Hitachi Vantara

Hitachi Vantara, Ltd.

Hitachi Storage Hardware Encryption Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy of the Hitachi Storage Hardware Encryption Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Hitachi Storage Hardware Encryption Module (hereafter denoted the module) provides data-at-rest encryption for Hitachi storage systems. In other words, the module encrypts data written to the DRAM and decrypts data read from the DRAM using XTS-AES. The XTS-AES mode has been approved by CMVP for protecting the confidentiality of data on storage devices.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

The black bold-bordered line in Figure 1-2 indicates the cryptographic boundary. As shown in the photos in the Cryptographic Module section (Figure 1-1), the cryptographic boundary

corresponds to the entire physical perimeter of the chassis unit. The four major components included within the cryptographic boundary in Figure 1-2 are the fan, power circuit, FPGA, and SPI ROM. The cryptographic functions are implemented by the FPGA.
The following cryptographic algorithms are implemented in the FPGA:
Hitachi Storage Hardware Encryption Module implementing
HMAC (A7561) / KW (A7562) / AES-XTS0 (A7563) / AES-XTS1 (A7564),
as well as ECDSA (A4875) and SHA3-384 (A4875).
The ECDSA and SHA3-384 algorithms are implemented in Versal ACAP SW (A4875).

Figure 1-1: Hitachi Storage Hardware Encryption Module

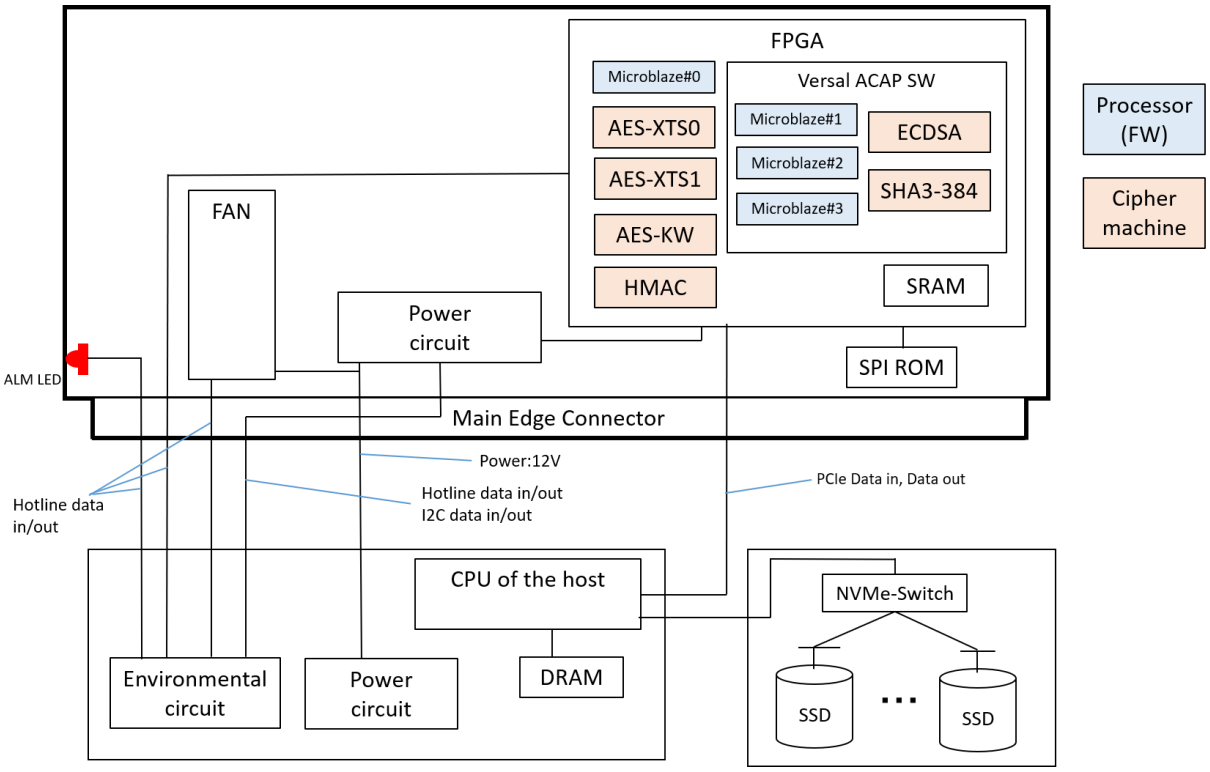

Figure 2-2: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
x0000_0000	e2000003_25101000_00000000	ED020009	MicroBlazes	

Table 2: Tested Module Identification – Hardware

The model and/or part number indicate the package version. The hardware version refers to the version of the FPGA configuration data, Boot FW, BootROM, PLM FW and PSM FW. The firmware version represents the version of the Main FW. The package version, hardware version, and firmware version can all be read from the registers.

2.3 Excluded Components

N/A.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	All services are available in this mode of operation (when configured as per the instructions in Section 11 of this document).	Approved	The successful completion of a service is an implicit indicator for the use of an approved service.

Table 3: Modes List and Description

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

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A7562	Direction - Decrypt Key Length - 256	SP 800-38A
AES-ECB	A7563, A7564	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-KW	A7562	Direction - Decrypt Key Length - 256	SP 800-38F
AES-XTS Testing Revision 2.0	A7563, A7564	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
ECDSA SigVer (FIPS186-4)	A4875	Curve - P-384 Hash Algorithm - SHA3-384	FIPS 186-4
HMAC-SHA2-256	A7561	Key Length - Key Length: 256	FIPS 198-1
SHA2-256	A7561	Message Length - Message Length: 8-4096 Increment 8	FIPS 180-4
SHA3-384	A4875	Message Length - Message Length: 0-64864 Increment 8	FIPS 202

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encryption	BC-UnAuth	Encryption using AES-XTS.		AES-XTS Testing Revision 2.0: (A7563, A7564) AES-ECB: (A7563, A7564)
Decryption	BC-UnAuth	Decryption using AES-XTS.		AES-XTS Testing Revision 2.0: (A7563, A7564) AES-ECB: (A7563, A7564)
KTS-Unwrap	KTS-Unwrap	Key unwrapping using AES-KW	Standard:SP 800-38F	AES-KW: (A7562) AES-ECB: (A7562)
SHA	SHA	Compute message digest using SHA2-256		SHA2-256: (A7561)
Message Authentication Code	MAC	Compute MAC tags using HMAC		HMAC-SHA2-256: (A7561)
ECDSA SigVer	DigSig-SigVer	Digital Signature Verification using ECDSA		ECDSA SigVer (FIPS186-4): (A4875) SHA3-384: (A4875)

Table 5: Security Function Implementations

2.7 Algorithm Specific Information

AES XTS:
In the AES algorithm's XTS mode, data exceeding 2^20 blocks (16MB) is not processed. Additionally, the module strictly checks that the Data Encryption Key (DEK) and the Tweak Key (IV_Key) are not identical during key registration (performing the register key service). During the Register key service, the module explicitly checks that Key_1 and Key_2 are not identical. If Key_1 equals Key_2, the key registration is rejected.

Per IG C.I, AES-XTS keys (i.e., Key_1 and Key_2) entered into the module shall be generated and/or established independently according to NIST SP 800-133rev2, Section 6.3. for an approved use of AES-XTS.

ECDSA:
The module implements ECDSA signature verification function that was CAVP-tested against FIPS PUB 186-4 prior to the Feb 5, 2024. This test is mathematically identical to the FIPS PUB 186-5 tests. Thus, as allowed per Additional Comment #3 under FIPS 140-3 IG C.K, compliance with the FIPS PUB 186-5 tests is claimed.

2.8 RBG and Entropy

N/A for this module.

2.9 Key Generation

N/A for this module.

2.10 Key Establishment

The Key Transport Schemes(KTS) as specified in SP 800-38F implemented by the module are listed in Section 2.5 Algorithms and Section 2.6 Security Function Implementations.

2.11 Industry Protocols

N/A for this module.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
PCI-express(Main Edge Connector)	Data Input Data Output Control Input Status Output	module control data (command) input, module status data(command response) output, plaintext data input/output, cipher text data input/output
Power(Main Edge Connector)	Power	12V power input
Hotline(Main Edge Connector)	Control Input Status Output	module control data input, module status data output, reset
I2C (Main Edge Connector)	Control Input Status Output	power circuit log information

Physical Port	Logical Interface(s)	Data That Passes
LED	Status Output	power supply status

Table 6: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Authentication Data	The module enforces role separation by requiring 256-bit Authentication Data for the two roles: USR and COR. The Authentication Data for each role is inputted in plaintext to authenticate the operator when it logs in as the role. The module can be logged in from the COR to the USR.	Password Based	1/2^256, The probability that a random attempt will succeed or a false acceptance will succeed or a false acceptance will occur depends on 256-bit Authentication Data. 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 Authentication Data 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.

Table 7: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
COR	Role	CO	Authentication Data
USR	Role	CO	Authentication Data

Table 8: Roles

The roles(COR and USR) support the services listed in the table.
Both COR and USR are defined as Crypto Officer(Operator Type) in the context of FIPS definitions.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Operator Management	Set Authentication Data for each operator(COR and USR) to log in	The ADMIN_STS field of the ACQ(command response) : 0x0	Command to Operator Management, Authentication Data	Status of the completion	SHA	COR - Authentication Data: W USR - Authentication Data: W
Decrypt	Decrypts data using XTS-AES	The IO_STS field of the IOCQ(command response for the data encryption/decryption/copy) :0x0	Command to Decrypt and Ciphertext	Plaintext	Decryption	USR - DEK: E
Encrypt	Encrypts data using XTS-AES	The IO_STS field of the IOCQ(command response for the data encryption/decryption/copy) :0x0	Command to Encrypt and Plaintext	Ciphertext	Encryption	USR - DEK: E
Logout	Operator logout of the module	The ADMIN_STS field of the ACQ(command response) : 0x0	Command to Logout FW	None	None	COR USR
Register key	Register keys(DEK, KEK,HMAC)	The ADMIN_STS field of the ACQ(command response) : 0x0	Command to Register key and the keys(DEK/KEK/HMAC)	None	KTS-Unwrap	COR - KEK: W,E - DEK: W - HMAC_Key: W USR - KEK: W,E - DEK: W -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						HMAC_Key: W
Delete key	zeroizes the Keys(KEK/DEK/HMAC_KEY)	The ADMIN_STS field of the ACQ(command response) : 0x0	Command to Delete key	None	None	COR - KEK: Z - HMAC_Key: Z - DEK: Z USR - KEK: Z - HMAC_Key: Z - DEK: Z
Firmware Update	Updates the firmware	The ADMIN_STS field of the ACQ(command response) : 0x0	Command to Firmware Update and Firmware Image	None	Message Authentication Code	COR - HMAC_Key: E
Module Reset(Periodic self-tests)	Resets the module by power off/on. Zeroizes SSPs, and perform the Self-Tests (Pre-operational self-tests and CASTs)	None	Power off/on	None	ECDSA SigVer	Unauthenticated - KEK: Z - HMAC_Key: Z - DEK: Z
Partial Reset	perform the Self-Tests(the CASTs excluding the ECDSA SigVer (FIPS 186-4) (A4875) CAST) from any role or from error#2 state	None	Recovery Reset	None	None	Unauthenticated COR USR
Login	Login by operator authentication	The ADMIN_STS field of the ACQ(command response) : 0x0	Command to Login	None	SHA	Unauthenticated - Authentication Data: E COR - Authentic

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ation Data: E
Revert	Zeroizes SSPs, and reset authentication data to factory default	The ADMIN_STS field of the ACQ(command response) : 0x0	Command to Revert	None	None	Unauthenticated - Authentication Data: Z - KEK: Z - HMAC_Key: Z - DEK: Z COR - Authentication Data: Z - KEK: Z - HMAC_Key: Z - DEK: Z
Show Status	Output the module status information such as the firmware-related information. The following information can be displayed: Login Status, HSTATUS(Status of error conditions and operational state within the cryptographic module), KEK bitmap/DEK bitmap(KEK or DEK registration information), FW Bootloader Status(Result of	None	Register Access(read)	Module status information	None	Unauthenticated COR USR

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the Integrity Test performed by Boot FW on Main FW), POST/KAT Status(result of CAST for Main FW)					
Show power circuit log	Get power circuit log information	None	Service request	Power circuit log information	None	Unauthenticated COR USR
Copy	Copy data from the input buffer to the output buffer	The IO_STS field of the IOCQ(command response for the data encryption/decryption/copy) :0x0	Command to copy, Data to be copied	None	None	USR
Show Version	Outputting the module identification and the version information.	None	Register Access(read)	Package version, Hardware version, and Firmware version	None	Unauthenticated COR USR

Table 9: Approved Services

The approved services implemented by the module are listed in the tables above. Each service description also details how the service uses SSPs. The "Roles SSP Access" column defines the relationship between access to SSPs and the various module services. The access modes shown in the table are as follows:

• E = Execute: The module executes using SSP.

• W = Write: The module writes to SSP. This typically occurs after SSP is imported into the module, when the module generates SSP, or when it overwrites an existing SSP.

• Z = Zeroize: The module zeroizes (erases) SSP.

4.4 Non-Approved Services
N/A.

4.5 External Software/Firmware Loaded

The module supports firmware load testing using HMAC-SHA2-256 when uploading newly validated firmware. The HMAC_Key used for the firmware load test, referred to as the HMAC_Key, is registered via Register key service and utilized during the firmware load process. To load new firmware, the COR(Crypto Officer role) must authenticate to the module, preventing unauthorized access and misuse of the module. After successfully loading the update, the module transitions to an Idle state. If verification fails, the update attempt is rejected, an error response is returned by the module, and the Firmware Update is disallowed.
Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

5 Software/Firmware Security

5.1 Integrity Techniques

The module contains six firmware (FPGA configuration data, Boot FW, BootROM, PLM FW, PSM FW, and Main FW).
The module includes the following firmware components that include separate firmware integrity tests:
− FPGA configuration data, Boot FW, PLM FW, and PSM FW: Signature Verification (ECDSA P-384),
− Main FW: CRC16
The BootROM firmware is implemented in non-reconfigurable memory as defined in IG 5.A. Therefore, the requirements of this area are not applicable to this firmware.

5.2 Initiate on Demand

Integrity tests are performed as part of the pre-operational self-tests. Thus, the integrity test can be initiated on demand by issuing the Module Reset.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evident Seal	See the right column	Shown on Figures 7-3 and 7-5 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 Crypto Officer should visually inspect the module, and the tamper evident seals found on the module. It is recommended that the Crypto Officer inspects the tamper evident seal, each time the module can be disconnected from the storage system (when the storage system is powered off, in the case of the system maintenance, etc.). If evidence of tampering (including scratches or scrapes, signs of peeling off, tearing or damage) is detected, the Crypto Officer shall immediately refuse the module installation and notify the management. Crypto Officer shall also request a new replacement module with tamper evident seals by contacting Hitachi Customer Support. If no evidence of tampering is detected, the Crypto Officer may proceed with the installation of the module into the storage system.
Metal frame with screw	See the right column	Shown on Figures 7-3 and 7-5 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 Crypto Officer should visually inspect the module and the screws that secure the FAN found on the module. It is recommended that the Crypto Officer inspects the screws, each time the module can be disconnected from the storage system (when the storage system is powered off, in the case of the system maintenance, etc.). If evidence of tampering (including loose screws) is detected, the Crypto Officer shall immediately refuse the module installation and notify the management. The Crypto Officer shall also request a new replacement module with screws that secure the FAN by contacting Hitachi Customer Support.

Table 10: Mechanisms and Actions Required

The physical form of the module is depicted in Figure 7-1 to 7-6; the physical boundary of the cryptographic module is the enclosure of metal frame shown in the Figures. The module board is covered with the metal frame, and the tamper seal is on the screw. In addition, the black sheet is implemented to the circuit board to disturb access from the opening of the top, bottom and back side of the module as shown in Figure 7-2. The black sheet and the metal frame are opaque within the visible spectrum.

Figure 7-1: Front side of the module

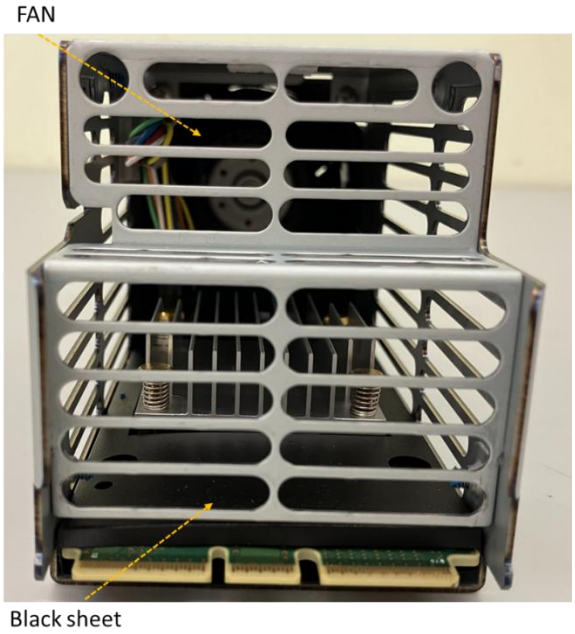

Figure 7-2: Back side of the module

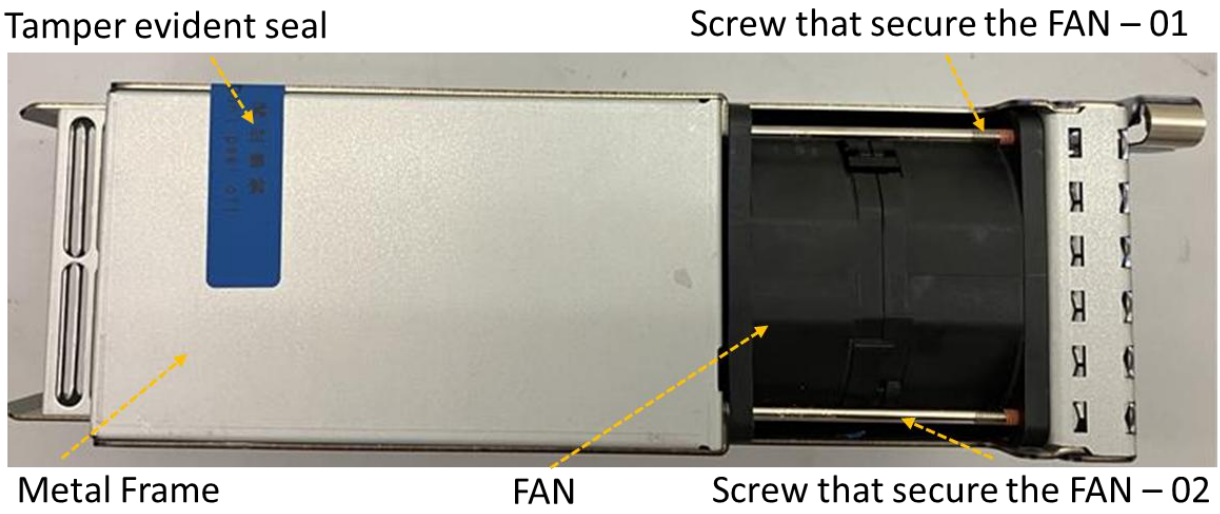

Figure 7-3: Top side of the module

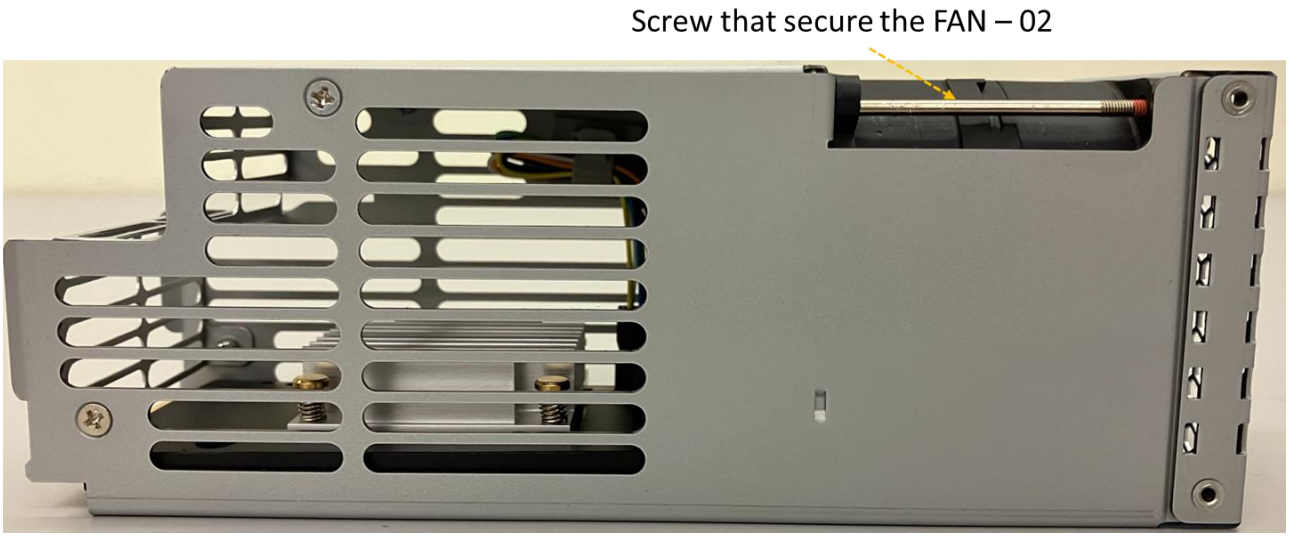

Figure 7-4: Left side of the module

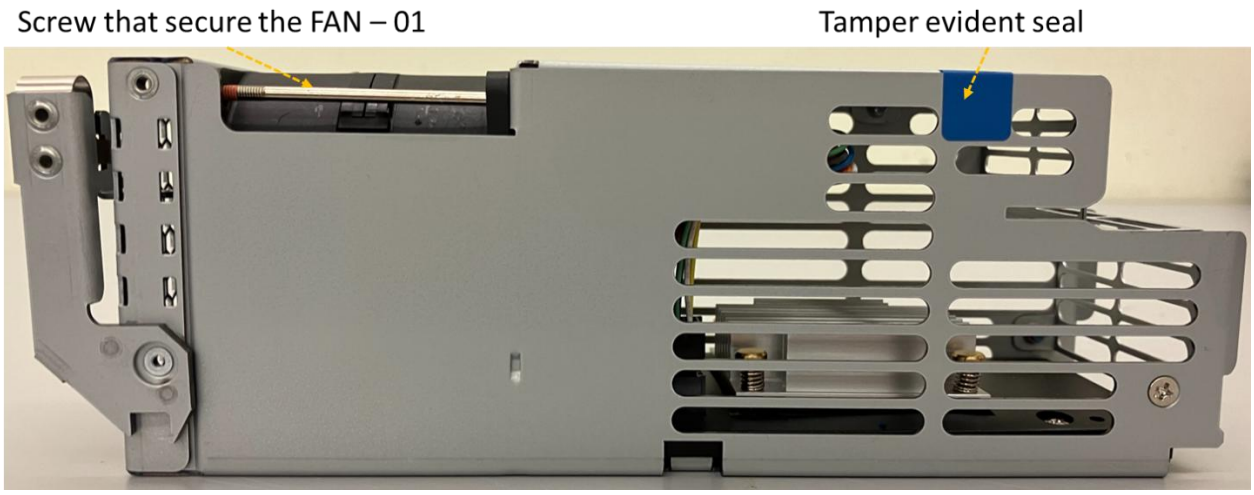

Figure 7-5: Right side of the module

Figure 7-6: Bottom side of the module

8 Non-Invasive Security

The module does not implement non-invasive security techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	A volatile memory	Dynamic
SPI ROM	Non-Volatile memory	Static

Table 11: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Edit auth	External (Outside of the cryptographic boundary)	SPI ROM	Plaintext	Automated	Electronic	SHA
Register Key	External (Outside of the cryptographic boundary)	RAM	Encrypted	Automated	Electronic	KTS-Unwrap

Table 12: SSP Input-Output Methods

The module does not support manual SSP input or intermediate SSP generation output.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Delete key	The command to delete the registered keys.	The deleted cryptographic key is overwritten with all 0x0 or all 0xF, resulting in an invalid state.	Perform the Delete key service
Revert	The command used to initialize SSPs(factory default).	The Authentication Data resets to the factory default value. All DEK, KEK, and HMAC_Key are deleted and overwritten with invalid values. The factory-default KEK is set as the initial value.	Perform the Revert service.
Module Reset	The operation to initialize SSP.	By turning off the power, the HMAC_Key, KEK, and DEK stored in RAM are volatilized. The factory-default KEK is set as the initial value.	Perform the Module Reset(Power off by removing the module).

Table 13: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Authentication Data	Pass phrase used for role authentication	256 bits - 256 bits	Authentication Data - CSP			SHA
KEK	Key encryption keys	256 bits - 256 bits	Symmetric Key - CSP		KTS-Unwrap	KTS-Unwrap
HMAC_Key	The key used to detect tampering of the firmware during a Firmware Update	256 bits - 256 bits	Symmetric Key - CSP		KTS-Unwrap	Message Authentication Code
DEK	Data encryption keys	256 bits - 256 bits	Symmetric Key - CSP		KTS-Unwrap	Encryption Decryption

Table 14: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Authentication Data	Edit auth	SPI ROM:Obfuscated		Revert	
KEK	Register Key	RAM:Plaintext	From input to zeroization or module power off.	Delete key Revert Module Reset	KEK:Wrapped by
HMAC_Key	Register Key	RAM:Plaintext	From input to zeroization or module power off.	Delete key Revert Module Reset	KEK:Wrapped by
DEK	Register Key	RAM:Plaintext	From input to zeroization or module power off.	Delete key Revert Module Reset	KEK:Wrapped by

Table 15: SSP Table 2

*The KEKs are stored in volatile memory. After executing the Module Reset or Revert service, register the KEKs using the factory-default KEK following the procedure described in SP 11.2.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA SigVer (FIPS186-4) (A4875)	P-384 with SHA3-384	KAT	SW/FW Integrity	Module becomes operational	Integrity test for Boot FW, PLM FW, PSM FW and FPGA configuration data
CRC16	CRC16	KAT	SW/FW Integrity	Module becomes operational	Integrity test for Main FW

Table 16: Pre-Operational Self-Tests

If the firmware integrity tests fail, the module enters the error state.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS(A7563) -Encrypt	Key sizes: 256 bits	KAT	CAST	Module becomes operational	Encrypt	Power on
AES-XTS(A7563) -Decrypt	Key sizes: 256 bits	KAT	CAST	Module becomes operational	Decrypt	Power on
AES-XTS(A7564) -Encrypt	Key sizes: 256 bits	KAT	CAST	Module becomes operational	Encrypt	Power on
AES-XTS(A7564) -Decrypt	Key sizes: 256 bits	KAT	CAST	Module becomes operational	Decrypt	Power on
AES-KW (A7562)	Key sizes: 256 bits	KAT	CAST	Module becomes operational	Unwrap	Power on
HMAC-SHA2-256 (A7561)	Key sizes: 256 bits	KAT	CAST	Module becomes operational	Message authentication	Power on
ECDSA SigVer (FIPS186-4) (A4875)	P-384 with SHA3-384	KAT	CAST	Module becomes operational	Verify	Power on
Firmware load test	HMAC-SHA2-256	Firmware Load Test	SW/FW Load	Success: the ADMIN_STS field of the ACQ(comman	Hash	Firmware Update Request

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				d response)=0x0, Failure: the ADMIN_STS field of the ACQ=0x1		

Table 17: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A4875)	KAT	SW/FW Integrity	On demand	Manually
CRC16	KAT	SW/FW Integrity	On demand	Manually

Table 18: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS(A7563)-Encrypt	KAT	CAST	On demand	Manually
AES-XTS(A7563)-Decrypt	KAT	CAST	On demand	Manually
AES-XTS(A7564)-Encrypt	KAT	CAST	On demand	Manually
AES-XTS(A7564)-Decrypt	KAT	CAST	On demand	Manually
AES-KW (A7562)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A7561)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-4) (A4875)	KAT	CAST	On demand	Manually
Firmware load test	Firmware Load Test	SW/FW Load	N/A	N/A

Table 19: Conditional Periodic Information

The above conditions allow integrity tests and CAST to be conducted within the cryptographic boundary.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error#1	A state when the module has encountered an error condition.	Failed the Pre-operational self-tests(Integrity test for Boot FW, PLM FW, PSM FW and FPGA configuration data) or the Cryptographic Known Answer self-tests of ECDSA SigVer (FIPS186-4) (A4875).	Recovery can be achieved by issuing the Module Reset.	The module is aborted and is not available for use.
Error#2	Failed the Cryptographic Known Answer self-tests.	Failed the Pre-operational self-test(Main FW) or the Cryptographic Known Answer self-tests excluding the ECDSA SigVer (FIPS 186-4) (A4875) CAST.	Recovery can be achieved by issuing the Module Reset.	Show status service outputs. The pre-operational self-test: FW Bootloader Status (Pass: 0x80000003/ Failed: 0x8000f070) The CASTs: KAT Status(Pass: 0xED000000/Failed: 0xEDEEEEEE)
FW load Test failed	A state where the FW load test has failed.	Failed the FW load test.	None	The ADMIN_STS field of the ACQ(command response) : 0x1(error)

Table 20: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Upon receiving of the new module from Hitachi, the Crypto Officer (COR or USR) should visually inspect the module, and the tamper evident seal found on the module, as described in Section 7.1 of this document.

The module meets all the Level 2 requirements for FIPS 140-3. Follow the secure operations provided below to place the module in compliant state. Operating this module without maintaining the following settings would put module operated in a non-compliance state.

Startup Procedures

Confirm by executing the show status that the following versions match the Module Identification specified in Section 2.2.

- Model/Part Number: PK_REV (package version)
- Hardware Version: LSI_VER (hardware version)
- Firmware Version: CCA_FW VERSION (firmware version)

The default authentication data of the COR and USR must be changed upon first use as following procedure.

1. Log in as the COR role using the factory default COR password and change the COR Authentication Data.
2. Change the USR Authentication Data.

The COR must register the KEKs and DEKs used during the operation. The procedure is as follows:

1. Wrap the KEKs with the factory-default KEK and register them to the module.
2. Zeroise the factory-default KEK using the Delete Key Service.

Note that this procedure must also be performed after powering off the module and after executing the Revert service.

The USR must configure and enforce the initialization procedures.

1. Enable encryption and then create the parity group.
2. Format the volumes at the parity group level.

The initialization procedures are performed automatically when the module is inserted into the main controller.

For other settings, please refer to Encryption License Key Users Guide Chapter 3.

11.2 Administrator Guidance

The COR must register the KEKs and DEKs used during the operation after powering off the module(Module Reset service) and after executing the Revert service. The procedure is as follows:

1. Wrap the KEKs with the factory-default KEK and register them to the module.
2. Zeroise the factory-default KEK using the Delete Key Service.

All ports and logical interfaces described in this document are available to the Crypto Officer role(COR and USR). For services available with COR and USR, refer to the Approved Services Table in this document.

11.3 Non-Administrator Guidance

N/A

11.4 Design and Rules

The module design corresponds to the module security rules. This subsection documents the security rules enforced by the module to implement the security requirements of this FIPS 140-3 Level 2 module.

1. The module shall provide the COR role and the USR role.
2. The operator shall be capable of commanding the module to perform the pre-operational self-tests and the cryptographic algorithm self-tests by issuing the Module Reset.

3. Pre-operational self-tests do not require any operator action.
4. Data output shall be inhibited during self-tests, zeroization, and error states.
5. Status information does not contain SSPs or sensitive data that if misused could lead to a compromise of the module.
6. The module does not support degraded operation.
7. The module does not support concurrent operators.
8. The module does not support a maintenance interface or role.
9. The module does not support manual key entry.
10. The module does not have any external input/output devices used for entry/output of data.

11.6 End of Life

The SSPs, such as KEK, HMAC_Key, and DEK, are stored in volatile memory (RAM), meaning they are lost when the power is turned off. In contrast, Authentication Data is stored in SPI ROM, so it remains intact even when the power is off. Therefore, the Crypto Officers(COR and USR roles) must perform the operational procedure to initialize the authentication data (the Revert service) when the cryptographic module is removed.

Based on the product life of internal components, the process for performing "End of Life" must occur at the point of maximum 20 years, starting from the manufacturing date of the module.

12 Mitigation of Other Attacks

The module does not provide mitigation of other attacks.