts and decrypts LBA Bands. Each key is only associated with one LBA band. The Cryptographic Module's DRBG generates MEKs without modification.
KEK – Key Encrypting Key (16 total)	SP 800-132 PBKDF (256 bits)	Ephemeral keys derived from BandMaster PINs and 256-bit KDF salts that wrap the MEKs using an [SP 800-38F] AES-256 Key Wrap. Note: Keys protected by this [SP 800-132] PBKDF derived key shall not leave the module.
NDRNG	256-byte Entropy output	Entropy source for DRBG
DRBG	Internal CTR_DRBG state (384 bits)	All properties and state associated with the [SP800-90A] Deterministic Random Bit Generator
Maintenance Role Credential	32-bit authentication	A 32-bit EDC authenticates the credentials of the VUC that enables the maintenance role.

5.4 Definition of Public Security Parameters

The Cryptographic Module contains two public keys. The cryptographic module uses the public keys to verify the digital signature of a firmware download image. If the digital signature verification process fails when utilizing the primary public key, the cryptographic module attempts to use the secondary public key to verify the digital signature. The cryptographic module rejects the downloaded firmware image if both attempts to verify the digital signature fail.

Table 12 - Public Security Parameters

Key Name	Type	Description
RSAPublicKey[0]	RSA 2048 public key	Primary public key used to verify the digital signature of a firmware image.
RSAPublicKey[1]	RSA 2048 public key	Secondary public key used to verify the digital signature of a firmware image.
PSID	Twenty-character alpha-numeric string	A unique value generated in the factory and printed on the Cryptographic Module's label. The PSID provides authentication data and proof of physical presence for the Zeroize service.
PIN salt (16 total)	256-bit key	The Cryptographic Module's DRBG generates PIN salts without modification.
KDF Salt - Key Derivation Function Salt (16 total)	256-bit key	The Cryptographic Module's DRBG generates KDF salts without modification.

5.5 SP800-132 Key Derivation Function Affirmations

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

- The cryptographic module complies with SP800-132 Option 2a.

[8] A concatenation of XTS-AES Key_1 (256 bits) and XTS-AES Key_2 (256 bits)

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

5.6 Definition of CSP Modes of Access

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

- **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.

Table 13 - CSP Access Rights within Roles & Services

Service	CSPs and Keys	Type of CSP Access
Initialize Cryptographic Module	CO PIN User PIN DRBG, NDRNG KEK MEK	E, W E, W E G G, W
Authenticate	CO PIN User PIN	E E
Lock/Unlock Firmware Download Control	CO PIN	E
Firmware Download	CO PIN RSAFW	E E
Set	CO PIN User PIN Maker PIN	E E E
Set LBA Band	User PIN	E
Lock/Unlock LBA Band	User PIN KEK MEK	E G E

Service	CSPs and Keys	Type of CSP Access
Write Data	User PIN MEK	E E
Read Data	User PIN MEK	E E
Set Data Store	User PIN	E
Set Vendor Data	None	None
Erase LBA Band	CO PIN KEK MEK	E G Z, G, W
Diagnostics	None	None
Self-Test	NDRNG DRBG	E W
Reset Module	None	None
Status Output	None	None
Get FIPS mode	None	None
Start Session	None	None
End Session	None	None
Generate Random	DRBG	E
Get Data Store	None	None
Get	None	None
Zeroize (TCG Revert)	CO PIN User PIN DRBG KEK MEK	W W G G Z, G, W
SCSI	None	None
FIPS 140 Compliance Descriptor	None	None

6. Operational Environment

The Cryptographic Module operating environment is non-modifiable. Therefore, the FIPS 140-2 operational environment requirements are not applicable to this module. While operational, the Cryptographic Module prohibits additions, deletions, or modification of the code working set. For firmware upgrades, the Cryptographic Module uses an authenticated download service to upgrade its firmware in its entirety. If the download operation is successfully, authorized and verified, the Cryptographic Module will begin operating with the new code working set. Firmware loaded into the module that is not on the certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

7. Security Rules

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

7.1 Invariant Rules

1. The Cryptographic Module supports two distinct types of operator roles: Crypto-Officer and User. The module also supports an additional role, the Maker role. Initialization disables the Maker role.
2. Cryptographic Module power cycles clear all existing authentications.
3. After the Cryptographic Module has successfully completed all self-tests and initialized according to the instructions provided in Section 7.2, it is in FIPS Approved mode. The Crypto-Officer shall not enable the Maker Authority after the cryptographic module enters FIPS Approved mode.

~~4.~~ When the Cryptographic Module is unable to authenticate TCG Credentials, operators do not have access to any cryptographic service other than the unauthenticated Generate Random service.

5. The Cryptographic Module performs the following tests. Upon failure of any test, the Cryptographic Module enters a soft error state. The Cryptographic module reports the error condition by transmitting an UEC via the [SCSI] protocol. After entering the soft error state, the cryptographic module does not process functional commands unless a power cycle occurs.

   A. Power up Self-Tests

      1) Firmware Integrity 32-bit EDC
      2) Firmware AES Encrypt KAT, Cert #4281
      3) Firmware AES Decrypt KAT, Cert #4281
      4) RSA 2048 PSS Verify KAT, Cert #2302
      5) DRBG KAT[9], Cert#1341
      6) SHA-256 KAT, Cert#3519
      7) HMAC-SHA-256 KAT, Cert #2817
      8) Hardware AES Encrypt KAT, Cert #4309
      9) Hardware AES Decrypt KAT, Cert #4309
      10) HW/FW SHA-256 KAT, Cert #3517

   B. Conditional Tests

      1) The Cryptographic Module performs a Continuous Random Number Generator test on the DRBG and the hardware NDRNG entropy source.
      2) The Cryptographic Module performs a key comparison test on XTS-AES Key$_1$ and XTS-AES Key$_2$ that satisfies IG A.9 XTS-AES Key Generation Requirements.
      3) Firmware Download Test, RSA 2048 PSS (Cert. #2302), SHA-256 (Cert. #3517)

6. An operator can command the Cryptographic Module to perform the power-up self-test by power cycling the device.
7. Power-up self-tests do not require operator action.
8. Data output is inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused, could compromise the Cryptographic Module.
10. The Zeroization service deletes all plaintext keys and CSPs.
11. The Cryptographic Module supports a maintenance role. The operator must execute the TCG Revert Method to zeroize the cryptographic module before entering and maintenance role. The operator must also execute the TCG Revert Method to zeroize the cryptographic module after exiting the maintenance role.
12. The Cryptographic Module does not support manual key entry.

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

13. The Cryptographic Module does not have any external input/output devices used for entry/output of data.
14. The Cryptographic Module does not output plaintext CSPs.
15. The Cryptographic Module does not output intermediate key values.
16. The Cryptographic Module does not support concurrent operators.
17. The End Session service deletes the current operator's authentication. The Cryptographic Module requires operators to re-authenticate upon execution of the End Session service.
18. The host shall authenticate to LBA Bands after a power cycle.
19. The Crypto-Officer shall assure that all host issued User PINs are 32-bytes in length.

7.2 Initialization Rules

The Crypto-Officer shall follow the instructions provided in the FIPS 140 Crypto-Officer Instructions section of the Ultrastar DC SS530 Product Manual and the Delivery & Operation (Crypto-Officer's) Manual for acceptance and end of life procedures. Acceptance instructions include:

- Establish authentication data for the TCG Authorities by replacing the MSID (default PIN value).
- Erase the LBA Bands. When the Cryptographic Module erases the LBA bands it also erases the Media Encryption Keys.
- Establish the LBA Bands. When the Cryptographic Module establishes LBA bands it also generates Media Encryption Keys.
- Disable the Maker Authority.
- Lock the Firmware Download service and set the Firmware Download service to lock automatically after a power cycle. The cryptographic module automatically locks the Firmware Download service after downloading new firmware.

At the end of these steps, the cryptographic module will be in a FIPS Approved Mode of operation. While in FIPS Approved mode, only an authenticated Crypto-Officer can change the state of the firmware download service.

7.3 Zeroization Rules

The Crypto-Officer shall use the TCG Revert Method to perform the zeroization function. Reverting the cryptographic module zeroizes all Critical Security Parameters.

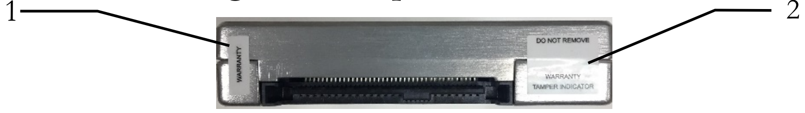
8. Physical Security Policy

8.1 Mechanisms

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

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

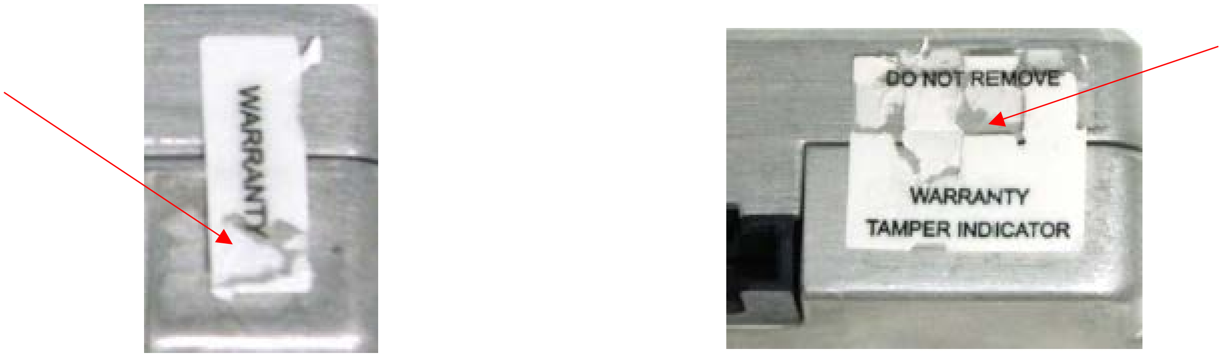
Figure 2: Tamper-Evident Seals



8.2 Operator Responsibility

The Crypto-Officer and/or User shall inspect the Cryptographic Module enclosure for evidence of tampering at least once a year. If the inspection reveals evidence of tampering, the Crypto-Officer should return the module to Western Digital.

Figure 3: Tamper Evidence on Tamper Seals



9. Mitigation of Other Attacks Policy

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

10. Definitions

- **Allowed**: NIST approved, i.e., recommended in a NIST Special Publication, or acceptable, i.e., no known security risk as opposed to deprecated, restricted and legacy-use. [SP800-131A]
- **Anybody**: A formal TCG term for an unauthenticated role. [TCG Core]
- **Approved mode of operation**: A mode of the cryptographic module that employs only approved security functions. [FIPS140]
- **Approved**: [FIPS140] approved or recommended in a NIST Special Publication.
- **Authenticate**: Prove the identity of an Operator or the integrity of an object.
- **Authorize**: Grant an authenticated Operator access to a service or an object.
- **Ciphertext**: Encrypted data transformed by an Approved security function.
- **Confidentiality**: A cryptographic property that sensitive information is not disclosed to unauthorized parties.
- **Credential**: A formal TCG term for data used to authenticate an Operator. [TCG Core]
- **Critical Security Parameter (CSP)**: Security-related information (e.g., secret and private cryptographic keys, and authentication data such as credentials and PINs) whose disclosure or modification can compromise the security of a cryptographic module. [FIPS140]
- **Cryptographic Boundar**y: An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module. [FIPS140]
- **Cryptographic key (Key)**: An input parameter to an Approved cryptographic algorithm
- **Cryptographic Module**: The set of hardware, software, and/or firmware used to implement approved security functions contained within the cryptographic boundary. [FIPS140]
- **Crypto-Officer**: An Operator performing cryptographic initialization and management functions. [FIPS140]
- **Data at Rest**: User data residing on the storage device media when the storage device is powered off.

- **Discovery**: A TCG method that provides the properties of the TCG device. [TCG Enterprise]
- **Drive Writes per Day (DWPD):** Drive Writes per Day defines how many times the entire capacity of the SSD can be overwrite every single day of its usable life without failure during the warranty period.
- **Integrity**: A cryptographic property to assure sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **Interface**: A logical entry or exit point of a cryptographic module that provides access to the cryptographic module for logical information flows. [FIPS140]
- **Key Derivation Function (KDF)**: An Approved cryptographic algorithm by which one or more keys are derived from a shared secret and other information.
- **Key Encrypting Key (KEK)**: A cryptographic key used to encrypt or decrypt other keys.
- **Key management**: The activities involving the handling of cryptographic keys and other related security parameters during the entire life cycle of the Cryptographic Module. The handling of authentication data is representative of a key management activity.
- **Key Wrap**: An Approved cryptographic algorithm that uses a KEK to provide Confidentiality and Integrity.
- **LBA Band**: A formal [TCG Core] term that defines a contiguous logical block range (sequential LBAs) to store encrypted User Data; bands do not overlap and each has its own unique encryption key and other settable properties.
- **Manufactured SID (MSID)**: A unique default value assigned to each SED during manufacturing. An externally visible MSID value is not required if the user can derive the MSID from other information printed on the drive. The MSID is readable with the TCG protocol. It is the initial and default value for all TCG credentials. [TCG Core]
- **Method**: A TCG command or message. [TCG Core]
- **Operator**: A consumer, either human or automation, of cryptographic services that is external to the Cryptographic Module. [FIPS140]
- **Personal Identification Number (PIN)**: A formal TCG term designating a string of octets used to authenticate an identity. [TCG Core]
- **Plaintext**: Unencrypted data.
- **Port**: A physical entry or exit point of a cryptographic module that. A port provides access to the Cryptographic Module's physical signals. [FIPS140]
- **PSID (Physical Security Identifier)**: A SED unique value printed on the Cryptographic Module's label used as authentication data and proof of physical presence for the Zeroize service.
- **Public Security Parameters (PSP)**: Public information, that if modified can compromise the security of the cryptographic module (e.g., a public key).
- **Read Data**: An external request to transfer User Data from the SED. [SCSI Block]
- **Reserved Area**: Private data on the Storage Medium that is not accessible outside the Cryptographic Boundary.
- **Security Identifier (SID)**: A TCG authority used by the Crypto-Officer. [TCG Core]
- **Self-Encrypting Drive (SED)**: A storage device that provides data storage services , which automatically encrypts all user data written to the device and automatically decrypts all user data read from the device.
- **Session**: A formal TCG term that envelops the lifetime of an Operator's authentication. [TCG Core]
- **Small Form Factor (SFF):** Small form factor is a computer form factor designed to minimize the volume and footprint of a desktop computer

- **Storage Medium**: The non-volatile, persistent storage location of a SED; it is partitioned into two disjoint sets, a User Data area and a Reserved Area.
- **Triple Level Cell (TLC)**: Triple level cells refer to NAND flash devices that store three bits of information per cell, with eight total voltage states.
- **User Data**: Data transferred from/to a SED using the Read Data and Write Data commands. [SCSI Block]
- **User**: An Operator that consumes cryptographic services. [FIPS140]
- **Write Data**: An external request to transfer User Data to a SED. [SCSI Block]
- **Zeroize**: Invalidate a Critical Security Parameter. [FIPS140]

11. Acronyms

- **CO**: Crypto-Officer [FIPS140]
- **CRC**: Cyclic Redundancy Check
- **CSP**: Critical Security Parameter [FIPS140]
- **DRAM**: Dynamic Random Access Memory
- **DRBG**: Deterministic Random Bit Generator
- **DW/D:** Drive Writes per Day
- **EDC:** Error Detection Code
- **EMI**: Electromagnetic Interference
- **FSEC:** Flash Security Data
- **FID:** Flash Internal Data
- **FIPS**: Federal Information Processing Standard
- **KAT**: Known Answer Test
- **KDF**: Key Derivation Function
- **LBA**: Logical Block Address
- **MEK**: Media Encryption Key
- **MSID**: Manufactured Security Identifier
- **NAND: N**egative AND, Flash Memory technology
- **NOR: N**egative OR, Flash Memory technology
- **NDRNG**: Non-deterministic Random Number Generator
- **NIST**: National Institute of Standards and Technology
- **PIN**: Personal Identification Number
- **PSID**: Physical Security Identifier
- **PSP**: Public Security Parameter
- **RID:** Reserved Area Internal Data
- **SAS**: Serial Attached SCSI
- **SECD:** Security Data
- **SCSI**: Small Computer System Interface

- **SED**: Self Encrypting Drive
- **SFF:** SSD Form Factor
- **SID**: TCG Security Identifier, the authority representing the Cryptographic Module owner
- **SSD**: Solid-state Drive
- **TCG**: Trusted Computing Group
- **TLC:** Triple Level Cell
- **UEC:** Universal Error Code
- **XTS**: A mode of AES that utilizes "Tweakable" block ciphers

12. References

12.1 NIST Specifications

- [AES] Advanced Encryption Standard, FIPS PUB 197, NIST, November 2001
- [DSS] Digital Signature Standard, FIPS PUB 186-4, NIST, July 2013
- [FIPS140] Security Requirements for Cryptographic Modules, FIPS PUB 140-2, NIST, December 2002
- [HMAC] The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, July 2008
- [SHA] Secure Hash Standard (SHS), FIPS PUB 180-4, NIST, August 2015
- [SP800 38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST, December 2001
- [SP800 38E] Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, SP800-38E, NIST, January 2010
- [SP800 38F] Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, NIST, December 2012
- [SP800 57] Recommendation for Key Management – Part I General (Revision 4), NIST, January 2016
- [SP800 90A] Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revision 1), NIST, June 2015
- [SP800 90B] Recommendation for the Entropy Sources Used for Random Bit Generation, NIST, January 2018
- [SP800 131A] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (Revision 1), NIST, November 2015
- [SP800 132] Recommendation for Password-Based Key Derivation, NIST, December 2010
- [SP800 133] Recommendation for Cryptographic Key Generation, NIST, December 2012

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)

- TCG Storage Interface Interactions Specification (SIIS), Version 1.02, (2011)

12.3 International Committee on Information Technology Standards T10 Technical Committee Standards

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

12.4 Corporate Documents

- [Product Manual] Ultrastar DC SS530 2.5-inch Serial Attached SCSI (SAS) Solid-State Drive Product Manual, Version 1.0 (October 2018), https://www.westerndigital.com/support
- [Datasheet] Ultrastar DC SS530 Datasheet, (July 2018), https://www.westerndigital.com/products/data-center-drives/ultrastar-sas-series-ssd

12.5 SCSI Commands

Table 14 - SCSI Commands

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

Description	Code		Description	Code
RELEASE	17h		WRITE BUFFER	3Bh
RELEASE	57h		WRITE LONG (10)	3Fh
REPORT DEVICE IDENTIFIER	A3h/05h		WRITE LONG (16)	9Fh/11h
REPORT LUNS	A0h		WRITE SAME (10)	41h
REPORT SUPPORTED OPERATION CODES	A3h/0Ch		WRITE SAME (16)	93h
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS	A3h/0Dh		WRITE SAME (32)	7Fh/0Dh
REQUEST SENSE	03h			