Hitachi Flash Module Drive HDE

FIPS 140-2
Non-Proprietary Cryptographic Module Security Policy

Version: 24

Date: November 26, 2018

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Hitachi Flash Module Drive HDE, hereafter denoted the module. The module is 2-port 12 Gb/s SAS storage device with encryption. The module provides high speed data at rest encryption for the internal storage media. In other words, the module encrypts data onto the internal NAND flash memory and decrypts data read from the internal NAND flash memory using XTS-AES. The module meets FIPS 140-2 overall Level 2 requirements.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version
1	Hitachi Flash Module Drive HDE	HW P/N: 3286810-A 3286811-A *1 Version: A	J0J0 J110 K060 K110

*1: The difference between 3286810-A and 3286811-A is capacity. 3286810-A is 7TB model. 3286811-A is 14TB model. There is no difference in cryptographic functions.

The module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated SAS storage device used for Hitachi storage system with data at rest encryption feature. The module is a hardware cryptographic module with multi-chip embedded embodiment.

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

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

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the module is depicted in Figure 1. Bold line shows the cryptographic boundary. Major components of the module are module board, several microprocessors (the flash controller, the SAS controller and the compression/encryption LSI), non-volatile memories and interfaces. The module is typically connected with RAID controller in Hitachi VSP storage as data storage media.

A set of firmware running on microprocessors is responsible for processing SAS IO commands as well as encrypting/decrypting data where applicable. XTS-AES, KeyWrap/Unwrap, SHA, HMAC and PBKDF2 hardware accelerators are integrated in the LSI.

Firmware images running on the flash controller and the SAS controller are stored in the NOR flash connected with the flash controller. Firmware image running on the LSI is stored in the NOR flash connected with the LSI. When the Module powers up, they are loaded into the flash controller, the SAS controller and the LSI, respectively.

An EDLC supplies power to the module internally in a short time after disaster power down to evacuate to the flash those cached data which must not be lost in the module.

All functions and system initialization performed in the module are initiated by the flash controller. CSPs and PSPs are stored in the NOR flash connected with the flash controller. Integrity test of the firmware images is performed on the DDR memory connected with the flash controller by transmitting them from each NOR flash to the DDR.

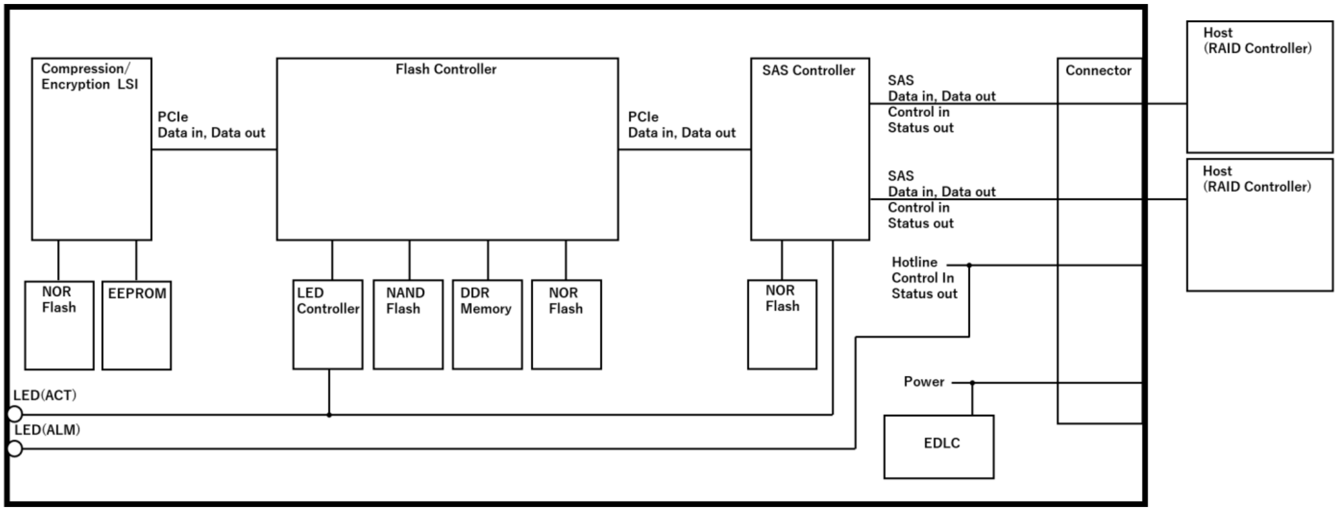


Figure 1 – Module Block Diagram

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
SAS	plaintext data input/output, module control input, module status output, firmware input	- Control in / Status out - Data in / Data out
Hotline	thermal alert output, connection status output, LED(ALM) control input	- Control in / Status out

Port	Description	Logical Interface Type
Power	power input	- Power
LED(ACT)	active status indicator	- Status out
LED(ALM)	alarm status indicator	- Status out

1.2 Mode of Operation

The module only supports FIPS-approved mode of operation, and therefore, only supports FIPS-approved and allowed security functions. No other modes of operation and no other security functions are implemented.

A FIPS-approved mode indicator is available by INQUIRY (12H) command and TEST UNIT READY (00H) command.

The Level 0 Discovery response includes a state of the module personalization step (see 8.1). When the state value indicates that the personalization has completed (i.e. all the PINs are updated from the default value and Global Range is both ReadLockEnabled and WriteLockEnabled), the module is in FIPS-approved mode of operation.

The TEST UNIT READY (00H) command's GOOD response indicates that the module has completed power up initialization and is ready to operate the security functions in FIPS-approved mode of operation. On the other hand, Its CHECK_CONDITION response with Sense Key=NOT_READY (02H) indicates that the module hasn't yet completed power up initialization, which means that the module is not yet ready to operate the security functions in FIPS-approved mode of operation.

2 Cryptographic Functionality

The module implements the FIPS Approved cryptographic functions listed in the tables below. The approved DRBG is used for the generation of cryptographic keys used by an Approved security function: XTS-AES.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197] Functions: Encryption, Decryption Mode: ECB Key size: 256 bits	5460
CKG	[NIST SP 800-133] The unmodified output of the DRBG is used for generating symmetric keys.	Vendor Affirmed
XTS-AES	[NIST SP 800-38E] Functions: Encryption, Decryption Key size: 256 bits	5460
Key Wrap/Unwrap	[NIST SP 800-38F] Functions: Key wrapping/unwrapping Base algorithm: AES Key size: 256 bits	5460
SHS	[FIPS 180-4] Functions: Calculation of HMAC, Hash_DRBG and RSASSA-PSS Algorithm: SHA-256	4382
HMAC	[FIPS 198-1] Functions: Calculation of PBKDF2 Hash algorithm: SHA-256	3618
PBKDF2	[NIST SP 800-132] Functions: PIN digesting, Key derivation *1 PRF: HMAC-SHA-256 Digest size of the hash function: 256 bits	Vendor Affirmed
Hash_DRBG	[NIST SP 800-90A] Functions: Key generation, Salt generation Hash algorithm: SHA-256	2143

Algorithm	Description	Cert #
RSASSA-PSS Verification	[FIPS 186-4] Functions: Loaded firmware verification Key size: 2048 bits Hash algorithm: SHA-256 Mask generation function: SHA-256 Salt length: 32 bytes	2932

*1: The keys derived by PBKDF2 are used for storage applications only.

The module implements the Allowed Random Number Generator listed in the tables below.

Table 5 – Allowed Random Number Generator

RNG	Description
NDRNG	NDRNG generates entropy and nonce used by Hash_DRBG. The estimated min-entropy rate is 7.99 bits per 8-bit sample from the NDRNG.

2.1 Critical Security Parameters

All CSPs used by the module are described in this section. Usage of these CSPs in the module services is described in Section 3.3 (Services).

Table 6 – Critical Security Parameters (CSPs)

CSP	Description / Usage
SID PIN	● 256-bit credential used to authenticate SID (CO) authority. SID PIN is digested by PBKDF2 and compared with the expected digest stored in NOR flash in the module. ● In the manufactured state, SID PIN value is the default PIN (MSID). Since MSID needs not to be protected, first authentication is performed by simple comparison with MSID stored in the module. ● Set PIN service by SID updates SID PIN digest stored in NOR flash with the digest of the new SID PIN. A 256-bit Salt used for PBKDF2 is also updated with random value using DRBG. ● Revert service by SID or Force Revert service using Revert Code zeroizes SID PIN digest and the Salt stored in NOR flash by overwriting with 0x00.
EraseMaster PIN	● 256-bit credential used to authenticate EraseMaster (User) authority. EraseMaster PIN is digested by PBKDF2 and compared with the expected digest stored in NOR flash in the module. ● In the manufactured state, EraseMaster PIN value is the default PIN (MSID). Since MSID needs not to be protected, first authentication is performed by simple comparison with MSID stored in the module. ● Set PIN service by EraseMaster updates EraseMaster PIN digest stored in NOR flash with the digest of the new EraseMaster PIN. A 256-bit Salt used for PBKDF2 is also updated with random value generated by DRBG. ● Revert service by SID or Force Revert service using Revert Code zeroizes EraseMaster PIN digest and the Salt stored in NOR flash by overwriting with 0x00.
BandMaster0 PIN	● 256-bit credential used to authenticate BandMaster0 (User) authority. BandMaster0 PIN is digested by PBKDF2 and compared with the expected digest stored in NOR flash in the module. It is also used to generate KEK by PBKDF2 using the other 256-bit Salt than that used to digest it. ● In the manufactured state, BandMaster0 PIN value is the default PIN (MSID). Since MSID needs not to be protected, first authentication is performed by simple comparison with MSID stored in the module. ● Set PIN service by BandMaster0 updates BandMaster0 PIN digest stored in NOR flash with the digest of the new BandMaster0 PIN. A 256-bit Salt used for PBKDF2 is also updated with random value generated by DRBG. ● Revert service by SID or Force Revert service using Revert Code zeroizes BandMaster0 PIN digest and the Salt stored in NOR flash by overwriting with 0x00.
KEK	● 256-bit AES key used to wrap/unwrap MEK. KEK is not used for any other purpose. KEK is generated (derived) from BandMaster0 PIN by PBKDF2. A 256-bit Salt value used for KEK generation is a random value generated by DRBG and is different from that for BandMaster0 PIN digest. KEK is not stored in any non-volatile memory in the module. KEK is cleared by module power down and EDLC full discharge thereafter.

CSP	Description / Usage
	● Set PIN service by BandMaster0 updates KEK with the derived value from the new BandMaster0 PIN. MEK is unwrapped with the old KEK and wrapped with the new KEK and stored in NOR flash. ● Revert by SID service or Force Revert service using Revert Code zeroizes KEK cached in volatile memory and the Salt stored in NOR flash by overwriting with 0x00.
MEK	● Two 256-bit keys used for XTS-AES encryption/decryption of GlobalRange data. MEK is wrapped with KEK and stored in NOR flash in the module. This MEK protection scheme with KEK is based on PBKDF2 Option 2a. ● In the manufactured state, MEK is all-zero which means invalid (unusable). ● When MEK is invalid, Set PIN service to change the default PIN (MSID) by BandMaster0 generates new MEK by DRBG. Since all-zero MEK is invalid (reserved for zeroization), MEK is re-generated as long as generated MEK is all-zero. Since XTS mode under the condition of Key1=Key2 is weak, MEK is re-generated as long as Key1=Key2. ● Revert service by SID or Force Revert service using Revert Code zeroizes the wrapped MEK stored in NOR flash by overwriting with 0x00.
DRBG entropy input	● 2048 bits of input for SHA-256 based Hash_DRBG's Instantiate functions. The entropy input is collected from flash controller's embedded random number generator based on sampling of free running oscillators. All-zero entropy is reserved for zeroization. It is not inputted to DRBG as long as it is all-zero. ● The entropy input is cleared by module power down and EDLC full discharge thereafter. ● Revert service by SID or Force Revert service using Revert Code zeroizes the cached entropy input by overwriting with 0x00
DRBG nonce	● 1024-bit input used for SHA-256 based Hash_DRBG's Instantiate function. The nonce is also collected from the above random number generator. All-zero nonce is reserved for zeroization. It is not inputted to DRBG as long as it is all-zero. ● The nonce is cleared by module power down and EDLC full discharge thereafter. ● Revert service by SID or Force Revert service using Revert Code zeroizes the nonce cached in volatile memory by overwriting with 0x00.
DRBG internal state	● Internal working_state of SHA-256 based Hash_DRBG: V (440 bits), C(440 bits) and reseed_counter (48 bits), which are initialized at module Power-on reset and stored in volatile memory in the module. ● The working_state is cleared by module power down and EDLC full discharge thereafter. ● Revert service by SID or Force Revert service using Revert Code zeroizes the working_state cached in volatile memory by overwriting with 0x00 (Uninstantiate).

2.2 Public Security Parameters

PSPs used by the module are described in this section. Usage of the PSPs in the module services is described in Section 3.3 (Services).

Table 7 – Public Security Parameters (PSPs)

PSP	Description / Usage
FW PuK	● 2048-bit RSA public key. ● FW PuK is written on manufacturing and stored in NOR flash. ● Firmware Download service uses FW PuK to verify an RSASSA-PSS signature attached with the new firmware image. ● FW PuK is protected from modification, disclosing or substitution. ● Neither Revert service by SID or Force Revert service using Revert Code zeroizes FW PuK.

3 Roles, Authentication and Services

3.1 Assumption of Roles

Table 8 lists all operator roles supported by the module. The module supports three distinct operator roles: SID (CO), EraseMaster (User) and BandMaster0 (User). The module does not support concurrent operators. The module does not support a maintenance role and bypass capability.

After the module power down and the EDLC full discharge thereafter, all the data stored in volatile memory (RAM), including previously authenticated operator, are cleared.

Table 8 – Roles Description

Role	Role Description	Authentication Type	Authentication Data
SID (CO)	The CO role assumed to perform Revert and Firmware Download Control services	Role-based	SID PIN
EraseMaster (User)	The User role assumed to enable/disable BandMasters *1	Role-based	EraseMaster PIN
BandMaster0 (User)	The User role assumed to perform Read/Write access control	Role-based	BandMaster0 PIN
Anybody	The role assumed not to require authentication to perform other services	Unauthenticated	N/A

*1: EraseMaster corresponds to same named role as defined in TCG Enterprise. The module does not support services to enable/disable BandMasters. This role exists for future enhancements.

3.2 Authentication Mechanism

The module enforces role separation by requiring 256-bit authentication credential (PIN) for the three roles: SID, EraseMaster and BandMaster0. The PIN for each role is inputted in plaintext to authenticate the operator when it logs in as the role.

The module holds the PIN digest to verify whether a digest of inputted PIN matches with it or not.

For each PIN, the number of PIN verification attempts allowed is unlimited.

Authentication process requires more than 300ms (actual measured value).

Table 9 – Authentication Mechanism Strengths

Authentication Mechanism	Probability of a Single Successful Random Attempt	Probability of a Successful Attempt within a Minute
Credential (PIN)	1/2^256 The probability that a random attempt will succeed or a false acceptance will occur depends on 256-bit PIN. Therefore, the probability is 1/2^256, which is less than 1/1,000,000.	200/2^256 Since authentication requires more than 300ms in a worst case scenario, the module can perform at most 200 times PIN verification per minute. Therefore, the probability that multiple attacks within a given minute will be successful is 200/2^256, which is less than 1/100,000.

3.3 Services

All services implemented by the module are listed in the tables below. The services permitted for the Anybody role (Table 11) don't modify, disclose or substitute CSPs.

Table 10 – Authenticated Services of CO and User

Service	Description	SID	Erase Master	Band Master0
Set Locking Table	Sets True/False to the Locking Table parameters for Global Range: - ReadLockEnabled: True = follows ReadLocked, False = Read is allowed - WriteLockEnabled: True = follows WriteLocked, False = Write is allowed - ReadLocked: True=Read is prohibited, False=allowed - WriteLocked: True=Write is prohibited, False=allowed This is applicable in LockingSP session. TCG Set Method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used.			X

Service	Description	SID	Erase Master	Band Master0
Firmware Download Control	Locks or Unlocks Firmware Download service. This is applicable in AdminSP session. - Firmware Download Enabled: True=Unlocked (firmware is downloadable), False=Locked (firmware is not downloadable) TCG Set method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used.	X		

Service	Description	SID	Erase Master	Band Master0
Revert	Revert service of this module includes Zeroise service. This is applicable in AdminSP session. Returns the module to its original manufactured state as follows: - SID PIN = EraseMaster PIN = BandMaster0 PIN = MSID (their digests and salts = zeroized) - Firmware Download Enabled = False (Locked) - KEK = zeroized - MEK = zeroized (write zero to wrapped MEK storage) - WriteLockEnabled = ReadLockEnabled = False - WriteLocked = ReadLocked = False - DRBG entropy input = zeroized - DRBG nonce = zeroized - DRBG internal state = zeroized. If succeeded, current session is automatically closed. TCG Revert Method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used.	X		
Set PIN	Inputs new authentication credential (PIN) for the current role itself and replaces the PIN digest stored in the module. Set PIN(SID) is applicable in AdminSP session. Set PIN(EM, BM0) is applicable in LockingSP session. TCG Set Method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used for the other roles.	X	X	X

Table 11 – Unauthenticated Services of Anybody

Service	Description
Power-on Reset	Power-on Resets the module and performs power up self-tests. It is also used to initiate on-demand self-tests
LU Reset	SCSI defined LU Reset clears TCG protocol state into Awaiting IF-SEND (SECURITY PROTOCOL OUT command), closes current session and makes the operator unauthenticated.
Get TCG features	Gets TCG features supported by the module. TCG Level 0 Discovery with SECURITY PROTOCOL IN (A2H) command is used
Get Properties	Gets TCG communication properties supported by the module. TCG Properties Method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used
Get MSID	Gets default PIN (MSID) for SID, EraseMaster and BandMaster0. This is applicable in AdminSP session. MSID is common for these 3 roles but unique for each module. TCG Get Method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used
Get Revert Code	Gets Revert Code used for Force Revert. This is applicable in AdminSP session. Revert Code is unique for each module. TCG Get Method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used
Start Session	Starts TCG session. There are two session environments: AdminSP and LockingSP. SID services are available when SID is authenticated in AdminSP session. EraseMaster/BandMaster0 services are available when EraseMaster /BandMaster0 is authenticated in LockingSP session. TCG StartSession/SyncSession Methods with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands are used
Authenticate	Authenticates an operator for SID, EraseMaster or BandMaster0 role. If authentication has already passed in a session, the session doesn’t accept further authentication until the session is closed. Authenticate(SID) is applicable in AdminSP session. Authenticate(EM, BM0) is applicable in LockingSP session. TCG Authenticate Method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used.

Service	Description
End of Session	Closes TCG session. It also makes the operator unauthenticated (i.e. logout). TCG End of Session with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used
Output Status	Output module status with LED (ACT) as follows: - Off: I/O disabled - On: I/O enabled - Blink (high speed): formatting or evacuating - Blink (low speed): charging EDLC
Read Data	Reads ciphertext user data from Global Range, decrypts it with MEK into plaintext user data using XTS-AES and outputs it. READ command is used
Write Data	Inputs plaintext user data, encrypts it with MEK into ciphertext user data using XTS-AES and writes it to Global Range. WRITE command is used
SCSI	Executes other SCSI command operations as shown in Table 16
Firmware Download	Loads a new set of Firmware images by WRITE BUFFER command (3BH) with ID=05H and verifies it using FW PuK with RSASSA-PSS by SEND DIAGNOSTIC command (1DH) with ID=23H. If successfully verified, the module executes the new code after automatic warm reboot. Firmware Download Control shall be unlocked by SID before Firmware can be downloaded

Table 12 – Unauthenticated Services for zeroization

Service	Description
Force Revert	Force Revert service of this module includes Zeroise service. This is applicable in AdminSP session. If SID PIN is lost and the module cannot be recovered, this service returns the module to its original manufactured state using Revert Code as follows: - SID PIN = EraseMaster PIN = BandMaster0 PIN = MSID (their digests and salts = zeroized) - Firmware Download Enabled = False (Locked) - KEK = zeroized - MEK = zeroized (write zero to wrapped MEK storage) - WriteLockEnabled = ReadLockEnabled = False - WriteLocked = ReadLocked = False - DRBG entropy input = zeroized - DRBG nonce = zeroized - DRBG internal state = zeroized. If succeeded, current session is automatically closed. Vendor-specific Method with SECURITY PROTOCOL OUT (B5H) and SECURITY PROTOCOL IN (A2H) commands is used

Table 13 defines the relationship between access to CSPs/PSPs and the module services. Those services which are not related to CSPs/PSPs are omitted. Access types used in the table are defined as :

- G = Generate: The module generates the CSP/PSP.
- E = Execute: The module executes using the CSP/PSP.
- W = Write: The module writes the CSP/PSP in non-volatile memory. The write access is typically performed after a CSP/PSP is imported into the module, when the module generates a CSP/PSP, or when the module overwrites an existing CSP/PSP.
- Z = Zeroize: The module zeroizes the CSP/PSP.

Table 13 – Access to CSPs/PSPs within Services

Service	CSPs/PSPs							
	SID PIN	Erase Master PIN	Band Master 0 PIN	KEK	MEK	DRBG entropy input/ nonce	DRBG internal state	FW PuK
Authenticate (SID)	(E *8)							
Authenticate (EraseMaster)		(E *8)						
Authenticate (BandMaster0)			(E *8)	(E*9/ G *7)	(E *9)			
Set PIN (SID)	W *1					(G *4 *6)	E(/G *4*6)	
Set PIN (EraseMaster)		W *1				(G *6)	E(/G*6)	
Set PIN (BandMaster0)			W *1	E/G	E/W (/G *2)	(G *6)	E(/G*6)	
Firmware Download						G *5	G *5	E
Revert / Force Revert	Z	Z	Z	Z	Z *3	Z	Z	
Read Data					E			
Write Data					E			
Power-on Reset				Z		G	G	

*1: PIN digest is written
*2: G is applicable only if MEK is all-zero (Erased) or does not exist (Reverted)
*3: Wrapped MEK storage is overwritten with zero

*4: If the module is in reverted (zeroized) state, G is applicable
*5: DRBG is re-instantiated on reset when the module activates new firmware
*6: If ReseedCounter exceeded the threshold, G is applicable
*7: G is applicable only if BM0 Pin has been already set and first authentication after Power-on Reset
*8: E is applicatble only if PIN is being changed from MSID
*9: E is applicable only if BM0 Pin has been already set and first authentication after Power-on Reset

4 Self-tests

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

On power up, the module performs self-tests described in Table 14 below. Firmware Integrity test and all Cryptographic Algorithm Known Answer tests (hereafter KATs) must be completed successfully prior to any other use of cryptography by the module. If Firmware Integrity test or one of the KATs fails, the module enters the fatal error state. Power up Self-tests do not require any intervention or input from the operator. They are automatically executed when the module is powered up.

The module shows the result of self-tests with TEST UNIT READY (00H) command. If self-tests successfully pass, it returns GOOD. Otherwise, it returns CHECK_CONDITION with Sense Key=04H and ASC/ASCQ=90XX and top of 2bytes of Additional Sense Byte=xxxxH which indicates self-tests failure or other initialization failures.

Table 14 – Power Up Self-tests

Test Target	Description
Firmware Integrity	16-bit CRC check of the firmware images
AES ECB	KAT: Encryption, Decryption Key size: 256 bits
XTS-AES	KAT: Encryption, Decryption Key sizes: 256 bits x 2 keys
SHA	KAT: Calculation Algorithm: SHA-256
HMAC	KAT: Calculation Hash algorithm: SHA-256
PBKDF2	KAT: Calculation PRF algorithm: HMAC-SHA-256
Key Wrap	KAT: Wrap, Unwrap Base Algorithm: AES Key size: 256 bits
Hash_DRBG	KAT: Instantiate, Generate and Uninstantiate Hash algorithm: SHA-256
RSASSA-PSS	KAT: Verification Key size: 2048 bits Hash algorithm and Mask generation function: SHA-256 Salt length: 32 bytes

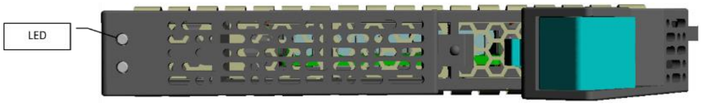
Conditional self-tests are automatically performed when an applicable security function or operation is invoked. As the firmware is being externally sent to the module, the firmware images are authenticated using the RSASSA-PSS verification technique.

Table 15 – Conditional Self-tests

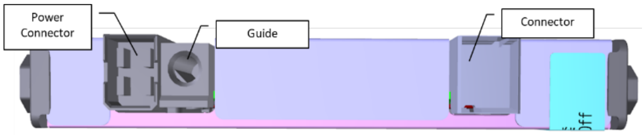
Test Target	Description
Firmware Load	SEND DIAGNOSTIC (1DH) command with ID=23H requests replacement of current firmware with new firmware downloaded by WRITE BUFFER (3BH) command with ID=05H. RSASSA-PSS verification for new firmware is automatically performed before replacement. If verification fails, the replacement is not executed and current firmware keeps working.
Repetition Count Test	This test is performed on the NDRNG output per IG 9.8. Each 8 bit of generated entropy is compared with previous 8 bit. If it was matched, count up repetition count. When repetition count is exceeded the threshold, Repetition count test fails.

5 Physical Security Policy

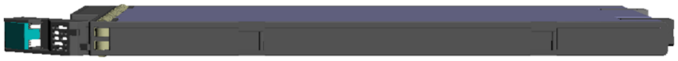
The module is a multi-chip embedded cryptographic module and conforms to Level 2 requirements for physical security. The cryptographic module consists of production-grade components. The cryptographic module provides evidence of tampering on the cover, enclosure and seal when physical access to the module is attempted. The enclosure is opaque. The tamper-evident seals are applied at the factory. The tamper-evident seals cannot be penetrated, removed and reapplied without evidence of tampering. The Crypto Officer and Users shall inspect the module enclosure for evidence of tampering periodically.



Front view

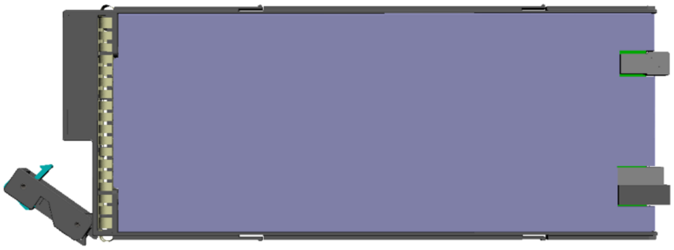


Rear view

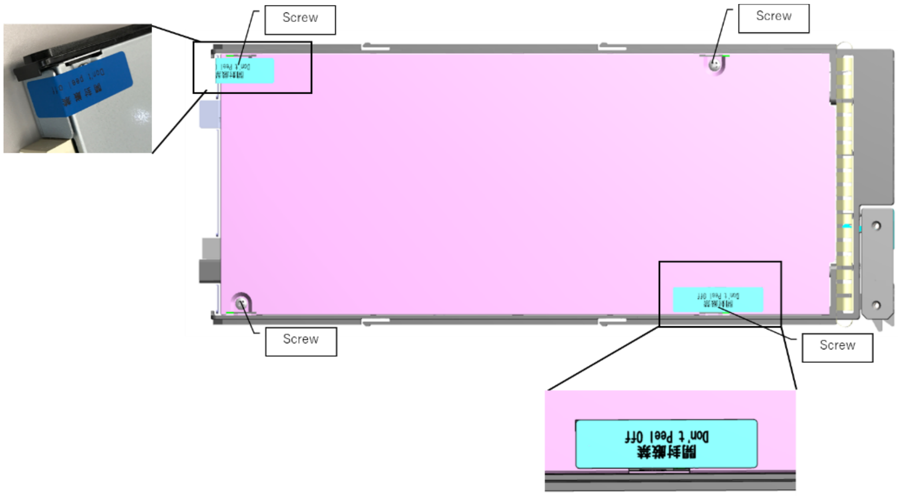


Right side view

Left side view



Top view



Bottom view and tamper-evident seal

6 Operational Environment

The module is designated as a limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The module does not mitigate other attacks.

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.

1. The module shall provide three distinct operator roles: SID, EraseMaster and BandMaster0, where BandMaster0 and EraseMaster are User roles and SID is a Crypto Officer role.
2. The module shall provide role-based authentication.
3. The module shall clear previous authentications on power cycle, LU Reset, reset for activating new firmware or warm reboot.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services shown in Table 10.
5. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power.
6. Power up self-tests do not require any operator action.
7. Data output shall be inhibited during self-tests and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. During module power up initialization, non-I/O SCSI commands among the SCSI service commands (Table 16) are available and some status information which does not include any CSPs or sensitive data can be outputted in response to the non-I/O SCSI commands.
10. There are no restrictions on which CSPs are zeroized by Revert or Force Revert service.
11. The module does not support 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 output plaintext CSPs.
16. The module does not support the update of the logical serial number or vendor ID.

8.1 Personalization Rules

The Crypto Officers and User must configure and enforce the following personalization procedures in order to enable user data encryption/decryption:

1. Get Firmware version by SCSI INQUIRY command and check the firmware version is equal or later of firmware version printed in Table 1. If not, update firmware with the procedure described in section 8.3.
2. StartSession in AdminSP.
3. Get MSID from the module.
4. Authenticate as SID with MSID.

5. Update SID PIN from the default value (MSID).
6. End of Session.
7. StartSession in LockingSP.
8. Authenticate as EraseMaster with MSID.
9. Update EraseMaster PIN from the default value (MSID).
10. End of Session.
11. StartSession in LockingSP.
12. Authenticate as BandMaster0 with MSID.
13. Update BandMaster0 PIN from the default value (MSID).
14. Set Global Range’s ReadLockEnabled and WriteLockEnabled to be True, respectively.
15. Set Global Range's ReadLocked and WriteLocked to be False, respectively.
16. End of Session.

8.2 Zeroization Rules

SID must enforce the following zeroization procedures:

1. StartSession in AdminSP.
2. Authenticate as SID.
3. Revert.

8.3 Firmware Download Rules

SID must enforce the following firmware download procedures:

1. StartSession in AdminSP.
2. Authenticate as SID.
3. Unlock Firmware Download Control.
4. End of Session.
5. Load firmware image by WRITE BUFFER command with ID=05H.
6. Verify firmware image by SEND DIAGNOSTIC command with ID=23H.
7. Reset the module to activate the new firmware (automatically).

8.4 Unauthenticated Zeroization Rules

If SID authentication data is lost and the module cannot be recovered, the unauthenticated operator (i.e. Anybody) must enforce the following procedures to revert the module:

1. StartSession in AdminSP.

2. Get Revert Code from the module.
3. Force Revert using Revert Code.

8.5 Physical Security Inspection

The Crypto Officer and Users shall inspect the module enclosure for evidence of tampering periodically.

9 Design Assurance Policy

9.1 Configuration Management Overview

Programs and documents are managed using proprietary web-based configuration management system (Electric Stock System). Documents for validation and hardware components are managed by revision management by proprietary ledger.

9.2 Installation, Initialization, and Start-up Overview

The procedure is described in section 8.1.

9.3 Secure Delivery and Operation Overview

The module shipped to customers from the factory or the distribution centers. The module is delivered by the contracted carrier and unpacked by the contacted service personnel on site, and its contents are confirmed by the personnel.

10 Supported SCSI commands

Table 16 shows those commands which are supported in the unauthenticated SCSI service in Section 3.3. Table 17 shows those commands which are used in the specific (named) services in Section 3.3. For detailed command operations, refer to [SCSI Core], [SCSI Block] and [SAS].

Table 16 – SCSI commands in the SCSI service

Code	Command Name	Code	Command Name
00 H	TEST UNIT READY	25 H	READ CAPACITY(10)
04 H	FORMAT UNIT	37 H	READ DEFECT DATA(10)
07 H	REASSIGN BLOCKS	3C H	READ BUFFER (*2)
12 H	INQUIRY	4D H	LOG SENSE
15 H	MODE SELECT(6)	55 H	MODE SELECT(10)
1A H	MODE SENSE(6)	5A H	MODE SENSE(10)
1B H	START STOP UNIT	9E/10 H	READ CAPACITY(16)
1C H	RECEIVE DIAGNOSTIC RESULTS	A0 H	REPORT LUNS
1D H	SEND DIAGNOSTIC (*1)	B7 H	READ DEFECT DATA(12)

*1: ID=00H(Supported page), 40H(Translate address) and A1H(Metadata Rebuild)
*2: Accessible to only the address ranges which are not related to cryptographic operations

Table 17 – SCSI commands in the named service

Code	Command Name	Service	Code	Command Name	Service
08H	READ (6)	Read Data	41 H	WRITE SAME(10)	Write Data
0AH	WRITE (6)	Write Data	88H	READ (16)	Read Data
1DH	SEND DIAGNOSTIC (ID=23H)	Firmware Download	8AH	WRITE (16)	Write Data
28H	READ (10)	Read Data	8E H	WRITE AND VERIFY(16)	Write Data
2AH	WRITE (10)	Write Data	8F H	VERIFY(16)	Read Data
2E H	WRITE AND VERIFY(10)	Write Data	93 H	WRITE SAME(16)	Write Data
2F H	VERIFY(10)	Read Data	A2H	SECURITY PROTOCOL IN	See 3.3
3BH	WRITE BUFFER (ID=05H)	Firmware Download	B5H	SECURITY PROTOCOL OUT	See 3.3

11 References and Definitions

The following standards are referred to in this Security Policy.

Table 18 – References

Abbreviation	Full Specification Name
[TCG Core]	TCG Storage Architecture Core Specification Version 1.0 Revision 0.9 – draft (May 24, 2007)
[TCG Enterprise]	TCG Storage Security Subsystem Class: Enterprise Specification Version 1.01 Revision 1.00 (August 5, 2015)
[TCG SIIS]	TCG Storage Interface Interactions Specification (SIIS) Version 1.04 Revision 1.00 (August 18 2015)
[SCSI Core]	SCSI Primary Commands ‐ 4 Rev.15 (SPC-4)
[SCSI Block]	SCSI Block Commands Rev.15 (SBC-3)
[SAS]	Serial Attached SCSI ‐ 2 Rev.13 (SAS-2)
[SAM]	SCSI Architectural Model - 5 Rev.XX (SAM-5)

Table 19 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CSP	Critical Security Parameter
CO	Crypto Officer
DDR	Double Data Rate
DRBG	Deterministic Random Bit Generator
EDLC	Electric Double-Layer Capacitor
FIPS	Federal Information Processing Standard
FW	Firmware
Global Range	The entire User-Addressable LBA Range. See [TCG Core]
HMAC	Hash-based Message Authentication Code
KAT	Known Answer Test
KEK	Key Encryption Key
LBA	Logical Block Address
MEK	Media Encryption Key
MSID	Manufactured Security Identifier. See [TCG Enterprise]
NIST	National Institute of Standards and Technology

Acronym	Definition
PBKDF	Password Based Key Derivation Function
PIN	Personal Identification Number
PRF	Pseudo-Random Function
PSP	Public Security Parameter
PSS	Probabilistic Signature Scheme
PuK	Convenient notation for Public Key
SAS	Serial Attached SCSI
SHA	Secure Hash Algorithm
SID	Security Identifier (defined by [TCG Core])
TCG	Trusted Computing Group