Hitachi Virtual Storage Platform (VSP) Encryption Module

FIPS 140-2
Non-Proprietary Cryptographic Module Security Policy

Version: 1.6

Date: March 7, 2016

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Hitachi Virtual Storage Platform (VSP) Encryption Module, hereafter denoted the Module. The Module is 12 Gb/s SAS I/O Module with Encryption. The Module provides high speed data at rest encryption for Hitachi storage. In other words, the Module encrypts data onto HDDs and decrypts data read from HDDs 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 Virtual Storage Platform (VSP) Encryption Module	P/N: 3289094-A(BS12GE) Version: B/D4, B/D5, B/D4a, B/D5a, B/D6	03.07.49.00 03.07.54.00 03.07.56.00

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated SAS I/O module used for Hitachi storage system with data at rest encryption feature. The Module is a multi-chip embedded embodiment; the cryptographic boundary is drawn at the Module's board and interfaces and includes all components within that boundary.

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

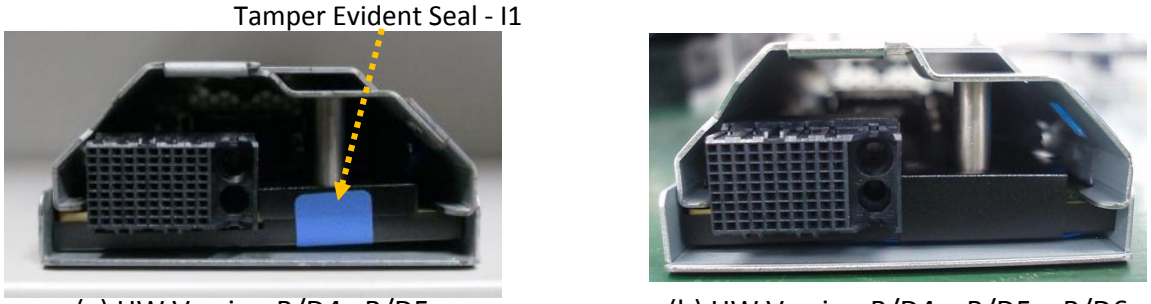
Table 2 – Security Level of Security Requirements

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 to 6; the physical boundary of the cryptographic module is the enclosure of metal frame shown in the Figures. Major components of the Module are module board, micro processor, non-volatile memories and interfaces. The module board is covered with the metal frame and the tamper seal is on the screw. In addition, the black sheet is put over the circuit of the module board to disturb the access from an opening as shown on the Figure 7 to 10. The black sheet and the metal frame are opaque within the visible spectrum. The Module relies on Hitachi storage as input/output devices.

Figure 1 – Front Side of the Module



(a) HW Version B/D4 , B/D5

(b) HW Version B/D4a, B/D5a, B/D6

Figure 2 – Back Side of the Module

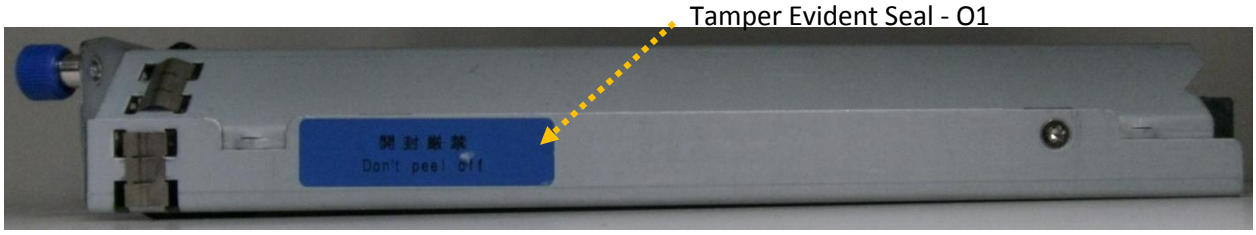


Figure 3 – Left Side of the Module

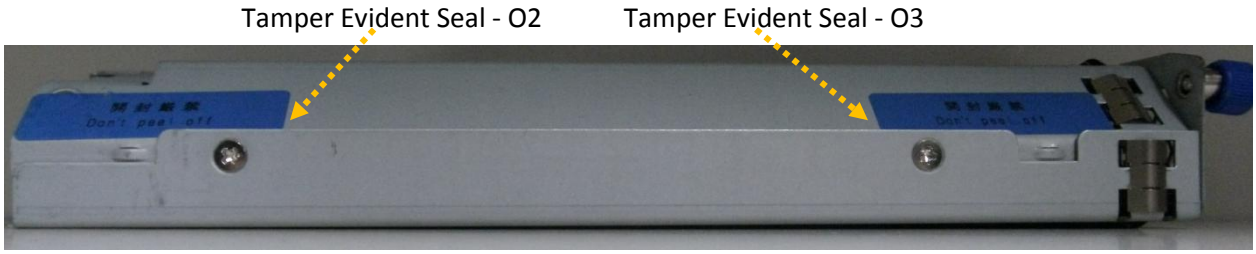


Figure 4 – Right Side of the Module

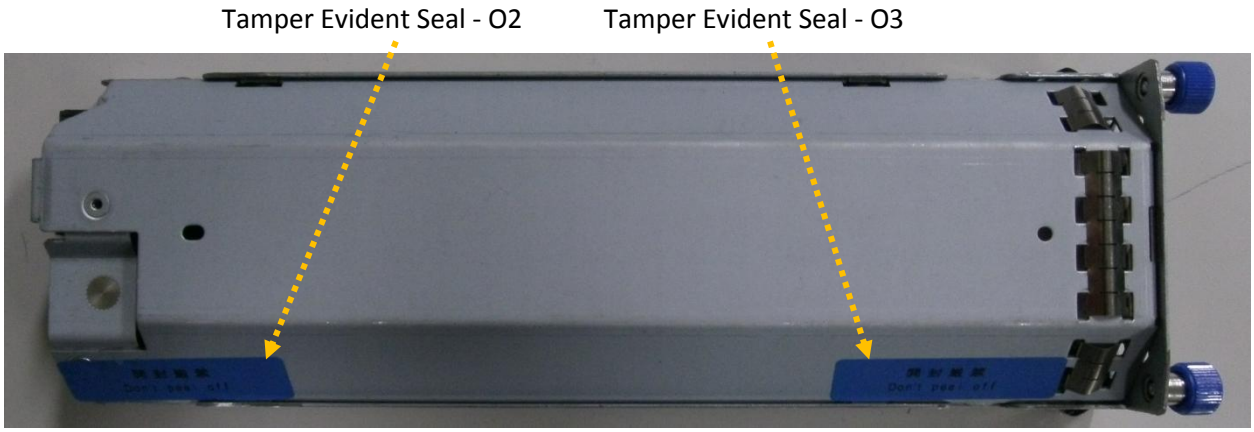


Figure 5 – Up Side of the Module

Figure 6 – Bottom Side of the Module

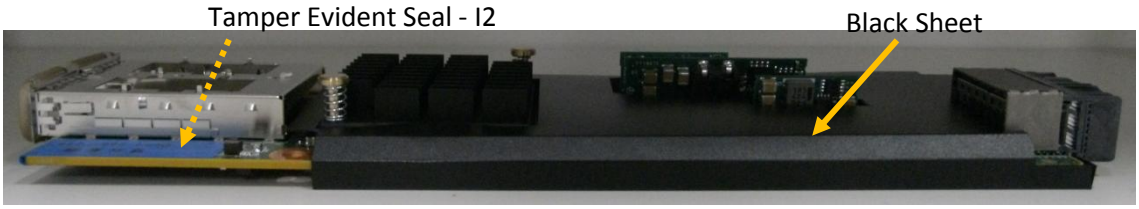


Figure 7 – Left Side of the Module without Metal Frame

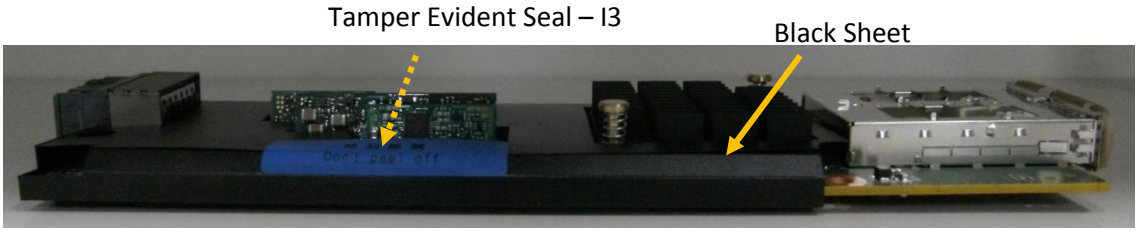
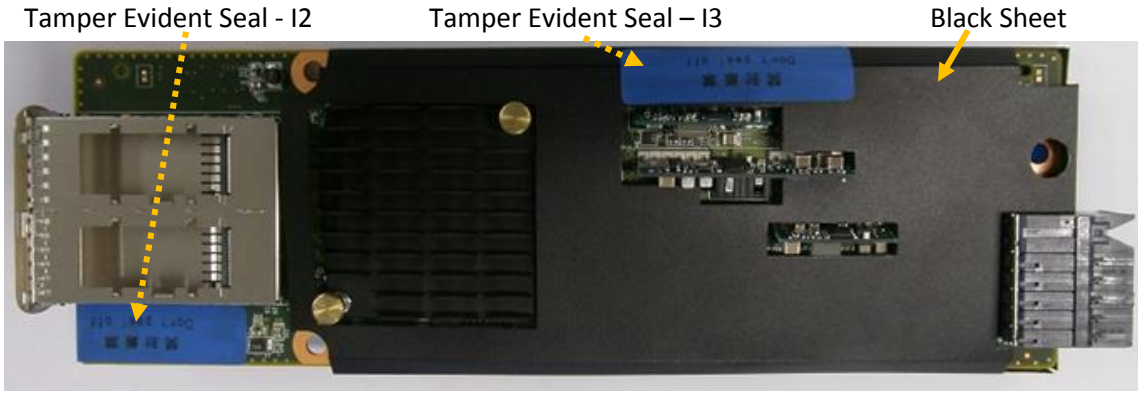


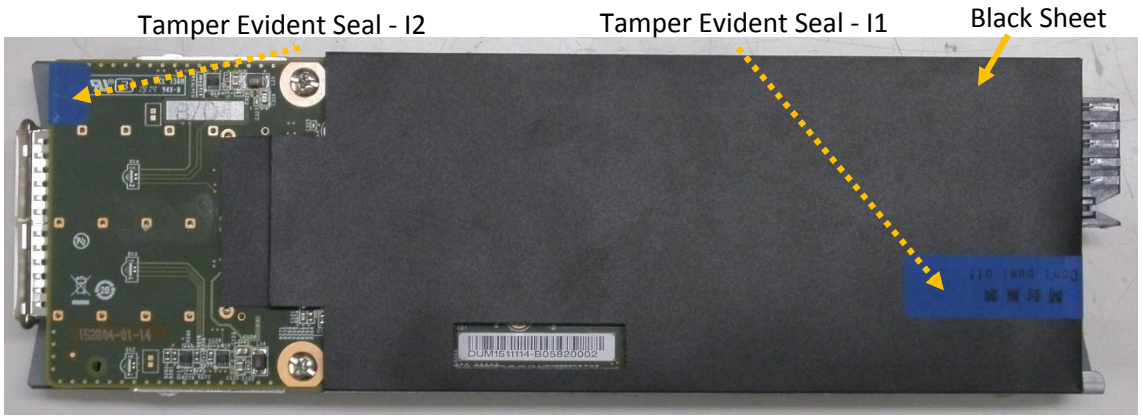
Figure 8 – Right Side of the Module without Metal Frame



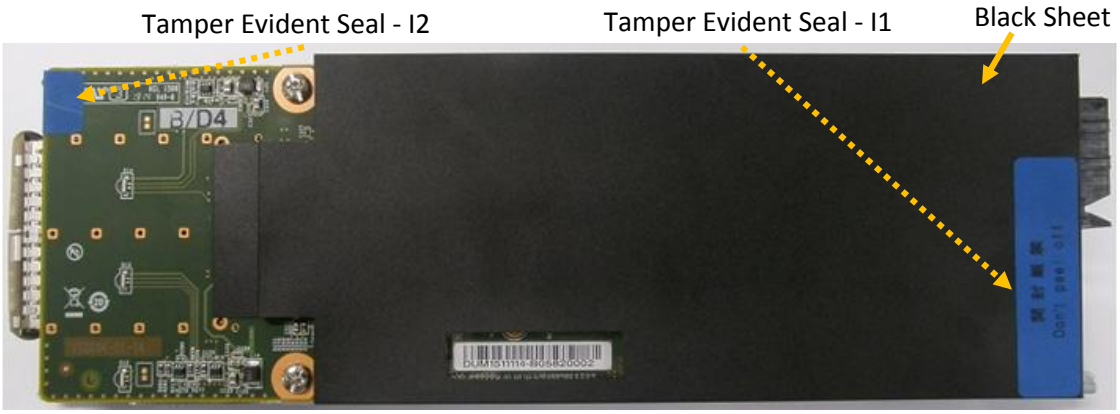
(a) HW Version B/D4, B/D4a

(b) HW Version B/D5, B/D5a, B/D6

Figure 9 – Top Side of the Module without Metal Frame



(a) HW Version B/D4 , B/D5



(b) HW Version B/D4a, B/D5a, B/D6

Figure 10 – Bottom Side of the Module without Metal Frame

1.2 Firmware and Logical Cryptographic Boundary

Figure 11 depicts the Module operational environment.

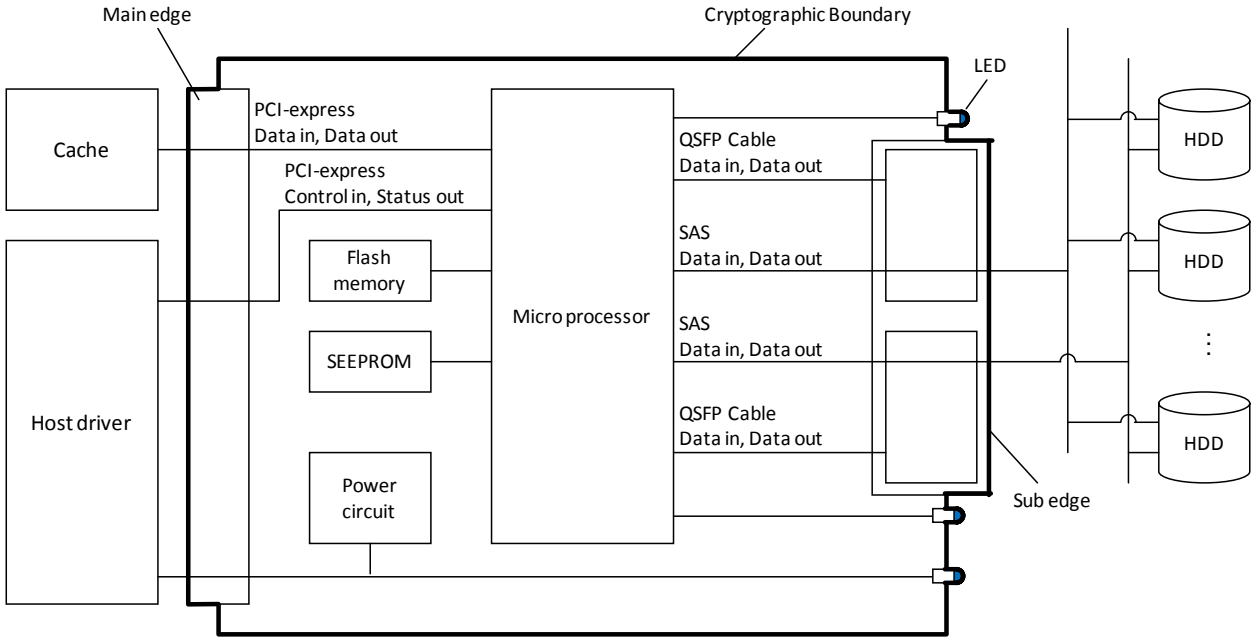


Figure 11 – Module Block Diagram

Black bold line shows the cryptographic boundary. The micro processor is responsible for processing IOs to HDDs as well as encrypting/decrypting IOs where applicable. Firmware images are stored in the flash memory. They are loaded to the micro processor when the Module power up. All functions and system initialization are performed by the micro processor, which is contained within the cryptographic boundary of the Module. CSPs are stored in flash memory or SEEPROM.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Main edge	- PCI-express: plaintext input/output, module control data input, module status data output - Hot-Line: module control data input, module status data output - I2C: module control data input - Power: 12V power input	- Power - Data in - Data out - Control in - Status out
Sub edge	- SAS: cipher text input/output	- Data in - Data out
LED	- LED: module status output	- Status out

1.3 Mode of Operation

The Module encrypts and decrypts data using only a FIPS-approved mode of operation. It does not have any functional non-approved modes.

2 Cryptographic Functionality

The Module implements the FIPS Approved cryptographic functions listed in the tables below.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[SP 800-38A] Functions: Encryption, Decryption Modes: ECB Key sizes: 256 bits	3305
XTS-AES mode	[SP 800-38E] Functions: Encryption, Decryption Key sizes: 256 bits	3305
AES Key Wrap/Unwrap	[NIST SP 800-38F] Functions: Key wrapping/unwrapping; key establishment methodology provides 256 bits of encryption strength Key sizes: 256 bits	3305
SHA	[FIPS 180-4] Functions: Calculation of HMAC SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2738
HMAC	[FIPS 198-1] Functions: MAC generation SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2097

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.

Table 5 – Critical Security Parameters (CSPs)

CSP	Description / Usage
KEKini	256-bit factory-set key used to unwrap KEK. KEK wrapped with KEKini is entered to the Module. KEK Management service zeroises KEKini by overwriting with 0xFF.
KEK	256-bit key used to unwrap DEKs and operator keys. DEKs and operator keys wrapped with KEK are entered to the Module. KEK Management service zeroises KEK by overwriting with 0xFF.
DEK	Two 256-bit keys used for XTS-AES encryption/decryption. DEK Management service zeroises DEK by overwriting with 0x00.
Operator Key	256-bit key used to unwrap operator certificate. Operator Management service zeroises Operator Key by overwriting with 0xFF.
HMAC Key	256-bit key used for authenticating firmware loaded from host. HMAC Key Management service zeroises HMAC Key by overwriting with 0x00.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles using one authentication is allowed per module reset. Re-authentication is enforced when changing roles. Each operator must be assigned to a single role. Concurrent operators are NOT supported. An operator must log out before another operator can log in.

Table 6 lists all operator roles supported by the Module. The Module does not support a maintenance role and bypass capability. The Module does not support concurrent operators. After the Module powers off or chip reset, all the data stored in internal memory (RAM), including previously authenticated operators, are cleared. All CSPs are protected through APIs and logic developed for the sole purpose of integration into specific Hitachi host platforms. Only Hitachi-authored drivers can access cryptographic APIs. Further, the Module functionally does not allow keys to be disclosed, modified, or substituted in FIPS mode of operation.

Table 6 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – The role assumed to perform cryptographic initialization or management functions.	Role-based	Operator certificate
User	User – The role assumed to perform general security services, including cryptographic operations and other approved security functions.	Role-based	Operator certificate

3.2 Authentication Methods

Operator Certificate Authentication Method

An operator is assigned to a 256-bit unique key, it called “operator key”. The operator key is stored together with its role and identity string in non-volatile memory. The key is used to authenticate the operator when it logs in.

An operator also owns a unique certificate that consists of a role and an identity string, which is wrapped by the operator key using the procedure outlined by the NIST SP800-38F. Therefore the probability that a random attempt will succeed or a false acceptance depend on operator key. When the operator wants to log in, they send the certificate to the Module. The Module unwraps the certificate using the preloaded operator key. If the unwrap is successful and if the role and the identity string from the certificate both match the ones stored in the Module, the operator authentication passes. The cryptographic services within the role are then activated.

Authentication requires more than 35µs (actual measured value).

Table 7 – Authentication Description

Authentication Method	Probability of a Single Successful Random Attempt	Probability of a Successful Attempt within a Minute
Operator Certificate Authentication Method	1/2^256 The probability that a random attempt will succeed or a false acceptance will occur depends on 256-bit operator key. Therefore, the probability is 1/2^256, which is less than 1/1,000,000.	1,714,285/2^256 Since authentication requires more than 35µs, in a worst case scenario, the Module can perform 1,714,285 per minute. Therefore, the probability that multiple attacks within a given minute will be successful is 1,714,285/2^256, which is less than 1/100,000.

3.3 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service. Also, Table 8 shows the role that is able to perform the service.

Table 8 – Authenticated Services

Service	Description	CO	User
Configure	Configures parameters	X	
Operator Management	Adds an operator's role, an identity string and an operator key, updates the operator key and zeroizes one or all operators and operator keys	X	X
Execute encryption tests	Execute encryption tests for diagnostic purposes	X	
Decrypt	Decrypts data using XTS-AES		X
Encrypt	Encrypts data using XTS-AES		X
DEK Management	Updates and zeroizes DEKs	X	X
KEK Management	Updates and zeroizes KEKs	X	X
HMAC Key Management	Sets and zeroizes the HMAC key	X	X
Firmware Update	Updates the firmware	X	X

Table 9 – Unauthenticated Services

Service	Description
Module Reset (On demand power up self-tests)	Reset the Module
Login	Authenticates operators
Logout	Operator logout of the Module This service can execute when no operator logged in
Get Current Operator	Get the operator's role and an identity string of the current operator
Get Configuration	Get module configuration parameters
Show Status	Show module status with LEDs or bits in a status register

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. (But "G" is not used in the table below, because this module does not have any key generation function.)
- 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.

Table 10 – CSP Access Rights within Services

Service	CSPs				
	KEKini	KEK	DEK	Operator Key	HMAC Key
Configure					
Operator Management		E		W/Z	
Logout				E	
Execute encryption test					
Decrypt			E		
Encrypt			E		
DEK Management		E	W/Z		
KEK Management	E/W/Z	E/W/Z			
Set HMAC Key		E			W/Z
Firmware Update					E
Module Reset(Self-tests)					
Login				E	
Get Current Operator					
Get Configuration					
Show Status					

4 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 or resetting the Module.

On power up or reset, the Module performs the self-tests described in Table 11 below. Firmware Integrity test and all 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. The Module shows the result of self-tests with bits in a status register. If Firmware Integrity test fails, the two bits of the status register for “Image Loader Agent (ILA)” are set to “10”. In this case, the boot process is halted by the ILA. If one of the KATs fails, the two bits of the status register for “Encryption Capability” are set to “01”. In addition, from other eight bits of the register, it is known which cryptographic algorithm engine (AES, SHA or KW) caused the error.

Self-tests do not require any intervention or input from the operator. Power up self-tests are automatically executed when the Module is powered up. Conditional self-tests are automatically performed when an applicable security function or operation is invoked.

Table 11 – Power Up Self-tests

Test Target	Description
Firmware Integrity	32 bit CRC performed over all code in Flash memory.
AES	KATs: Encryption, Decryption Modes: ECB Key sizes: 256 bits
HMAC	KATs: Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
XTS-AES mode	KATs: Encryption, Decryption Key sizes: 256 bits
AES Key Wrap	KATs: Wrap, Unwrap Key sizes: 256 bits

As the firmware is being externally sent to the Module, the firmware images are authenticated using the HMAC authentication technique. Both a firmware image and the HMAC key are fed into the SHA engine, together with the proper SHA-256 algorithm, the calculated HMAC digest is compared with the one embedded in the firmware image. If they don't equal, the firmware authentication fails and the Module indicate the state. If “Firmware Update” results in failure, the status field code of 0x0000000E is sent from the micro processor as the response. This code means “Firmware image HMAC authentication failure”. Conditional self-tests are automatically performed when an applicable security function or operation is invoked.

As the encryption test execute command is sent to the Module, the Module executes Cryptographic Algorithm Known Answer tests or HMAC test. The Cryptographic Algorithm Known Answer tests have positive test cases and negative ones. For a positive test case, the test passes if the result matches the known answer. For a negative test case, the result is expected to mismatch the known answer. For the HMAC test, the Module feeds the message and the HMAC key input from the host into the SHA engine, and returns the digest to the host. The command for Execute encryption test will change hardware

configuration when running the Cryptographic Algorithm Known Answer tests or HMAC test. Therefore use it only for diagnostic purposes. To return to normal mode operations, execute a Module reset.

Table 12 – Conditional Self-tests

Test Target	Description
Firmware Load	HMAC authentication performed when firmware is loaded.
Encryption Engine Diagnosis	Cryptographic Algorithm Known Answer tests or HMAC test performed by command only when no active IOMBs.

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. Six tamper evident seals are pre-installed (at factory) as shown on the Figure 1-10 with dashed arrows. These tamper evident seals are very fragile and cannot be removed without clear signs of damage to the labels. The Module is covered with the black sheet and the metal frame that is opaque within the visible spectrum.

Table 13 – Physical Security Inspection Guidelines

Physical Security Mechanism	Inspection/Test Guidance Details
Tamper Evident Seals	Shown on the Figure 1-10 with dashed arrows. Upon receipt of the new module from Hitachi or whenever the existing module in the storage system is removed and re-installed, the CO should visually inspect the module and the tamper evident seals found on the module. If an evidence of tampering (including scratches or scrapes, signs of peeling off, tearing or damage) is detected, the CO shall immediately refuse the module installation and notify the management. CO shall also request a new replacement module with tamper evident seals by contacting Hitachi Customer Support.
Sheet	Black sheet shown on the Figure 7-10.

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 two distinct operator roles: User and Cryptographic Officer.
2. The Module shall provide role-based authentication.
3. The Module shall clear previous authentications on power cycle.
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 8.
5. The operator shall be capable of commanding the Module to perform the power up self-tests by cycling power or resetting the Module.
6. Power up self-tests do not require any operator action.
7. Data output shall be inhibited during self-tests, zeroization, 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. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual key entry.
13. The Module does not have any external input/output devices used for entry/output of data.
14. The Module does not enter or output plaintext CSPs.
15. The Module does not support the update of the logical serial number or vendor ID.

8.1 Crypto Officer Guidance

The Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

1. Verify that the name and part number of module is 3289094-A (BS12GE) and version is B/D4, B/D5, B/D4a, B/D5a or B/D6.
2. Verify that the firmware version of module is 03.07.49.00, 03.07.54.00 or 03.07.56.00.
3. Enable the encryption feature.
4. Configure encryption environmental settings.

The Module provides only FIPS-Approved mode of operation.

See [User Guide] Chapter 2 for detail of initialization procedures.

Otherwise, no specific commands or settings are required to place the Module in FIPS-approved mode of operation.

8.2 User Guidance

The User must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

1. Enable data encryption on the parity group.
2. Format the Volumes at the parity-group level.

See [User Guide] Chapter 4 for detail of initialization procedures.

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 References and Definitions

The following standards are referred to in this Security Policy.

Table 14 – References

Abbreviation	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
[SP800-38A]	*Recommendation for Block Cipher Modes of Operation Methods and Techniques,* 2001 Edition
[FIPS 198-1]	*The Keyed-Hash Message Authentication Code(HMAC)*, July 2008
[SP800-38E]	*Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, January 2010
[IG D.9]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, *FIPS 140-2 Annex D – Approved Key Establishment Techniques*, *D.9 Key Transport Methods*, July 25, 2013
[NIST SP 800-38F]	*Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012
[User Guide]	*Hitachi Virtual Storage Platform G400/G600/G800 Encryption License Key User Guide*

Table 15 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DEK	Data Encryption Key
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
KAT	Known Answer Test
KEK	Key Encryption Key
NIST	National Institute of Standards and Technology