Western Digital Corporation

Verdi
Self Encrypting Drive (SED)

FIPS 140-2 Cryptographic Module Security Policy

Version: 1.1

Date: June 18, 2014

Table of Contents

List of Tables

List of Figures

1. Introduction

This document defines the Security Policy for the Western Digital Verdi Self Encrypting Drive (SED) module, hereafter denoted the “Module”. The Module, validated to FIPS 140-2 overall Level 2, is a storage device with SecureDrive functionality that protects against unauthorized access to Data. “Data” in this context is both User accessible data and metadata.

The Module is a multi-chip embedded embodiment; the cryptographic boundary is the outer enclosure of the hard disk drive (HDD).

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

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

Table 1 – Security Level of Security Requirements

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1; the enclosure is the cryptographic boundary.

Figure 1: Verdi Self Encrypting Drive (SED) Module

Port	Description	Logical Interface Type
SAS Interface	Serial Attached SCSI interface	This port transfers the following data types: Power In, Control in Data in, Data out, & Status out. This port is enabled by module Firmware. No direct access to any persistent memory is supported.
JTAG Port	MFG Test Access Port. This port supports the following functionality: processor trace access, special SoC test modes, SoC scan functionality, and SoC boundary scan control	This port is enabled in the manufacturing environment only. Internal SoC one time programmable fuses control port access. This port is disabled when SED Module is delivered to customer.

Port	Description	Logical Interface Type
SIO Port	MFG Serial Input/Output Port. This port is a manufacturer access port only. It is enabled for use during Module build and testprocesses.	This port is disabled outside of the manufacturing environment.
LEDs	No Error Status on LED	Status out

Table 2 – Ports and Interfaces

1.2 Logical Module Diagram

Figure 2 depicts the Module operational environment.

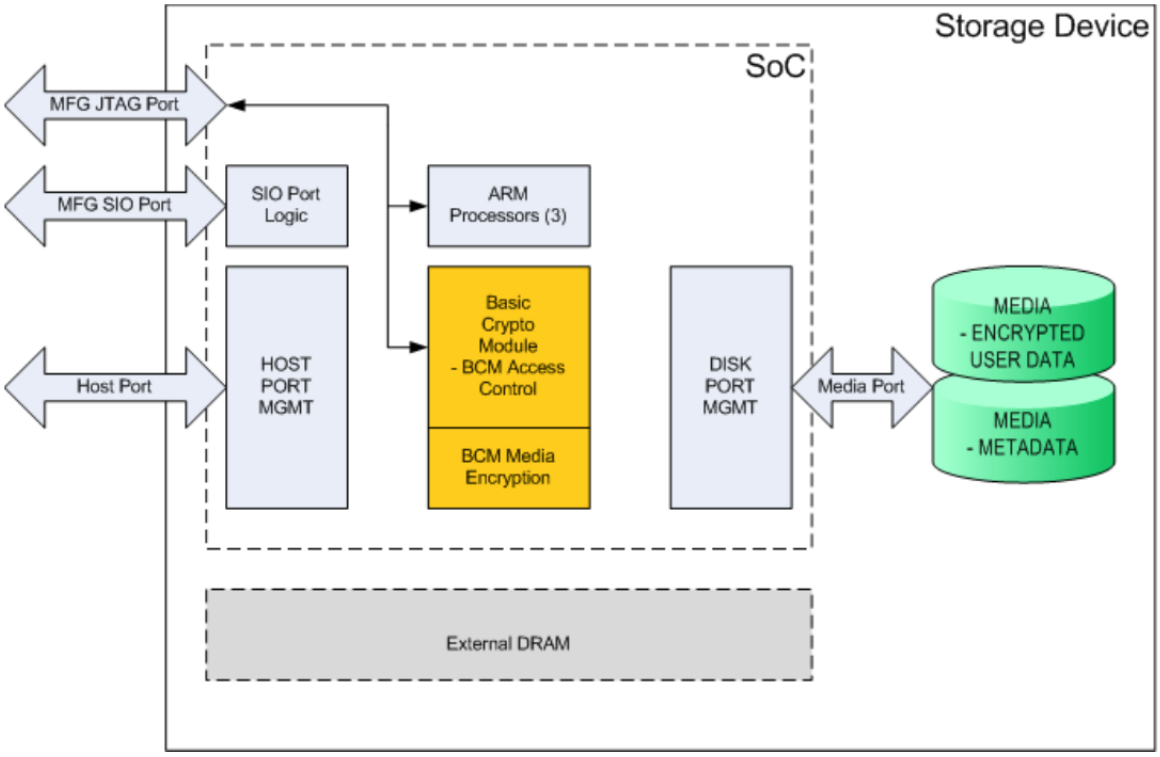

Figure 2: Module Block Diagram

The Verdi Self Encrypting Drive (SED) is designed to protect against unauthorized access to data. The primary function is providing protection for data at rest. All authorities 1) require authentication, and 2) have an assigned role (specific function/responsibility). The SED enforces defined access policies via 1) strong CSP protection, 2) port access management, clear Lifecycle access policies.
The above diagram identifies these major SED components:

- System on a Chip (SoC): a single chip controller that contains:

  - Basic Crypto Module (BCM) that transiently stores and operates on clear text CSP data, and
  - media encryption engine that encrypts and decrypts user data as it is written to or read from the persistent rotating memory.
- Persistent Rotating Memory: persistently stores both
  - encrypted Userdata, and
  - cryptographically protected nonUserData (nonUserData includes: HDD FW, encrypted and/or signed CSPs).
- Transient Memory (DRAM): This memory transiently stores
  - UserData, and
  - crypto module metadata (FW and FW objects)
- Ports: A SED HDD has an SAS interface that is the User's access port

1.3 Versions and Mode of Operation

	Module	HW P/N and Version	FW Version
1	Verdi Self Encrypting Drive (SED)	WD4001FYUG-01UVZ	VR08

The module only operates in a FIPS Approved mode of operation. To verify that a module is in the Approved mode of operation, an authority invokes a:

- SAS Inquiry Command response for FW version VR08
- SAS Inquiry Command response for Model Number WD4001FYUG-01UVZ

2. Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved algorithms indicated in Table 3 and 4, respectively. Allowed cryptographic functions are listed in Table 4 below.

Algorithm	Description	Cert #	CAVP Info
AES (BCM)	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, XTS Key sizes: 128/256	1678	**Marvell_Einstein2_BCM_AES/XTS_HW_Engine** Version BCM_EINSTEIN_2.0_02281 (Firmware) VCS Compiler version C-2009.06-7 simulation environment **ECB** (e/d; 128 , 192 , 256); **CBC** (e/d; 128 , 192 , 256); **XTS(KS: XTS_128**((e/d) (f)) **KS: XTS_256**((e/d) (f)))
AES (media encryptor)	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, CTR, XTS Key sizes: 128/256	1669	**Marvell_Monet2_Media_AES/XTS_HW_Engine** **ECB** (e/d; 128 , 256); **CBC** (e/d; 128 , 256); **CTR** (ext only; 128 , 256) **XTS(KS: XTS_128**((e/d) (f)) **KS: XTS_256**((e/d) (f)))
HMAC	[FIPS 198-1] Functions: SHA sizes: SHA-1, SHA-256	1062	**EINSTEIN2_HMAC_RTL**, Version 1.0 (Firmware) Synopsys VCS C-2009.06-7 simulator **HMAC-SHA1** (Key Sizes Ranges Tested: KS<BS KS=BS) SHS Val#1580 **HMAC-SHA256** (Key Size Ranges Tested: KS<BS KS=BS) SHS Val#1580
RNG	[ANSI X9.31-1998]	951	**hana_bcm_microcode_production** Version3.00.02(Firmware) part # 88i1248 88i1248 **ANSIX9.31**[AES-128Key]
RSA	[FIPS 186-2 and PKCS1.5] Functions: Signature Verification Key sizes: 2048 bits	901	**hana_bcm_microcode_production** Version 3.00.02 (Firmware)Part # 88i1248 88i1248 **FIPS186-2:** **ALG[RSASSA-PKCS1_V1_5]:** SIG(ver): 2048 , SHS: SHA-256Val#1580
SHA	[FIPS 180-3] SHA sizes: SHA-1, SHA-256	1580	**EINSTEIN2_SHA2_RTL** Version 1.0 (Firmware) Synopsys VCS C-2009.06-7 simulator **SHA-1** (BYTE-only) **SHA-256** (BYTE-only)

Table 3 –Approved Cryptographic Functions

Algorithm	Description
NDRNG	[Annex C] Hardware Non-Deterministic RNG (entropy source); 16 bits per access. The NDRNG output seeds the FIPS Approved DRBG.

Table 4 – Non-Approved But Allowed 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 3.

CSP	Description / Usage
Active Encryption Key (AEK)	256-bit AES key. Encrypts local objects
Active Signing Key (ASK)	HMAC-256 key. Signs local objects
Authority Passwords	Minimum 4-byte value. Each authority has its own password
Media Encryption Key (MEK[a])	256-bit AES key. Each LBA range has its own media encryption key
ANSI x9.31 Seed and Seed Key	Values used to generate random numbers

Table 5 – Critical Security Parameters

2.2 Public Keys

Key	Description / Usage
SD_FW_PKey	2048-bit RSA key. WD manufacturer Public key. Signs MFG Commands, keys, and secure FW images
OEM_CSP_PKey	2048-bit RSA key. Signs WD MFG CSP objects
OEM_FW_DL_PKey	2048-bit RSA key. Signs storage device FW download objects

Table 6 – Public Keys

3. Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles: Admin (CO) and User The cryptographic module enforces the separation of roles using session separation. Authentication is session-based, and the module tracks each individual session.

Table 7 lists all operator roles supported by the Module. The Module does not support a maintenance role or bypass capability. The Module supports concurrent operators. The module clears all previous authenticated states upon power cycle. Only a hash of the Admin and User authentication data is stored on the module, protecting it from unauthorized disclosure, modification, and substitution.

Role ID	Role Description	Authentication Type	Authentication Data
Admin (CO)	**SID:** This authority: 1) enables/disables access (single or multiple MFG access modes). 2) enables Firmware Download. **EraseMaster:** This authority: 1) returns LBA ranges to Original Factory State including Bandmaster credentials.	Role-based	Password
User	**Bandmasters[0:15]**: This authority type 1) configures an LBA ranges. 2) manages the locking state of each LBA range. There are a total of 16 Bandmasters.	Role-based	Password

Table 7 – Roles Description

3.2 Authentication Method

Authentication Method	Probability	Justification
Password	4-byte minimum to 32-byte maximum . Standard ASCII characters.	See Section 8.1 Security Installation for credential recommendations. **Password protection:** • When the password is set, it is hashed and stored to persistent media. Subsequent authentication events compare the hashed User/CO authentication password to the persistently stored hash. •

Authentication Method	Probability	Justification
		Verdi Strength: • Enforces a minimum C_PIN minimum length of 4 bytes. • Enforces a maximum number of C_PIN authentication based upon User configuration (TRY_LIMIT). When authentication limit is reached, no more authentications are allowed for that authority. • From the factory, the authentication limit is 1024. The C_PINs are set to a default value of 20 bytes. • A single authentication event takes ~30-50millisec. Verdi Protection: • Probability of a random guess of a 4 byte C_PIN is 1 in 2^{32} bits (over 1 in 4.2 billion). • Max authentication per minute are limited to: ◦ 1024 attempts based upon TRY_LIMIT ◦ OR ~1,980 attempts based on time per authentication per minute
		Initial Conditions & Personalization: All CO & User passwords are delivered from WD with a default password (MSID). To personalize the password, the authority must open a TCG session, authenticate with default password, and then modify (TCG Set) the new password.

Authentication Method	Probability	Justification
RSA Public Key	2048 bit key	Protects all MFG loaded CSPs, Firmware Downloads, and MFG access. All RSA Keys are 2048 bit in length.

3.3 Services

All services implemented by the Module are listed in Table 8 and Table 9 below. Each service description also describes all usage of CSPs by the service.

Service	Description	CO	U	M
Each authority (CO, and Users) shall authenticate using their unique credentials. They shall only be able to modify their own credentials.	• Original Factory State: Admin and User PINs are MSID. • ADMIN, and USERs authenticate with MSID credentials (TCG AUTHENTICATE method) • Algos: HMAC, SHA-256	x	x	x
Set CO (ERASEMASTER, SID) and USER C_PINs They shall only be able to modify their own credentials.	• After ADMIN or USERS are authenticated, the ADMIN or USER configures their new PIN value (TCG SET method) • Algos used: HMAC, SHA-256 •	x	x	
CO (SID) Enable/Disable MFG FW download	• SID enables/disables FW download capability	x		
CO (SID) SID Enable/Disable MFG diagnostic access	• SID enables/disables MFG diagnostic port access • Algos used: AES, HMAC, SHA-256 • CSPs: Active Encryption Key, Active Signing Key, stored	x		
USERS (BANDMASTER[0:15])Configure LBA Ranges	Bandmaster configures LBA range size, and Locks/Unlocks LBA Range. • Algos used: AES, HMAC, SHA-256 • CSPs: Active Encryption Key, Active Signing Key, stored		x	

Service	Description	CO	U	M
ERASEMASTER cryptographically erases an LBA Range media encryption key	• ERASEMASTER eradicates MEK (via TCG ERASE method) and returns selected LBA range to OFS and generates a new MEK • Algos used: AES, HMAC, SHA-256, RNG • CSPs: Active Encryption Keys, Active Signing Keys, stored,	x		
Encrypt LBA Ranges	• When LBA range is unlocked and Host requests an unlocked data transfer (direction dependent), the Media Encryption engine decrypts or encrypts UserData as it is read or written from persistent media.		x	
Power Down Event	• A power down event o erases all transient CSPs and Firmware stored in any SRAM, DRAMs			
Power Up Event	• On a power up event, the HDD performs a self test of all Crypto algorithm accelerators, RNG (w/entropy source), and initializes crypto subsystem SRAM • Crypto Algos: AES, HMAC, RSA, RNG			
Download FW	• Verifies Download Firmware and Download objects signatures • Algos uses: PKCS1.5 (SHA-1, RSA2048 • CSPs: OEM_FW_DL_PKey	x		
Zeroize Storage Device CSPs	• MFG can zeroize all local (internal) protection keys. OTP bits are zeroized (programmed to all 1s). Results: cryptosubsystem is permanently disabled. CSPs: Encrypted and Signed objects protected with Active Encryption Key & Active Signing Key			x

Table 8 – Authenticated Services

Authentication is performed via two (2)protocol levels. The first protocol level is defined in the Trusted Computing Group Storage Work Group Core Specification and TCG Enterprise SSC. This protocol is

session based. Session Based means a connection/session is established between the Host system and the SED HDD. Within the session, Authorities authenticate themselves and perform selected TCG functions (called Methods). The SED HDD authenticates the authorities, and checks authority functional requests against the TCG Enterprise SSC defined roles.

Service	Description
Module Reset (Self-test)	Reset the Module by Power On Reset.
NoAuth FunctionA	TCG Specifications include an ability to read some TCG objects without authentication (no TCG Authenticate Method required for ANYBODY authority objects). The specific objects are defined in the TCG protocol specifications.
Show Status	The SED HDD returns: - Native SAS protocol status associated with SED serial number, FW revision - TCG Level 0 discovery that defines basic SED TCG configuration options - HDD logs associated with the HDD operational history

Table 9 – Unauthenticated Services

The SED HDD provides some information without authentication. This type of information is used for:

- Auditing
  - the current SED HDD state
  - FW version
  - Basic TCG protocol support
- Verify:
  - Cryptographic functionality before usage (e.g., Power up self test)

Table 10 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

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

Service	CSPs							
	Active Encrpytion Key	Active Signing Key	PIN	MFG PKye	OEM_FW_DL_PKey	OEM_CSP_Pkey	MEK[x]	TCG Table Object
Authenticates Admin, and User	R,E	R,E	R,E					R,E
Set ADMIN and USER PINs	R,E	R,E	R,E,W					R,E
SID Enable/Disable MFG FW download	R,E	R,E			R,E	R,E		R,E
SID Enable/Disable MFG diagnostic access	R,E	R,E						R,E,W
USERS Configure LBA Ranges	R,E	R,E						R,E,W
Erasemaster cryptographically Erases an LBA Range	R,E	R,E	R,E,W				W	R,E, W,G
Encrypt LBA Ranges							R,E	R,E
Power Down Event								
Power Up Event								
Download FW				R,E	R,E			
Zeroize Storage Device CSPs				R,E				

Table 10 – CSP Access Rights within Services

4. Self-test

4.1 Power Up Self-tests

Each time the Module is powered up, it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self-tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 11 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module:

- enters the error state, and
- returns the following SAS error status, “HARDWARE ERROR/VENDOR SPECIFIC”, for any subsequent SAS command.

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code in EEPROM.
MAES assist HW	AES KATS: Encryption & Decryption Mode: ECB mode, Key Size: 128 bit key
AES(BCM) HW	KATs: Encryption & Decryption Mode: XTS Key sizes: 128 bits
Hashing (SHA-1 & HMAC)	KATs: Generation Mode: SHA-1 (HW), HMAC SHA-256 (SW) Mode SHA sizes: SHA-1, SHA-256 in HMAC mode
RNG HW	KATs: ANSI X9.31 **16-bits per access to the hardware RNG**: the entropy is harvested in 16-bit pieces, concatenated into 32-bits per call by a routine, which gathers the entropy. An outer routine ("get_entropy()), which is a Layer-1service and is available to EROMs, aggregates the 32-bit clusters into any amount requested, modulo-128,up to a maximum of 512 bits.
RSA (ZMOD) HW	KATs: Signature Verification ZMOD using a modular multiply, with 1024-bit operands. Key sizes: 1024 bits

Table 11 – Power Up Self-tests

4.2 Conditional Self-tests

Test Target	Description
NDRNG	NDRNG Continuous Test is performed when a random value is requested from the NDRNG at each TCG ERASE Method invocation.

Test Target	Description
RNG	RNG Continuous Test is performed when a random value is requested from the RNG at each TCG ERASE Method invocation.
BCM Firmware Load	RSA 2048 signature verification is performed when BCM firmware is loaded.

Table 12 – Conditional Self-tests

5. Physical Security Policy

5.1 Tamper Evidence Mechanisms

The cryptographic module (CM) is compliant with FIPS 140-2 Level 2 physical security mechanisms. The module utilizes tamper-evident labels. These labels break away when physical access is attempted or attained or show signs of tamper. These labels are designed to prevent reapplication without showing signs of tampering.

The following physical security items have been designed for this product:

- High quality tamper evident labels made of robust, production-grade materials
- One single label that covers all test points and components on the PCBA, not included on the exclusion list, and folded over the connector edge of the CM
- Three smaller top-cover labels, two of which overlap the edge of the CM, and one that is completely contained on the top surface and partially covers a single screw access concavity
- All labels are applied by Western Digital during manufacturing and is inspected to ensure proper application before shipment
- The CM exterior and tamper evidence labels are opaque and no components are visible
- The tamper evidence labels cannot be penetrated, removed, or reapplied without tamper evidence
- The tamper evidence labels are custom ordered and designed for the CM and are not easily accessible or duplicable given a short attack time
- All labels will be applied in the same positions and configuration as shown in the images that follow

Figure 3: Verdi Module Showing PCBA & Connector Edge Tamper Evidence Label on Underside

Figure 4: Verdi Module Showing Three (3) Top-Cover Tamper Evidence Labels (See Arrows)

Figure 5: Verdi Module Showing No Tamper Label on Right Side

Figure 6: Verdi Module Showing No Tamper Label on Left Side

Figure 7: Verdi Module Showing One Overlapping Tamper Label on Connector Side

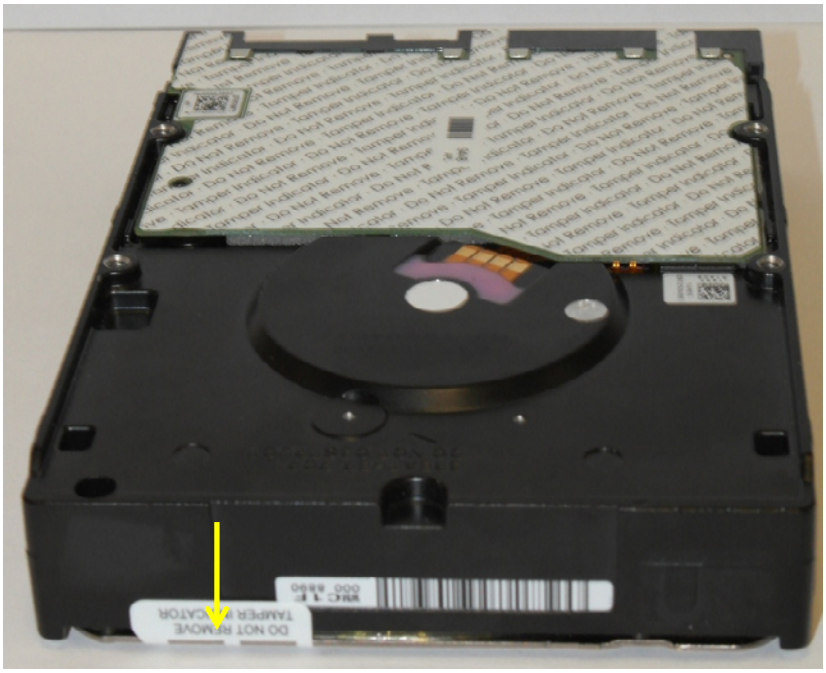

Figure 8: Verdi Module Showing Portion of Small Tamper Label Wrapped onto Back Side (See Arrow)

5.2 Operator Requirements

To ensure the CM has not been tampered with, the operator is required to inspect the CM periodically for any tamper evidence. This should be done in accordance with the end user needs/requirements, but no less than every 12 months(See Table 13). A few examples are shown in images below.

If the CM shows signs of tampering through the tamper evidence labels or other visible signs of damage, the module is to be removed from service immediately.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Description
PCBA & connect label	12 months	Covers PCBA & connector edge
3 Top cover labels	12 months	Covers 2 edges & 1 screw concavity

Table 13 - List of Physical Security Mechanisms and Description

In addition to Figures 9 through 12, the following are a few examples of tamper evidence:

- Label is broken, torn, or deformed in any way, shape, or form
- A checkered pattern is left on any of the surfaces in place of the label
- A tampered label that is reapplied appears with a checkerboard pattern.
- Punctures where screws are located
- Text does not match original: “DO NOT REMOVE” & “TAMPER INDICATOR”
- Any indication that the labels do not match/align with the images provided

Figure 9: A Top Cover Label Showing Signs of Tamper (Pealing and Cutting)

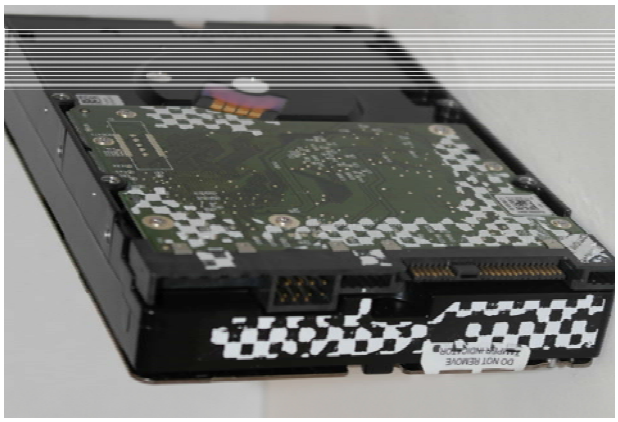

Figure 10: PCBA & Connector Label Showing Signs of Tamper (Peeled Off Left Over Checkboard Pattern)

Figure 11: PCBA & Connector Label Showing Signs of Tamper (Reapplied Label)

Figure 12: Label (Punctured and Distorted Text)

6. Operational Environment

The Module operates in a limited operational environment when active. All Firmware Download are secure and signed.

7. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks outside the scope of FIPS 140-2.

8. Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

8.1 Security Installation

1. Installation
    a. CO: examine the shipped products for any tampering evidence.
    b. CO and Users: set their respective credentials (passwords). Credentials (passwords) are recommended to be the full credential size (32 bytes).
2. CO and User Module Periodic Examination
    a. CO and Users: periodically examine Module for tamper evidence.
    b. CO and Users: periodically examine Module state: (still supporting TCG Functionality: Level 0 discovery and any TCG Table access.
3. The Module:
    a. Performs Self-Test operation at every power up event only.
    b. Clears previous authentication states, transient cleartext CSPs, and Firmware on power cycles.
    c. Prevents the operator from having access to any cryptographic services until the Module has been placed in a valid (or authenticated) role
4. Power Up Self-Test:
    a. The operator is capable of commanding the module to perform the power up self-tests by cycling power only.
    b. Power up self-test execution does not require any operator action.
    c. Data output is inhibited during key generation, self-tests, zeroization, and error states.
        1. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
        2. Installation

8.2 General Operational Mode

The Module:

a. supports two distinct operator roles:
    i. User(s): Bandmasters[0:15]
    ii. Cryptographic Officer(s) : Admin[1], EraseMaster
b. provides role-based authentication.
c. clears previous authentication states, transient cleartext CSPs, and Firmware on power cycles.
d. requires the operator to be authenticated before having access to any cryptographic services.
e. supports multiple roles and enforces the separation of roles & responsibilities via the TCG Tables when a TCG session has only one authenticated authority per session.
f. supports concurrent operators (multiple authentications) per TCG session rules. It is recommended that only one authority be authenticated per TCG session to maximize the protection that the storage device enforces.
g. does not support a maintenance interface or role.
h. does not support manual key entry.
i. does not have any external input/output devices used for entry/output of data.
j. does not enter or output plaintext CSPs.
k. does not output intermediate key values.
l. does not support an update to the logical serial number.
m. does not provide access to any plaintext CSPs.

9. References

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011

Table 14 - References

10.Acronyms and Definitions

Acronym	Definition
PCBA	Printed Circuit Board Assembly
TCG	Trusted Computing Group. An industry standards body that defines a Storage Device security protocol
TCG Session	A security protocol message protocol connection between a storage device and a host manager
TCG ERASE	A TCG method (command) for invoking media encryption key erasure
SAS	Serial Attached SCSI is a storage transport and command protocol. Within this protocol, TCG session and associated commands are transferred
SoC	System on a Chip
BCM	Base Crypto Module
SID	Security Identifier

Table 155 – Acronyms and Definitions