HSSD_V6 Series

Non-Proprietary FIPS 140-2 Security Policy

Version: 2.3

Date: 2022-05-19

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Huawei Technologies Co., Ltd. HSSD_V6 family module, hereafter denoted the Module. The Module is designed to protect unauthorized access to the user data stored in its NAND Flash memories. The built-in AES HW engines in the cryptographic module's controller provide on-the-fly encryption and decryption of the user data without performance loss. The SED's nature also provides instantaneous sanitization of the user data via cryptographic erase.

Due to different capacity the HSSD_V6 series modules contains 3 configurations.

Table 1 - HSSD_V6 Module Configurations

No.	Model	Capacity Size(TB)	Physical Interface	Hardware Platform Version	FW Version
1	HSSD-D7294DL1T9E	1.92	PALM	P34(HIP2EBPD VERA)	1063
2	HSSD-D7294DL3T8E	3.84	PALM	P34(HIP2EBPD VERA)	1063
3	HSSD-D7294DL7T6E	7.68	PALM	P34(HIP2EBPD VERA)	1063

Note: Model refers to the Hardware version of each cryptographic module.

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-2 validated. 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 Module Description and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1 and Figure 2. The Module is a multi-chip standalone embodiment (hardware module). The physical cryptographic boundary consists of two aluminum alloy cases. The top and bottom cases are assembled by screws and a tamper-evident label is applied for detection of any opening of the cases. The core of the cryptographic module is the built-in Huawei-developed controller Hi1812E V110, which provides functions such as data encryption algorithm or random number generation.

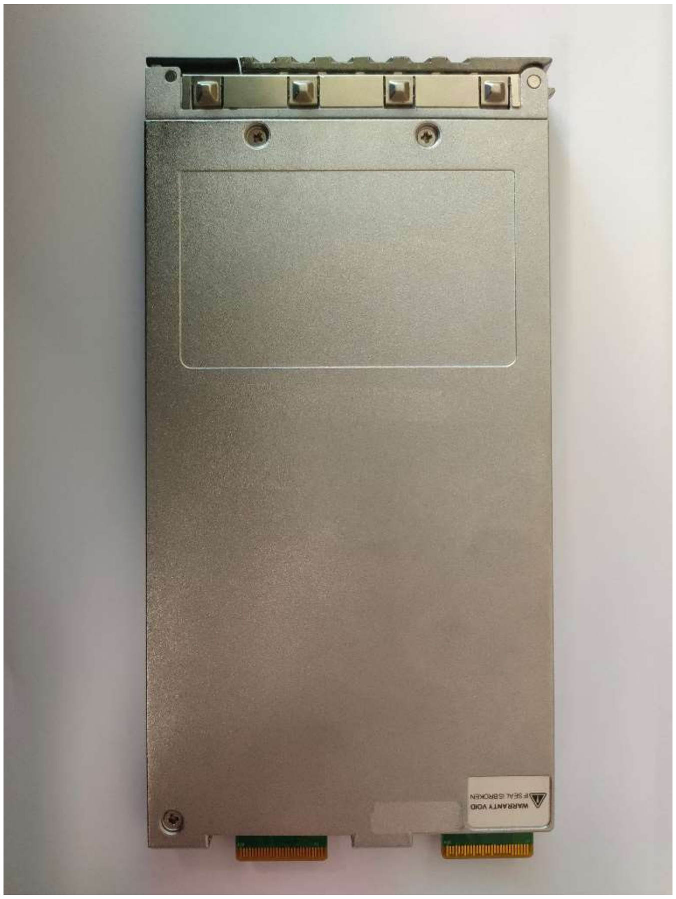

Figure 1 – HSSD_V6 (PALM interface)

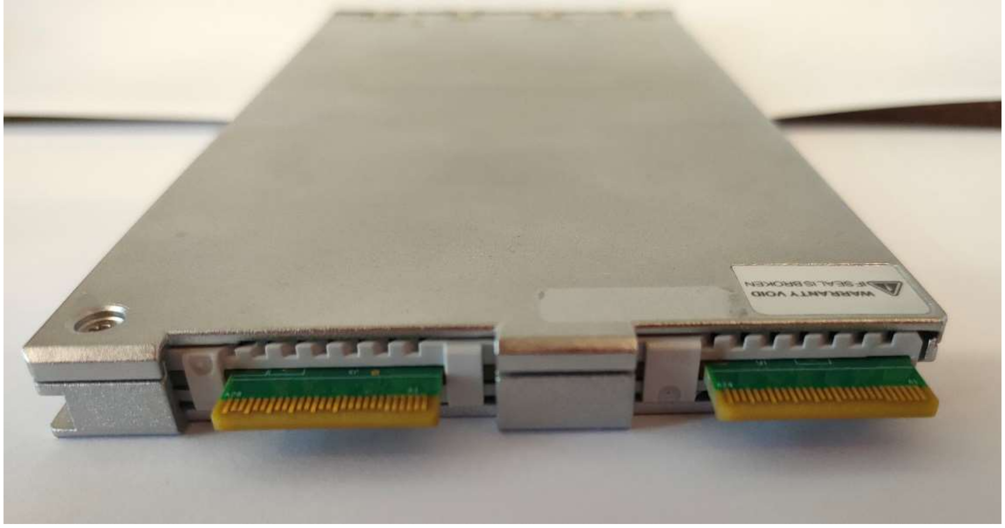

Figure 2 – HSSD_V6 (PALM interface details)

1.2 Logical Cryptographic Boundary

Figure 3 depicts the elements of the logical boundary of the HSSD_V6 family:

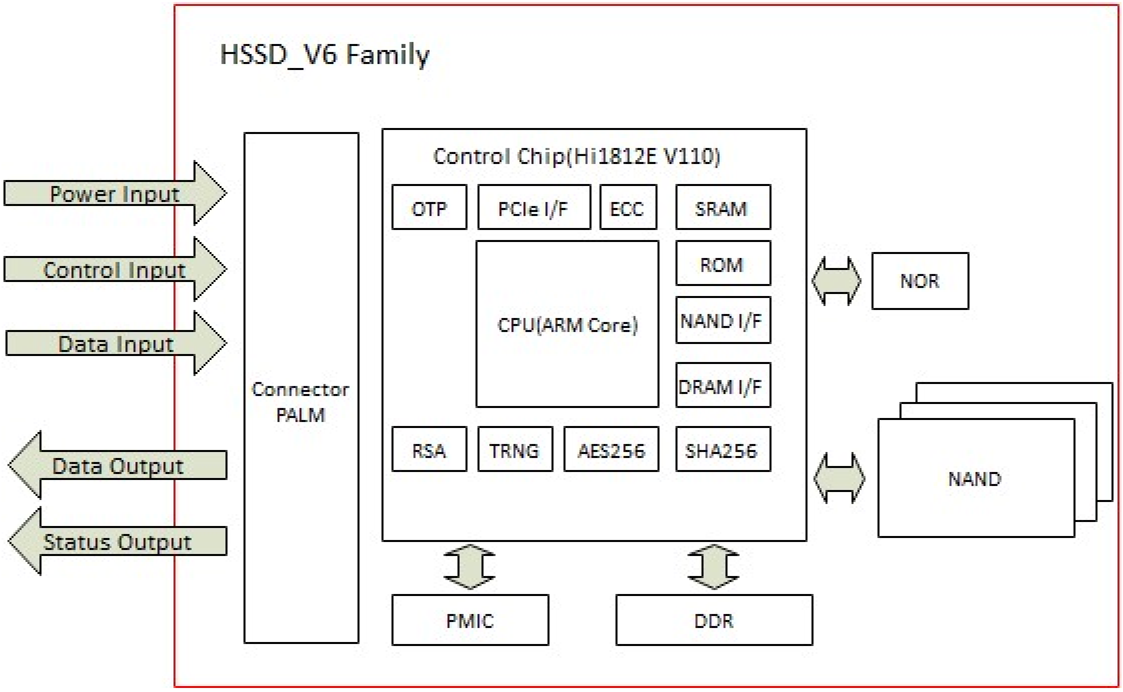

Figure 3 – Module Block Diagram

The TRNG-IP-76 integrated chip is used for key generation and vector initialization or nonces includes a True Random Number Generator (TRNG) compliant with NIST FIPS SP 800-90B as a nondeterministic random number generator used as an entropy source as well as a Deterministic Random Bit Generator (DRBG) compliant with the NIST FIPS SP 800-90A.

1.3 Mode of Operation

The Module operates always in a FIPS Approved mode of operation. If any of the self-tests fail, the Module enters an error state. The cryptographic module does not allow non-Approved modes. To verify that the Module is in the Approved mode of operation, the Show Status service shall be invoked.

2 Acronyms

The following acronyms are used throughout this document.

Table 3 – Acronyms

Acronyms	Meaning
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
DDR	Double Data Rate SDRAM
DRAM	Dynamic Random Access Memory
DRBG	Deterministic Random Bit Generator
ECC	Error Correction Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FW	Firmware
HUK	Hardware Unique Key
HW	Hardware
KAT	Known Answer Test
KEK	Key Encrypting Key
MEK	Media Encryption Key
MSID	Manufacturing SID
NAND	NAND Flash Memory, NAND is short for "NOT AND", a boolean operator and logic gate
NOR	NOR Flash Memory, NOR is short for "NOT OR", a boolean operator and logic gate
OTP	One Time Programmable
NVMe	NVM Express, Non-Volatile Memory Express
PCIe	PCI Express, Peripheral Component Interconnect Express

PIN	Personal Identification Number
PMIC	Power Management Integrated Circuit
PSID	Physical Presence SID
PSP	Public Security Parameter
ROM	Read-Only Memory
SED	Self-Encrypting Drive
SID	Security Identifier
SRAM	Static Random Access Memory
TCG	Trusted Computing Group
TRNG	True Random Number Generator
UID	Unique Identifier
Hi1812E	Name of the main control chip in the module
V110	Version of the control chip

3 Cryptographic Functionality

3.1 Approved Algorithms

Table 4 – Approved Algorithms

Implementation type	Chip involved	Cert	Algorithm	Standard	Mode	Description	Functions/ Caveats
HARDWARE	HI1812E V110	#A1478	AES	FIPS SP 800-38E	XTS	Key size: 256 bits	Encrypt/Decrypt
		# A1478	AES	FIPS SP 800-38A	ECB	Key Size: 256 bits	Encrypt/Decrypt Note: AES-ECB is a prerequisite for AES-XTS; AES-ECB is not supported by the cryptographic module
		# A1478	SHS	FIPS 180-4	SHA-256	SHA-256	Message Digest
		# A1478	RSA	FIPS 186-4	PKCS1_V1.5	n = 2048 SHA-256	Digital Signature Verification

	TRNG-IP-76	# A1478	AES	FIPS SP 800-38A	ECB	Key size: 256	Encrypt
		# A1478	SHS	FIPS 180-4	SHA-256	Input message length = 512*n+256 (n=1,2,3,4,…, 31)	Message Digest Requirement from section 3.1.5.2 of SP 800-90. Vetted conditioning component.
		# A1478	DRBG	FIPS SP 800-90A	CTR	Without derivation function Security Strength = 256	Deterministic Random Bit Generator
		N/A	ENT(P)	FIPS SP 800-90B		Entropy Source	Nondeterministic Random Bit Generator
Firmware	HI1812E V110	# A1479	SHS	FIPS 180-4	SHA-256	SHA-256	Message Digest
		# A1479	HMAC	FIPS 198-1	HMAC with SHA-256	Key size = 128 bits Mac Size= 32 bytes	Message Authentication
		# A1479	PBKDF	FIPS SP 800-132		HMAC SHA-256 Salt = 32 bytes DRBG generated Iteration count=1000 to Authentication Iteration count=1500 to Generate KEK	Secrets Protection and Key Generation

						Option 2a Key length = 256 bits	
		# A1479	AES	FIPS SP 800-38F	KW	Key size = 256 bits	Encrypt/Decrypt
		# A1479	AES	FIPS SP 800-38A	ECB	Key Size = 256 bits	Encrypt/Decrypt Note: AES-ECB is a prerequisite for the Key Wrapping algorithm. AES-ECB is not supported by the cryptographic module

Note: AES-XTS compliant with FIPS 140-2 Implementation Guidance A.9.

Note: the PBKDF algorithm is only used for internal pins and keys storage according FIPS SP 800-132.

Note: the entropy source from the TRNG IP-76 provides an overall amount of entropy of 1 bit per output bit and an estimated amount of entropy of 1 bit per output bit.

3.2 Vendor Affirmed Algorithms

Table 5 – Vendor Affirmed Algorithms

Cert	Algorithm	Standard	Description	Functions/Caveats
vendor affirmed	CKG (per FIPS IG D.12)	FIPS SP 800-133	key generation using unmodified approved RBG output	Key Generation

3.3 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 5.3.

Table 6 – Critical Security Parameters (CSPs)

CSP	Description / Usage
Cryptographic Officer PIN	Generation: Authentication data of CO role, the allowed length is 256 bits, generated by the operator. Storage: CO Pin plaintext is an input for the module during CO role authentication. The module uses the PBKDF algorithm to generate an

CSP	Description / Usage
	obscured value of the CO PIN, then uses the Key Wrapping approved algorithm to encrypt the data to generate the CO PIN ciphertext, and saves the ciphertext to the NOR flash. Description: The default value is MSID. Zeroization: For details, see Table 13 – Security Parameters Access by Service.
User PIN (32 total)	Generation: Authentication data of User role, the allowed length is 256 bits, generated by the operator. Storage: User Pin plaintext is input for the module during User role authentication. The module uses the PBKDF algorithm to generate an obscured value of the User PIN, then uses the Key Wrapping approved algorithm to encrypt the data to generate the User PIN ciphertext, and saves the ciphertext to the NOR flash. Description: The default value is MSID. Each User role has an independent PIN. Zeroization: For details, see Table 13 – Security Parameters Access by Service.
MEK (32 total)	Generation: generated from the DRBG, 512 bits. Storage: module uses the Key Wrapping approved algorithm to encrypt MEK, and saves the MEK ciphertext to the NOR flash. Description: use as the key of AES-256-XTS for encrypting and decrypting user data. Each MEK is only associated with one LBA band. Zeroization: For details, see Table 13 – Security Parameters Access by Service.
KEK (32 total)	Generation: SP 800-132 PBKDF output; 256 bits, derived from User PINs and 256-bit KEK Salt. Storage: module uses the Key Wrapping approved algorithm to encrypt KEK, and saves the KEK ciphertext to the NOR flash. Description: use as the key of the Key Wrapping algorithm for encrypting and decrypting the MEKs. One-to-one mapping between KEKs and MEKs. Zeroization: For details, see Table 13 – Security Parameters Access by Service.
HUK	Generation: generated from the DRBG, 256 bits. Storage: programmed in OTP memory. Description: use as the key of the Key Wrapping approved algorithm for encrypting and decrypting the Key parameter (Salt, KEK, PSID and PIN digests). Zeroization: HUK can be zeroized via “Zeroize HUK” service. Each bit of the HUK is programmed to 1. After the HUK is zeroized, the module can’t be used. In addition, when module power up, the module will detect the HUK zeroized state and enter an error state.

CSP	Description / Usage
Erase Master PIN	Generation: Authentication data of Erase Master role, the allowed length is 256 bits, generated by the operator. Storage: Erase Master Pin plaintext is an input for the module during role authentication. The module uses the PBKDF algorithm to generate an obscured of the PIN, then uses the Key Wrapping algorithm to encrypt the data to generate the PIN ciphertext, and saves the ciphertext to the NOR flash. Description: The default value is MSID. Zeroization: For details, see Table 13 – Security Parameters Access by Service.
Salt	Generation: generated from DRBG, 256 bits. Storage: encrypted by Key Wrapping algorithm and saved the ciphertext to the NOR flash. Description: Input of SP 800-132 PBKDF. Zeroization: For details, see Table 13 – Security Parameters Access by Service.
DRBG Internal State	Generation: via SP800-90A CTR DRBG. Storage: Not persistently stored. Description: The values of V and Key. Zeroization: via “Module Reset” service.
DRBG Entropy Input	Generation: via SP800-90B TRNG entropy source. Storage: Not persistently stored. Description: used to generate seed. Zeroization: via “Module Reset” service.
DRBG Seed	Generation: via SP800-90A CTR DRBG. Storage: Not persistently stored. Description: used to instantiate DRBG. Zeroization: via “Module Reset” service.

3.4 Public Security Parameters

Table 7 – Public Security Parameters (PSPs)

Key	Description / Usage
RSA Public Key	Generation: externally generated. Storage: plaintext header of firmware image. Description: Public key of a 2048-bit RSA key pair used to verify the digital signature of a firmware image. Zeroization: N/A.
MSID	Generation: MSID is generated during disk manufacturing, 256 bits. Storage: MSID is stored in the NOR flash in plaintext.

Key	Description / Usage
	Description: MSID is the initial authentication data for all operator roles (except PSID and FW loader). The host can obtain the MSID plaintext through the TCG protocol command. Zeroization: N/A.
PSID	Generation: PSID is generated during disk manufacturing, the allowed length is 256 bits. Storage: The module uses the PBKDF algorithm to generate an obscured value of the PSID, uses the Key Wrapping algorithm to encrypt the data to generate the PSID ciphertext, and saves the ciphertext to the NOR flash. Description: PSID is the authentication data for PSID role. The plaintext of PSID is printed on the disk's nameplate. Zeroization: N/A.

4 Physical Ports and Logical Interfaces

The module's physical interface and logical interface categories are as follows.

Table 8 – Ports and Interfaces

Physical Interface	Logical Interface
PALM	Data Input Data Output Control Input Status Output Power Input

5 Roles, Authentication and Services

5.1 Assumption of Roles

The module supports only one operator, and the operator supports 5 distinct operator roles, CO, Erase Master, User, PSID and FW loader. The cryptographic module enforces the separation of roles using role-based authentication.

Table 9 lists all operator roles supported by the module. The Module does not support a maintenance role and/or bypass capability. The module does not support concurrent operators.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
Cryptographic Officer	A Cryptographic Officer role that initializes the Cryptographic Module and authorizes Firmware download as well as executing OTP zeroization	Role-based	64-bit UID and Cryptographic Officer PIN
Erase Master	After successful authentication, this role can execute Erase Band and Set PIN service	Role-based	64-bit UID and Erase Master PIN
User (32)	The Band Master [0-31] Authority is a User role that controls read/write access to LBA Bands	Role-based	64-bit UID and User PIN
PSID	After successful authentication, the PSID role can execute the Revert service	Role-based	64-bit UID and PSID
FW loader	Firmware download role in charge of performing the Firmware Download service	Role-based	2048 RSA public key

5.2 Authentication Methods

The authentication mechanism allows 256-bit length PIN, for the Cryptographic Officer/Erase Master/User and PSID role supported by the module, which means a single random attempt can succeed with the probability of $1/2^{256}$, which is much less than the FIPS 140-2 requirement 1/1,000,000. Each authentication attempt takes at least 7ms. Therefore, the number of attempts for one minute cannot exceed 8572 (60*1000/7). Therefore, the probability of multiple random attempts to succeed in one minute is $8572/2^{256}$, which is much less than the FIPS 140-2 requirement 1/100,000.

The authentication mechanism for FW Loader role is RSA PKCS1_V1.5-2048 with SHA256 digital signature verification, which means a single random attempt, can succeed with the probability of $1/2^{112}$, which is much less than the FIPS 140-2 requirement 1/1,000,000. Each RSA Signature Verification authentication attempt takes at least 10ms. Therefore, the number of attempts for one minute cannot exceed 6000 ((60*1000)/10). Therefore, the probability of multiple random attempts to succeed in one minute is $6000/2^{112}$, which is much less than the FIPS 140-2 requirement 1/100,000.

Table 10 – Authentication Description

Role	Authentication Method	Probability
Cryptographic Officer Erase Master User PSID	256-bit authentication data	-Probability of $1/2^{256}$ in a single random attempt -Probability of $8572/2^{256}$ in multiple random attempts in a minute
FW loader	RSA Signature Verification	-Probability of $1/2^{112}$ in a single random attempt -Probability of $6000/2^{112}$ in multiple random attempts in a minute

5.3 Services

All services implemented by the Module are listed in the Table 11 and Table 12. For unauthenticated services defined in Table 12, any of the provided services can be executed for each role but authentication is not required.

Table 11 – Authenticated Services

Service	Description	CO	ERASE MASTER	User	PSID	FW loader
Lock/Unlock Firmware Download Control	Deny/Permit access to Firmware Download service	√				
Set PINs	This service can change roles' PIN. For User roles, Set PIN will generate new KEK and salt to replace the old data. Once the KEK is changed, the MEK needs to be re-encrypted by new KEK for storage.	√	√	√		
Set Band	Set the starting location, size, and attributes of a set of contiguous Logical Blocks			√		
Lock/Unlock User Band	Deny/Permit access to a LBA Band			√		

Service	Description	CO	ERASE MASTER	User	PSID	FW loader
Erase Band	Band cryptographic-erasure by changing LBA band encryption keys to new values. Erasing an LBA band with Erase Master sets the TCG Credential to the default value.		√			
Revert	Revert method to return the Cryptographic Module to its original manufactured state; authentication data (PSID) is printed on the external label				√	
Firmware Download	Load and utilize RSA2048 PKCS1.5 and SHA-256 to verify the entire firmware image. If the self-tests complete successfully, the SED executes the new code. Unlocking the Firmware Download Control enables the downloading of firmware.					√
Zeroize HUK	Each bit of the HUK is programmed to 1. After the HUK is zeroized, the module can’t be used. In addition, the module detects whether the HUK has been zeroized at power up.	√				
Read/Write	Read/write user data from/to user band			√		

Table 12 - Unauthenticated Services

Service	Description
Authenticate	Input a TCG Credential for authentication
Module Reset	Reset the Module by power cycle
Get MSID	Get default TCG PIN installed during manufacturing

Self-Test on demand	The Cryptographic Module performs self-tests by power cycle of the module
Start Session	Start TCG session
End Session	End a TCG session by clearing all session state
Generate Random	TCG Random method generates a random number from the NIST FIPS SP 800-90A DRBG
IF-RECV	NVMe Security Receive command which provides a method to receive responses for the TCG protocol
IF-SEND	NVMe Security Send command which provides a method to send requests for the TCG protocol
Show status	To verify that the Module is in the Approved mode of operation and retrieve the firmware version.

Table 13 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP.
- R = Read: The service Read and uses the CSP in an algorithm.
- 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 service zeroizes the CSP.

Table 13 – Security Parameters Access by Service

Service	CSPs and PSPs												
	Cryptographic Officer PIN	User PIN	MEK	KEK	HUK	Erase Master PIN	Salt	DRBG Internal State	DRBG Entropy Input	DRBG Seed	RSA Public Key	MSID	PSID
Authenticate	R	R	-	-	R	R	R	-	-	-	-	-	-
Firmware Download	-	-	-	-	-	-	-	-	-	-	R	-	-

Service	CSPs and PSPs												
	Cryptographic Officer PIN	User PIN	MEK	KEK	HUK	Erase Master PIN	Salt	DRBG Internal State	DRBG Entropy Input	DRBG Seed	RSA Public Key	MSID	PSID
Set PINs	W	W	-	GZW	R	W	GZW	R	R	R	-	-	-
Lock/Unlock User Band	-	-	ZW	-	-	-	-	-	-	-	-	-	-
Erase Band	-	ZW	GZW	GZW	R	-	GZW	R	R	R	-	R	-
Revert	ZW	ZW	GZW	GZW	R	ZW	GZW	R	R	R	-	R	R
Module Reset	-	-	R	R	-	-	-	Z	Z	Z	-	-	-
Get MSID	-	-	-	-	-	-	-	-	-	-	-	R	-
Generate Random	-	-	-	-	-	-	-	R	R	R	-	-	-
Zeroize HUK	-	-	-	-	Z	-	-	-	-	-	-	-	-
Read/Write			R										
Set Band Self-Test Start Session End Session IF-RECV IF-SEND Show Status Lock/Unlock Firmware Download Control	-	-	-	-	-	-	-	-	-	-	-	-	-

6 Self-tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the module.

All algorithm Known Answer Tests (KATs) are completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters an error state. To clear the error condition, the cryptographic module must be rebooted by invoking the Module Reset service. The module performs the following algorithm KATs on power-up.

Table 14 – Self-Tests

Test Type	Algorithm	Mode	Self-Test Type	Functions/Caveats
Cryptographic algorithm test	HW AES [197]	ECB [38A]	power-up test	Encrypt, Decrypt, used by AES-XTS
		XTS [38E]	power-up test	Encrypt, Decrypt
Cryptographic algorithm test	HW SHA	SHA-256	power-up test	Message Digest
Cryptographic algorithm test	HW RSA [186]	PKCS1_v1.5	power-up test	Signature Verification
Cryptographic algorithm test	HW AES [197]	ECB	power-up test	Encrypt, used by DRBG CTR of TRNG-IP-76
Cryptographic algorithm test	HW SHA	SHA-256	power-up test	Message Digest, used as Vetted Conditioning Component in TRNG-IP-76 as specified in SP 800-90B
Cryptographic algorithm test	FW AES	KW	power-up test	Key wrap, unwrap using AES 256 bit
Cryptographic algorithm test	FW SHA	SHA-256	power-up test	Message Digest
Cryptographic algorithm test	FW HMAC	SHA-256	power-up test	Generation, Verification
Cryptographic algorithm test	FW PBKDF		power-up test	Key Derivation
Firmware integrity test	HW RSA with SHA-256		power-up test	Perform integrity test and signature verification test on firmware when power up

Continuous random number generator test	Entropy source health tests		power-up test	APT and RCT during the start-up of the entropy source as specified in SP 800-90B
Firmware load test	HW RSA with SHA-256		conditional test	Perform integrity test and signature verification test on firmware when firmware update
Continuous random number generator test	Entropy source health tests		conditional test	APT and RCT during the normal running of the entropy source as specified in SP 800-90B
Critical function test	DRBG CTR Health tests		power-up test	Instantiate, Generate and Reseed functions as specified in SP 800-90A
Critical function test	OTP memory test		power-up test	Check if the OTP memory has been zeroized
Critical function test	OTP memory test		conditional test	Check if the OTP memory has been zeroized

Note: the AES-ECB with cert. #A1479 is not self-tested, as allowed per section 9.4 Known Answer Tests for Cryptographic Algorithms, comment #4 from the [IG] document, since it is the underlying of the Key Wrapping algorithm. Forward and inverse cipher functions are executed for the Key Wrapping algorithm.

7 Physical Security Policy

The HSSD_V6 Series devices are applied with one tamper evident seal as an extra security measure. The three modules listed in Table - 1 HSSD_V6 Module Configuration include the feature. The cryptographic modules are delivered with a tamper-evident seal installed and ready to operate in the FIPS approved mode of operation. One tamper-evident seal that is intact will look smooth and uniform. Its edges will be firmly adhered to the surface of the drive. Careful scrutiny of the seal should reveal whether or not the seal has been tampered with. Attempts to remove the seal may be manifested by one or more of the following indicators in Table 15.

Table 15 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seal	12 months	One tamper-evident seal that is intact will look smooth and uniform. Its edges will be firmly adhered to the surface of the drive. Careful scrutiny of the seal should reveal whether or not the seal has been tampered with. Attempts to remove the seal may be manifested by one or more of the following indicators: 1. The adhesive layer is separated or non-uniform, leaving a visible pattern. 2. The seal's surface has blistered, bubbled up, or has bumps beneath it, and is no longer smooth or flat. Surface irregularities can be highlighted by tilting the seal back and forth in the light. 3. Edges of seal are lifted, or will not stay adhered. The seal will lift very easily by gently sliding a pick or fingernail under its edge. 4. Residue of adhesive is visible around edges of seal indicating the seal has been removed and replaced.

Note: If a tamper evident mark is revealed, the module must not be used and Huawei must be contacted.

7.1 Tamper-Evident Seals and Locations

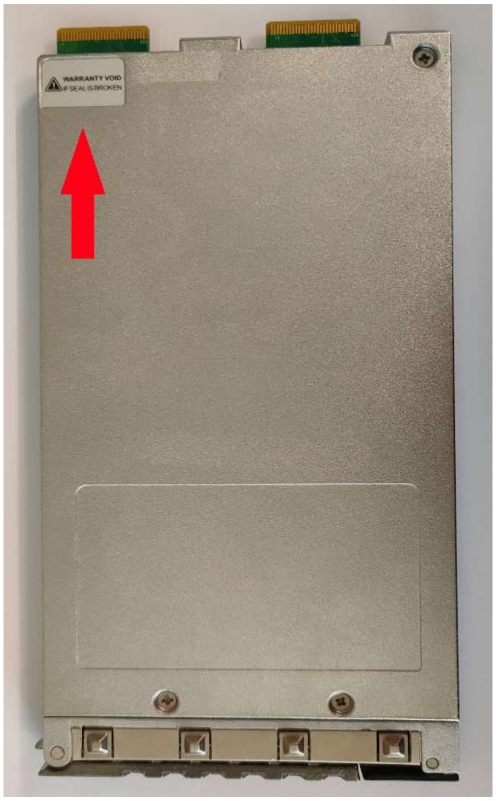

Figure 4 – Tamper-Evident Seal in PALM

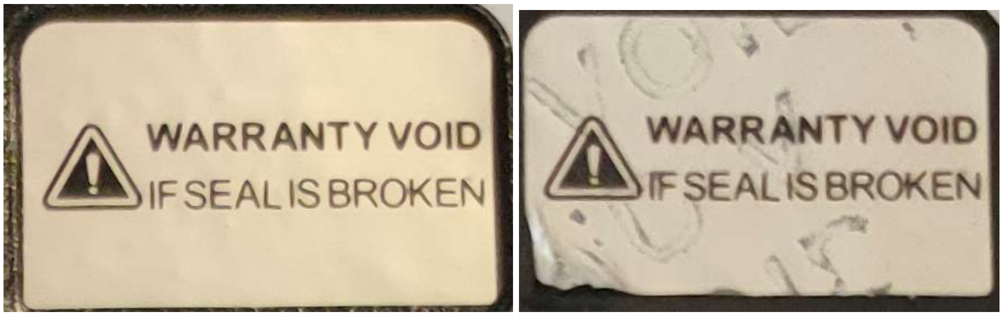

Figure 5 – Tamper-Evident Seal

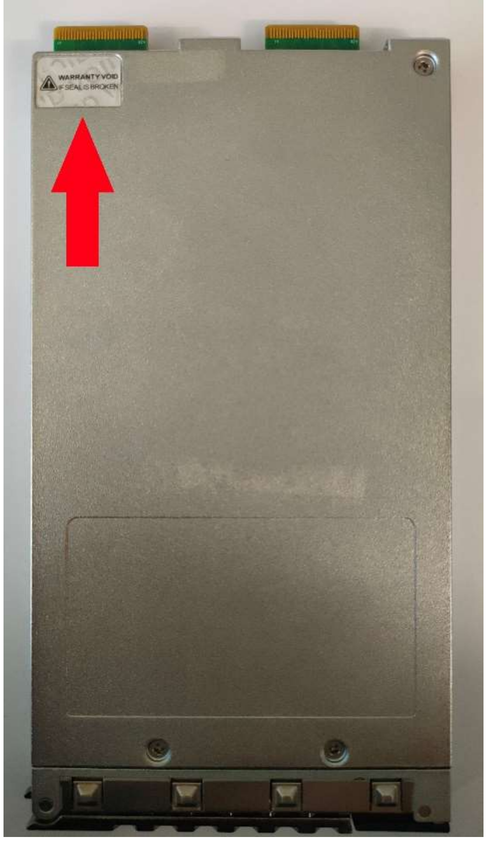

Figure 6 – Tamper-Evident Seal Broken in PALM

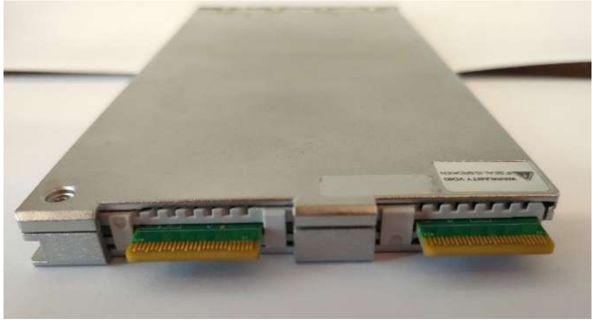

Figure 7 – Tamper-Evident Seal in PALM

8 Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC)

The HSSD_V6 series have been independently tested and issued the FCC&IC SDoC statement No. FI-06065088.

9 Operational Environment

The operating environment is non-modifiable. While the Module is operational, the environment cannot be modified; the code working set cannot be added, deleted or modified. Parts of the Firmware can be upgraded with an authenticated download service. If the download operation is successfully authorized and verified, then the Module will begin operating with the new code working set after successful completion of the Reset service.

10 Mitigation of Other Attacks Policy

The cryptographic module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2.

11 Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

11.1 Secure Installation

1. Crypto Officer shall examine the tamper evident seal
   Inspect the entire perimeter and if there is any sign of tampering, do not use the product and contact Huawei.
2. Insert disk into Host
   Ensure that the hard disk is correctly inserted into the host.
3. Power on
   The disk is automatically powered on after being inserted into the host.
4. Check FW Version
   The cryptographic module is always in the FIPS Approved mode of operation. Invoke the Show Status service to verify that the module is in the Approved mode of operation. The FW version must match 1063 and the critical warning value 0. If not, don't use the disk.
5. Change role's PIN
   CO, Erase Master and User roles pins shall be changed first time that the cryptographic module is powered on.
   Periodically change these role's pin must be performed.
6. Lock the Firmware Download using the Lock Firmware Download Control Service.
7. Lock all the User Bands using the Lock User Band Service.

11.2 Security rules

1. Perform Lock/Unlock Firmware Download Control Service
   When firmware download is needed, perform Unlock Firmware Download Control Service to permit access to Firmware Download service.

After firmware downloaded, perform Lock Firmware Download Control Service to deny access to Firmware Download service.

2. Perform Lock/Unlock User Band Service.
   First, perform Unlock User Band Service to permit access to Read/Write Service.
   After read/write, perform Lock User Band Service to deny access to Read/Write Service.
3. Periodically examine the tamper evident seal
   Ensure that the disk is not tampered during running.
4. To clear Critical Error 1 and Critical Error 2, restart the module, if the error persists, you are advised to send the module back to the manufacturer for repair.

Note: 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 140-2 validation.

11.3 Other Guidance

1. The module clears previous authentications on power cycle.
2. An operator does not have access to any authenticated services prior to assuming an authorized role.
3. The module allows the operator to initiate power-up self-tests by power cycling or resetting the module.
4. Power up self-tests do not require any operator action.
5. Data output is inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. There are no restrictions on which keys or CSPs are zeroized by the zeroization services. If HUK is zeroized, the user data can’t be restored, and module is no longer available.
8. The module supports only one operator.
9. The module does not support a maintenance interface or role.
10. The module does not output intermediate key values.
11. The End Session service deletes all ephemeral operator roles authentication data. The Module requires operator roles to re-authenticate upon execution of the End Session service.
12. The module does not provide bypass services or ports/interfaces.
13. If the Revert Service is successfully executed, steps 4 and 5 of the Secure Installation need to be done.