Hitachi Vantara, Ltd.

Hitachi Storage Hybrid Firmware 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 defines the Security Policy for the Hitachi Storage Hybrid Firmware Encryption Module, hereafter denoted as the module. The module meets FIPS 140-3 overall Level 1 requirements.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module provides data at rest encryption for Hitachi storage system, Hitachi Virtual Storage Platform One Block. In other words, the module encrypts data onto drives and decrypts data read from drives using XTS-AES. The XTS-AES mode was approved by CMVP for protecting the confidentiality of data on storage devices.

Module Type: Firmware-hybrid

Module Embodiment: MultiChipEmbed

Module Characteristics:

Cryptographic Boundary:

The cryptographic boundary for the module consists of disjoint firmware and hardware components within a same tested operational environment's physical perimeter (TOEPP). The firmware component is defined as binary CRYPTLOAD, and the hardware component is a CPU. The hardware component implements AES-NI (PAA) and SHA Extensions (PAA). The firmware component of the module is designed to utilize AES-NI and SHA Extensions provided by the CPU. Red dashed lines in Figure 1 show the cryptographic boundary.

Tested Operational Environment's Physical Perimeter (TOEPP):

The operational environment hardware for the module is dedicated hardware for Hitachi storage system, Storage Controller Board (hereafter denoted as the board). The enclosure of the board is TOEPP. The hardware component of the module, CPU, is implemented in the board. Operating system for Hitachi storage system works on the CPU. The module works on the operating system.

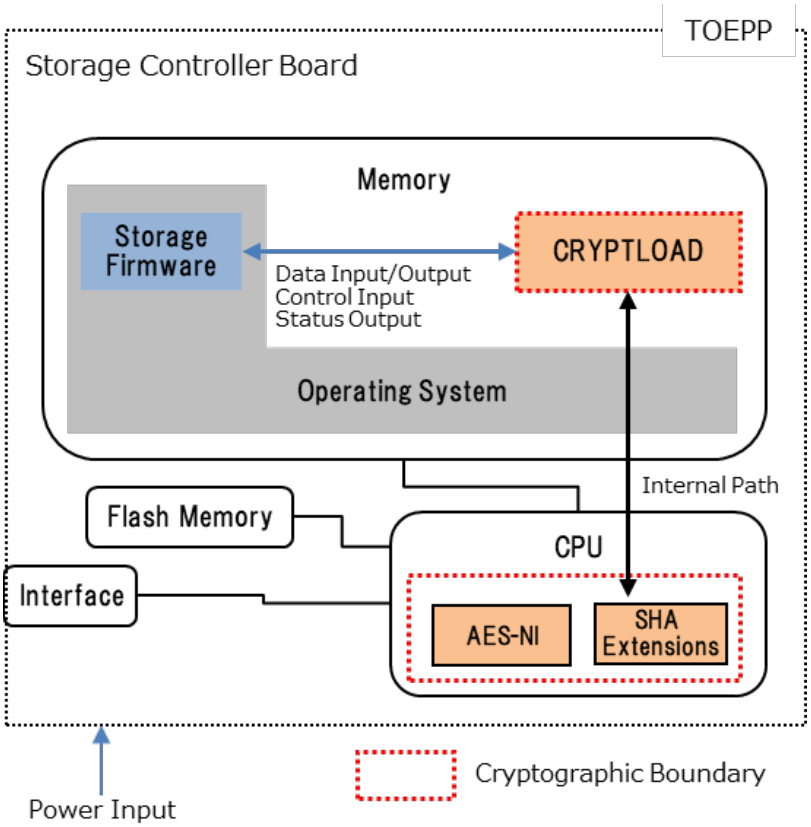

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
Storage_Encryption_Module_20	A0-01-00-00		SHA2-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Intel® Xeon® Silver 4410Y	Intel® Xeon® Silver 4410Y	N/A	Intel® Xeon® Silver 4410Y	
Intel® Xeon® Gold 6421N	Intel® Xeon® Gold 6421N	N/A	Intel® Xeon® Gold 6421N	

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
SVOS10	Storage Controller Board	Intel® Xeon® Silver 4410Y	Yes		A0-01-00-00
SVOS10	Storage Controller Board	Intel® Xeon® Gold 6421N	Yes		A0-01-00-00

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

The module has no excluded components.

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.	Approved	A status code indicating the completion of service

Table 5: Modes List and Description

The module implements only the approved mode of operation. No special API calls or settings are required to place the module in the approved mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A5023	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5025	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5026	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5027	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5028	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5029	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A5030	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5031	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5032	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5033	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5034	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5035	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5036	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5037	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5038	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5039	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5040	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5041	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5042	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5043	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5044	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-KW	A5023	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
AES-XTS Testing Revision 2.0	A5046	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5047	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5048	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5049	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5050	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5051	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5052	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5053	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
SHA2-256	A5024	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4

Table 6: 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
Secure Hash	SHA	Used to generate hash value from inputted data.		SHA2-256: (A5024)
AES-ECB Core	BC-UnAuth	Used to encrypt/decrypt inputted data. The underlying block cipher of AES-KW.		AES-ECB: (A5023)
AES-KW Core	KTS-Wrap	Used to wrap/unwrap an inputted key.		AES-KW: (A5023) AES-ECB: (A5023)
AES-ECB Core 4	BC-UnAuth	Used to encrypt/decrypt inputted data. The underlying block cipher of AES-XTS.		AES-ECB: (A5025, A5026, A5027, A5028)
AES-ECB Core 16	BC-UnAuth	Used to encrypt/decrypt inputted data. The underlying block cipher of AES-XTS.		AES-ECB: (A5029, A5030, A5031, A5032, A5033, A5034, A5035, A5036, A5037, A5038, A5039, A5040, A5041, A5042, A5043, A5044)
AES-XTS Core 512	BC-UnAuth	Used to encrypt/decrypt inputted data in units of 512 byte.		AES-XTS Testing Revision 2.0: (A5046, A5047, A5048, A5049) AES-ECB: (A5025, A5026, A5027, A5028, A5029, A5030, A5031, A5032, A5033, A5034, A5035, A5036, A5037, A5038, A5039, A5040, A5041, A5042, A5043, A5044)
AES-XTS Core 520	BC-UnAuth	Used to encrypt/decrypt inputted data in units of 520 byte.		AES-XTS Testing Revision 2.0: (A5050, A5051, A5052, A5053) AES-ECB: (A5025, A5026, A5027, A5028, A5029,

Name	Type	Description	Properties	Algorithms
				A5030, A5031, A5032, A5033, A5034, A5035, A5036, A5037, A5038, A5039, A5040, A5041, A5042, A5043, A5044)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

The module has a function that checks if two keys for AES XTS mode are different from each other.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

2.9 Key Generation

N/A for this module.

2.10 Key Establishment

N/A for this module.

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
N/A	Data Input	Data to be read from the memory area specified in the API parameters
N/A	Data Output	Data to be written to the memory area specified in the API parameters
N/A	Control Input	API function calls
N/A	Status Output	Responses of the invoked API function

Table 8: Ports and Interfaces

The module utilizes APIs as its interfaces and has no physical ports. Additionally, the module does not implement any control output interfaces.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not support authentication for roles.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Cryptographic Officer	Role	CO	None

Table 9: Roles

Cryptographic Officer role is implicitly and always assumed.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Expand AES Key	Expand AES key to round keys.	API return value: 0 (Success)	DEK	Round Key	AES-ECB Core 4 AES-ECB Core 16 AES-XTS Core 512 AES-XTS Core 520	Cryptographic Officer - DEK: W,E - Round Key: G,R
Encrypt (512B)	Encrypt data using XTS-AES in units of 512 byte.	API return value: 0 (Success)	Data to encrypt, Round Key	Encrypted data	AES-XTS Core 512	Cryptographic Officer - Round Key: W,E
Decrypt (512B)	Decrypt data using XTS-AES in units of 512 byte.	API return value: 0 (Success)	Data to decrypt, Round Key	Decrypted data	AES-XTS Core 512	Cryptographic Officer - Round Key: W,E
Encrypt (520B)	Encrypt data using XTS-AES in units of 520 byte.	API return value: 0 (Success)	Data to encrypt, Round Key	Encrypted data	AES-XTS Core 520	Cryptographic Officer - Round Key: W,E
Decrypt (520B)	Decrypt data using XTS-AES in units of 520 byte.	API return value: 0 (Success)	Data to decrypt, Round Key	Decrypted data	AES-XTS Core 520	Cryptographic Officer - Round Key: W,E
Encrypt (ECB 16B)	Encrypt 16 byte data using AES-ECB.	API return value: 0 (Success)	Data to encrypt, KEK	Encrypted data	AES-ECB Core	Cryptographic Officer - KEK: W,E
Decrypt (ECB 16B)	Decrypt 16 byte data using AES-ECB.	API return value: 0 (Success)	Data to decrypt, KEK	Decrypted data	AES-ECB Core	Cryptographic Officer - KEK: W,E
Encrypt (ECB 64B)	Encrypt 64 byte data using AES-ECB.	API return value: 0 (Success)	Data to encrypt, DEK	Encrypted data	AES-ECB Core 4	Cryptographic Officer - DEK: W,E
Decrypt (ECB 64B)	Decrypt 64 byte data using AES-ECB.	API return value: 0 (Success)	Data to decrypt, DEK	Decrypted data	AES-ECB Core 4	Cryptographic Officer - DEK: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Encrypt (ECB 256B)	Encrypt 256 byte data using AES-ECB.	API return value: 0 (Success)	Data to encrypt, DEK	Encrypted data	AES-ECB Core 16	Cryptographic Officer - DEK: W,E
Decrypt (ECB 256B)	Decrypt 256 byte data using AES-ECB.	API return value: 0 (Success)	Data to decrypt, DEK	Decrypted data	AES-ECB Core 16	Cryptographic Officer - DEK: W,E
Wrap Key	Wrap a key using a KEK.	API return value: 0 (Success)	Key, KEK	Wrapped key	AES-KW Core	Cryptographic Officer - KEK: W,E
Unwrap Key	Unwrap a key using a KEK.	API return value: 0 (Success)	Wrapped key, KEK	Unwrapped key	AES-KW Core	Cryptographic Officer - KEK: W,E
Generate Hash	Generate hash value from inputted data.	API return value: 0 (Success)	Data to hash	Hash Value	Secure Hash	Cryptographic Officer
Initialize	Startup the module.	None	None	None	None	Cryptographic Officer
Show Status	Show module ID, version, and status.	None	None	Module ID, module version, module status	None	Cryptographic Officer
Enable CSP Output	Enable CSPs output in plaintext.	None	None	None	None	Cryptographic Officer
Disable CSP Output	Disable CSPs output in plaintext.	None	None	None	None	Cryptographic Officer
Forcibly Stop	Change the module state to Error state.	None	None	None	None	Cryptographic Officer
Reset	Reset the module.	None	None	None	None	Cryptographic Officer
Zeroise	Cycle the power of the operational environment.	None	None	None	None	Cryptographic Officer - DEK: Z - Round Key: Z - KEK: Z
On-demand integrity test	Initiate the integrity test on demand by power cycle of the operational environment.	None	None	None	None	Cryptographic Officer
On demand self test	Initiate the self-tests on demand by power cycle of the operational environment or performing the Reset service, and performing the Initialize service.	None	None	None	None	Cryptographic Officer

Table 10: Approved Services

The module provides only approved services. Accordingly, API return codes that confirm the successful completion of these services serve as the indicators. All approved services implemented by the module are listed in above. Each service description also describes all usage of SSPs by the service. The access rights to keys and/or SSPs modes shown in the table are defined as:

- G = Generate: The module generates or derives the SSP.
- R=Read: The SSP is read from the module (e.g., the SSP is output).

- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module executes using the SSP in performing a cryptographic operation.
- Z = Zeroise: The module zeroises the SSP.

“AES-ECB Core 4”, “AES-ECB Core16”, “AES-XTS Core 512” and “AES-XTS Core 520” use a common AES key expansion implementation specified in Section 5.2 of FIPS 197 to generate a set of the round keys as part of encryption/decryption process. “Expand AES Key” service also utilizes the same AES key expansion implementation and provides only the round key generation function.

“Enable CSP Output” service shall be executed before execution of “Expand AES Key” service.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

External firmware can be loaded through a complete image replacement of SVOS10. The new firmware image is executed after the module transitions through a power-on reset. All SSPs are zeroised prior to execution of the new image. A complete image replacement constitutes an entirely new module. Administrators of the module can obtain ID and version of the module as described in Chapter 11.2 to verify that the new module is validated version of the module.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of CRYPTLOAD (the firmware component of the module) is tested by comparing a SHA2-256 digest value calculated at startup with the SHA2-256 digest value stored in the module that was calculated at compile.

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 power cycle of the operational environment of the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The module does not store SSPs in persistent storage. SSPs are temporarily stored in process memory when the module is being used. The module has control over its own SSPs. The

operational environment is a single-process system and provides the time separation of the process memory. When the process memory is used by the module, no other process or component can concurrently access the memory.

There are no security rules settings or restriction to the configuration of the operational environment.

7 Physical Security

7.1 Mechanisms and Actions Required

N/A for this module.

The module is a multi-chip embedded cryptographic module and conforms to Level 1 requirements for physical security. The cryptographic module consists of production-grade components.

8 Non-Invasive Security

N/A. The module does not implement non-invasive security techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Memory	A volatile memory on the operational environment	Dynamic

Table 11: Storage Areas

The module does not store SSPs in persistent storage. SSPs are temporarily stored in process memory when the module is being used.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API Input	Memory area specified in the API parameters	Memory area for the module	Plaintext	Manual	Electronic	
API Output	Memory area for the module	Memory area specified in the API parameters	Plaintext	Manual	Electronic	

Table 12: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power cycle	Power cycle of the operational environment	All SSPs of the module are zeroised by Power cycle because all SSPs are on a volatile memory.	Yes

Table 13: SSP Zeroization Methods

Administrators of the module can zeroise all SSPs of the module by power cycle of Hitachi storage system. Power cycle can be done in Maintenance Utility, which is Management tool of Hitachi storage system. In details, see System Administrator Guide.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KEK	Key encryption key	256 bits - 256 bits	Symmetric Key - CSP			AES-ECB Core AES-KW Core
DEK	Data encryption key	256 bits - 256 bits	Symmetric Key - CSP			AES-ECB Core 4 AES-ECB Core 16 AES-XTS Core 512 AES-XTS Core 520
Round Key	AES round key	1920 bits - 256 bits	Round Key - CSP			AES-ECB Core 4 AES-ECB Core 16 AES-XTS Core 512 AES-XTS Core 520

Table 14: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KEK	API Input	Memory:Plaintext	While the module is executing Encrypt (ECB 16B), Decrypt (ECB 16B), Wrap Key or Unwrap Key.	Power cycle	
DEK	API Input	Memory:Plaintext	While the module is executing Expand AES Key, Encrypt (ECB 64B), Decrypt (ECB 64B), Encrypt (ECB 256B) or Decrypt (ECB 256B).	Power cycle	
Round Key	API Input API Output	Memory:Plaintext	While the module is executing Expand AES Key, Encrypt (512B), Decrypt (512B), Encrypt (520B), Decrypt (520B).	Power cycle	DEK:Derived From

Table 15: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA2-256 (A5024)	SHA2-256	KAT	SW/FW Integrity	None	Hash

Table 16: Pre-Operational Self-Tests

Once the “Initialize” service is called and all Cryptographic Algorithm Self-tests (CAST) are completed, the module automatically performs firmware integrity test using SHA2-256 over the CRYPTLOAD. If the firmware integrity test fails, 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 (512B)	Key sizes: 256 bits	KAT	CAST	None	Encrypt	From the module startup to integrity testing
AES-XTS (512B)	Key sizes: 256 bits	KAT	CAST	None	Decrypt	From the module startup to integrity testing
AES-XTS (520B)	Key sizes: 256 bits	KAT	CAST	None	Encrypt	From the module startup to integrity testing
AES-XTS (520B)	Key sizes: 256 bits	KAT	CAST	None	Decrypt	From the module startup to integrity testing
AES-KW (A5023)	Key sizes: 256 bits	KAT	CAST	None	Wrap	From the module startup to integrity testing
AES-KW (A5023)	Key sizes: 256 bits	KAT	CAST	None	Unwrap	From the module startup to integrity testing
SHA2-256 (A5024)	SHA2-256	KAT	CAST	None	Hash	From the module startup to integrity testing

Table 17: Conditional Self-Tests

When the “Initialize” service is called, the module starts to perform cryptographic algorithm self-tests for XTS-AES mode, AES Key Wrap, AES Key Unwrap and SHA2-256. If one of the self-tests fails, the module enters the error state.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A5024)	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 (512B)	KAT	CAST	On Demand	Manually
AES-XTS (512B)	KAT	CAST	On Demand	Manually
AES-XTS (520B)	KAT	CAST	On Demand	Manually
AES-XTS (520B)	KAT	CAST	On Demand	Manually
AES-KW (A5023)	KAT	CAST	On Demand	Manually
AES-KW (A5023)	KAT	CAST	On Demand	Manually
SHA2-256 (A5024)	KAT	CAST	On Demand	Manually

Table 19: Conditional Periodic Information

Pre-operational self-tests, and cryptographic algorithm self-tests for XTS-AES mode, AES Key Wrap, AES Key Unwrap and SHA2-256 are available on demand by performing the following a) and b); a) Cycle power of the operational environment or execute “Reset” service. b) Execute “Initialize” service.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	A state when the module has encountered an error condition.	Failed the Pre-operational self-tests. Failed the Cryptographic algorithm self-tests.	Power cycling of the operational environment.	Error response to Show Status service.

Table 20: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is integrated into SVOS10. When SVOS10 is installed by the vendor of Hitachi storage system, the module is also installed. To initialize the module, enable the encryption feature of Hitachi storage system (See Encryption License Key Users Guide Chapter 3). No other special procedure is required to securely install and initialize the module.

11.2 Administrator Guidance

Administrators can verify that an ID and a version of the module is identical to the ID (Storage_Encryption_Module_20) and the version (A0-01-00-00). See REST API Reference guide Chapter 17.5 to show an ID and a version of the module.

Administrators can identify the processor by checking the model of storage system. In the case where the model is VSP One B28, the processor is Intel® Xeon® Gold 6421N. For the models VSP One B23, VSP One B24 or VSP One B26, the processor is Intel® Xeon® Silver 4410Y. See REST API Reference guide to show the model of storage system.

All the functions, physical ports, and logical interfaces of the module are available to the Crypto Officer. The module provides only an approved mode of operation. Therefore, no special API calls or settings are required to place the module in an approved mode of operation.

11.3 Non-Administrator Guidance

There are no requirements for non-administrator.

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 1 module.

1. The module shall provide a Cryptographic Officer 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 cycling power of the operational environment.
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 CSPs 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. Two independent internal actions shall be required in order to output any plaintext CSP.

12 Mitigation of Other Attacks

N/A. The module does not provide mitigation of other attacks.