Shenzhen IBestChain Technology Co., Ltd.
RIGFORT Pro Blockchain HSM
Non-Proprietary FIPS 140-3 Security Policy

Version: 1.6
Date: October 17, 2024

Table of Contents

List of Tables

List of Figures

1 General

This document defines the Security Policy for the RIGFORT Pro Blockchain HSM, hereafter denoted the Module. The Module is a multiple-chip standalone cryptographic module. It is a security module that supports the encryption algorithm approved by FIPS 140-3 and with physical security protection measures, key management mechanisms, and security features to provide secured and applicable cryptographic services for customer systems. Specifically, the security features include key wrapping, message authentication code (MAC), message digest, data encryption and decryption, digital signature generation and verification, etc.

The FIPS 140-3 security levels for the Module are as follows:

Table 1 – Security Level of Security Requirements

ISO/IEC 24759 section	Security Requirement	Security Level
1	General	3
2	Cryptographic Module Specification	3
3	Cryptographic Module Interfaces	3
4	Roles, Services and, Authentication	3
5	Software/Firmware Security	3
6	Operational Environment	N/A
7	Physical Security	3
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	3
10	Self-Tests	3
11	Life-Cycle Assurance	3
12	Mitigation of Other Attacks	N/A
Overall		3

2 Cryptographic Module Specification

The Module is a hardware cryptographic module. The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated Data Encryption Cryptographic implementation. The Module is intended to be used in customer systems requiring security features include key wrapping, message authentication code (MAC), message digest, data encryption and decryption, digital signature generation and verification, etc.

2.1 Operational Environment

IBestChain Data Encryption cryptographic module is tested on the following operational environment.

Table 2 – Tested Operational Environment

#	Model	Hardware Part Number and version	Firmware version	Distinguishing Features
1	RIGFORT Pro Blockchain HSM	3.4.0	1.4.0	hard metal 1U chassis

NOTE: No Components were excluded from the cryptographic boundary

2.2 Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. The Module is a multiple-chip standalone embodiment. The cryptographic boundary is defined as an entire hardware module, and its physical boundary is defined by the hard metal chassis that surrounds all hardware and firmware of the module. The physical dimensions of the module are 482mm*45.5mm*360mm (W*H*L).

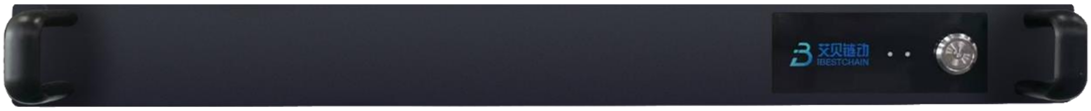


Figure 1 – Front of RIGFORT Pro Blockchain HSM

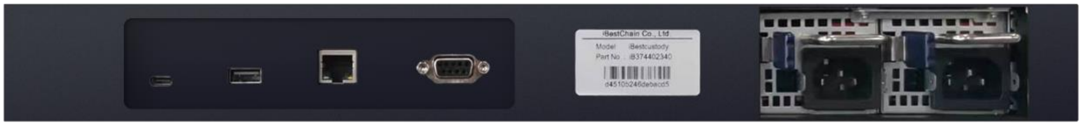


Figure 2 – Back of RIGFORT Pro Blockchain HSM

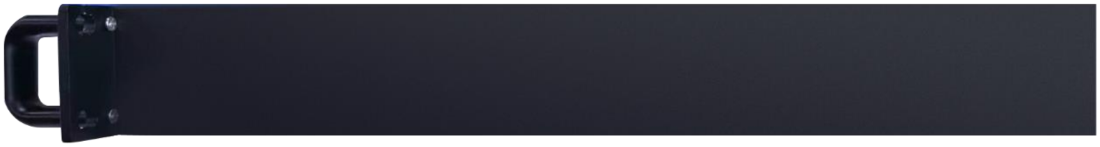


Figure 3 – Right Side of RIGFORT Pro Blockchain HSM

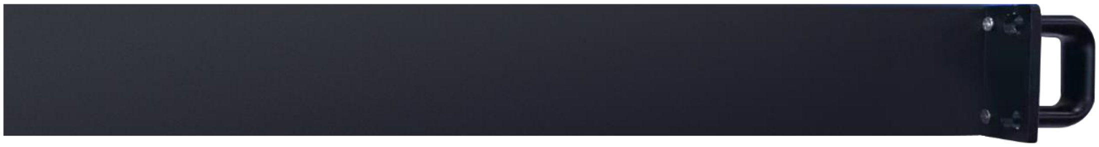


Figure 4 – Left Side of RIGFORT Pro Blockchain HSM

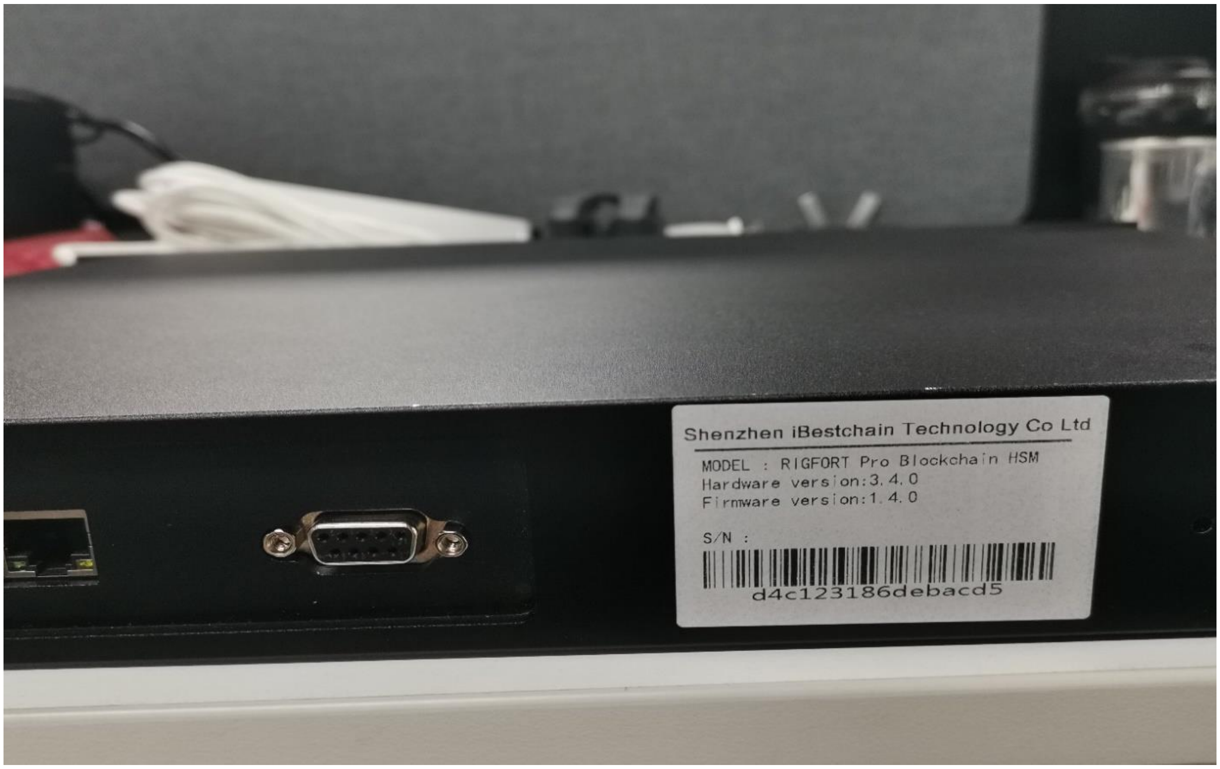

Shenzhen iBestchain Technology Co Ltd
MODEL : RIGFORT Pro Blockchain HSM
Hardware version:3.4.0
Firmware version:1.4.0
S/N :
d4c123186debacd5

Figure 5 – Manufacturer Label Sticker of the Module

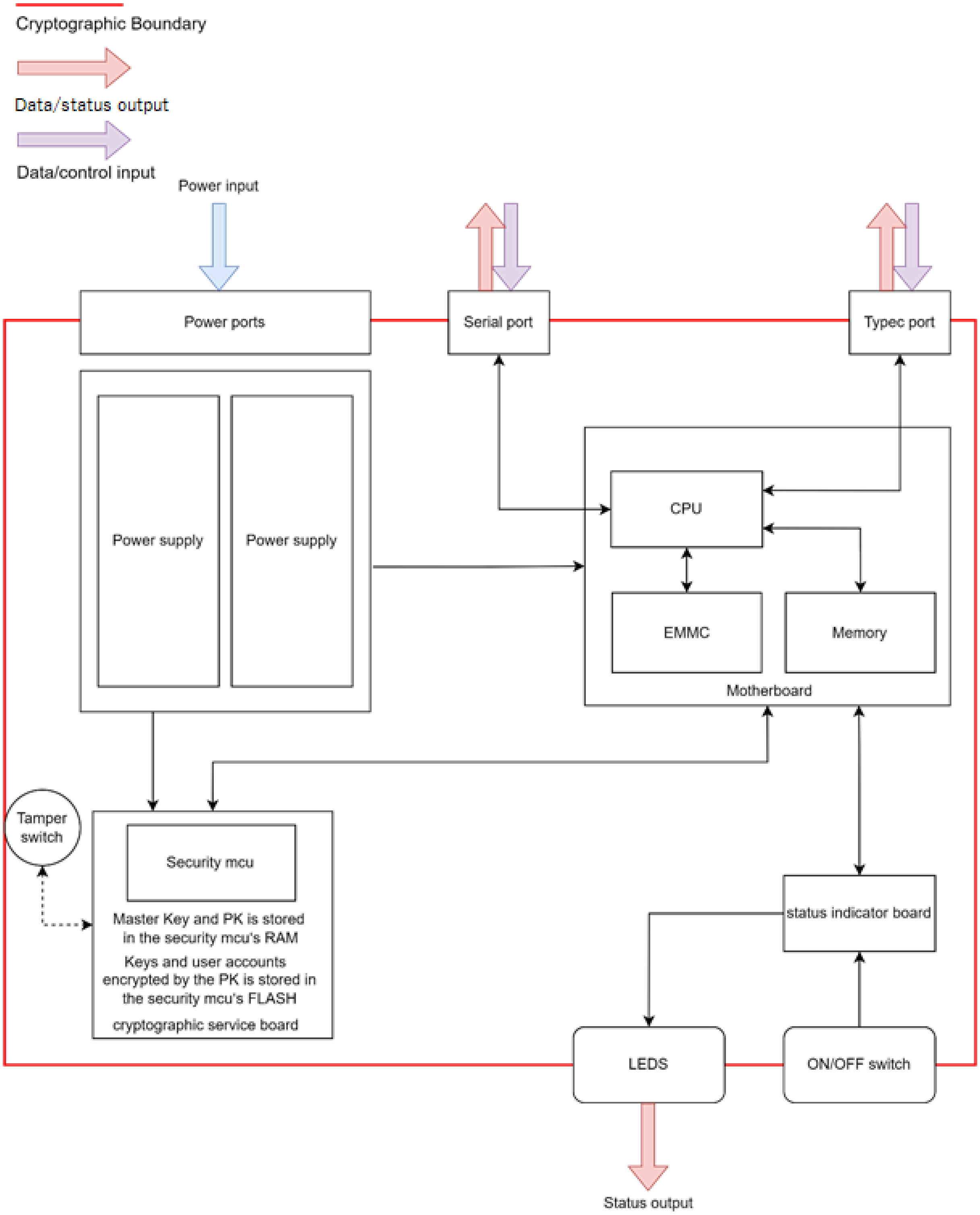


Figure 6 – Cryptographic Boundary Block Diagram

2.3 Modes of Operation

The Module supports both an Approved and non-Approved mode of operation. To verify that the Module is in the Approved mode of operation, the operation mode indicator can be seen on the left side of the management software or check the operation mode status via the menu: Tools → Display Module Status.

Table 3 – Modes of Operation

Name	Description	FIPS [Non-FIPS/FIPS]	Status Indicator
Approved Mode	Normal Operation with only approved services and security functions available	FIPS	See HSM mode in Figure 8
Non-Approved Mode	Non-approved security functions are available	Non-FIPS	See HSM mode in Figure 9

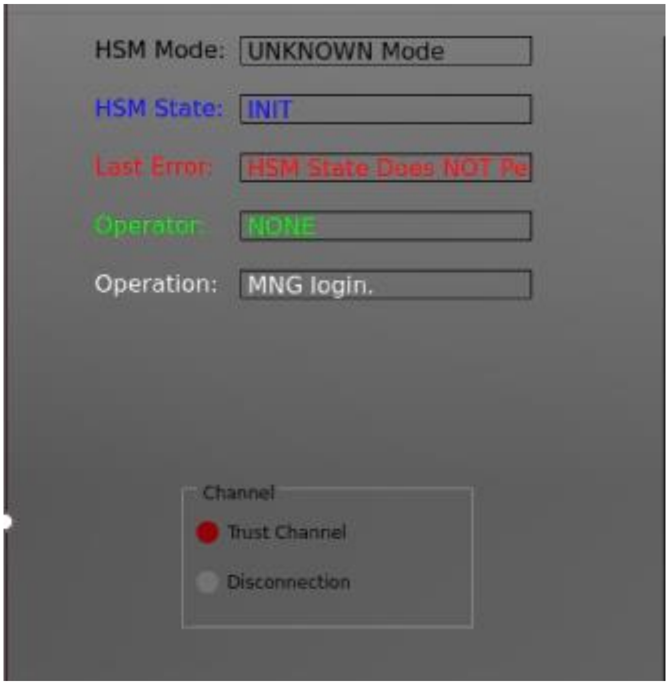
2.3.1 Configuration of the Approved Mode of Operation

The Approved mode of operation is configured at reception of the Module by the CO role who implements the instructions in Section 11.2 Cryptographic Officer Guidance. The operation mode can be selected at initialization through the management software and cannot be changed once selected unless restored to factory settings.

2.3.2 Configuration of the Non-Approved Modes of Operation

The non-Approved mode of operation is configured at reception of the Module by the CO role who implements the instructions in Section 11.2 Cryptographic Officer Guidance. The operation mode can be selected at initialization through the management software and cannot be changed once selected unless restored to factory settings.

In order to switch modes, the CO must perform a reset of the module by selecting from Management Console menu: Tools → Reset HSM, which zeroizes all the SSPs.



HSM Mode: UNKNOWN Mode

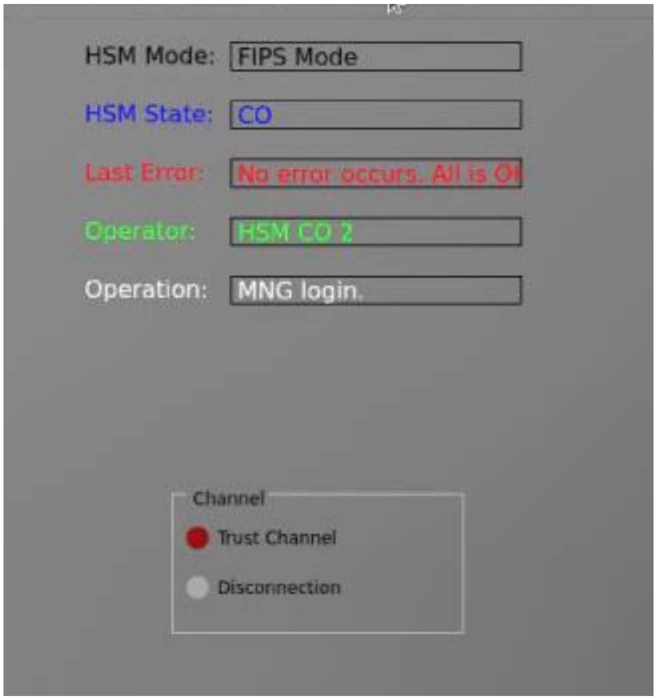
HSM State: INIT

Last Error: HSM State Does NOT Pe

Operator: NONE

Operation: MNG login.

Figure 7 – Management Console - Unknown Mode during Initialization



HSM Mode: FIPS Mode

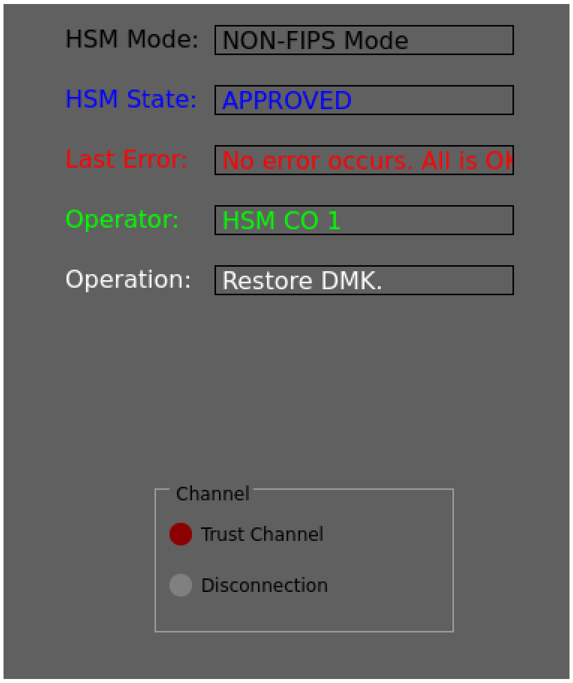
HSM State: CO

Last Error: No error occurs. All is Ol

Operator: HSM CO 2

Operation: MNG login.

Figure 8 – Management Console - Approved Mode



HSM Mode: NON-FIPS Mode

HSM State: APPROVED

Last Error: No error occurs. All is Ok

Operator: HSM CO 1

Operation: Restore DMK.

Channel

● Trust Channel

○ Disconnection

Figure 9 – Management Console - Non- Approved Mode

2.4 Security Functions

The Module implements the Approved and Non-Approved but Allowed cryptographic functions listed in the table(s) below.

Table 4 – Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Strength(s)	Use / Function
A2750	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
A2750	DRBG [90A]	Hash	SHA-256	Deterministic Random Bit Generation Security Strength = 256 bits
A2750	ECDSA [186]	Mode: SHA-256 Curves: P-256	Keys Length: 128	KeyGen
				SigGen
				SigVer
A2750	HMAC [198]	SHA-256	Key Length: 256	Key Derivation for the Session and Session HMAC Keys
A2750	KBKDF [108]	Counter	HMAC-SHA2-256	Key Derivation
A2750	KTS-IFC [56Br2]	Method: KTS-OAEP-Basic; OAEP-Party_V-confirmation Modulus Length: 2048 Hash: SHA2-256	Keys Length: 112	Key Transport: encapsulation and un-encapsulation
A2750	RSA [186]		n = 2048 SHA-256	KeyGen

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Strength(s)	Use / Function
		PKCS1_v1.5	n = 2048 SHA-256	SigGen
		PKCS1_v1.5	n = 2048 SHA-256	SigVer Integrity check
A2750	SHS [180]	SHA2-256		ECDSA, HMAC, RSA, Message Digest ECDSA, RSA Key Generation
A2749	SHS [180]	SHA2-256		Integrity check, Message Digest

Table 5 – Vendor Affirmed Approved Algorithms

Algorithm	Algorithm Properties	OE	Reference
VA	CKG [IG D.H]	[133] Sections 4 and 5.1 Asymmetric signature key generation using unmodified DRBG output	Key Generation
		[133] Sections 4 and 6.1 Direct symmetric key generation using unmodified DRBG output	
		[133] Section 6.2.2 Derivation of symmetric keys from a pre-shared key	

Note: The module does not implement any Non-Approved Algorithms Allowed in the Approved Mode of Operation.

Note: The module does not implement any Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Table 6 – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

Algorithm	Description
ECDSA_secp256k1	Signature Algorithms of Blockchain
ed25519	Signature Algorithms of Blockchain
ripmd160	Message Digest algorithm of Blockchain
sha3-256 (FIPS 202)	Message Digest algorithm of Blockchain
SM2	Chinese Elliptic Curve Digital Signature Algorithm (asymmetric encryption/decryption, key agreement, signature generation/verification)
SM3	Chinese Message Digest Algorithm (message digest)
SM4	Chinese Block Cipher Symmetric Algorithm (symmetric encryption/decryption)
sr25519	Signature Algorithms of Blockchain

Table 7 – Security Function Implementations

Name	Type	Description	SF Properties	Algorithms	Algorithm Properties
KTS1	KTS	SP 800-56Brev2. KTS-IFC [56Br2] (Key encapsulation and un-encapsulation) per IG D.G	2048-bit modulus providing 112 bits of encryption strength	KTS-IFC (Cert. #A2750) Hash: SHA2-256	Modulus Length: 2048 Keys Length: 112
KTS2	KTS	SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	256- bit keys providing 256 bits of encryption strength	AES-256 (CBC) and HMAC-SHA-256 (Cert. #2750)	Keys Length: 256

Below in Table 8 are the procedures for the Shamir Secret Share for Split Knowledge.

Table 8– Split Knowledge Procedures

Algorithm	Caveat	Description
Shamir Secrets Share	Split Knowledge Procedures: Polynomial method used only for secret-sharing. Note: As per NISTIR 8214, Section 6.2, implementation of Shamir Secret Sharing is used to satisfy section 7.9.5 of the FIPS 140-3 standard which defines security requirements for split-knowledge procedures.	The secret sharing algorithm divides the secret and shares the secret among n participants more than specific t participants can calculate or recover the secret, and less than t participants cannot get it.

2.5 Entropy Sources

The Module uses the following entropy sources:

Vendor Name	Cert. Number
Shenzhen IBestChain Technology Co Ltd	ESV Cert. #E17

Table 9 – Entropy Sources

Entropy Source/ Name	Type	Operating Environment	Sample Size	Entropy per Sample	Conditioning Components
AS578 Entropy Source	Physical	ARM Cortex-M	1 bit	.83 bits	SHA2-256 (Cert. #A2750)

2.6 Overall Security Design

1. The Module provides two distinct operator roles: User (User Application external entity) and Cryptographic Officer (Manager).
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. Pre-Operational self-tests do not require any operator action.
7. Data output are inhibited during key generation, 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 restrictions on which SSPs are zeroized by the zeroization service. Factory reset will zeroize all SSPs of the module, tamper detection or EFP failure will zeroize all unprotected SSPs of the module.
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 SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module enters or outputs plaintext CSPs using trusted channel and split knowledge.
15. The Module does not store any plaintext CSPs.
16. The Module does not output intermediate key values.
17. The Module does not provide bypass services or ports/interfaces.

2.7 Rules of Operation

The Module shall be installed as described in Section 11 secure installation, initialization, startup and operation of the Module, and Section 7 Physical Security.

The Module shall be operated such that only the approved mode is enabled.

3 Cryptographic Module Interfaces

The Module’s ports and associated logical interface categories are listed in Table 10.

Table 10 – Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port/interface
Power Ports (2)	Power	Connect the module to the power outlet via the redundant power supply
Power button	Control In	Electrical signal passes through
LEDs	Status out	Display the working status of the module through different combinations
Serial Port (RS-232)	Control in | Data in | Data out | Status out	Connected to the management computer to provide management services
Type-c Port	Control in | Data in | Data out | Status out	Connected to the communication computer to provide cryptographic services for user applications

* Control Output is not available in this module

Table 11 – Trusted Channel

Trusted Channel	Description
Directly connected cable through a Serial Port (RS-232) from the Management Console to the module	The Trusted Channel must be setup per section 11.1 Secure Installation, Initialization, Startup and Operation of the Module. The Management Console connects directly to module via a serial port (RS-232). To protect the plaintext CSPs, the physical ports used for the trusted channel are physically separated from all other ports and will be under the direct supervision of the CO. A status indicator through the management console is provided when the trusted channel is in use or not. See the Channel section of Figure 8

4 Roles, Services and Authentication

4.1 Assumption of Roles and Related Services

The Module supports two distinct operator roles, User (User Application external entity) and Cryptographic Officer (CO) (Manager). The cryptographic module enforces the separation of roles using identity-based authentication. Re-authentication is enforced when changing roles. If the CO logs in while the user is logged in, the user will be automatically logged out.

Table 12 lists all operator roles supported by the Module and their related services. In addition, the Module supports services which does not require to be authenticated, listed UA in Table 12.

The Module does not support a maintenance role and bypass capability. The Module does not support concurrent operators. Previous authentications will be cleared on power cycle. The physical security mechanisms employed by the module protect the SSPs from unauthorized disclosure, modification, and substitution via physical intrusions.

Table 12 – Roles, Service Commands, Input and Output

Role			Service	Input	Output
CO	User	UA			
✓			Create DMK	Command In	Generated DMK.
✓			Restore DMK	Command In	DMK restored.
✓			Add MNG	Command In	The MNG account is created. Success/failure status.
✓			MNG Login	Password	Login CO role.
✓			MNG Logout	Command In	Logout CO role.
✓			Add User Application	Command In	The User Application user account is created. Success/failure status.
✓			Delete User Application	Command In	The User Application user account is deleted. Success/failure status.
✓			Reset User Application password	Command In	The User Application default password. Success/failure status.
✓			List User Application	Command In	User list
✓			Create User Key	Command In	Creates AES/HMAC/HASH/RSA2048/ECDSA-P256 keys for the user
✓			Remove User Key	Command In	Deletes User Keys
✓			List User Key	Command In	User key list
✓			Key Derivation Function	DMK	PK
✓			View Log	Command In	Log

Role			Service	Input	Output
CO	User	UA			
	✓		User Application Login	Command In	Login User role
	✓		User Application Logout	Command In	Logout User role
	✓		Modify User Application password	User Application password	Updated the User Application password. Success/failure status.
	✓		AES CBC Encryption	Plaintext	Ciphertext. Success/failure status
	✓		AES CBC Decryption	Cyphertext	Plaintext. Success/failure status
	✓		AES ECB Encryption	Plaintext	Ciphertext. Success/failure status
	✓		AES ECB Decryption	Cyphertext	Plaintext. Success/failure status
	✓		RSA2048 Signature generation	Command In	Generated signature. Success/failure status
	✓		RSA2048 Signature verification	Signature data	Success/failure status
✓	✓		Random Bit Generation	Entropy data, DRBG state values	DRBG Seed
	✓		ECDSA Signature generation	Command In	Generated signature. Success/failure status
	✓		ECDSA Signature verification	Signature data	Success/failure status
✓		✓	Display Module Version	Command In	Module HW version, FW version information
✓		✓	Display Module Status	Command In	FIPS status.
✓		✓	Zeroize	Factory reset Command In	All keys zeroized
				Tamper switch triggered, EFP failed	All unprotected SSPs zeroized
✓		✓	Self-Tests	Command In (Reset, automatic periodic self-tests)	Success/Reset.
✓			Set Mode of operation	Command In	Success/failure status

4.2 Authentication Methods

The module uses identity-based authentication to identify and verify users of the module. For roles as the manager are identified by UKEY_ID and verified using a challenge-response mechanism based on a 2048-bit RSA key pair, and user are identified by username and verified using a challenge-response mechanism based on sha2-256. The public key is stored in the module in plaintext, and the private key is stored in the user's USB token.

The module ensures that there is no visible display of the authentication data.

Table 13 – Authentication Description

Role	Authentication Method	Authentication Strength
CO	Identity-based - The CO is authenticated by UKEY_ID and verified using challenge-response mechanism based on a 2048-bit RSA key pair. The public key is stored in the module in plaintext, and the private key is stored in the user's USB token.	112 bits strength of the authentication method, the probability of a successful random attempt is 1 in 2^{112} Each RSA Signature Verification authentication attempt takes at least 60ms. So, the number of attempts for one minute cannot exceed 1000. The USB token corresponding to CO allows six (6) consecutive failed attempts before locking. After a successful attempt, the number of failures will be reset to zero. After six (6) consecutive failed attempts, the USB token cannot be used.
User	Identity-based – The User role sends assigned username to HSM, and HSM utilizes a challenge-response mechanism for user role authentication. The user's password is protected with a cryptographic hash (SHA-256 message digest).	Since the password length is eight (8) ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in {(10)*(26^2)*(95^5)} (at least one number, one uppercase, one lowercase). 1. HSM waits for the user to log in. 2. When the user enters the wrong PIN code for the first time, HSM sets the number of consecutive PIN code errors to 1 and starts the consecutive PIN code error cycle timing. 3. Within the consecutive PIN code error cycle (24 hours), if the user enters the wrong PIN code 6 times, the HSM will be locked for 60 minutes. 4. After 60 minutes, HSM will clear the number of consecutive PIN code errors, and the consecutive PIN code error cycle will end and be cleared. 5. Loop back to step 1 and provide login service to the user again.

4.3 Services

All services implemented by the Module are listed in Table 14 and Table 15 below.

The SSPs modes of access shown in Table 14 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 uses the SSP in performing a cryptographic operation.
- **Z** = Zeroize: The Module zeroizes the SSP

Table 14 – Approved Services

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator

Create DMK	Create a DMK, use the Shamir Secrets Share algorithm to divide the DMK into 3 component keys, and back up these three keys to three external USB tokens respectively. Then derive PK through DMK	HASH_DRBG,
		KBKDF [108]
		(Cert. #A2750)
			Device Master Key (DMK),
			Protection Key (PK)
				CO	G, R, E	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

Restore DMK	Import 2 component keys stored in the USB token into the cryptographic module, synthesize the DMK through the Shamir Secrets Share algorithm, and then derive the PK through the DMK.	KBKDF
		(Cert. #A2750)
			Device Master Key (DMK),
			Protection Key (PK)
				CO	W, E	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

Add MNG	Write ID and RSA public key from management console to the module.	AES-256,
		SHA2-256, RSA-2048 SigVer.
		(Cert. #A2750)
			CO RSA-pub Key	CO	G	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

MNG Login	The cryptographic module authenticates the manager's identity	RSA-2048 SigVer, HASH_DRBG
		(Cert. #A2750)
			CO RSA-pub Key	CO	R	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

MNG Logout	Manager logout	RSA-2048 SigVer.
		(Cert. #A2750)
			N/A	CO	N/A	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator

Add User Application	Create a user, write the user name and default password to module, and store it with PK protection.	AES-256,
		SHA2-256, RSA-2048 SigVer.
		(Cert. #A2750)
			User Password,
			Protection Key (PK)
				CO	G	Approved mode;
						ERROR_OK；
						ERROR_HSM_STATE;

Delete User Application	Delete user's information	AES-256,
		SHA2-256, RSA-2048 SigVer.
		(Cert. #A2750)
			User password,
			Protection Key (PK)
				CO	Z	Approved mode;
						ERROR_OK；
						ERROR_HSM_STATE;

Reset User Application password	modify user password, write the new default password to the module, and store it with PK protection.	AES-256,
		SHA2-256, RSA-2048 SigVer.
		(Cert. #A2750)
			Protection Key (PK)	CO	W	Approved mode;
						ERROR_OK；
						ERROR_HSM_STATE;

List User Application	List all currently existing User Application users	N/A	N/A	CO	R	Approved mode;
						ERROR_OK；
						ERROR_HSM_STATE;

Create User Key	Create user key, and store it with PK protection.	AES-256, SHA2-256,
		RSA-2048,
		ECDSA-P256
		(Cert. #2750)
			User AES key,
			User ECDSA-pub Key,
			User ECDSA-priv Key,
			User RSA-pub Key,
			User RSA-priv Key,
			Protection Key (PK)
				CO	G	Approved mode;
						ERROR_OK；
						ERROR_HSM_STATE;

Remove User Key	Remove user key	AES-256, SHA2-256,
		RSA-2048,
		ECDSA-P256
		(Cert. #2750)
			User AES key,
			User ECDSA-pub Key,
			User ECDSA-priv Key,
			User RSA-pub Key,
			User RSA-priv Key,
			Protection Key (PK)
				CO	Z	Approved mode;
						ERROR_OK；
						ERROR_HSM_STATE;

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator

List User Key	List user key types	AES-256, SHA2-256,
		RSA-2048,
		ECDSA-P256
		(Cert. #2750)
			N/A	CO	R	Approved mode;
						ERROR_HSM _STATE;
						ERROR_OK；

Key Derivation Function	Perform Key Derivation using NIST SP800-108 KDF in CTR mode	KBKDF with HMAC-SHA-256
		(Cert. #2750)
			Device Master KEY (DMK),
			Protection Key (PK)
				CO	R, W, E	Approved mode;
						ERROR_HSM _STATE;
						ERROR_OK；

View Log	View HSM log	N/A	N/A	CO	R	Approved mode;
						ERROR_HSM _STATE;
						ERROR_OK；

User Application Login	Verify Username and PASSWORD	AES-256, HMAC-SHA-256, HASH_DRBG, SHA2-256, KTS-RSA-2048
		(Cert. #A2750)
			User Password,
			RSA Key Decryption Key (KDK),
			RSA Key Encryption Key (KEK),
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	R	Approved mode;
						ERROR_OK；
						ERROR_HSM _STATE;

User Application Logout	User Application Logout	N/A	Session AES Key,
			Session HMAC Key
				User	R	Approved mode;
						ERROR_OK；
						ERROR_HSM _STATE;

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator

Modify User Application password	modify user password, write the new password to module, and store it with PK protection.	AES-256, HMAC-SHA-256, KTS-RSA-2048
		(Cert. #A2750)
			User password,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	W	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

AES CBC Encryption	User uses AES CBC encryption service	AES-256 CBC
		(Cert. #A2750)
			User AES Key,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	E	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

AES CBC Decryption	User uses AES CBC decryption service	AES-256 CBC
		(Cert. #A2750)
			User AES Key,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	E	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

AES ECB Encryption	User uses AES ECB encryption service	AES-256 ECB
		(Cert. #A2750)
			User AES Key,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	E	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

AES ECB Decryption	User uses AES ECB decryption service	AES-256 ECB
		(Cert. #A2750)
			User AES Key,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	E	Approved mode;
						ERROR_OK;
						ERROR_HSM_STATE;

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator

RSA2048 Signature generation	User uses RSA 2048 signature generation service	RSA-2048 SigGen (Cert. #A2750)	User RSA-priv Key,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	E	Approved mode;
						ERROR_OK;
						ERROR_HSM _STATE;

RSA2048 Signature verification	User uses RSA 2048 Signature verification service	RSA-2048 SigVer (Cert. #A2750)	User RSA-pub Key,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	E	Approved mode;
						ERROR_OK;
						ERROR_HSM _STATE;

ECDSA Signature generation	User uses ECDSA signature generation service	ECDSA SigGen (Cert. #A2750)	User ECDSA-priv Key,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	E	Approved mode;
						ERROR_OK;
						ERROR_HSM _STATE;

ECDSA Signature verification	User uses ECDSA Signature verification service	ECDSA SigVer (Cert. #A2750)	User ECDSA-pub Key,
			Session AES Key,
			Session HMAC Key,
			Protection Key (PK)
				User	E	Approved mode;
						ERROR_OK;
						ERROR_HSM _STATE;

Random Bit Generation	Provide random bits from the DRBG	DRBG [90A] (CERT. #A2750)	DRBG-EI,
			DRBG-State,
			DRBG Seed
				CO,
				User
					R, W, E	Approved mode;
						ERROR_OK;
						ERROR_HSM _STATE;

Display Module Version	Display version number of modules in HSM/hardware/ firmware	N/A	N/A	CO,
				UA
					R, E	Approved mode;
						ERROR_OK;
						ERROR_HSM _STATE;

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator

Display Module Status	View Module status	N/A	N/A	CO,
				UA
					R, E	Approved mode;
						ERROR_OK；
						ERROR_HSM_STATE;

Zeroize	Zeroization through Factory reset of the module, tamper switch or EFP failure.	N/A	Device Master Key (DMK), Protection Key (PK), User AES Key, User ECDSA-priv Key, User ECDSA-pub Key, User RSA-priv key, User RSA-pub keys, User Password, CO RSA-pub Key	CO, UA	Z	Approved mode; ERROR_OK；
Self-Tests	Perform the self-tests automatically when the module is powered on or restarted	AES-256, HASH_DRBG [90A], ESV [90B] HMAC-SHA-256 KBKDF [108] KTS-RSA-2048 SHA2-256, RSA-2048, ECDSA-P256 (Cert. #2750)	N/A	CO, UA	R, E	Approved mode; ERROR_OK；

Set Mode of operation	Set the mode of operation	RSA-2048 SigVer
		HASH_DRBG
		(Cert. #A2750)
			CO RSA-pub Key	CO	W, E	Approved mode;
						ERROR_OK；
						ERROR_HSM_STATE;

Table 15 – Non-Approved Services

Service	Description	Algorithm Accessed	Roles	Indicator

Create User Key	Create user key	ECDSA_secp256k1, ed25519, SM2, SM4, SR25519	CO	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

Remove User Key	Remove user key	ECDSA_secp256k1,
		ed25519,
		SM2,
		SM4,
		SR25519
			CO	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

List User Key	List user key types	ECDSA_secp256k1,
		ed25519,
		SM2,
		SM4,
		SR25519
			CO	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

SM4 Decryption	User uses sm4 decryption service	SM4	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

SM4 Encryption	User uses sm4 encryption service	SM4	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

Service	Description	Algorithm Accessed	Roles	Indicator

SM2 Signature generation	User uses sm2 signature generation service	SM2	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

SM2 Signature verification	User uses sm2 Signature verification service	SM2	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

ECDSA_secp256k1 Signature generation	User uses ECDSA_secp256k1 signature generation service	ECDSA_secp256k1	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

ECDSA_secp256k1 Signature verification	User uses ECDSA_secp256k1 Signature verification service	ECDSA_secp256k1	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

sr25519 Signature generation	User uses sr25519 signature generation service	sr25519	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

Service	Description	Algorithm Accessed	Roles	Indicator

sr25519 Signature verification	User uses sr25519 Signature verification service	sr25519	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

ed25519 Signature generation	User uses ed25519 signature generation service	ed25519	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

ed25519 Signature verification	User uses ed25519 Signature verification service	ed25519	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

ripmd160 digest	User uses ripmd160 message digest service	ripmd160	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

SHA3-256 digest	User uses sha3-256 message digest service	SHA3-256	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

SM3 digest	User uses SM3 message digest service	SM3	User	Non-Approved Mode;
				ERROR_OK;
				ERROR_HSM_STATE;
				ERROR_HSM_MODE;

Service	Description	Algorithm Accessed	Roles	Indicator
Zeroize	Zeroization through Factory reset of the module, tamper switch or EFP failure.	ECDSA_secp256k1, ed25519, SM2, ripmd160, SHA3-256, SM3, SM4, SR25519	CO	Non-Approved Mode; ERROR_OK；

NOTE: All non-approved services are only available in Non-Approved mode. If invoke any non-approved service in approved mode, the module will return error code ERROR_HSM_MODE.

NOTE: All services in Table 14 and Approved SSPs in Table 20 and Table 21 are available in Non-Approved mode. These services are considered non-approved services.

5 Software/Firmware Security

The Module is a Level 3 multi-chip standalone hardware module.

Firmware integrity verification uses an approved digital signature cryptographic mechanism, if the calculated result is not successfully verified, the test fails, and the module enters the error state.

In the production process, the public key of the firmware integrity key pair is written into the flash of the AS578 in plaintext. Use the sha256 algorithm to calculate the message digest of the bootloader, kernel, and application of the IMX6 and the message digest of the executable code of the AS578, sign these message digests with the private key of the firmware integrity key pair, and write these signatures into the flash of the AS578. The firmware integrity check of IMX6 and AS578 is performed as follows:

AS578:

- Read the digital signature of executable code message digest stored in the flash of AS578, verify the signature with the public key of the firmware integrity key pair, and get the message digest.
- Read executable code and use sha256 algorithm to calculate message digest.
- Compare the two message digests, if the digests are consistent, the firmware integrity check will pass, otherwise module enters the error state.

imx6:

- Read the images of bootloader, kernel and application on EMMC respectively, use sha256 algorithm to calculate the message digest, and transfer the message digest to AS578.
- Read the digital signature of bootloader, kernel, and application stored in the flash of AS578, verify the signature with the public key of the firmware integrity key pair, and obtain the message digest.
- Compare the two message digests, if the digests are consistent, the firmware integrity check will pass, otherwise module enters the error state.

The operator can initiate the integrity test on demand by rebooting the module.

6 Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-3 definitions. The tested operational environment is listed in Table 2.

The Module does not include a firmware load service to support necessary updates. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7 Physical Security

The module is a multiple-chip standalone cryptographic module. Physical security is designed according to Level 3 standards.

7.1 Tamper-Evident Seals

The cryptographic module is contained within a strong enclosure with four (4) tamper-evident seals on the top, left side and bottom and right side and bottom as described in Table 17. Each tamper evident seal is individually identifiable. The cryptographic module will perform EFP. If the voltage falls outside the normal operating range of the module, the module will shut down immediately. The Voltage range is 68V-280V. If the temperature falls outside the normal operating range of the module, the module will immediately zeroizes all unprotected SSPS. The temperature range is -2℃---46℃.

Table 16 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-Evident Seals	Inspect tamper-evident seals monthly.	Look for signs of tampering. If tampering is suspected, then the module must be removed from service.

The Module will be shipped from the manufacturer with tamper-evident seals pre-installed. To operate the Module in an Approved mode of operation, the CO role shall inspect the tamper-evident seals IB6127370XXX as shown in Figure 10 to Figure 13 on the reception of the Module. Detailed information is provided in Table 17.

If the CO determines that the seals were tampered with, the module is to be removed from service and no longer allowed to be used and is not to be returned to the vendor. The CO will perform the factory reset to zeroize all SSPs.

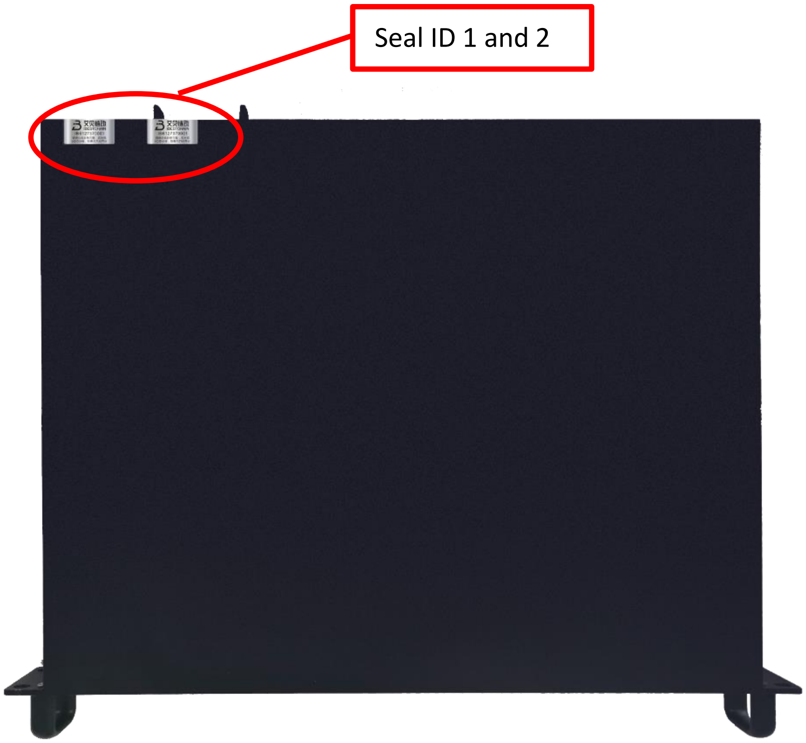


Figure 10 – Module Seal Locations (Top)

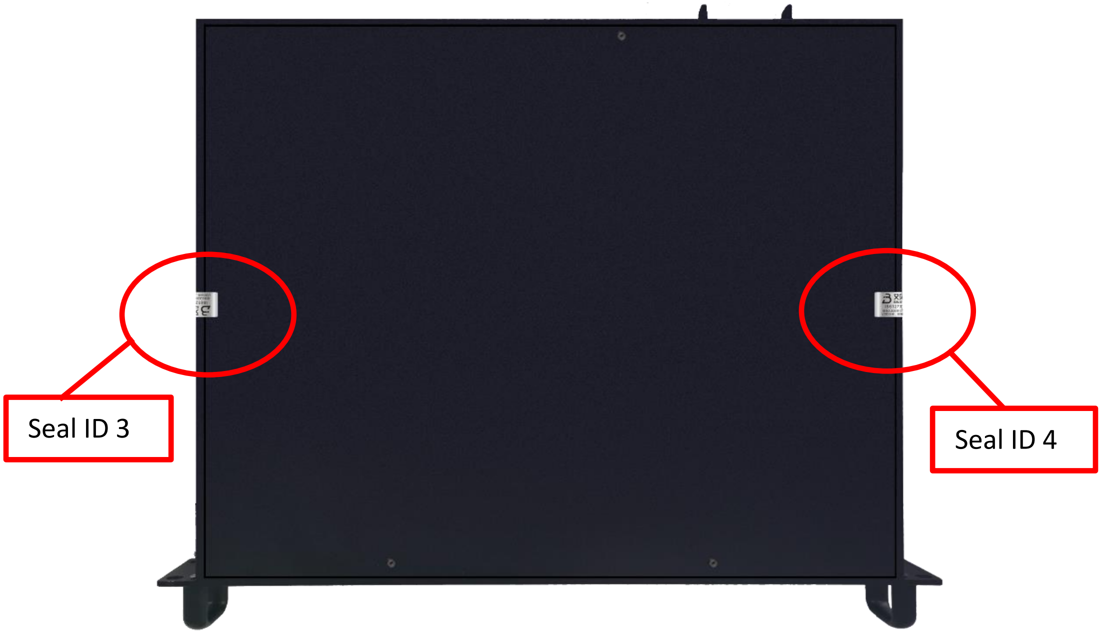


Figure 11 – Module Seal Locations (Bottom)

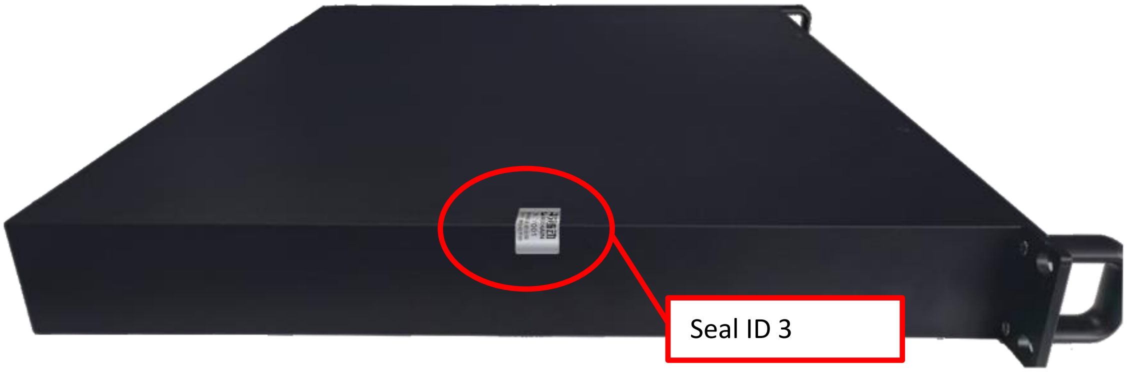


Figure 12 – Module Seal Location (Left side)

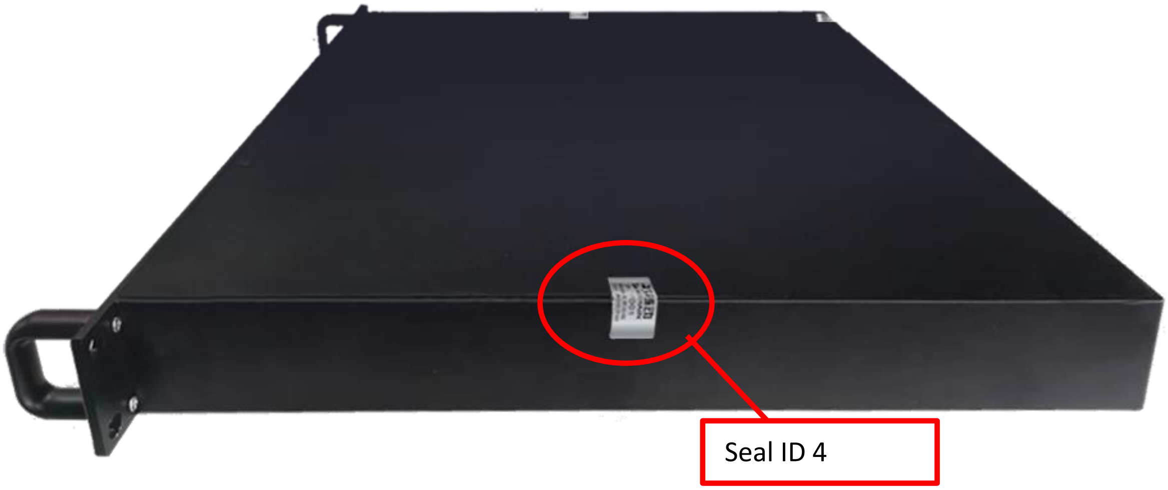


Figure 13 – Module Seal Location (Right side)

Table 17 – Tamper-Evident Seal Locations Guidance

Seal ID	Placement
1	Top side
2	Top side
3	Left side and bottom
4	Right side and bottom

7.2 Tamper Detection

The cryptographic module includes a tamper detection feature that will immediately zeroize all SSPs when the module's cover is removed. This forces a factory reset and will put the module into the Invasive Error State. This will also close all external interfaces and stop providing all services.

The tamper detection remains active at all times including when the module is powered off, which at that point, will operate with an internal battery.

As the tamper-evident seals will need to be broken to remove the cover, there is no recovery from the error state as the module will no longer be in service.

7.3 Environmental Failure Protection (EFP)

The cryptographic module includes Environmental Failure Protection (EFP). If the voltage falls outside the normal operating range of the module, the module will shut down immediately.

If the temperature falls outside the normal operating range of the module, the module will immediately zeroizes all unprotected SSPS.

See Table 18 for the temperature and voltage measurements

Table 18 – Environmental Failure Protection

	Temperature or voltage measurement	EFP description	Results
Low Temperature	-2.6℃	A tamper flag is raised, zeroization will proceed.	Zeroization
High Temperature	46℃	A tamper flag is raised, zeroization will proceed.	Zeroization
Low Voltage	68V	A tamper flag is raised, triggering the product to shut down immediately	Shut down
High Voltage	280V	A tamper flag is raised, triggering the product to shut down immediately	Shut down

8 Non-Invasive Security

The Module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameter (SSP) Management

The SSPs access methods are described in Table 19 below:

Table 19 – SSP Management Methods

Method	Description
G1	Generated internally by using the internal CAVP validated DRBG during module initialization
G2	Derived by DMK using SP800-108 CTR KDF (HMAC-SHA256 PRF)
G3	FIPS 186-4 compliant RSA key generation, using the internal CAVP validated DRBG
G4	Symmetric key generated by internal CAVP validated DRBG
G5	FPS 186-4 compliant ECDSA key generation, using the internal CAVP validated DRBG.
G7	Generated external to the Module and installed during manufacturing
G8	Generated internally by using the internal entropy source
E1	Input in plaintext from 2 of the 3 components stored in the token during module initialization using trusted channel and split knowledge
E2	Split into 3 components and Output to 3 tokens in plaintext using trusted channel and split knowledge.
E3	Public key output in plaintext
E4	Generated by SDK using AES algorithm and transmitted into the module through KTS-RSA
E5	Encrypted by session key and Input by User application
E6	Generate by USB_TOKEN and imported as identify Key
E7	Input at manufacturer
E8	Generated by SDK using HMAC-SHA256 algorithm and transmitted into the module through KTS-RSA
S1	Only stored in volatile memory (RAM).
S2	Stored in flash encapsulated by PK
S3	Stored in flash in plaintext
Z1	Zeroized by Module power cycle
Z2	Zeroized by the “zeroize” service by overwriting with a fixed pattern of 0s.
Z3	Dereferenced by session termination and zeroized by OS memory cleanup.
Z4	Zeroized when the tamper switch is triggered or EFP failed.
Z5	Zeroized by Factory reset

NOTE: Zeroization is implicit and is considered complete either after boot sequence is complete or when User/CO initiates zeroization via Zeroize service and the module provides success/fail status.

9.1 Critical Security Parameters (CSP)

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module is described in the services detailed in 0.

Table 20 – CSPs Management

CSP	Strength (in bits)	Security Function / Cert.	Generation	Import /Export	Establishment	Storage	Zeroization	Use / Related SSPs
Device Master Key (DMK)	256	DRBG (Cert. #A2750)	G1	I, E	E1, E2	S1	Z1, Z2, Z4, Z5	Used to derive the Protection Key (PK)
Protection Key (PK)	256	KBKDF SP800-108 CTR (Cert. #A2750)	G2	N/A	N/A	S1	Z1, Z2, Z4, Z5	Encrypt SSPs with AES algorithm and store (S2) in flash inside the module.
RSA Key Decryption Key (KDK)	112	KTS-RSA 2048 (Cert. #A2750)	G3	N/A	N/A	S1	Z1, Z2, Z4, Z5	RSA (2048) key transport key used to decrypt the RSA Key Encryption Key (KEK)
Session AES Key	256	AES CBC, (Cert. #A2750)	N/A	I	E4	S1	Z1, Z3, Z4, Z5	Encryption key (along with the Session HMAC key) to protect links in the data transmission between user application/manager computer and HSM
Session HMAC Key	256	HMAC-SHA256 (Cert. #A2750)	N/A	I	E8	S1	Z1, Z3, Z4, Z5	HMAC generation and verification with the Session AES Key
DRBG-EI	256	ESV Cert. #E17	G8	N/A	N/A	S1	Z1, Z2, Z4, Z5	The noise source inputs 512 bits of entropy to the Conditioning Component, and the Conditioning Component uses the Sha2-256 algorithm to output 256 bits of entropy. 0.86323 per entropy source output bit.

CSP	Strength (in bits)	Security Function / Cert.	Generation	Import /Export	Establishment	Storage	Zeroization	Use / Related SSPs
								Output of the Entropy Source entered into the DRBG
DRBG-State (V and C value (Per IG D.L entropy meets the requirement based on SP800-90A and SP800-90B)	256	Hash DRBG (Cert. #A2750)	G1	N/A	N/A	S1	Z1, Z2, Z4, Z5	Internal state information and temporary variables for approved DRBG function.
DRBG Seed (Per IG D.L entropy meets the requirement based on SP800-90A and SP800-90B)	256	Hash DRBG (Cert. #A2750)	G1	N/A	N/A	S1	Z1, Z2, Z4, Z5	Output of the DRBG and used in the generation of SSPs
User AES Key	128/192/256	AES CBC, ECB (Cert. #A2750)	G4	N/A	N/A	S2	Z2, Z5	User encryption and decryption service use and protected by the Protection Key (PK)
User ECDSA-priv Key	128	ECDSA P-256 (Cert. #A2750)	G5	N/A	N/A	S2	Z2, Z5	User Signature service use and protected by the Protection Key (PK)
User RSA-priv Key	112	RSA 2048 (Cert. #A2750)	G3	N/A	N/A	S2	Z2, Z5	User Signature service use and protected by the Protection Key (PK)
User Password	8 characters	N/A	N/A	I	E5	S2	Z2, Z5	User identity authentication and protected by the Protection Key (PK)

9.2 Public Security Parameters (PSP)

All PSPs used by the Module are described in this section. All usage of these PSPs by the Module is described in the services detailed in Table 150.

Table 21 – PSPs

PSP	Strength (in bits)	Security Function / Cert.	Gener-ation	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
CO RSA-pub Key	112	RSA 2048 (Cert. #A2750)	N/A	N/A	E6	S2	Z2, Z4, Z5	[FIPS 186-4] CO Authentication Key
RSA Key Encryption Key (KEK)	112	KTS-RSA 2048 (Cert. #A2750)	G3	E3	N/A	S1	Z1, Z3, Z4, Z5	RSA (2048) key transport (Encryption) key
User ECDSA-pub	128	ECDSA P256 (Cert. #A2750)	G5	N/A	N/A	S2	Z2, Z5	[FIPS 186-4] ECDSA signature verification key and protected by the Protection Key (PK)
User RSA-pub	112	RSA 2048 (Cert. #A2750)	G3	N/A	N/A	S2	Z2, Z5	[FIPS 186-4] RSA signature verification key and protected by the Protection Key (PK)

10 Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational self–tests are periodically performed by the Module every 720 hours automatically after the module is powered on, without external input or control. The Module will not accept any commands when a periodic self-test is required; the commands still in the I/O buffer will be processed by The Module and the periodic self-test executed when the I/O buffer is emptied. The Module logs self-test errors in the system log, the CO can consult the error log by View system logs on management software.

When HSM powers on, the operator can perform the on-demand self-test through power cycling.

The self-tests error states and status indicator are described in table below:

Table 22 – Self-Test Error States and Indicators

Error State	Description	Indicator
ES1	The Module fails a KAT, PCT or firmware integrity pre-operational self-test. When HSM enters ES1, the input and output are all closed, and the only operation to recovery from error state is to switch power button to restart HSM. After restart, the HSM performs self-test, that will determine which state HSM will enter. If HSM enters error state again, the CO must send the HSM to vendor.	The Module enters the critical error state and outputs status of the red LED stays on, the blue LED flashes quickly, otherwise it indicates successful completion by Red LED flashes quickly, blue LED flashes normally.

The Module performs the following pre-operational self-tests:

Table 23 – Pre-Operational Self-Test

Security Function	Method	Description	Error State
Firmware integrity	RSA Digital Signature FIPS 186-4	The public key of the firmware integrity key pair is written into the flash of the AS578 in plaintext. Use the sha256 algorithm to calculate the message digest of the bootloader, kernel, and application of the IMX6 and the message digest of the executable code of the AS578, sign these message digests with the private key of the firmware integrity key pair, and write these signatures into the flash of the AS578. When HSM powers on, after self-test of the entropy source and algorithm, HSM calculates the digests of bootloader, kernel and IM6 application, and executable code of the AS578, then use the public key and the signatures which have been written in AS578, to verify the firmware integrity.	ES1
Entropy Critical Function	APT and RCT	When HSM powers on, SP800-90B health tests are performed before the first use of the entropy source. When the entropy source fails health test, the entropy source cannot generate the sufficient amount of entropy.	ES1

Security Function	Method	Description	Error State
		At this time, the module must be restarted via the power button to return for service.	

The Module performs the following conditional self-tests:

Table 24 – Conditional Self-Tests

Security Function	Method	Description	Error State
AES – ECB	KAT	AES(ECB) with 256-bit key, encryption AES(ECB) with 256-bit key, decryption	ES1
AES – CBC	KAT	AES(CBC) with 256-bit key, encryption AES(CBC) with 256-bit key, decryption	ES1
DRBG	KAT	Hash_DRBG using SHA-256, with PR	ES1
ECDSA	KAT	ECDSA with P-256 and SHA-256, signature generation ECDSA with P-256 and SHA-256, signature verification	ES1
ECDSA Key Generation	PCT	ECDSA P-256 Key Generation Pairwise Consistency Test	ES1
ESV	SP 800-90B Health-Test	An RCT and APT as specified in [90B] section 4.4 are executed before generation of the DRBG entropy input. When the entropy source fails health test, the entropy source cannot generate enough entropy. At this time, the module must be restarted via the power button to return for service.	ES1
HMAC	KAT	HMAC-SHA2-256	ES1
KBKDF SP800-108	KAT	HMAC-SHA2-256 in Counter Mode	ES1
RSA	KAT	RSA PKCS#1v1.5 with 2048-bit key and SHA-256, signature generation RSA PKCS#1v1.5 with 2048-bit key and SHA-256, signature verification	ES1
RSA Key Generation	PCT	2048-bit RSA Encryption and Decryption per IG D.G.	ES1
		2048-bit RSA Sign and Verify per IG D.G	
SHS (Cert. #A2749)	KAT	SHA2-256	ES1
SHS (Cert. #A2750)	KAT	SHA2-256	ES1

NOTE: Conditional KAT tests are run during the startup of the module as part of the Pre-Operational Self-Test phase

NOTE: KAT RSA PKCS#1v1.5 with 2048-bit key and SHA-256, signature verification is performed prior to the Firmware Integrity.

11 Life-Cycle Assurance

11.1 Secure Installation, Initialization, Startup and Operation of the Module

The module will be securely delivered to the operators via UPS with tracking codes to ensure there is no tampering during delivery. Upon receipt of the module, the CO must check that the module's outer packaging is intact or that the packaging has been opened during transport.

Upon delivery, the operator must initialize the module as follows:

1. The operator must ensure that the initial security configuration of the module is completed in a restricted environment using a direct cabled serial connection from the management console (standalone PC).
2. From the management program on the console, the operator must select the COM port by selecting “Connect” from the menu bar.
3. Next, the operator must create the Manager role (CO) by selecting from the Management program menu: Device → Add MNG. The operator then must insert the first of 3 USB tokens. A new PASSWORD (8 characters) will be required and stored on the USB token.
4. Repeat this process twice more with different USB Tokens. When the three Manager roles have been created, HSM can be initialized.
5. Next, the operator will create DMK for the HSM, and export DMK components to USB tokens. Select from the Management program menu: Device → Create DMK. With 3 different USB token, CO must sign in the HSM three (3) times, and store DMK component to each USB token. One DMK component, one USB token.
6. With one of 3 USB tokens, the operator selects from menu, choose: Device → Set Mode of Operation, and choose “FIPS Mode”. Once “OK” is selected, the module will reboot and perform the Pre-Operational and Conditional KAT Self-Tests.
7. Select from menu Tools → Reset HSM, which zeroizes all the SSPs, will remove the module from the Approved Mode of Operation

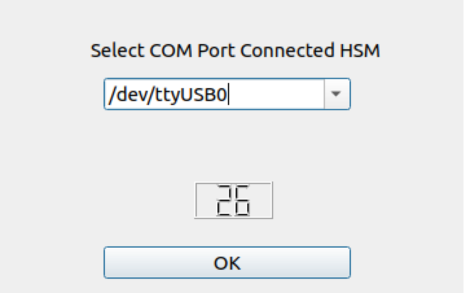
11.2 Cryptographic Officer Guidance

The serial port is used to connect the cryptographic module and the management computer.

The CO implements management functions such as Add MNG, Restore DMK, user application management, and key management through the management computer. The following is the specific function description.

Connect HSM

Before use HSM, you have to connect to it first. Choose “Connect” from menu, then the dialog below will appear:



Select COM Port Connected HSM

/dev/ttyUSB0

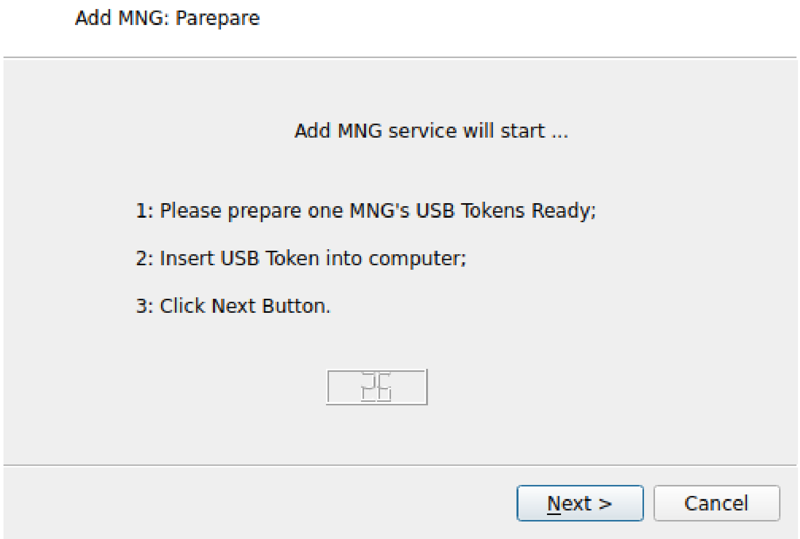
Figure 14 – Choose COM Port

From pull-down control, select COM port which connects to HSM. If the port used are not listed, please input the device full path in the edit control. After selection, please click “OK” button。

Add MNG

The first step to use HSM, is to create HSM manager.

From menu: Device → Add MNG, Follow the instructions shown in the figure below to complete the process.



Add MNG: Parepare

Add MNG service will start ...

1: Please prepare one MNG's USB Tokens Ready;

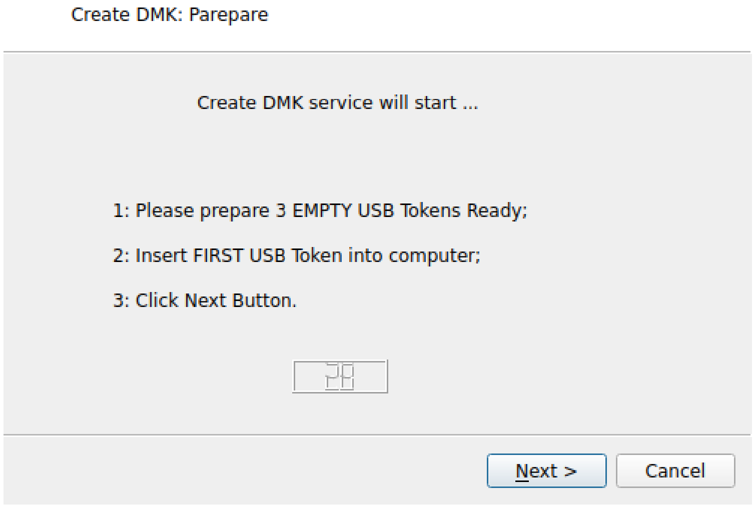
2: Insert USB Token into computer;

3: Click Next Button.

Figure 15 – Add MNG

Create DMK

From menu: Device → Create DMK, Follow the instructions shown in the figure below, the manager can store DMK components to 3 USB Tokens.



Create DMK: Parepare

Create DMK service will start ...

1: Please prepare 3 EMPTY USB Tokens Ready;

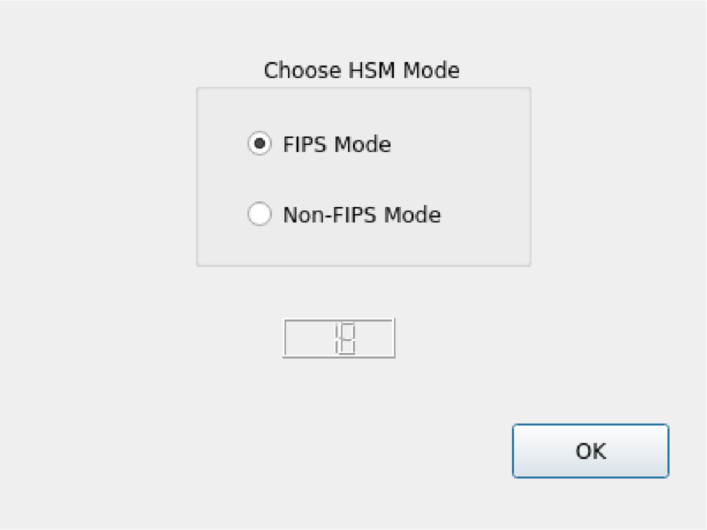
2: Insert FIRST USB Token into computer;

3: Click Next Button.

Figure 16 – Create DMK

Set Mode of Operation

The next step sets the HSM operation mode. From menu, choose: Device→ Set Mode of Operation. The CO will have two choices, to select "FIPS Mode" or "Non-FIPS Mode" Once selected, the CO will follow the instructions shown in the figure below to complete the process.



Choose HSM Mode

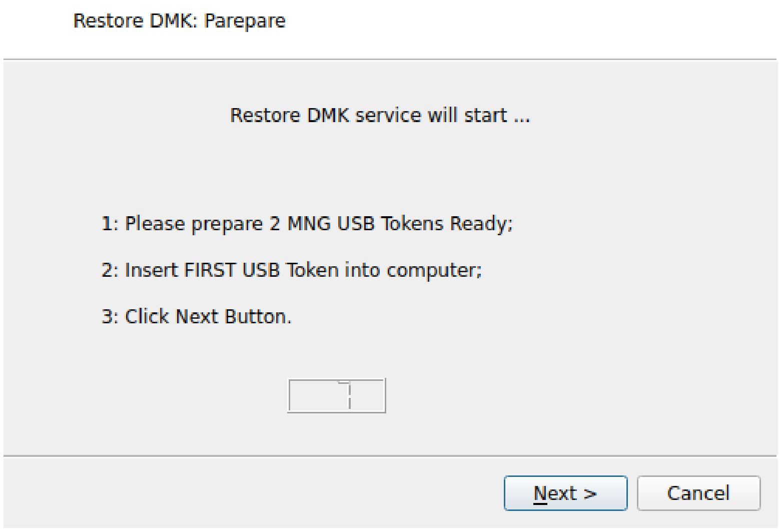
● FIPS Mode

○ Non-FIPS Mode

Figure 17 – Set Mode of Operation

Restore DMK

After initialization is complete, when the HSM restarts, the first step is to restore DMK. From menu, choose: Device→ Restore DMK, Follow the instructions below to complete the process.



Restore DMK: Parepare

Restore DMK service will start ...

1: Please prepare 2 MNG USB Tokens Ready;

2: Insert FIRST USB Token into computer;

3: Click Next Button.

Figure 18 – Restore DMK

Other functions can be selected on the menu of the management software and operated according to the instructions.

COs is responsible for protecting USB tokens and passwords from theft.

COs must periodically check that the tamper evidence seals are intact and located in the correct position on the chassis. If evidence of tampering is detected, the module shall be considered non-compliant, and shall be scrapped.

11.3 User Guidance

The Type-C Port is used to connect the cryptographic module and the communication computer. The communication computer is connected to the application server via Ethernet.

When CO creates a user account, a default password is generated. The default password is emailed to the appropriate user. The user must change the password when logging in for the first time. Users can access the services of the cryptographic module only after their identity authentication is passed. The cryptographic module provides user applications with services such as user login/logout, data encryption and decryption, data signature and verification.

Users are responsible for protecting their passwords from theft.

12 Mitigation of Other Attacks

The Module does not implement any mitigation method against other attacks.

13 References and Definitions

The following standards are referred to in this Security Policy.

Table 25 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program,* October 7, 2022
[108]	*NIST Special Publication 800-108 rev1, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), August 17, 2022*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*

Abbreviation	Full Specification Name
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38E]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Br2]	*NIST Special Publication 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Finite Field Cryptography, March 2019*
[56Cr2]	*NIST Special Publication 800-56C Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, August 2020*
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67rev2, November 17 2017*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*

Table 26 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
APT	Adaptative Proportion Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CSP	Critical Security Parameter
CTR	Counter

Acronym	Definition
DMK	Device Master Key
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECDSA	Elliptic Curve Digital Signature Algorithm
EFP	Environmental Failure Protection
ENT	Approved SP800-90B Entropy Source
ESV	Entropy Source Validation
FIPS	Federal Information Processing Standard
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
KAT	Know Answer Test
KBKDF	Key-Based Key Derivation Functions
KDF	Key Derivation Function
KTS	Key Transport Methods
NIST	National Institute of Standards and Technology
OAEP	Optimal Asymmetric Encryption Padding
PCT	Pairwise Consistency Test
PK	Protection Key
PKCS	Public-Key Cryptography Standards
PR	Prediction Resistance
RAM	Random Access Memory
RCT	Repetition Count Test
RSA	Rivest-Shamir-Adleman
PUB	Publication
SDK	Software Develop Kit
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter