Sansec Technology Co., Ltd.

Sansec HSM Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 3.6
Date: July 31st, 2026

Table of Contents

List of Tables

List of Figures

1 – General

1.1 Overview

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

1.2 Security Levels

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

Section	Title	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 Level	3

Table 1: Security Levels

2 – Cryptographic Module Specification

This Sansec HSM Cryptographic Module is hereafter denoted as the Module. The Module is a cryptographic module that provides core functions including device management, key management, and cryptographic services. It delivers key storage and cryptographic services to external applications through virtual security modules (VSMs).

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated Cryptographic Module, the Module is intended to be used in private cloud environments in financial, government, e-commerce, and other fields.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 1. The Module is a multi-chip standalone embodiment. The cryptographic boundary consists of the host HSM (hardware security module), virtual security module (VSM), cryptographic card (protection card), VSM cryptographic service program, HSM/VSM management program, and other components.

Figure 1 – Sansec HSM Cryptographic Module

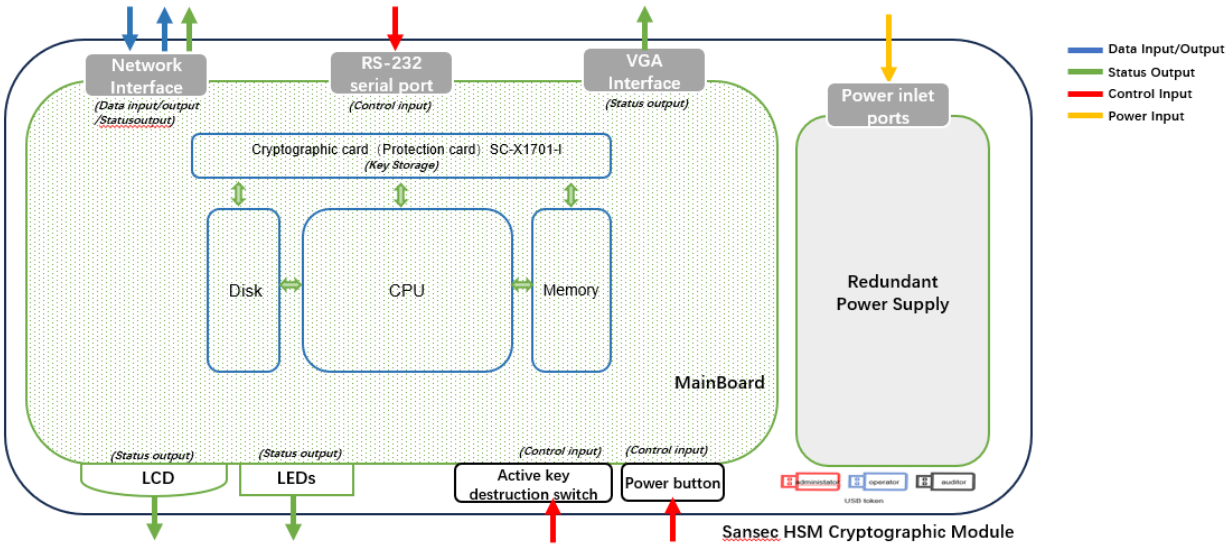


Figure 2 – Block diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Sansec HSM Cryptographic Module is tested on the following operational environment.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Model: Sansec HSM Cryptographic Module Part Number(s): HI74S62-2410	V4.5	V4.5.2	Intel Xeon Gold 5218	N/A

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

The module does not have any excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
approved mode	Enter this mode either after first-time use and initialization, or after switching and initializing via the VSM management program by selecting "Set Approved Mode". The current mode status can be viewed in the VSM management service or cryptographic service. When the module is running in approved mode of operation, only approved services are available.	Approved	The module uses a global indicator for that supports approved services in an approved manner or non-approved services in a non-approved manner. Explicitly indicate the current mode status using static code. The user will know that the Module is in approved mode or non-approved mode by: 1) Using the "view approved mode" function in the management console. It will show "approved mode" or "non-approved mode". 2) By external entities (e.g., user applications) that connect through the network, using the service "Get FIPS status ". The indicator of approved mode is obtained by using the 'Get FIPS status' service. The 'Status' field of the 'Get FIPS status' service indicates the mode. The value of the parameter 'Status' passed into the call specifies the mode.

Mode Name	Description	Type	Status Indicator
			The following values are allowed for the parameter: 1 - approved mode.
non-approved mode	Enter this mode after switching and initializing by selecting "Set non-approved Mode" through the VSM management program. The current mode status can be viewed in the VSM management service or cryptographic service. Once the mode is switched, the module will compulsorily perform the initialization operation to ensure that the SSPs are not shared between approved and non-approved mode of operation. NOTE: All non-approved services are only available in non-approved mode. NOTE: All services included in SP section 4.3 Approved Services and Approved SSPs in SP section 9.4 SSPs are available in non-approved mode. These services are considered non-approved services.	Non-Approved	The module uses a global indicator for that supports approved services in an approved manner or non-approved services in a non-approved manner. Explicitly indicate the current mode status using static code. The user will know that the Module is in approved mode or non-approved mode by: 1) Using the "view approved mode" function in the management console. It will show "approved mode" or "non-approved mode". 2) By external entities (e.g., user applications) that connect through the network, using the service "Get FIPS status ". The indicator of approved mode is obtained by using the 'Get FIPS status' service. The 'Status' field of the 'Get FIPS status' service indicates the mode. The value of the parameter 'Status' passed into the call specifies the mode. The following values are allowed for the parameter: 2 - non-approved mode.

Table 3: Modes List and Description

Mode Change Instructions and Status:

The FIPS approved of operation is default selected when a user initializes the VSM for the first time. Once the VSM is operational, a user with the administrator role can reset the mode of operation through the “Set approved mode” management service—selects “approved mode” or “non-approved mode”. Once the mode is switched, the module will compulsorily perform the initialization operation to ensure that the SSPs are not shared between approved and non-approved mode of operation. At this point, the module will forcibly re-enter the initialization process.

2.5 Algorithms

Approved Algorithms:

The Module implements the FIPS Approved cryptographic algorithms listed in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6703	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A6703	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56-104 Increment 8 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0-256 Increment 8	SP 800-38C
AES-CFB1	A6703	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A6703	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6703	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A6703	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 0-16384 Increment 8	SP 800-38B
AES-CTR	A6703	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - No Incremental Counter - No Counter Tests Performed - No	SP 800-38A
AES-ECB	A6703	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6703	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 8-65536 Increment 8 AAD Length - AAD Length: 0-65536 Increment 8	SP 800-38D
AES-OFB	A6703	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A6703	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
Counter DRBG	A6703	Prediction Resistance - Yes Supports Reseed - No	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Mode - AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0 Returned Bits - 256	
ECDSA KeyGen (FIPS186-5)	A6703	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6703	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6703	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - Yes	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A6703	Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A6703	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
Hash DRBG	A6703	Prediction Resistance - Yes Supports Reseed - No Mode - SHA3-256 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0 Returned Bits - 256	SP 800-90A Rev. 1
HMAC-SHA-1	A6703	MAC - MAC: 160 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1
HMAC-SHA2-224	A6703	MAC - MAC: 224 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1
HMAC-SHA2-256	A6703	MAC - MAC: 256 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1
HMAC-SHA2-384	A6703	MAC - MAC: 384 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1
HMAC-SHA2-512	A6703	MAC - MAC: 512 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1
HMAC-SHA3-224	A6703	MAC - MAC: 224 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-256	A6703	MAC - MAC: 256 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1
HMAC-SHA3-384	A6703	MAC - MAC: 384 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1
HMAC-SHA3-512	A6703	MAC - MAC: 512 Key Length - Key Length: 128-256 Increment 64	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6703	Domain Parameter Generation Methods - P-256, P-384, P-521 Hash Function Z - SHA2-512 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SP800-108	A6703	KDF Mode - Counter MAC Mode - HMAC-SHA2-256 Supported Lengths - Supported Lengths: 256 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KTS-IFC	A6703	Function - keyPairGen IUT ID - 1234567890ABCDEF Modulo - 2048 Key Generation Methods - rsakpg1-crt Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Hash Algorithms - SHA2-256 Supports Null Associated Data - Yes Associated Data Pattern - uPartyInfo||vPartyInfo Associated Data Encoding - concatenation Key Length - 512	SP 800-56B Rev. 2
ML-DSA KeyGen	A6703	Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87	FIPS 204
ML-DSA SigGen	A6703	Signature Interfaces - external Pre Hash - preHash, pure Deterministic - No, Yes External Mu - No Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87 Message Length - Message Length: 8-65536 Increment 8 Hash Algorithms - SHA2-512 Context Length - Context Length: 0	FIPS 204
ML-DSA SigVer	A6703	Signature Interfaces - external Pre Hash - preHash, pure	FIPS 204

Algorithm	CAVP Cert	Properties	Reference
		External Mu - No Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87 Message Length - Message Length: 8-65536 Increment 8 Hash Algorithms - SHA2-512 Context Length - Context Length: 0	
ML-KEM EncapDecap	A6703	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768 Functions - Decapsulation, Encapsulation	FIPS 203
ML-KEM KeyGen	A6703	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768	FIPS 203
RSA KeyGen (FIPS186-5)	A6703	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 p mod 8 - 1 Primality Tests - 2powSecStr q mod 8 - 1 Fixed Public Exponent - 010001 Info Generated By Server - Yes Private Key Format - crt Public Exponent Mode - fixed	FIPS 186-5
RSA SigGen (FIPS186-5)	A6703	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5
RSA SigVer (FIPS186-4)	A6703	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA SigVer (FIPS186-5)	A6703	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
SHA-1	A6703	Message Length - Message Length: 160, 8-65536 Increment 8	FIPS 180-4
SHA2-224	A6703	Message Length - Message Length: 224, 8-65536 Increment 8	FIPS 180-4
SHA2-256	A6703	Message Length - Message Length: 256, 8-65536 Increment 8	FIPS 180-4
SHA2-384	A6703	Message Length - Message Length: 384, 8-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-512	A6703	Message Length - Message Length: 512, 8-65536 Increment 8	FIPS 180-4
SHA3-224	A6703	Message Length - Message Length: 8-65536 Increment 8	FIPS 202
SHA3-256	A6703	Message Length - Message Length: 8-65536 Increment 8	FIPS 202
SHA3-256	A6704	Message Length - Message Length: 8-65536 Increment 8	FIPS 202
SHA3-384	A6703	Message Length - Message Length: 8-65536 Increment 8	FIPS 202
SHA3-512	A6703	Message Length - Message Length: 8-65536 Increment 8	FIPS 202
SHAKE-128	A6703	Supports Bit-Oriented Messages - Yes Supports Empty Message - No Supports Bit-Oriented Output - Yes Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A6703	Supports Bit-Oriented Messages - Yes Supports Empty Message - No Supports Bit-Oriented Output - Yes Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SLH-DSA KeyGen	A6703	Parameter Sets - SLH-DSA-SHA2-128f, SLH-DSA-SHA2-128s, SLH-DSA-SHA2-192f, SLH-DSA-SHA2-192s, SLH-DSA-SHA2-256f, SLH-DSA-SHA2-256s, SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s	FIPS 205
SLH-DSA SigGen	A6703	Deterministic - No, Yes Signature Interfaces - external Pre Hash - preHash, pure Parameter Sets - SLH-DSA-SHA2-128f, SLH-DSA-SHA2-128s, SLH-DSA-SHA2-192f, SLH-DSA-SHA2-192s, SLH-DSA-SHA2-256f, SLH-DSA-SHA2-256s, SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s Message Length - Message Length: 8-65536 Increment 8 Hash Algorithms - SHA2-512, SHAKE-256 Context Length - Context Length: 0-8 Increment 8	FIPS 205
SLH-DSA SigVer	A6703	Signature Interfaces - external Pre Hash - preHash, pure Parameter Sets - SLH-DSA-SHA2-128f, SLH-DSA-SHA2-128s, SLH-DSA-SHA2-192f, SLH-DSA-SHA2-192s, SLH-DSA-SHA2-256f, SLH-DSA-SHA2-256s, SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s,	FIPS 205

Algorithm	CAVP Cert	Properties	Reference
		SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s Message Length - Message Length: 8-65536 Increment 8 Hash Algorithms - SHA2-512, SHAKE-256 Context Length - Context Length: 0-8 Increment 8	
TLS v1.2 KDF RFC7627 (CVL)	A6703	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 512-1024 Increment 8	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The module implements the FIPS vendor affirmed cryptographic algorithms listed below.

Name	Properties	Implementation	Reference
CKG	Key Type: Asymmetric and Symmetric	N/A	SP800-133rev2 Section 4 Example 1 and IG D.H
CKG-XTS	Key Type: Symmetric	N/A	SP800-133rev2 Sections 6.3 #2 and IG C.I

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module implements the FIPS Non-Approved but allowed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
ECDSA_secp256K1	Key Type:Asymmetric Curve Type:secp256k1 (128-bits)	csmsc1	IG C.A SP800-186 H.2
ECDSA_Brainpool	Key Type:Asymmetric Curve Type:brainpoolP224r1 (112-bits), brainpoolP256r1 (128-bits), brainpoolP320r1 (160-bits), brainpoolP384r1 (192-bits), brainpoolP512r1 (256-bits), brainpoolP224t1 (112-bits), brainpoolP256t1 (128-bits), brainpoolP320t1 (160-bits), brainpoolP384t1 (192-bits), brainpoolP512t1 (256-bits)	csmsc1	IG C.A SP800-186 H.1

Table 6: Non-Approved, Allowed Algorithms

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The Module implements the FIPS Non-Approved, Not Allowed cryptographic algorithms listed.

Name	Use and Function
SM2 [ISO/IEC14888-3:2018]	keySize:256 bit, function: Key Pair Generation, Signature Generation and Signature Verification, Data Encryption and Decryption
SM3 [ISO/IEC10118-3:2018]	Message Digest
SM4 [ISO/IEC18033-3]	ECB/CBC keySize:128 bit, function: keygen, Data Encryption and Decryption
Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	ECB, CBC, OFB, CFB1, CFB8, CFB64, CMAC key sizes 128/192 bits (effective security strength is 112bits), function: keygen, Data Encryption and Decryption, CMAC Generation and Verification
DSA [FIPS 186-4]	L=1024, N=160 L=2048, N=224 L=2048, N=256 L=3072, N=256 function: Key Pair Generation\Signature Generation\Signature Verification
RSA [FIPS 186-4]	keySize:1024 bits. Function: Key Generation, Signature Generation
ECIES	P192/224/256/384/521, brainpoolP224/256/320/384/512r1, brainpoolP224/256/320/384/512t1 Elliptic Curve Integrated Encryption Scheme function: Data Encryption and Decryption

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

The SFI table shows the Security Function Implementations that the module implements:

Name	Type	Description	Properties	Algorithms
ECDSAKeyGen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation	Publication: [IG C.A] [IG C.E]	ECDSA KeyGen (FIPS186-5): (A6703) Hash DRBG: (A6703) Counter DRBG: (A6703) CKG: () Key Type: Asymmetric and Symmetric ECDSA KeyVer (FIPS186-5): (A6703)
RSAKeyGen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation	Publication: [IG C.E],[IG C.F]	RSA KeyGen (FIPS186-5): (A6703) Hash DRBG: (A6703) Counter DRBG: (A6703) CKG: () Key Type: Asymmetric and Symmetric
AES Encryption	BC-UnAuth BC-UnAuthEncrypt	Block Cipher Encryption		AES-CBC: (A6703) AES-ECB: (A6703) AES-CTR: (A6703) AES-OFB: (A6703) AES-CFB1: (A6703) AES-CFB8: (A6703) AES-CFB128: (A6703)
AES Decryption	BC-UnAuth BC-UnAuthDecrypt	Block Cipher Decryption		AES-CBC: (A6703) AES-ECB: (A6703) AES-CTR: (A6703) AES-OFB: (A6703) AES-CFB1: (A6703)

Name	Type	Description	Properties	Algorithms
				AES-CFB8: (A6703) AES-CFB128: (A6703)
AES Encryption-XTS	BC-UnAuth BC-UnAuthEncrypt	Block Cipher Encryption		AES-XTS Testing Revision 2.0: (A6703)
AES Decryption-XTS	BC-UnAuth BC-UnAuthDecrypt	Block Cipher Decryption		AES-XTS Testing Revision 2.0: (A6703)
AES Encryption-Auth	BC-Auth BC-AuthEncrypt	Authenticated Block Cipher Encryption		AES-CCM: (A6703) AES-GCM: (A6703)
AES Decryption-Auth	BC-Auth BC-AuthDecrypt	Authenticated Block Cipher Decryption		AES-CCM: (A6703) AES-GCM: (A6703)
TLS-AES-Encrypt-GCM	BC-Auth BC-AuthEncrypt	Authenticated Block Cipher Encryption		AES-GCM: (A6703) AES Size: 128,256
TLS-AES-Decrypt-GCM	BC-Auth BC-AuthDecrypt	Authenticated Block Cipher Decryption		AES-GCM: (A6703) AES Size: 128,256
SymKeyGen	CKG	Symmetric Key Generation		Counter DRBG: (A6703) Hash DRBG: (A6703) CKG: () Key Type: Asymmetric and Symmetric CKG-XTS: () Key Type: Symmetric
ECDSASigGen	DigSig-SigGen	Digital Signature Generation		ECDSA SigGen (FIPS186-5): (A6703) SHA2-224: (A6703) SHA2-256: (A6703) SHA2-384: (A6703) SHA2-512: (A6703) SHA3-224: (A6703) SHA3-256: (A6703) SHA3-384: (A6703) SHA3-512: (A6703)
RSASigGen	DigSig-SigGen	Digital Signature Generation		RSA SigGen (FIPS186-5): (A6703) SHA2-224: (A6703)

Name	Type	Description	Properties	Algorithms
				SHA2-256: (A6703) SHA2-384: (A6703) SHA2-512: (A6703) SHA3-224: (A6703) SHA3-256: (A6703) SHA3-384: (A6703) SHA3-512: (A6703)
ECDSASigVer	DigSig-SigVer	Digital Signature Verification		ECDSA SigVer (FIPS186-4): (A6703) ECDSA SigVer (FIPS186-5): (A6703) SHA-1: (A6703) SHA2-224: (A6703) SHA2-256: (A6703) SHA2-384: (A6703) SHA2-512: (A6703) SHA3-224: (A6703) SHA3-256: (A6703) SHA3-384: (A6703) SHA3-512: (A6703)
RSASigVer	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-4): (A6703) RSA SigVer (FIPS186-5): (A6703) SHA-1: (A6703) SHA2-224: (A6703) SHA2-256: (A6703) SHA2-384: (A6703) SHA2-512: (A6703) SHA3-224: (A6703) SHA3-256: (A6703) SHA3-384: (A6703) SHA3-512: (A6703)
Entropy Conditioner	ENT-Cond	Entropy Source	Publication: [IG 9.3.A] [IG D.J] [IG D.K]	

Name	Type	Description	Properties	Algorithms
Entropy	ENT-ESV	Entropy Source	Publication: [IG 9.3.A] [IG D.J] [IG D.K]	
RBG	DRBG	Random Number Generation	Publication: [IG D.L]	Counter DRBG: (A6703) Hash DRBG: (A6703) SHA3-256: (A6704) AES-CTR: (A6703) AES Size: 256
KAS-ECC	KAS-Full KAS-SSC/KDF	Key Agreement For TLS session	Caveat: Key Agreement Scheme provides between 112 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A6703) TLS v1.2 KDF RFC7627: (A6703) SHA2-256: (A6703) SHA2-384: (A6703)
TLSKDF	KAS-135KDF	Key Derivation function Key Agreement	Publication: [IG 2.4.B] [IG D.F] [IG D.G]	TLS v1.2 KDF RFC7627: (A6703) SHA2-256: (A6703) SHA2-384: (A6703) SHA2-512: (A6703)
KBKDF	KBKDF	Key-Based Key Derivation		KDF SP800-108: (A6703) HMAC-SHA2-256: (A6703)
KTS-AES-Wrap	KTS-Wrap	Key Transport -Key Wrapping	Publication: [IG D.G]	AES-ECB: (A6703) AES Size: 256 HMAC-SHA2-256: (A6703)
KTS-AES-UnWrap	KTS-Unwrap	Key Transport -Key Unwrapping	Publication: [IG D.G]	AES-ECB: (A6703) AES Size: 256 HMAC-SHA2-256: (A6703)
AES-CMAC	MAC	Message Authentication Generation	:	AES-CMAC: (A6703)
HMACGen	MAC	Message Authentication Generation	Publication: [IG C.B]	HMAC-SHA-1: (A6703) HMAC-SHA2-224:

Name	Type	Description	Properties	Algorithms
				(A6703) HMAC-SHA2-256: (A6703) HMAC-SHA2-384: (A6703) HMAC-SHA2-512: (A6703) HMAC-SHA3-224: (A6703) HMAC-SHA3-256: (A6703) HMAC-SHA3-384: (A6703) HMAC-SHA3-512: (A6703)
TLS-HMAC	MAC	Message Authentication Generation	Publication: [IG C.B]	HMAC-SHA2-256: (A6703) HMAC-SHA2-384: (A6703)
Hash	SHA	Secure Hash Standard	Publication: [IG C.B] [IG C.C]	SHA-1: (A6703) SHA2-224: (A6703) SHA2-256: (A6703) SHA2-384: (A6703) SHA2-512: (A6703) SHA3-224: (A6703) SHA3-256: (A6703) SHA3-384: (A6703) SHA3-512: (A6703)
KTS-RSA-Encap	KTS-Encap	Key Transport (Key Encapsulation)	Publication: [IG D.G]	KTS-IFC: (A6703)
KTS-RSA-Decap	KTS-Decap	Key Transport (Key Decapsulation)	Publication: [IG D.G]	KTS-IFC: (A6703)
ML-DSA KeyGen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation		ML-DSA KeyGen: (A6703) CKG: ()

Name	Type	Description	Properties	Algorithms
				SHAKE-128: (A6703) SHAKE-256: (A6703)
ML-DSA SigGen External Pure	DigSig-SigGen	Digital Signature Generation	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:external Pre Hash:pure Deterministic:Yes, No	ML-DSA SigGen: (A6703) SHAKE-128: (A6703) SHAKE-256: (A6703)
ML-DSA SigGen External Pre-hash	DigSig-SigGen	Digital Signature Generation	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:external Pre Hash:preHash Deterministic:No Hash Algorithms:SHA2-512 Message Input:Message	ML-DSA SigGen: (A6703) SHAKE-128: (A6703) SHAKE-256: (A6703)
ML-DSA SigVer External Pure	DigSig-SigVer	Digital Signature Verification	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:external Pre Hash:pure	ML-DSA SigVer: (A6703) SHAKE-128: (A6703) SHAKE-256: (A6703)
ML-DSA SigVer External Pre-hash	DigSig-SigVer	Digital Signature Verification	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:external Pre Hash:preHash Hash Algorithms:SHA2-512	ML-DSA SigVer: (A6703) SHAKE-128: (A6703) SHAKE-256: (A6703)

Name	Type	Description	Properties	Algorithms
			Message Input:Message	
ML-KEM KeyGen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation		ML-KEM KeyGen: (A6703) CKG: () SHA3-256: (A6703) SHA3-512: (A6703) SHAKE-128: (A6703) SHAKE-256: (A6703)
ML-KEM encapsulation	KEM-Encap	Key Encapsulation	IG:IG D.S Scenario 1	ML-KEM EncapDecap: (A6703) SHA3-256: (A6703) SHA3-512: (A6703) SHAKE-128: (A6703) SHAKE-256: (A6703)
ML-KEM decapsulation	KEM-Decap	Key Decapsulation	IG:IG D.S Scenario 1	ML-KEM EncapDecap: (A6703) SHA3-512: (A6703) SHAKE-128: (A6703) SHAKE-256: (A6703) SHA3-256: (A6703)
SLH-DSA KeyGen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation		SLH-DSA KeyGen: (A6703) CKG: () SHAKE-256: (A6703) SHA2-512: (A6703) SHA2-256: (A6703)
SLH-DSA SigGen External Pure	DigSig-SigGen	Digital Signature Generation	Hash: Pure	SLH-DSA SigGen: (A6703) SHAKE-256: (A6703) SHA2-512: (A6703) HMAC-SHA2-512: (A6703) SHA2-256: (A6703)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-256: (A6703)
SLH-DSA SigGen External Pre-hash	DigSig-SigGen	Digital Signature Generation	Hash: Pre-hash	SLH-DSA SigGen: (A6703) SHAKE-256: (A6703) SHA2-512: (A6703) HMAC-SHA2-512: (A6703) SHA2-256: (A6703) HMAC-SHA2-256: (A6703)
SLH-DSA SigVer External Pure	DigSig-SigVer	Digital Signature Verification	Hash: Pure	SLH-DSA SigVer: (A6703) SHAKE-256: (A6703) SHA2-512: (A6703) SHA2-256: (A6703)
SLH-DSA SigVer External Pre-hash	DigSig-SigVer	Digital Signature Verification	Hash: Pre-hash	SLH-DSA SigVer: (A6703) SHAKE-256: (A6703) SHA2-512: (A6703) SHA2-256: (A6703)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

KAS-ECC [56Ar3] - Per [IG] D.F Scenario 2 path (2), compliant with the derivation of a shared secret Z in one or more of the key agreement schemes in Section 6 of SP 800-56Arev3. SP800-135 TLS KDF is used to derive symmetric keys from the shared secret Z.

AES GCM IV Uniqueness

FIPS 140-3 IG C.H, Option 1

TLS v1.2**:** The Module is compliant with TLS v1.2 and SP800-52 Rev2, Section 3.3.1.
The Module supports TLS 1.2 GCM Cipher Suites for TLS, as described in RFCs 5116, 5246, 5288 and 5289 and shall only be used for the TLS protocol version 1.2 to be compliant with FIPS 140-3 IG C.H, Option 1.

The operations of one (the server) of the two parties involved in the TLS key establishment scheme are performed entirely within the cryptographic boundary of the module. IV is generated internally to the cryptographic module. The counter portion of the IV is set by the Module within its cryptographic boundary.

The nonce_explicit part of the IV is incremented each time an AES GCM computation is performed. The Module establishes a new session key when the nonce_explicit part of the IV exhausts the maximum number of possible values (2^{32}-1).

In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

Note: No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

FIPS140-3 IG C.H, Option 2

For AES GCM encryption, the module generates a random, 96-bit initialization vector (IV), using the SP800-90A DRBG implemented in the module's boundary as defined in section 8.2.2 of [SP800-38D]. The module is compliant with scenario 2 of FIPS 140-3 IG C.H.

In case of loss of power, any request provided with a specific IV will need to be re-initiated.

AES-XTS

The AES algorithm in XTS mode can be only used for the cryptographic protection of data on storage devices, as specified in [SP800-38E]. In addition, the length of a single data unit encrypted with the XTS-AES shall not exceed 2^{20} AES blocks, that is, 16 MiB of data. The module verifies that each key stored in the module is not used for data encryption beyond the limit of 215 blocks by using a counter of the number of encryptions performed with each key since its generation.

For those keys provided by external entities as part of the cryptographic service requests, the verification of this limit must be enforced by the entities that request the service (e.g. server

applications).

In addition, to meet the requirement in [FIPS140-3_IG] C.I, the module implements a check to ensure that the two AES keys used in XTS-AES algorithm are not identical.

ML-KEM
The module does not establish SSPs using an approved key encapsulation mechanism (KEM). However, it does offer some or all of the underlying KEM cryptographic functionality to be used by an external operator/application as part of an approved KEM.

When using an externally obtained ML-KEM static public encapsulation key, the operator shall ensure that proof of possession of the private key prior to invoking the ML-KEM encapsulation service. Such assurance may be obtained through a trusted third party (e.g., a certificate authority) or another mechanism appropriate for the deployment, consistent with RM3 and the guidance of Section 4.5 of SP 800-227.

2.8 RBG and Entropy

Cert Number	Vendor Name
E267	Sansec Technology Co., Ltd.

Table 9: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Sansec Jent Entropy Source for HSM	Non-Physical	Intel Xeon Gold5218; KVM CPU passthrough on QEMU virtualization on Intel Xeon Gold 5218	256 Bit	256 bits	SHA3-256 (Cert. #A6704)

Table 10: Entropy Sources

2.9 Key Generation

For Key Generation, see Section 2.5 and Section 2.6 above.

2.10 Key Establishment

Key Agreement Information

For Key Agreement, see Section 2.5 and Section 2.6 above.

Key Transport Information

For Key Transport, see Section 2.5 and Section 2.6 above.

2.11 Industry Protocols

The module implements the following TLS Cipher Suites.

Protocol*	Key Exchange	Server/ Host Auth	Cipher	Integrity
TLS [IG D.F and SP 800-135]	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS v1.2			
	Ephemeral ECDH	RSA	AES-GCM-256	AES-GCM SHA2-384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS v1.2			
	Ephemeral ECDH	RSA	AES-GCM-128	AES-GCM SHA2-256
	TLS_RSA_WITH_AES_128_GCM_SHA256 TLS v1.2			
	RSA	RSA	AES-GCM-128	AES-GCM SHA2-256
	TLS_RSA_WITH_AES_256_GCM_SHA384 TLS v1.2			
	RSA	RSA	AES-GCM-256	AES-GCM SHA2-384

Table 11 Protocol Cipher Suites

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
Power switch button	Control Input	Machine Power On/Power Off
Power inlet ports	Power	Redundant power supply units, Power Input
LCD	Status Output	Show error state, processor info, network info, OS info.
Cryptographic Card LED	Status Output	Show the working status of the Cryptographic Card
Machine working status LED	Status Output	Show the working status of the machine
Network Interface LED	Status Output	Show the working status of the network interface, such as LAN1 and LAN2
HDD status LED	Status Output	Show the working status of the hard disk
Power On LED	Status Output	System power-on
Ethernet (RJ-45 ports/LC fiber ports)	Data Input Data Output Status Output	Input data: raw data, ciphertext or signature data, encryption key and other key management data, status information from external sources, other input data. Output data: raw data, ciphertext data and digital signatures, encryption key and other key management data, and other information output from the module after processing or storage Status out: Success or error status out.
RS232	Control Input	Serial management instruction; Management port
Active key destruction switch	Control Input	Control signal
VGA	Status Output	Display the startup status of the module

Table 12: Ports and Interfaces

Note: The module does not support Control Output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The Module's authentication methods are listed in table below.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
TokenAuthenticationMethod	Identity-based - The module uses a role selection mechanism, identifying roles and identities by obtaining an ID and type.	Challenge-response mechanism (RBG, RSASigVer) with the user's credentials (a 2048-bit RSA key pair (Cert #A6703) stored in the user's USB token).	2048-bit RSA key pair. According to [SP800-57],such a key provides a security strength of 112 bits. 2^-112 10^-33	The probability of successful authentication by guessing the private key is 2^-112 10^-33. The module performs RSA-2048 signature verification internally, with each verification taking approximately 1ms (in practice, it may take longer). Since concurrent authentication is not supported, the maximum number of attempts per minute is capped at 60,000. Hence, the probability of success per minute is: 60000*2^-112 10^-29.
CertAuthenticationMethod	Identity-based - The module uses certificate CN and challenge-response	Challenge-response mechanism with the standard TLS protocol	2048-bit RSA key pair. According to [SP800-57],such a	The module performs RSA-2048 signature verification internally, with each

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	mechanism for user role authentication. (All certificates are issued by trusted Certificate Authorities).	(RBG, RSASigGen, RSASigVer) and user's credentials (a 2048-bit RSA key pair (Cert #A6703) stored in the user's PKCS#12 (pfx) file).	key provides a security strength of 112 bits. 2^-112 10^-33	verification taking approximately 1ms (in practice, it may take longer). The maximum number of attempts per minute is capped at 60,000. The probability of success per minute is: 60000*2^-112 10^-29.

Table 13: Authentication Methods

4.2 Roles

The Module supports four distinct roles, User (User Application), and Cryptographic Officer (CO: Administrator, Auditor and Operator). The CO's three roles can be assigned to users of the module that performs management operations. The User Application role is a user role assigned to external entities (user application) that connect to the module through the network port to request cryptographic services.
A CO can have only one fixed role assigned: Administrator, Operator or Auditor. After the CO identifies and authenticates to the module, the associated role is automatically assigned to the CO.
The cryptographic module enforces the separation of roles, a CO remains authenticated until the CO logs out from the module, or the module is powered off (no authentication data remains in the module). A User Application remains authenticated only during the life span of the network session, or until the module is powered off (no authentication data remains in the module).

The Roles Table below lists all operator roles supported by the Module.

The module does not support a maintenance role.

The Module does not support concurrent operators, such as operator or auditor is authenticated next after the administrator authentication, The module will prompt that the authenticated role must be logged out first. But multiple administrator roles can authenticate to the module through the same session of a web management terminal, there is no need for the previously authenticated administrator to log out.

Different CO roles are not allowed to authenticate simultaneously through different web management terminals.

Within the VSM, the management service and the cryptographic service are two separate independent processes. For each client connection, the cryptographic service starts a corresponding subprocess. COs authenticate to the management service and obtain the corresponding permissions to access the management interface. User applications authenticate to the cryptographic service and obtain the corresponding permissions to access the cryptographic service. The results of role authentication are stored in the corresponding process space in the VSM. The module maintains the separation of roles and services through these independent processes associated with each access.

Name	Type	Operator Type	Authentication Methods
Administrator	Identity	CO	TokenAuthenticationMethod
Auditor	Identity	CO	TokenAuthenticationMethod
Operator	Identity	CO	TokenAuthenticationMethod
User Application	Identity	User	CertAuthenticationMethod

Table 14: Roles

Every CO role requires a unique USB token. By default, three administrators, one operator, and one auditor are required, which means five USB tokens are needed by default. In addition, three more USB tokens are provided as backups (One allocated to the administrator, operator, and auditor respectively).

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:
Services that do not require an authorized role are marked as “Unauthenticated”.

The SSPs modes of access shown in the table below 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 (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
View device information (Show Version)	Show module's VSM versioning information.	Success: Successfully navigated to the Device Info page. Error Failed to navigate to the Device Info page.	N/A	sPn, msg, sManufacturer, nVersion, sHn, nSystemVersion, sDn, hardareVersion, sSn, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
View device operating information (Show Status)	Show module's VSM running status information.	Success: Successfully navigated to the Service status page. Error Failed to navigate to the Service status page.	N/A	msg, serviceStatus, currentCount, run, isRun, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
View approved mode	Show module's FIPS mode ("approved mode" or "non-	Success: Successfully navigated to the Set Approved mode page. Error Failed to navigate to the Set Approved mode page.	N/A	deviceType, msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	approved mode").					
Set approved mode	Set module into approved or non-approved mode.	Success: Config Approved mode successfully. Please log in to the system again or Config non-Approved mode successfully. Please log in to the system again. Error: Management operation failed.	fType	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - SPK: Z - Root LMK: Z - LMK: Z - User RSA-priv: Z - User RSA-pub: Z - User ECDSA-priv: Z - User ECDSA-pub: Z - User MLDSA-priv: Z - User MLDSA-pub: Z - User MLKEM-priv: Z - User MLKEM-pub: Z - User SLHDSA-priv: Z - User SLHDSA-pub: Z - User AES-128 keys: Z - User AES-192 keys: Z - User AES-256 keys: Z - User HMAC keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Crypto Officer RSA public key: Z - TLS-Host-Pub: Z - TLS-Host-Priv: Z - TLS-SENC: E
Self-test	Start pre-operational and conditional self-tests of VSM	Success: Device self-test Log refreshed successfully. Error Management operation failed.	N/A	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E
View selftest log	view self-test log information.	Success: Successfully view self-test log information. Error Failed to view self-test log information.	N/A	File stream	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
Download selftest log	download self-test error log information.	Success: Successfully download self-test error log. Error Management operation failed.	N/A	fileName, success, fileCode, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E
View management logs	Show Administrator and Operator's management logs	Success: Successfully Show Administrator and Operator's management logs. Error Management operation failed.	N/A	code, data:msg, ipAddress, operateType, id, audited, createTimeS, operator, count	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Auditor - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
audit management log	Audit management logs	Success: Audit log successfully. Error: Management operation failed	id	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Auditor - TLS-SENC: E
export management log	Export management logs	Success: Export management log successful Error: Management operation failed	N/A	file stream	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Auditor - TLS-SENC: E
View login status	Show current id's auth login status.	Success: Successfully navigated to the User login page Error: Failed to navigate to the User login page.	N/A	msg, ManagerExist, OperatorCount, OperatorPINExist, OperatorLogonStatus, auditor, spkFlag, InitState, ManagerCount, AuditorLogon, ReserveStates, AuditorExist, OperatorLogon, AuditorCount, ManagerLogon, OperatorExistStatus, OperatorExist, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
User login	CO auth Login	Success: No.1 Auditor/Operator/Administrator remote login succeeded. Error:Failure in vsm	userValue, signData	status	RSASigVer RBG Entropy Entropy Conditioner TLS-AES-	Administrator - DRBG-EI: E,G - DRBG-State: E,G - DRBG-Seed: E,G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		Crypto Officer authentication			Encrypt-GCM TLS-AES-Decrypt-GCM	- Crypto Officer RSA public key: E - TLS-SENC: E Auditor - DRBG-EI: E,G - DRBG-State: E,G - DRBG-Seed: E,G - Crypto Officer RSA public key: E - TLS-SENC: E Operator - DRBG-EI: E,G - DRBG-State: E,G - DRBG-Seed: E,G - Crypto Officer RSA public key: E - TLS-SENC: E
User logout	CO auth Logout	Suceess: Logout {Auditor/Operator/Administrator} successfully.	nSel	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
Modify USB token PIN	Modify CO usb-token PIN	Success: PIN changed successfully. Error: Management operation failed	oldPin,newPin,pinType	status, value	TLS-AES-Encrypt-GCM TLS-AES-	Administrator - TLS-SENC: E Auditor - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Decrypt-GCM	Operator - TLS-SENC: E
Add administrator	Add a new administrator CO	Success: Remote add No.{index} Administrator succeeded. Error: Management operation failed	updateFlag, step, pubkeyStr, pubkeyIdStr, usrValue, addType	msg, usrId, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - Crypto Officer RSA public key: W - TLS-SENC: E
Delete administrator	Delete an administrator CO	Success: Delete the administrator success. Error: Mangement opration failed	unMgrNo	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E
Add operator	Add a new operator CO	Success Remote add No.1 Operator succeeded. Error Mangement opration failed	updateFlag, step, pubkeyStr, pubkeyIdStr, usrValue, addType	msg,usrId,status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - Crypto Officer RSA public key: W - TLS-SENC: E
delete operator	Delete an operator CO	Success Delete the operator successfully. Error Mangement opration failed	nSel	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E
Add auditor	Add a new auditor CO	Success Remote add No.1 Auditor succeeded. Error Mangement opration failed	updateFlag, step, pubkeyStr, usrValue, addType	msg, usrId, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - Crypto Officer RSA public key: W - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
delete auditor	Delete an auditor CO	Success Delete the auditor successfully. Error Mangement opration failed	nSel	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E
VSM initialization	Clear all permission information and key information stored in the VSM. use DRBG generate System Protection Key during VSM initialization	Success: Initialize the hsm successfully. Error: Management operation failed	N/A	status, spk components	KTS-RSA-Encap SymKeyGen RBG Entropy Entropy Conditioner TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - SPK: G,R,Z - Root LMK: Z - LMK: Z - User RSA-priv: Z - User RSA-pub: Z - User ECDSA-priv: Z - User ECDSA-pub: Z - User MLDSA-priv: Z - User MLDSA-pub: Z - User MLKEM-priv: Z - User MLKEM-pub: Z - User SLHDSA-priv: Z - User SLHDSA-pub: Z - User AES-128 keys: Z - User AES-192 keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- User AES-256 keys: Z - User HMAC keys: Z - Crypto Officer RSA public key: E,Z - TLS-Host-Priv: Z - TLS-Host-Pub: Z - DRBG-EI: G,E - DRBG-Seed: G,E - DRBG-State: G,E - TLS-SENC: E
Import System Protection Key	Import System Protection Key during CO login after the VSM restarts	Success Import spk Successful. Error Management operation failed	spk components	status	KTS-RSA-Decap TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM AES Decryption	Administrator - SPK: W,E - TLS-Host-Pub: R - TLS-Host-Priv: E - TLS-SENC: E
Generate Local Master Key (LMK)	Generate Local Master Key (LMK) Use DRBG	Success Generate LMK successfully. Error Management operation failed	N/A	msg, status	SymKeyGen KBKDF AES Encryption RBG Entropy	Administrator - Root LMK: G,E - LMK: G,E - SPK: E - DRBG-EI: E - DRBG-Seed:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and KBKDF				Entropy Conditioner TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	E - DRBG-State: E - TLS-SENC: E
View LMK check value	View LMK check value	Success Successfully navigated to the LMK management page. Error Failed to navigate to the LMK management page.	index	msg, operationMsg, logMsg, status	AES Encryption TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - LMK: E - TLS-SENC: E Auditor - LMK: E - TLS-SENC: E Operator - LMK: E - TLS-SENC: E
Generate RSA key pair	Generate RSA key pair Use DRBG	Success Generate {index} key pair successfully. Error Management operation failed	algorithm=RSA, index, length, usage, curetype Command and parameters	msg, status	RSAKeyGen Entropy RBG AES Encryption Entropy Conditioner TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - User RSA-priv: G - User RSA-pub: G - SPK: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E - TLS-SENC: E
Delete RSA key pair	Delete RSA key pair	Success Delete {index} key pair successfully.	algorithm=RSA, index, usage	msg, status	TLS-AES-Encrypt-GCM	Administrator - User RSA-priv: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		Error Management operation failed			TLS-AES-Decrypt-GCM	- User RSA-pub: Z - TLS-SENC: E
View RSA key status	View RSA key status	Success Successfully navigated to the RSA key management page. Error Failed to navigate to the RSA key management page.	algorithm=RSA	msg, code, data:index, level, model, count, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
Generate ECDSA key pair	Generate ECDSA key pair Use DRBG	Success Generate {index} key pair successfully. Error Management operation failed	algorithm=ECC, index, length, usage, curetype	msg, status	ECDSAKeyGen Entropy RBG AES Encryption Entropy Conditioner TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - User ECDSA-priv: G - User ECDSA-pub: G - SPK: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E - TLS-SENC: E
Delete ECDSA key pair	Delete ECDSA key pair	Success: Delete {index} key pair successfully. Error: Management operation failed.	algorithm=ECC, index, usage	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - User ECDSA-priv: Z - User ECDSA-pub: Z - TLS-SENC: E
View ECDSA key status	View ECDSA key status	Success: Successfully navigated to the ECDSA key status page. Error: Failed to navigate to the	algorithm=ECC	msg, code, data:cureType, index, level, model, count, status	TLS-AES-Encrypt-GCM TLS-AES-	Administrator - TLS-SENC: E Auditor - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		ECDSA key status page.			Decrypt-GCM	Operator - TLS-SENC: E
Generate PQC key pair	Generate ML-DSA or ML-KEM key or SLH-DSA pair Use DRBG. The key is not output and stays inside the module.	Success: Generate {index} key pair successfully. Error: Management operation failed.	index, algorithm, level, slh_mode, hash_mode	msg, status	AES Encryption TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM Entropy Conditioner Entropy RBG ML-DSA KeyGen ML-KEM KeyGen SLH-DSA KeyGen	Administrator - User MLDSA-priv: G - User MLDSA-pub: G - User MLKEM-priv: G - User MLKEM-pub: G - User SLHDSA-priv: G - User SLHDSA-pub: G - SPK: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E - ML-DSA seed: G,E - ML-KEM seed: G,E - TLS-SENC: E
Delete PQC key pair	Delete ML-DSA or ML-KEM or SLH-DSA key pair	Success: Delete {index} key pair successfully. Error: Management operation failed.	algorithm=PQC, index	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - User MLDSA-priv: Z - User MLKEM-priv: Z - User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						SLHDSA-priv: Z - User MLDSA-pub: Z - User MLKEM-pub: Z - User SLHDSA-pub: Z - TLS-SENC: E
View PQC key status	View PQC key status	Success: Successfully navigated to the PQC key status page. Error: Failed to navigate to the PQC key status page.	algorithm=PQC	msg, code, data:algorithm, index, level, model, count, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
Generate symmetric key	Generate symmetric key for AES Use DRBG	Success: Successfully generated {index} sysmmetric key. Error: Management operation failed.	keyIndex, keyLength, algorithm	msg, status	SymKeyGen AES Encryption RBG Entropy Entropy Conditioner TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - User AES-128 keys: G - User AES-192 keys: G - User AES-256 keys: G - User HMAC keys: G - SPK: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E - TLS-SENC: E
Delete symmetric key	Delete symmetric key for AES	Success: Delete {index} symmetric key successfully. Error:	index	msg, status	TLS-AES-Encrypt-GCM TLS-AES-	Administrator - User AES-128 keys: Z - User AES-192

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		Management operation failed.			Decrypt-GCM	keys: Z - User AES-256 keys: Z - User HMAC keys: Z - TLS-SENC: E
View symmetric key status	View symmetric key status	Success: Successfully navigated to the symmetric key status page. Error: Failed to navigate to the symmetric key status page.	N/A	msg, code,data:index, length, serialNumber, tag, usage, count, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
View symmetric key check value	View symmetric key check value	Success: Successfully show check value. Error: Failed to show check value.	index	verifyValue, msg, status	AES Encryption TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - User AES-128 keys: E - User AES-192 keys: E - User AES-256 keys: E - TLS-SENC: E Auditor - User AES-128 keys: E - User AES-192 keys: E - User AES-256 keys: E - TLS-SENC: E Operator - User AES-128 keys: E - User AES-192 keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- User AES-256 keys: E - TLS-SENC: E
Backup cryptographic module	Backup cryptographic module	Success: Successfully download backup file. Error: Management operation failed.	part, usrValue; FileStr, envelope, partInfo, type; bacType, alg, index; methodtoken	envBase64, msg, status; encStr,status; msg, status; FileStream	AES Encryption TLS-AES-Encrypt-GCM KTS-RSA-Encap SymKeyGen RBG Entropy Entropy Conditioner TLS-AES-Decrypt-GCM	Administrator - Backup key: G,R,E,Z - Backup file: R,Z - Crypto Officer RSA public key: E - TLS-SENC: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E
Restore cryptographic module	Restore cryptographic module	Success: Recover the key successfully.Delete the recovery file successfully. Error: Management operation failed.	File Stream; restoreType; FileStr; FileStr,envelope,partInfo,type; Part,envBase64; restoreTypestartIndex	msg, partCount, status; msg, status; msg, pukBase64_4,pukBase64, status; encStr,status; encStr,status; msg, pukBase64, status; msg, status	AES Decryption TLS-AES-Decrypt-GCM KTS-RSA-Decap TLS-AES-Encrypt-GCM	Administrator - Backup key: W,E,Z - Backup file: W,Z - TLS-Host-Pub: R - TLS-Host-Priv: E - TLS-SENC: E
View service status (Show Status)	View service running status	Success: Successfully navigated to the service status page. Error: Failed to navigate to the service status page.	N/A	msg, serviceStatus, currentCount, run, isRun, status	TLS-AES-Encrypt-GCM TLS-AES-	Administrator - TLS-SENC: E Auditor - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Decrypt-GCM	Operator - TLS-SENC: E
View service configuration	View service configuration parameters	Success: Successfully navigated to the service configuration page. Error: Failed to navigate to the service configuration page.	N/A	sslmode, msg, nSessionTimeout, nOnboot, nMaxConcurrent, sslalgorithm, nPort, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
Modify service configuration	Modify service configuration parameters	Success: Start the service successfully. Error: Management operation failed.	nPort, nSessionTimeout, nOnboot, nMaxConcurrent, sslmode, sslalgorithm	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E
View white list	View ip white-list	Success: Successfully navigated to the Whitelist management page. Error: Failed to navigate to the Whitelist management page.	N/A	msg, code, data:count, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
Add white list	Add ip white-list	Success: Add in the white list successfully. Error: Management operation failed	family=ipv4, address, port	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E
Delete white list	delete ip white-list	Success: Delete in the white list successfully. Error: Management operation failed	Addres, family=IPv4	msgstatus	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
View CN item	View the CN of client certificates that allow access to cryptographic devices	Success: Successfully navigated to the CN item management page. Error: Failed to navigate to the CN item management page.	N/A	msg, code,data:count, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Administrator - TLS-SENC: E Auditor - TLS-SENC: E Operator - TLS-SENC: E
CN item configuration	Add the CN of client certificates that allow access to cryptographic devices	Success Add CN item successfully Error: Management operation failed	CNInfo	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E
Delete CN item	Delete the CN of client certificates that allow access to cryptographic devices	Success Successfully delete CN item Error: Management operation failed	name	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E
Start service	Start service	Success: Start the service successfully. Error: Management operation failed	N/A	msg, status	KBKDF TLS-AES-Encrypt-GCM	Operator - hmackey_masterkey: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					TLS-AES-Decrypt-GCM	- hmackey for KTS-AES: G - TLS-SENC: E
Restart service	Restart service	Success Start the service successfully. Error: Management operation failed	N/A	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E
Stop service	Stop service	Success Start the service successfully. Error: Management operation failed	N/A	msg, status	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-SENC: E
Generate TLS certificate request	Generate certificate request using TLS keypair	Successoperation_successful Error: Management operation failed	commonName, organizationName, unitName, localityName, provinceName, countryName, keyAlgorithm, keySize	msg, status	RSAKeyGen AES Encryption RSASigGen RBG Entropy Entropy Conditioner TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	Operator - TLS-Host-Priv: G,E - TLS-Host-Pub: G - SPK: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E - TLS-SENC: E
update TLS certificate	Update TLS and	Success Service_restart_in_prog	Ca cert, Server cert,	msg, status	TLS-AES-Encrypt-GCM	Operator - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	root certificate	ress Error Management operation failed			TLS-AES-Decrypt-GCM	
mgt login	VSM management ervice web login	Success: Login successfully. Error: Management operation failed	Password - NOT a FIPS Password	status	None	Unauthenticated
mgt logout	VSM management ervice web logout	Success: Logout successfully.	N/A	status	None	Unauthenticated
Display host hsm information (Show Version)	Display module's host hsm version, network, vsm list info	Status: 4**/5**-error, 200-success.	chsm info	id, version, productName, productModel, hardwareVersion, ip, ntpaddr, ntpsyncperiod, imageuploadurl, syslogurl, vsmids, netaddr, dnslist, extensions	None	Unauthenticated
Modify host hsm network configuration	Modify host hsm network configuration	Status: 4**/5**-error, 200-success.	chsm network name, ip, mask, gateway	status, message	None	Unauthenticated
start self-test	Start pre-operational self-tests of host/hsm.	Status: result 1-error, result 0-success.	selfCheck	The result of command 'selfCheck'	None	Unauthenticated
Modify vsm	Modify vsm	Status: 4**/5**-error, 200-success.	vsm network vsmId, ip, mask, gateway	status, message	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
network configuration	network configuration					
view vsm info	View vsm info	Status: 4**/5**-error, 200-success.	vsm info vsmId	status, msg ,result	None	Unauthenticated
Start vsm	Start vsm	Status: 4**/5**-error, 200-success.	vsm start vsmId	status, message	None	Unauthenticated
Stop vsm	Stop vsm	Status: 4**/5**-error, 200-success.	vsm stop vsmId	status, message	None	Unauthenticated - SPK: Z - Root LMK: Z - LMK: Z - User RSA-priv: Z - User RSA-pub: Z - User ECDSA-priv: Z - User ECDSA-pub: Z - User MLDSA-priv: Z - User MLDSA-pub: Z - User MLKEM-priv: Z - User MLKEM-pub: Z - User SLHDSA-priv: Z - User SLHDSA-pub: Z - User AES-128 keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- User AES-192 keys: Z - User AES-256 keys: Z - User HMAC keys: Z - hmackey for KTS-AES: Z - DRBG-EI: Z - DRBG-Seed: Z - DRBG-State: Z - TLS-MS: Z - TLS-SENC: Z - TLS-SMAC: Z
Create vsm	Create vsm	Status: 4**/5**-error, 200-success.	vsm create vsmType vsmVer	status, message, vsmId	None	Unauthenticated
Delete vsm	Delete vsm	Status: 4**/5**-error, 200-success.	vsm delete vsmId	status, message	None	Unauthenticated - Root LMK: Z - LMK: Z - User RSA-priv: Z - User RSA-pub: Z - User ECDSA-priv: Z - User ECDSA-pub: Z - User MLDSA-priv: Z - User MLDSA-pub: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- User MLKEM-priv: Z - User MLKEM-pub: Z - User SLHDSA-priv: Z - User SLHDSA-pub: Z - User AES-128 keys: Z - User AES-192 keys: Z - User AES-256 keys: Z - User HMAC keys: Z - hmackey_masterkey: Z - Crypto Officer RSA public key: Z - TLS-Host-Priv: Z - TLS-Host-Pub: Z
Key generation	Generate key using DRBG	Data out-success. No data output-error	Command code: A0, Mode, Key type, Key Scheme	Key, keyHmac, Key check value	SymKeyGen KTS-AES-Wrap RBG Entropy Entropy Conditioner	User Application - User AES-128 keys: G,R - User AES-192 keys: G,R - User AES-256 keys: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	- User HMAC keys: G,R - LMK: E - hmackey for KTS-AES: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E - TLS-SENC: E
Data encryption	Encrypt data using a symmetric key	Data out-success. No data output-error	Command code: DF,Algorithm flag, Mode flag, Key Type, Key, keyHmac, Key 2, Key2Hmac, Padding mode, IV, Data length, Data,	Cipher data length, Cipher data	AES Encryption AES Encryption-XTS KTS-AES-UnWrap TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User AES-128 keys: E,W - User AES-192 keys: E,W - User AES-256 keys: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
Data decryption	Decrypt data using a symmetric key	Data out-success. No data output-error	Command code:DH, Algorithm flag, Mode flag, Key Type, Key, keyHmac, Key 2, Key2Hmac, Padding mode, IV, Data length, Data,	Plain data length, Plain data	AES Decryption AES Decryption-XTS KTS-AES-UnWrap TLS-AES-Encrypt-GCM	User Application - User AES-128 keys: E,W - User AES-192 keys: E,W - User AES-256 keys: E,W - LMK: E - hmackey for

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					TLS-AES-Decrypt-GCM	KTS-AES: E - TLS-SENC: E
AES GCM Data encryption	Encrypt data using AES-GCM	Data out-success. No data output-error	Command code: TO, Algorithm flag, Mode flag, Key Type, Key, tag length, AAD Length, AAD, Data Length, Data	Cipher data length, Cipher data, tag length, Tag, IV Length, Iv	AES Encryption-Auth KTS-AES-UnWrap TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User AES-128 keys: E,W - User AES-192 keys: E,W - User AES-256 keys: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
AES GCM Data decryption	Decrypt data using AES-GCM	Data out-success. No data output-error	Command code: TP, Algorithm flag, Mode flag, Key Type, Key, IV length, IV, AAD Length, AAD, tag length, Tag, Cipher data length, Cipher data	Authentication status, Data Length, Data	AES Decryption-Auth KTS-AES-UnWrap TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User AES-128 keys: E,W - User AES-192 keys: E,W - User AES-256 keys: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
AES CCM Data decryption	Decrypt data using AES-CCM	Data out-success. No data output-error	Command code: TS, Algorithm flag, Mode flag, Key Type, Key, Nonce length, Nonce, Adata length, Adata, TagLen, Tag, Cipher	Authentication status, Plain data length, Plain data	AES Decryption-Auth KTS-AES-UnWrap TLS-AES-Encrypt-	User Application - User AES-128 keys: E,W - User AES-192 keys: E,W - User AES-256

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			data length, Cipher data		GCM TLS-AES-Decrypt-GCM	keys: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
AES CCM Data encryption	Encrypt data using AES-CCM	Data out-success. No data output-error	Command code: TR, Algorithm flag, Mode flag, Key Type, Key, Nonce Length, Nonce, Adata Length, Adata, Payload data length, Payload data	Cipher data length, Cipher data, tag length, Tag	AES Encryption-Auth KTS-AES-UnWrap TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User AES-128 keys: E,W - User AES-192 keys: E,W - User AES-256 keys: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
CMAC generation and verification	Generate and verify CMAC	Data out-success. No data output-error	Command code: TQ,Mode, Algorithm flag, Key type, Key, CMAC length, Mac, Data length, Data	CMAC Length, CMAC	AES-CMAC KTS-AES-UnWrap TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User AES-128 keys: E,W - User AES-192 keys: E,W - User AES-256 keys: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
HMAC generation	Genarate HMAC	Data out-success. No data output-error	Command code: XE, Algorithm type, Key type, Key, Data length, Data,	HMAC Length, HMAC	HMACGen KTS-AES-UnWrap TLS-AES-Encrypt-	User Application - LMK: E - hmackey for KTS-AES: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					GCM TLS-AES-Decrypt-GCM	- User HMAC keys: E,W - TLS-SENC: E
RSA key pair generation	Generate RSA key pair	Data out-success. No data output-error	Command code: EI, Key type, Key length, Public key encoding, Public exponent length, Public exponent,	Public key, Secret key length, Secret key, keyHmac	RSAKeyGen KTS-AES-Wrap TLS-AES-Encrypt-GCM RBG Entropy Entropy Conditioner TLS-AES-Decrypt-GCM	User Application - User RSA-priv: G,R - User RSA-pub: G,R - LMK: E - TLS-SENC: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E
RSA public key export	Export RSA public key	Data out-success. No data output-error	Command code: EJ, Key index	Public key	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User RSA-pub: R - TLS-SENC: E
RSA public key encryption	Encrypt data using RSA public key	Data out-success. No data output-error	Command code: ER, Algorithm Identifiers, Pad Mode, Data length, Message data, Delimiter, Key index, Public key	Encrypted data length, Encrypted data	KTS-RSA-Encap TLS-AES-Decrypt-GCM TLS-AES-Encrypt-GCM	User Application - User RSA-pub: E,W - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
RSA private key decryption	Decrypt data using RSA private key	Data out-success. No data output-error	Command code: EP, Algorithm Identifiers, Pad Mode, Data length, Message data, Delimiter, Key index, Private key length, Private key	Decrypted data length, Decrypted data	KTS-RSA-Decap KTS-AES-UnWrap TLS-AES-Decrypt-GCM TLS-AES-Encrypt-GCM	User Application - User RSA-priv: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
RSA digital signature generation	Generate signature for data	Data out-success. No data output-error	Command code: EW, HASH Algorithm Identifiers, Signature Algorithm Identifiers, Padding mode, Data length, Message data, Delimiter, Key index, Private key length, Private key	Signature data length, Signature data	RSASigGen KTS-AES-UnWrap TLS-AES-Decrypt-GCM TLS-AES-Encrypt-GCM	User Application - User RSA-priv: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
RSA digital signature verification	Signature verification	Data out-success. No data output-error	Command code: EY, HASH Algorithm Identifiers, Signature Algorithm Identifiers, Pad mode,saltlen, Signature data length, Signature data, Delimiter, Data length, Message data, Delimiter, Key index, Public key	Error code	RSASigVer TLS-AES-Decrypt-GCM TLS-AES-Encrypt-GCM	User Application - User RSA-pub: E,W - TLS-SENC: E
ECDSA key pair	Generate ECDSA key pair	Data out-success. No data output-error	Command code: TA, Curve flag, Modulus length	Public key length, Public key, Secret	ECDSAKeyGen Entropy	User Application - User ECDSA-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
generation				key length, Secret key, keyHmac	RBG KTS-AES-Wrap TLS-AES-Encrypt-GCM Entropy Conditioner TLS-AES-Decrypt-GCM	priv: G,R - User ECDSA-pub: G,R - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E
ECDSA public key export	Export ECDSA public key	Data out-success. No data output-error	Command code: TH, Key index	Curve flag, Key Bite Length, Public key length, Public key	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User ECDSA-pub: R - TLS-SENC: E
ECDSA digital signature generation	Generate signature for data	Data out-success. No data output-error	Command doce:TB, HASH Flag, Data block length, Data, End message delimiter, Key index, Curve flag, Modulus length, Private key cipher length, Private Key	Signature data length, Signature data	ECDSASigGen KTS-AES-UnWrap TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User ECDSA-priv: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E
ECDSA digital signature verification	Signature verification	Data out-success. No data output-error	Command code: TC, HASH flag, Signature length, Signature, Delimiter, Data length, Message data, Delimiter, Key index,	Error code	ECDSASigVer TLS-AES-Decrypt-GCM TLS-AES-	User Application - User ECDSA-pub: E,W - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			Curve flag, Modulus length, Public key length, Public key		Encrypt-GCM	
ML-DSA key pair generation	Generate ML-DSA key pair	Data out-success. No data output-error	None	Public key and private key	KTS-AES-Wrap ML-DSA KeyGen TLS-AES-Encrypt-GCM RBG Entropy Entropy Conditioner TLS-AES-Decrypt-GCM	User Application - User MLDSA-priv: G,R - User MLDSA-pub: G,R - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E - ML-DSA seed: G,E
ML-DSA public key export	Export ML-DSA public key	Data out-success. No data output-error	Command code: TJ, Key index	level flag, Public key length, Public key	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User MLDSA-pub: R - TLS-SENC: E
ML-DSA digital signature generation (external function)	Generate signature for data	Data out-success. No data output-error	Command code: TK, Hash Flag, Data length, Message data, Delimiter, Key index, Level flag, Private key length, Private key	Signature data length, Signature data	ML-DSA SigGen External Pure ML-DSA SigGen External Pre-hash	User Application - User MLDSA-priv: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					KTS-AES-UnWrap TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	
ML-DSA digital signature verification (external function)	Signature verification	Data out-success. No data output-error	Command code: TL, Hash flag, Signature data length, Signature data, Delimiter, Data length, Message data, Delimiter, Key index, level flag, Public key length, Public key	Valid/invalid result	ML-DSA SigVer External Pure ML-DSA SigVer External Pre-hash TLS-AES-Decrypt-GCM TLS-AES-Encrypt-GCM	User Application - User MLDSA-pub: E,W - TLS-SENC: E
ML-KEM key pair generation	Generate ML-KEM key pair	Data out-success. No data output-error	Command code: TU, level flag	Public key length, Public key, Secret key length, Secret key, keyHmac	KTS-AES-Wrap ML-KEM KeyGen TLS-AES-Encrypt-GCM RBG Entropy Entropy Conditioner TLS-AES-	User Application - User MLKEM-priv: G,R - User MLKEM-pub: G,R - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E - DRBG-EI: E - DRBG-Seed:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Decrypt-GCM	E - DRBG-State: E - ML-KEM seed: E - ML-KEM shared secret key: E
ML-KEM public key export	Export ML-KEM public key	Data out-success. No data output-error	Command code: TV, Key index	level flag, Public key length, Public key	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User MLKEM-pub: R - TLS-SENC: E
ML-KEM encapsulation	Key encapsulation	Data out-success. No data output-error	Command code: TW, Data length, Message data, Delimiter, Key index, level flag, Public key length, Public key	Encrypted data length, Encrypted data, Shared Key length, Shared Key, ciphertext	TLS-AES-Decrypt-GCM ML-KEM encapsulation TLS-AES-Encrypt-GCM KTS-AES-Wrap	User Application - User MLKEM-pub: E,W - hmackey for KTS-AES: E - TLS-SENC: E - ML-KEM shared secret key: G,R
ML-KEM decapsulation	Key decapsulation	Data out-success. No data output-error	Command code: TX, Data length, Message data, Delimiter, Key index, level flag, Private key length, Private key, ciphertext	Shared Key length, Shared Key	KTS-AES-UnWrap KTS-AES-Wrap ML-KEM decapsulation TLS-AES-Encrypt-	User Application - User MLKEM-priv: E,W - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E - ML-KEM

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					GCM TLS-AES-Decrypt-GCM	shared secret key: G,R
SLH-DSA key pair generation	Use DRBG generate SLH-DSA key pair	Data out-success. No data output-error	Command code: YA, mode, level flag, Hash mode	Public key length, Public key, Secret key length, Secret key, keyHmac	KTS-AES-Wrap SLH-DSA KeyGen TLS-AES-Encrypt-GCM RBG Entropy Entropy Conditioner TLS-AES-Decrypt-GCM	User Application - User SLHDSA-priv: G,R - User SLHDSA-pub: G,R - LMK: E - hmackey for KTS-AES: E - TLS-SENC: E - DRBG-EI: E - DRBG-Seed: E - DRBG-State: E
SLH -DSA public key export	Export SLH-DSA public key	Data out-success. No data output-error	Command code: YB, Key index	level flag, Public key length, Public key, Error code	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - User SLHDSA-pub: R - TLS-SENC: E
SLH -DSA digital signature generation	Generate signature for data	Data out-success. No data output-error	Command code: YC, Hash Flag, Data length, Message data, Delimiter, Key index, Level flag, Private key length, Private key	Signature data length, Signature data	KTS-AES-UnWrap SLH-DSA SigGen External Pure SLH-DSA	User Application - User SLHDSA-priv: E,W - LMK: E - hmackey for

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SigGen External Pre-hash TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	KTS-AES: E - TLS-SENC: E
SLH -DSA digital signature verification	Signature verification	Data out-success. No data output-error	Command code: YD, Hash flag, Signature data length, Signature data, DelimiterData length, Message data, Delimiter, Key index, level flag, Public key length, Public key	Error code	SLH-DSA SigVer External Pure SLH-DSA SigVer External Pre-hash TLS-AES-Decrypt-GCM TLS-AES-Encrypt-GCM	User Application - User SLHDSA-pub: E,W - TLS-SENC: E
Message digest	Generate hash for data	Data out-success. No data output-error	Command code:3C, Hash identifier, Data length, Message data, User ID, length, User ID, Encoded, Public key	Hash value	Hash TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - TLS-SENC: E
Random number generation	Generate random data with DRBG	Data out-success. No data output-error	Command code: DR, Length	Random number	RBG Entropy Entropy Conditioner	User Application - DRBG-EI: E - DRBG-Seed:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	E - DRBG-State: E - TLS-SENC: E
Get FIPS status (Show Status)	Get info for approved or non-approved mode	Data out-success. No data output-error	Command code: XA, flag:0	Status: 1: approved, 2: non-approved	TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM	User Application - TLS-SENC: E
tls connect	User application connect service and certAuth login	No data output-error	vsm ip, port, client pfx file, CA certificate, cipher suites	sockfd, ssl handle	KAS-ECC TLSKDF TLS-HMAC TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM ECDSAKeyGen RSASigGen RSASigVer RBG Entropy Entropy Conditioner	User Application - TLS-ECDH-Priv: G,E,Z - TLS-ECDH-Pub: G,R,W,E,Z - TLS-PMS: G,E,Z - TLS-MS: G,E - TLS-SENC: G,E - TLS-SMAC: G,E - TLS-Host-Priv: E - TLS-Host-Pub: E - DRBG-EI: G - DRBG-Seed: G - DRBG-State: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
tls disconnect	User application disconnect service and certAuth logout	N/A	sockfd, ssl handle	N/A	None	User Application - TLS-MS: Z - TLS-SENC: Z - TLS-SMAC: Z - DRBG-EI: Z - DRBG-Seed: Z - DRBG-State: Z
check hard disk rw status	Check hard disk write and read, control hard disk status LED	Disk status LED (the 5th from front panel's left) blink	Read and write signal	LED status	None	Unauthenticated
check service status (Show Status)	Check service running status, control service status LED	service status LED (the 2nd from front panel's left) green/red	Service path	Running status	None	Unauthenticated
check card status (Show Status)	Check protection card status, control card status LED	card status LED (the 1st from front panel's left) green/red	Card info	Card status	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
check tamper status	Check tamper status, control zeroized	card status LED (the 1st from front panel's left) red-success.	voltage signal	Zeroized card status/shutdown	None	Unauthenticated - SPK: Z - DRBG-EI: Z - DRBG-Seed: Z - DRBG-State: Z - TLS-MS: Z - TLS-SENC: Z - TLS-SMAC: Z - Root LMK: Z - LMK: Z - User RSA-priv: Z - User RSA-pub: Z - User ECDSA-priv: Z - User ECDSA-pub: Z - User MLDSA-priv: Z - User MLDSA-pub: Z - User MLKEM-priv: Z - User MLKEM-pub: Z - User SLHDSA-priv: Z - User SLHDSA-pub: Z - User AES-128

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						keys: Z - User AES-192 keys: Z - User AES-256 keys: Z - User HMAC keys: Z - hmackey for KTS-AES: Z
check manual destruction status	Check manual destruction status, control zeroized	card status LED (the 1st from front panel's left) red-success.	voltage signal	Zeroized card status/shutdown	None	Unauthenticated - SPK: Z - DRBG-EI: Z - DRBG-Seed: Z - DRBG-State: Z - TLS-MS: Z - TLS-SENC: Z - TLS-SMAC: Z - Root LMK: Z - LMK: Z - User RSA-priv: Z - User RSA-pub: Z - User ECDSA-priv: Z - User ECDSA-pub: Z - User MLDSA-priv: Z - User MLDSA-pub: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- User MLKEM-priv: Z - User MLKEM-pub: Z - User SLHDSA-priv: Z - User SLHDSA-pub: Z - User AES-128 keys: Z - User AES-192 keys: Z - User AES-256 keys: Z - User HMAC keys: Z - hmackey for KTS-AES: Z
check self-test status	Check self-test status, control service stop,start and poweroff.	service status LED (the 2nd from front panel's left) green/red	Self-test log path	Service stop/start result	None	Unauthenticated
check temperature status	Check temperature sensor, control module power off	poweroff	temperature value	Poweroff result	None	Unauthenticated - SPK: Z - DRBG-EI: Z - DRBG-Seed: Z - DRBG-State: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS-MS: Z - TLS-SENC: Z - TLS-SMAC: Z - Root LMK: Z - LMK: Z - User RSA-priv: Z - User RSA-pub: Z - User ECDSA-priv: Z - User ECDSA-pub: Z - User MLDSA-priv: Z - User MLDSA-pub: Z - User MLKEM-priv: Z - User MLKEM-pub: Z - User SLHDSA-priv: Z - User SLHDSA-pub: Z - User AES-128 keys: Z - User AES-192 keys: Z - User AES-256 keys: Z - User HMAC keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- hmackey for KTS-AES: Z

Table 15: Approved Services

4.4 Non-Approved Services

All non-approved services implemented by the Module are listed in the table below:

Name	Description	Algorithms	Role
Generate SM2 key pair	Use DRBG generate SM2 key pair through the management program	SM2 [ISO/IEC14888-3:2018]	Administrator
Delete SM2 key pair	Delete SM2 key pair through the management program	SM2 [ISO/IEC14888-3:2018]	Administrator
View SM2 key status	View SM2 key status through the management program	SM2 [ISO/IEC14888-3:2018]	Administrator, Auditor, Operator
Generate symmetric key	Use DRBG generate symmetric key for SM4\Triple-DES through the management program	SM4 [ISO/IEC18033-3] Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	Administrator
Delete symmetric key	Delete symmetric key for SM4\Triple-DE through the management program	SM4 [ISO/IEC18033-3] Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	Administrator
View symmetric key status	View symmetric key status through the management program	SM4 [ISO/IEC18033-3] Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	Administrator, Auditor, Operator
View symmetric key check value	View symmetric key check value through the management program	SM4 [ISO/IEC18033-3] Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	Administrator, Auditor, Operator
Generate RSA key pair	Use DRBG generate RSA key pair through the management program	RSA [FIPS 186-4]	Administrator
Delete RSA key pair	Delete RSA key pair through the management program	RSA [FIPS 186-4]	Administrator
View RSA key status	View RSA key status through the management program	RSA [FIPS 186-4]	Administrator, Auditor, Operator
Generate DSA key pair	Use DRBG generate DSA key pair through the management program	DSA [FIPS 186-4]	Administrator
Delete DSA key pair	Delete DSA key pair through the management program	DSA [FIPS 186-4]	Administrator
View DSA key status	View DSA key status through the management program	DSA [FIPS 186-4]	Administrator, Auditor, Operator
Key generation	Symmetric key generation for SM4\ Triple-DES through the cryptographic service	SM4 [ISO/IEC18033-3] Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	User Application

Name	Description	Algorithms	Role
Data encryption	Encrypt data through the cryptographic service	SM4 [ISO/IEC18033-3] Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	User Application
Data decryption	Decrypt data through the cryptographic service	SM4 [ISO/IEC18033-3] Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	User Application
CMAC generation and verification	CMAC through the cryptographic service	Triple-DES [SP800-67] [SP800-38A] [SP800-38B]	User Application
SM2 key pair generation	Generate SM2 key pair through the cryptographic service	SM2 [ISO/IEC14888-3:2018]	User Application
SM2 public key export	Export SM2 public key through the cryptographic service	SM2 [ISO/IEC14888-3:2018]	User Application
SM2 public key encryption	SM2 public key encrypt data through the cryptographic service	SM2 [ISO/IEC14888-3:2018]	User Application
SM2 private key decryption	SM2 private key decrypt data through the cryptographic service	SM2 [ISO/IEC14888-3:2018]	User Application
SM2 digital signature generation	Generate SM2 signature through the cryptographic service	SM2 [ISO/IEC14888-3:2018]	User Application
SM2 digital signature verification	Verify SM2 signature through the cryptographic service	SM2 [ISO/IEC14888-3:2018]	User Application
DSA key pair generation	Generate DSA key pair through the cryptographic service	DSA [FIPS 186-4]	User Application
DSA digital signature generation	Generate DSA signature through the cryptographic service	DSA [FIPS 186-4]	User Application
DSA digital signature verification	Verify DSA signature through the cryptographic service	DSA [FIPS 186-4]	User Application
RSA key pair generation	Generate RSA key pair through the cryptographic service	RSA [FIPS 186-4]	User Application
RSA digital signature generation	Generate RSA signature through the cryptographic service	RSA [FIPS 186-4]	User Application
Message digest	SM3 digest through the cryptographic service	SM3 [ISO/IEC10118-3:2018]	User Application
ECIES public key encryption	ECIES public key encrypt data through the cryptographic service	ECIES	User Application

Name	Description	Algorithms	Role
ECIES private key decryption	ECIES private key decrypt data through the cryptographic service	ECIES	User Application

Table 16: Non-Approved Services

4.5 External Software/Firmware Loaded

NOTE: There is no External Software/Firmware Loaded.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module is composed of the following firmware component(s):

- dynamic library – binary:
  libcsmsc1.so, jent.so, libkmapi.so, libdmapi.so, libpmapi.so, libinstructpay.so, libalgorithmCall.so, libswsds.so, libcrypto.so, libssl.so
- executable – binary:
  chsmcligo, hsm_checker, hsm_selfcheck, swlcdgo, HostServiceServer, swhsmd2(swserver), vsm_selfcheck, hsm.zip
- non-modifiable operating system – binary:
  Rocky-8.9-x86_64-minimal.iso

The firmware components are protected with the authentication technique(s) CRC32 EDC is performed as FW integrity technique.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by module power cycling.
The operator can initiate self-test service to perform the firmware integrity test on demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The Module has a non-modifiable operational environment at Level 3 under the FIPS 140-3 definitions therefore per the FIPS 140-3 Management Manual Section 7.5 Partial validations and non-applicable areas this section is not applicable.

Type of Operational Environment: Non-Modifiable

7 Physical Security

7.1 Mechanisms and Actions Required

The chassis adopts a hard structural shell, primarily using SGCC 1.2mm material and the cover uses stainless steel material. All interfaces are closely connected, and the air vent adopts two layers of mesh interleaving and bending air duct design, which prevent direct visibility of the internal components. A layer of black foam is placed in the middle of the two-layer metal mesh of the vent, which can prevent dust and block the line of sight.

The physical ports on the front and rear panels are fixed to the chassis from inside and cannot be removed. Only the cover can be removed. The cover is secured to the chassis by screws, chassis lock, and is affixed with labels to prevent unauthorized removal.

Tamper dent seals are applied at multiple locations on the chassis cover to leave visible evidence of forced removal. Each tamper evident seal is individually identifiable. For the applied placement, please refer to table 3 of section 7.2.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-Evident Seals	monthly	Look for signs of tampering. If tampering is suspected, then the module must be removed from service.
Tamper-Response switch	monthly	The module includes a tamper detection and response circuitry in the event the enclosure is ever opened. When the chassis cover is opened, the tamper switch is triggered, SPK in card is zeroized, and then the module power off, Z1 power-off zeroing was triggered simultaneously, zeroizing unprotected SSPs stored in the RAM. After the module restarts, all VSM service cannot be started.

Table 17: Mechanisms and Actions Required

7.2 User Placed Tamper Seals

The Module will be shipped from the manufacturer with number (Format: 'L'+YY+MM+Number, eg: L250700001) tamper-evident seals pre-installed, as shown in Figure 3 to Figure 6.

Number:

There is a total of eleven (11) tamper-evident seals on the module.

Placement:

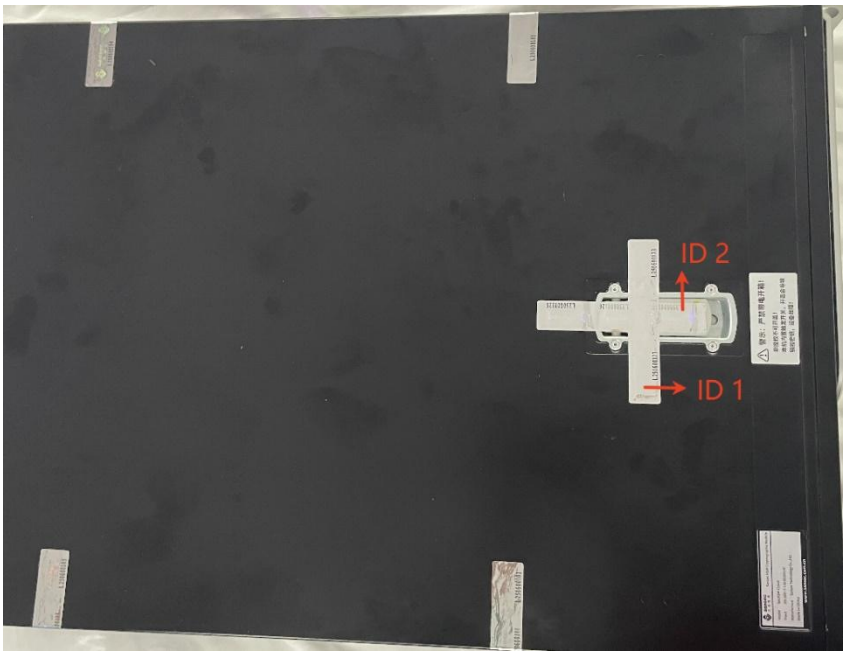


Figure 3– Module A Seal Application Locations (Top)

Figure 4– Module A Seal Application Locations (Left side)

Figure 5 – Module A Seal Application Locations (Right side)

Figure 6 – Module A Seal Application Locations (Back)

Label ID	Placement
1	Top side (cover lock)
2	Top side (cover lock)
3	Left side and top
4	Left side and top
5	Left side and top
6	Left side and top
7	Right side and top
8	Right side and top
9	Right side and top
10	Right side and top
11	Back side (power supply) and inner top

Table 18 Tamper-Evident Seal Locations Guidance

Surface Preparation:

The tamper-evident seals cannot be removed. If the tamper-evident seals are found to be removed or damaged, it indicates that the module has been illegally opened. And the module will not be allowed to be used.

Operator Responsible for Securing Unused Seals:

The Warehouse Security Administrator (WSA), appointed by Sansec, is the singularly authorized role responsible for securing, managing, and distributing all unused seals. Strict procedures prevent any unauthorized access or distribution.

Part Numbers:

The part number of tamper-evident seals is unique, and it cannot be reordered from the vendor.

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	0C	EFP	Shut down
HighTemperature	50C	EFP	Shut down
LowVoltage	74V	EFP	Shut down
HighVoltage	289V	EFP	Shut down

Table 19: EFP/EFT Information

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-20C
HighTemperature	55C

Table 20: Hardness Testing Temperatures

8 Non-Invasive Security

This section is currently not applicable. The Module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
System Memory (S1)	Stored in module's volatile memory (RAM) in plain text.	Dynamic
Disk Drive (S2)	Stored in Hard Drive Disk encrypted with the System Protection Key (SPK), algorithm is AES ECB with 256 bits (CAVP cert: #A6703).	Static
Protection Card (S3)	Stored in Protection Card's volatile memory (RAM) in plain text.	Dynamic
Disk Drive (S4)	Stored in Hard Drive Disk in plain text.	Static
Disk Drive (S5)	Temporarily stored in Hard Drive Disk encrypted with Backup key, algorithm is AES ECB (CAVP cert: #A6703).	Static

Table 21: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input unwrapped by AES KW (IO1)	Application Software (outside)	System Memory (S1)	Encrypted	Automated	Electronic	KTS-AES-UnWrap
Output wrapped by AES KW (IO2)	System Memory (S1)	Application Software (outside)	Encrypted	Automated	Electronic	KTS-AES-Wrap
Input decapsulated by RSA (IO3)	Application Software (outside)	System Memory (S1)	Encrypted	Automated	Electronic	KTS-RSA-Decap
Output encapsulated by RSA (IO4)	System Memory (S1)	Application Software (outside)	Encrypted	Automated	Electronic	KTS-RSA-Encap
Input unwrapped	Application Software (outside)	Disk Drive (S4)	Encrypted	Automated	Electronic	TLS-AES-Decrypt-GCM

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
by AES (IO5-1)						
Input unwrapped by AES (IO5-2)	Application Software (outside)	Disk Drive (S5)	Encrypted	Automated	Electronic	TLS-AES-Decrypt-GCM
Input unwrapped by AES (IO5-3)	Application Software (outside)	System Memory (S1)	Encrypted	Automated	Electronic	TLS-AES-Decrypt-GCM
Output wrapped by AES (IO6-1)	Disk Drive (S4)	Application Software (outside)	Encrypted	Automated	Electronic	TLS-AES-Encrypt-GCM
Output wrapped by AES (IO6-2)	Disk Drive (S5)	Application Software (outside)	Encrypted	Automated	Electronic	TLS-AES-Encrypt-GCM
Output wrapped by AES (IO6-3)	System Memory (S1)	Application Software (outside)	Encrypted	Automated	Electronic	TLS-AES-Encrypt-GCM

Table 22: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroized that SSPs stored in volatile memory (RAM) and in card when the module is powered off. This can be triggered simultaneously by the shutdown operation in Z5 or stopping VSM in HSM.	Zeroized by Module power cycle or hard reset. by overwriting the storage of keys and CSPs (in card and in RAM) with "zeros".	CO starts or stops the module
Z2	Zeroized when the module is switched from non-approved mode to approved mode, or vice versa.	Zeroized by the "Set Approved mode" service by overwriting the storage of keys and CSPs (in disk, in card and in RAM) with "zeros".	Adm role can change approved mode
Z3	A user with the Administrator role can completely erase the contents of the module.	Zeroized by the "zeroization" service by overwriting the storage of keys and CSPs (in disk, in card and in RAM) with "zeros".	Adm role can perform the initialization operation

Zeroization Method	Description	Rationale	Operator Initiation
Z4	A management service that performs the deletion of keys (such as deleting a specific key).	Zeroized when Crypto Officer deletes the key (user keys in disk and in RAM) through key management services. with "zeros" Delete RSA key pair, Delete ECDSA key pair, Delete PQC key pair, Delete symmetric key.	Adm role can perform the deletion operation
Z5	Zeroized when the tamper or key destruction switch is triggered, and then shutdown the module.	Zeroized when tamper detected, or key destruction switch activated. overwriting CSPs in protection card with "zeros",delete logfile and database tables.	N/A
Z6	Zeroized backup key in RAM; zeroized and delete backup file."	Zeroized when backup or restore keys finished, overwriting the backup key and backup file with "zeros.	Adm role can perform the backup/restore operation
Z7	Zeroized TLS session key in RAM when close session. When zero function in OpenSSL does not provide a return status, if no error occurs when the function is called, it indicates that the zeroization operation was successful.	Zeroized when TLS session is terminated, overwriting with "zeros".	N/A
Z8	Zeroized in RAM. When zero function in OpenSSL does not provide a return status, if no error occurs when the function is called, it indicates that the zeroization operation was successful.	Zeroized by OpenSSL internal methods (uninstantiate, free, cleanse) when no longer used, overwriting with "zeros".	N/A
Z9	Zeroized SPK stored in protection card.	Zeroized by DeleteSPK function, overwriting with "zeros".	Adm role can perform the operation
Z10	Zeroized the VSM disk file first, then removing the file.	Zeroized by deleting VSM (user keys in disk) in HSM with "zeros".	N/A

Table 23: SSP Zeroization Methods

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG-EI	DRBG entropy input	256 - N/A	N/A - CSP	Entropy		RBG
DRBG-Seed	Entropy input, Nonce from the entropy source	384 - 384	N/A - CSP	RBG		RBG
DRBG-State	Hash_DRBG (V, C) or CTR_DRBG internal state (V and Key)	256 - 256	N/A - CSP	RBG		RBG
TLS-ECDH-Priv	TLS session ECDH Private Key	P-256, P-384, P-521 - 112-256	ECDH Private Key - CSP	ECDSAKeyGen		KAS-ECC
TLS-Host-Priv	(TLS Host Key) RSA n=2048 Private Key	2048 - 112	Asymmetric Private Key - CSP	RSAKeyGen		RSASigGen KTS-RSA-Decap
TLS-PMS	(TLS Master Secret) 384 bits secret key material	384 - 128	Shared secret - CSP		KAS-ECC-SSC Sp800-56Ar3 (A6703)	TLSKDF
TLS-MS	(TLS Master Secret) 384 bits secret key material	384 - 128	Shared secret - CSP	TLSKDF		TLSKDF
TLS-SENC	TLS Session Encryption Key	128, 256 - 128, 256	Session Key - CSP	TLSKDF		TLS-AES-Encrypt-GCM TLS-AES-Decrypt-GCM

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS-SMAC	TLS Session Authentication Keys	128,256 - 128, 256	Session Key - CSP	TLSKDF		TLS-HMAC
SPK	System Protect Key	256 - 256	Symmetric Key - CSP	SymKeyGen		AES Encryption AES Decryption
Root LMK	Key derivation of LMKs	256 - 256	Symmetric Key - CSP	SymKeyGen		KBKDF
LMK	VSM LMKs	256 - 256	Symmetric Key - CSP	KBKDF		KTS-AES-Wrap KTS-AES-UnWrap AES Encryption
User RSA-priv	VSM user RSA Private Key	2048, 3072, 4096 - 112-152	Asymmetric Private Key - CSP	RSAKeyGen		RSASigGen KTS-RSA-Decap
User ECDSA-priv	VSM user ECDSA Private Key	P-224, P-256, P-384, P-521 - 112-256	Asymmetric Private Key - CSP	ECDSAKeyGen		ECDSASigGen
User MLDSA-priv	VSM user ML-DSA Private Key	2,560 bytes, 4,032 bytes, 4,896 bytes - 128, 192, 256	Asymmetric Private Key - CSP	ML-DSA KeyGen		ML-DSA SigGen External Pure ML-DSA SigGen External Pre-hash
User MLKEM-priv	VSM user ML-KEM Private Key	1,632 bytes, 2,400 bytes, 3,168 bytes - 128, 192, 256	Asymmetric Private Key - CSP	ML-KEM KeyGen		ML-KEM decapsulation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
User SLHDSA-priv	VSM user SLH -DSA Private Key	64 bytes, 96 bytes, 128 bytes - 128, 192, 256	Asymmetric Private Key - CSP	ML-KEM KeyGen		SLH-DSA SigGen External Pure SLH-DSA SigGen External Pre-hash
User AES-128 keys	VSM user symmetric Key	128 - 128	Symmetric Key - CSP	SymKeyGen		AES Encryption AES Decryption AES Encryption-XTS AES Decryption-XTS AES Encryption-Auth AES Decryption-Auth AES-CMAC
User AES-192 keys	VSM user symmetric Key	192 - 192	Symmetric Key - CSP	SymKeyGen		AES Encryption AES Decryption AES Encryption-Auth AES Decryption-Auth AES-CMAC
User AES-256 keys	VSM user symmetric Key	256 - 256	Symmetric Key - CSP	SymKeyGen		AES Encryption AES Decryption AES Encryption-XTS AES Decryption-XTS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						AES Encryption-Auth AES Decryption-Auth AES-CMAC
User HMAC keys	VSM user HMAC key	128-256 - 128-256	MAC Key - CSP	SymKeyGen		HMACGen
Backup key	VSM Backup key	128 - 128	Symmetric Key - CSP	SymKeyGen		AES Encryption AES Decryption
Crypto Officer RSA public key	USB token, 2048 RSA Public Key	2048 - 112	Asymmetric Public Key - PSP			KTS-RSA-Encap RSASigVer
TLS-Host-Pub	(TLS Host Key) RSA 2048 public key	2048 - 112	Asymmetric Public Key - PSP	RSAKeyGen		RSASigGen
TLS-ECDH-Pub	TLS session ECDH public Key	P-256, P-384, P-521 - 112-256	Asymmetric Public Key - PSP	ECDSAKeyGen		KAS-ECC
User RSA-pub	VSM user RSA Pub Key	2048 - 112	Asymmetric Public Key - PSP	RSAKeyGen		RSASigVer KTS-RSA-Encap
User ECDSA-pub	VSM user ECDSA Pub Key	P-224, P-256, P-384, P-521 - 112-256	Asymmetric Public Key - PSP	ECDSAKeyGen		ECDSASigVer
User MLDSA-pub	VSM user ML-DSA Pub Key	1,312 bytes, 1,952 bytes, 2,592 bytes -	Asymmetric Public Key - PSP	ML-DSA KeyGen		ML-DSA SigVer External Pure ML-DSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128, 192, 256				External Pre-hash
User MLKEM-pub	VSM user ML-KEM Pub Key	800 bytes, 1,184 bytes, 1,568 bytes - 128, 192, 256	Asymmetric Public Key - PSP	ML-KEM KeyGen		ML-KEM encapsulation
User SLHDSA-pub	VSM user SLH-DSA Pub Key	32 bytes, 48 bytes, 64 bytes - 128, 192, 256	Asymmetric Public Key - PSP	SLH-DSA KeyGen		SLH-DSA SigVer External Pure SLH-DSA SigVer External Pre-hash
hmackey_masterkey	Key only used to derive the hmackey key KTS-AES	256 - 256	Symmetric Key - CSP			KBKDF
hmackey for KTS-AES	hmackey used in the HMAC algorithm part of KTS-AES-Wrap/KTS-AES-UnWrap	128 - 128	MAC Key - CSP	KBKDF		KTS-AES-Wrap KTS-AES-UnWrap
Backup file	File including user keys encrypted by Backup key	N/A - N/A	Symmetric Key/ Asymmetric Private Key/ Public Key - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ML-DSA seed	Seed used in ML-DSA keypair generation	32 bytes - 256	N/A - CSP	RBG		ML-DSA KeyGen
ML-KEM seed	Seed used in ML-KEM keypair generation	64 bytes - 256	N/A - CSP	RBG		ML-KEM KeyGen
ML-KEM shared secret key	Shared secret key established by ML-KEM	256 - 256	Symmetric Key - CSP		ML-KEM encapsulation ML-KEM decapsulation	

Table 24: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG-EI		System Memory (S1):Plaintext	Until Reboot	Z1 Z8	DRBG-Seed: Derives
DRBG-Seed		System Memory (S1):Plaintext	Until Reboot	Z1 Z8	DRBG-EI: Derived From DRBG-State: Derives
DRBG-State		System Memory (S1):Plaintext	Until Reboot	Z1 Z8	DRBG-Seed: Derived From
TLS-ECDH-Priv		System Memory (S1):Plaintext	Until KAS-ECC is completed in TLS handshake	Z8	TLS-ECDH-Pub: Paired With TLS-PMS: Derives
TLS-Host-Priv		Disk Drive (S2):Encrypted	N/A	Z2 Z3 Z10	SPK: Encrypted by SPK: Decrypted by SPK: Decapsulates Backup Key: Decapsulates TLS-Host-Pub: Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS-PMS		System Memory (S1):Plaintext	Until generate master secret is completed in TLS handshake	Z8	TLS-ECDH-Priv: Derived From TLS-ECDH-Pub: Derived From TLS-MS: Derives
TLS-MS		System Memory (S1):Plaintext	Until TLS session completed	Z1 Z7	TLS-PMS: Derived From TLS-SENC: Derives TLS-SMAC: Derives
TLS-SENC		System Memory (S1):Plaintext	Until TLS session completed	Z1 Z7	TLS-MS: Derived From TLS-Host-Pub: Wraps User RSA-pub: Wraps User ECDSA-pub: Wraps User MLDSA-pub: Wraps User MLKEM-pub: Wraps User SLHDSA-pub: Wraps TLS-ECDH-Pub: Wraps Backup File: Wraps TLS-Host-Pub: UnWraps User RSA-pub: UnWraps User ECDSA-pub: UnWraps User MLDSA-pub: UnWraps User MLKEM-pub: UnWraps User SLHDSA-pub: UnWraps TLS-ECDH-Pub: UnWraps Backup File: UnWraps
TLS-SMAC		System Memory (S1):Plaintext	Until TLS session	Z1 Z7	TLS-MS: Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			completed		
SPK	Input decapsulated by RSA (IO3) Output encapsulated by RSA (IO4)	Protection Card (S3):Plaintext	Until Reboot or Active zeroization	Z1 Z2 Z3 Z5 Z9	Root LMK: Encrypts LMK: Encrypts User RSA-priv: Encrypts User ECDSA-priv: Encrypts User MLDSA-priv: Encrypts User MLKEM-priv: Encrypts User SLHDSA-priv: Encrypts User AES-128: Encrypts User AES-192: Encrypts User AES-256: Encrypts User HMAC keys: Encrypts TLS-Host-Priv: Encrypts Root LMK: Decrypts LMK: Decrypts User RSA-priv: Decrypts User ECDSA-priv: Decrypts User MLDSA-priv: Decrypts User MLKEM-priv: Decrypts User SLHDSA-priv: Decrypts User AES-128: Decrypts User AES-192: Decrypts User AES-256: Decrypts User HMAC keys: Decrypts TLS-Host-Priv: Decrypts Crypto Officer RSA public key:

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Encapsulated by TLS-Host-Priv: Decapsulated by
Root LMK		System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z10	SPK: Encrypted by SPK: Decrypted by LMK: Derives
LMK		System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z10	Root LMK: Derived From SPK: Encrypted by SPK: Decrypted by User RSA-priv: Wraps User ECDSA-priv: Wraps User MLDSA-priv: Wraps User MLKEM-priv: Wraps User SLHDSA-priv: Wraps User AES-128: Wraps User AES-192: Wraps User AES-256: Wraps User HMAC keys: Wraps User RSA-priv: UnWraps User ECDSA-priv: UnWraps User MLDSA-priv: UnWraps User MLKEM-priv: UnWraps User SLHDSA-priv: UnWraps User AES-128: UnWraps User AES-192: UnWraps User AES-256: UnWraps User HMAC keys: UnWraps

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
User RSA-priv	Input unwrapped by AES KW (IO1) Output wrapped by AES KW (IO2)	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by User RSA-pub: Paired With
User ECDSA-priv	Input unwrapped by AES KW (IO1) Output wrapped by AES KW (IO2)	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by User ECDSA-pub: Paired With
User MLDSA-priv	Input unwrapped by AES KW (IO1) Output wrapped by AES KW (IO2)	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by User MLDSA-pub: Paired With
User MLKEM-priv	Input unwrapped by AES KW (IO1) Output wrapped by AES KW (IO2)	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by User MLKEM-pub: Paired With
User SLHDSA-priv	Input unwrapped by AES KW (IO1) Output wrapped by AES KW (IO2)	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by User SLHDSA-pub: Paired With
User AES-128 keys	Input unwrapped by AES KW (IO1) Output wrapped	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	by AES KW (IO2)				
User AES-192 keys	Input unwrapped by AES KW (IO1) Output wrapped by AES KW (IO2)	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by
User AES-256 keys	Input unwrapped by AES KW (IO1) Output wrapped by AES KW (IO2)	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by
User HMAC keys	Input unwrapped by AES KW (IO1) Output wrapped by AES KW (IO2)	System Memory (S1):Plaintext Disk Drive (S2):Encrypted	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	SPK: Encrypted by SPK: Decrypted by LMK:Wrapped by LMK: UnWrapped by
Backup key	Input decapsulated by RSA (IO3) Output encapsulated by RSA (IO4)	System Memory (S1):Plaintext	Until backup or restore completed.	Z6	Backup File: Encrypts Backup File: Decrypts Crypto Officer RSA public key: Encapsulated by TLS-Host-Priv: Decapsulated by
Crypto Officer RSA public key	Input unwrapped by AES (IO5-1)	Disk Drive (S4):Plaintext	Until Active zeroization	Z2 Z3 Z10	SPK:Encapsulates Backup key:Encapsulates TLS-SENC: UnWrapped by
TLS-Host-Pub	Output wrapped by AES (IO6-1)	Disk Drive (S4):Plaintext	Until Active zeroization	Z2 Z3 Z10	TLS-Host-Priv: Paired With TLS-SENC:Wrapped by
TLS-ECDH-Pub	Input unwrapped by AES (IO5-3)	System Memory (S1):Plaintext	Until KAS-ECC is complet	Z8	TLS-ECDH-Priv: Paired With TLS-PMS: Derives TLS-SENC:Wrapped

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Output wrapped by AES (IO6-3)		ed in TLS handshake		by TLS-SENC: UnWrapped by
User RSA-pub	Input unwrapped by AES (IO5-3) Output wrapped by AES (IO6-3)	System Memory (S1):Plaintext Disk Drive (S4):Plaintext	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	User RSA-priv: Paired With TLS-SENC:Wrapped by TLS-SENC: UnWrapped by
User ECDSA-pub	Input unwrapped by AES (IO5-3) Output wrapped by AES (IO6-3)	System Memory (S1):Plaintext Disk Drive (S4):Plaintext	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	User ECDSA-priv: Paired With TLS-SENC:Wrapped by TLS-SENC: UnWrapped by
User MLDSA-pub	Input unwrapped by AES (IO5-3) Output wrapped by AES (IO6-3)	System Memory (S1):Plaintext Disk Drive (S4):Plaintext	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	User MLDSA-priv: Paired With TLS-SENC:Wrapped by TLS-SENC: UnWrapped by
User MLKEM-pub	Input unwrapped by AES (IO5-3) Output wrapped by AES (IO6-3)	System Memory (S1):Plaintext Disk Drive (S4):Plaintext	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	User MLKEM-priv: Paired With TLS-SENC:Wrapped by TLS-SENC: UnWrapped by
User SLHDSA-pub	Input unwrapped by AES (IO5-3) Output wrapped by AES (IO6-3)	System Memory (S1):Plaintext Disk Drive (S4):Plaintext	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	User SLHDSA-priv: Paired With TLS-SENC:Wrapped by TLS-SENC: UnWrapped by
hmackey_masterkey		Disk Drive (S4):Plaintext		Z10	hmackey for KTS-AES: Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
hmackey for KTS-AES		System Memory (S1):Plaintext	Until Reboot	Z1	hmackey_masterkey:Derived by
Backup file	Input unwrapped by AES (IO5-2) Output wrapped by AES (IO6-2)	Disk Drive (S5):Encrypted	Until backup or restore completed.	Z6	Backup key: Encrypted by Backup key: Decrypted by User RSA-priv:Saved within User RSA-pub:Saved within User ECDSA-priv:Saved within User ECDSA-pub:Saved within User MLDSA-priv:Saved within User MLDSA-pub:Saved within User MLKEM-priv:Saved within User MLKEM-pub:Saved within User SLHDSA-priv:Saved within User SLHDSA-pub:Saved within User AES-128:Saved within User AES-192:Saved within User AES-256:Saved within User HMAC keys:Saved within Root LMK:Saved within LMK:Saved within TLS-SENC:Wrapped by TLS-SENC: UnWrapped by
ML-DSA seed		System Memory (S1):Plaintext	Until Reboot	Z1 Z8	User MLDSA-priv:Derived From User MLDSA-pub:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ML-KEM seed		System Memory (S1):Plaintext	Until Reboot	Z1 Z8	User MLKEM-priv:Derived From User MLKEM-pub:Derived From
ML-KEM shared secret key		System Memory (S1):Plaintext	Until Reboot or Active zeroization	Z1 Z2 Z3 Z4 Z10	

Table 25: SSP Table 2

9.5 Transitions

Beginning in 2031, keys providing 112 bits of security strength shall no longer be used to apply cryptographic protection and are limited to legacy use for processing, as specified in Table 4 of NIST SP 800-57 Part 1 Rev. 5.

10 Self-Tests

10.1 Pre-Operational 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.

The Module performs the following pre-operational self-tests in table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity	CRC-32	EDC	SW/FW Integrity	LCD shows Success or Failure Code/Error log also show info.	Executed on the whole HSM firmwares stored in HSM disk.
Firmware integrity_VSM	CRC-32	EDC	SW/FW Integrity	LCD shows Success or Failure Code/Error log also show info.	Executed on the whole vsm firmwares stored in vsm disk.
ENT_VSM	RCT and APT	SP 800-90B Health-Test	Critical Function	LCD shows Success or Failure Code/Error log also show info.	An RCT and APT as specified in [90B] section 4.4 are executed before generation of the DRBG entropy input. (Note:HSM does not include ENT self-test)

Table 26: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Conditional self-tests are only performed in VSM.

The Module performs the following conditional self-tests in the table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ENT	RCT and APT	SP 800-90B Health-Test	CAST	LCD shows Success or Failure Code/Error log also show info.	An RCT and APT as specified in [90B] section 4.4 are executed before generation of the DRBG entropy input	When entropy is requested
Hash DRBG (A6703)	Hash_DRBG using SHA3-256 with PR	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Hash_DRBG - SHA3-256 instantiation, generate, KATs performed before the first random data generation.	Bootup/When a periodic interval is reached
Counter DRBG (A6703)	CTR_DRBG using AES-256, without DF	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES-256 CTR_DRBG, instantiation, generate, KATs performed before the first random data generation.	Bootup/When a periodic interval is reached
AES-ECB (A6703) encrypt	AES ECB encrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES encryption	Bootup/When a periodic interval is reached
AES-ECB (A6703) decrypt	AES ECB decrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES ECB decryption	Bootup/When a periodic interval is reached
AES-CBC (A6703) encrypt	AES CBC encrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES CBC encryption	Bootup/When a periodic interval is reached

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A6703) decrypt	AES CBC decrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES CBC decryption	Bootup/When a periodic interval is reached
AES-CTR (A6703) encrypt	AES CTR encrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES CTR encryption	Bootup/When a periodic interval is reached
AES-CTR (A6703) decrypt	AES CTR decrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES CTR decryption	Bootup/When a periodic interval is reached
AES-CCM (A6703) encrypt	AES CCM encrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES CCM encryption	Bootup/When a periodic interval is reached
AES-CCM (A6703) decrypt	AES CCM decrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES CCM decryption	Bootup/When a periodic interval is reached
AES-GCM (A6703) encrypt	AES GCM encrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES GCM Authenticated encryption	Bootup/When a periodic interval is reached
AES-GCM (A6703) decrypt	AES GCM decrypt with 128-bit key	KAT	CAST	LCD shows Success or Failure	AES GCM Authenticated decryption	Bootup/When a periodic interval is reached

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Code/Error log also show info.		
AES-CMAC (A6703)	AES CMAC with 128-bit key	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES CMAC Message Authenticated	Bootup/When a periodic interval is reached
AES-XTS Key Uniqueness	Generate two 128bits keys and compare	Comparison Test	Critical Function	Error log show info	Generate two 128bits keys and Compare Key1Key2	After key generation and before XTS encryption
AES-XTS (A6703) encrypt	AES XTS with two 128-bit keys, encryption	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES XTS encryption	Bootup/When a periodic interval is reached
AES-XTS (A6703) decrypt	AES XTS with two 128-bit keys, decryption	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	AES XTS decryption	Bootup/When a periodic interval is reached
SHA-1 (A6703)	SHA-1	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Digest	Bootup/When a periodic interval is reached
SHA2-224 (A6703)	SHA2-224	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Digest	Bootup/When a periodic interval is reached
SHA2-256 (A6703)	SHA2-256	KAT	CAST	LCD shows Success or Failure	Message Digest	Bootup/When a periodic interval is reached

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Code/Error log also show info.		
SHA2-384 (A6703)	SHA2-384	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Digest	Bootup/When a periodic interval is reached
SHA2-512 (A6703)	SHA2-512	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Digest	Bootup/When a periodic interval is reached
SHA3-224 (A6703)	SHA3-224	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Digest	Bootup/When a periodic interval is reached
SHA3-256 (A6703)	SHA3-256	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Digest	Bootup/When a periodic interval is reached
SHA3-384 (A6703)	SHA3-384	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Digest	Bootup/When a periodic interval is reached
SHA3-512 (A6703)	SHA3-512	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Digest	Bootup/When a periodic interval is reached

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 (A6703)	HMAC-SHA-1	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Authentication	Bootup/When a periodic interval is reached
HMAC-SHA2-224 (A6703)	HMAC-SHA2-224	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Authentication	Bootup/When a periodic interval is reached
HMAC-SHA2-256 (A6703)	HMAC-SHA2-256	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Authentication	Bootup/When a periodic interval is reached
HMAC-SHA2-384 (A6703)	HMAC-SHA2-384	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Authentication	Bootup/When a periodic interval is reached
HMAC-SHA2-512 (A6703)	HMAC-SHA2-512	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Message Authentication	Bootup/When a periodic interval is reached
ECDSA SigGen (FIPS186-5) (A6703)	ECDSA with P-256 and SHA2-512, signature generation	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Signature generation	Bootup/When a periodic interval is reached
ECDSA SigVer (FIPS186-5) (A6703)	ECDSA with P-256 and SHA2-512, signature verification	KAT	CAST	LCD shows Success or Failure	Signature verification	Bootup/When a periodic interval is reached

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Code/Error log also show info.		
RSA SigGen (FIPS186-5) (A6703)	RSA PSS with 2048-bit key and SHA2-256, signature generation	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Signature generation	Bootup/When a periodic interval is reached
RSA SigVer (FIPS186-5) (A6703)	RSA PSS with 2048-bit key and SHA2-256, signature verification	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Signature verification	Bootup/When a periodic interval is reached
ML-DSA SigGen (A6703)	ML-DSA (ML-DSA-44) with SHA2-512, signature generation	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Signature generation	Bootup/When a periodic interval is reached
ML-DSA SigVer (A6703)	ML-DSA (ML-DSA-44) with SHA2-512, signature verification	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Signature verification	Bootup/When a periodic interval is reached
ML-KEM KeyGen (A6703)	ML-KEM-512 keypair generation	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	ML-KEM keypair generation	Bootup/When a periodic interval is reached
ML-KEM EncapDecap (A6703) Encap	ML-KEM(ML-KEM-512) with encapsulation	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Key encapsulation	Bootup/When a periodic interval is reached

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ML-KEM EncapDecap (A6703) Decap	ML-KEM(ML-KEM-512) with decapsulation	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Key decapsulation	Bootup/When a periodic interval is reached
SLH-DSA SigGen (A6703)	SLH-DSA(SLH-DSA-SHAKE-128s) with SHAKE-256 and SLH-DSA(SLH-DSA-SHA2-128s) with SHA2-512, signature generation	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Signature generation	Bootup/When a periodic interval is reached
SLH-DSA SigVer (A6703)	SLH-DSA(SLH-DSA-SHAKE-128s) with SHAKE-256 and SLH-DSA(SLH-DSA-SHA2-128s) with SHA2-512, signature verification	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Signature verification	Bootup/When a periodic interval is reached
KTS-RSA Encap	RSA with 2048-bit key encrypt	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	2048-bit RSA-OAEP encryption with SHA2-256	Bootup/When a periodic interval is reached
KTS-RSA Decap	RSA with 2048-bit key decrypt	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	2048-bit RSA-OAEP decrypt with SHA2-256	Bootup/When a periodic interval is reached
KDF SP800-108 (A6703)	Counter mode with HMAC-SHA2-256	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	KBKDF with HMAC-SHA2-256 as PRF options	Bootup/When a periodic interval is reached

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KTS-AES ECB and HMAC	AES-ECB and HMAC	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Key Transport with 256bit AES-ECB encryption and HMAC-SHA2-256 authentication	Bootup/When a periodic interval is reached
KAS-ECC-SSC Sp800-56Ar3 (A6703)	Shared Secret Calculation	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	Key Agreement with P-256, P-384, P-521, SHA2-256 Shared Secret Calculation	Bootup/When a periodic interval is reached
TLS v1.2 KDF RFC7627 (A6703)	TLS 1.2	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	TLS 1.2 KDF (Revision RFC7627) with SHA2-256 as PRF	Bootup/When a periodic interval is reached
ECDSA KeyGen (FIPS186-5) PCT	PCT using SHA2-256, signature generation and verification	PCT	PCT	LCD shows Success or Failure Code/Error log also show info.	Key pairs generation for signature generation, verification, and KAS	On generation
RSA KeyGen (FIPS186-5) PCT	PCT using SHA2-256, signature generation and verification. PCT using public key encryption and private key decryption.	PCT	PCT	LCD shows Success or Failure Code/Error log also show info.	Key pairs generation for signature generation and verification	On generation
ML-DSA KeyGen PCT	PCT using SHA2-512, signature generation and verification	PCT	PCT	LCD shows Success or Failure Code/Error log also show info.	Key pairs generation for signature generation and verification	On generation
ML-KEM KeyGen PCT	PCT using encapsulation and decapsulation	PCT	PCT	LCD shows Success or Failure	Key pairs generation for encapsulation and decapsulation.	On generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Code/Error log also show info.		
SLH-DSA KeyGen PCT	PCT using SHA2-512, signature generation and verification	PCT	PCT	LCD shows Success or Failure Code/Error log also show info.	Key pairs generation for signature generation and verification	On generation
SLH-DSA KeyGen CAST with SHA2	SHA2-128	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	SLH-DSA KeyGen KAT using SHA2	Bootup/When a periodic interval is reached
SLH-DSA KeyGen CAST with SHAKE	SHAKE-128	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	SLH-DSA KeyGen KAT using SHAKE	Bootup/When a periodic interval is reached
ML-DSA KeyGen KAT	SHA2-512	KAT	CAST	LCD shows Success or Failure Code/Error log also show info.	ML-DSA KeyGen KAT using SHA2	LCD shows Success or Failure Code/Error log also show info.

Table 27: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware integrity	EDC	SW/FW Integrity	Power on/On demand/Every 60 minutes	Programmatically automatically
Firmware integrity_VSM	EDC	SW/FW Integrity	Power on/On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ENT_VSM	SP 800-90B Health-Test	Critical Function	Power on/On demand	Manually

Table 28: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ENT	SP 800-90B Health-Test	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
Hash DRBG (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
Counter DRBG (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-ECB (A6703) encrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-ECB (A6703) decrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-CBC (A6703) encrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-CBC (A6703) decrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-CTR (A6703) encrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-CTR (A6703) decrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM (A6703) encrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-CCM (A6703) decrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-GCM (A6703) encrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-GCM (A6703) decrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-CMAC (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-XTS Key Uniqueness	Comparison Test	Critical Function	On demand	Programmatically automatically
AES-XTS (A6703) encrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
AES-XTS (A6703) decrypt	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SHA-1 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SHA2-224 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SHA2-256 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SHA2-384 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-512 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SHA3-224 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SHA3-256 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SHA3-384 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SHA3-512 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
HMAC-SHA-1 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
HMAC-SHA2-224 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
HMAC-SHA2-256 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
HMAC-SHA2-384 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
HMAC-SHA2-512 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
ECDSA SigGen (FIPS186-5) (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
RSA SigGen (FIPS186-5) (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
RSA SigVer (FIPS186-5) (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
ML-DSA SigGen (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
ML-DSA SigVer (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
ML-KEM KeyGen (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
ML-KEM EncapDecap (A6703) Encap	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
ML-KEM EncapDecap (A6703) Decap	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SLH-DSA SigGen (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SLH-DSA SigVer (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
KTS-RSA Encap	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KTS-RSA Decap	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
KDF SP800-108 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
KTS-AES ECB and HMAC	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
KAS-ECC-SSC Sp800-56Ar3 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
TLS v1.2 KDF RFC7627 (A6703)	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
ECDSA KeyGen (FIPS186-5) PCT	PCT	PCT	On demand	Programmatically automatically
RSA KeyGen (FIPS186-5) PCT	PCT	PCT	N/A	Programmatically automatically
ML-DSA KeyGen PCT	PCT	PCT	N/A	Programmatically automatically
ML-KEM KeyGen PCT	PCT	PCT	N/A	Programmatically automatically
SLH-DSA KeyGen PCT	PCT	PCT	N/A	Programmatically automatically
SLH-DSA KeyGen CAST with SHA2	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
SLH-DSA KeyGen CAST with SHAKE	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically
ML-DSA KeyGen KAT	KAT	CAST	Power on/On demand/Every 60 minutes	Programmatically automatically

Table 29: Conditional Periodic Information

The periodic self-tests do not require operator input to initiate.

The Periodic self-tests include conditional self-tests in VSM and include pre-operational self-tests in HSM. After power-on, HSM will first perform a pre-operational self-test (VSM will execute both pre-operational self-test and conditional self-test). Once self-test is passed, the periodic self-test task will be started, and module will wait until the next cycle to perform the periodic self-test. The periodic self-test task runs asynchronously in the background of the module and is automatically executed every 60 minutes without external input or control. During its execution, all services will be stopped, and data output will be inhibited. It does not affect other cryptographic functions of the module unless the periodic self-test fails, in which case the module enters an error state.

If any of the self-tests fail, the module enters the error state and displays the self-test error message on the LCD.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Integrity Error	The Module fails the firmware integrity pre-operational self-test.	The Module enters the Integrity error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:crc32][result]:[1]"indicates Integrity error; "[alg]:crc32][result]:[0]"indicates Integrity success.
ENT Error	The Module fails in ENT RCT and APT in pre-operational or conditional self-test.	The Module enters the ENT error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:ENT][result]:[1]"indicates ENT error; "[alg]:ENT][result]:[0]"indicates ENT success.
AES Error	The Module fails in one of the AES KATs in conditional self-test.	The Module enters the AES error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:AES][result]:[1]"indicates AES error; "[alg]:AES][result]:[0]"indicates AES success.
RSA Error	The Module fails in one of the RSA KATs in conditional self-test.	The Module enters the RSA error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:RSA][result]:[1]"indicates RSA error; "[alg]:RSA][result]:[0]"indicates RSA success.
ECDSA Error	The Module fails in one of the ECDSA KATs in conditional self-test.	The Module enters the ECDSA error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:ECDSA][result]:[1]"indicates ECDSA error; "[alg]:ECDSA][result]:[0]"indicates ECDSA success.
ML-DSA Error	The Module fails in one of the ML-DSA KATs in conditional self-test.	The Module enters the ML-DSA error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:ML-DSA][result]:[1]"indicates ML-DSA error; "[alg]:ML-DSA][result]:[0]"indicates ML-DSA success.
ML-KEM Error	The Module fails in one of the ML-KEM KATs in	The Module enters the ML-KEM error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:ML-KEM][result]:[1]"indicates ML-KEM error; "[alg]:ML-KEM][result]:[0]"indicates ML-KEM success.

Name	Description	Conditions	Recovery Method	Indicator
	conditional self-test.			
SLH-DSA Error	The Module fails in one of the SLH-DSA KATs in conditional self-test.	The Module enters the SLH-DSA error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:SLHDSA][result]:[1]"indicates SLHDSA error; "[alg]:SLHDSA][result]:[0]"indicates SLHDSA success.
HASH Error	The Module fails in one of the SHS KATs in conditional self-test.	The Module enters the SHS error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:HASH][result]:[1]"indicates HASH error; "[alg]:HASH][result]:[0]"indicates HASH success.
HMAC Error	The Module fails in one of the HMAC KATs in conditional self-test.	The Module enters the HMAC error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:HMAC][result]:[1]"indicates HMAC error; "[alg]:HMAC][result]:[0]"indicates HMAC success.
KBKDF Error	The Module fails in one of the KBKDF KATs in conditional self-test.	The Module enters the KBKDF error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:KBKDF][result]:[1]"indicates KBKDF error; "[alg]:KBKDF][result]:[0]"indicates KBKDF success.
KTS-RSA Error	The Module fails in one of the KTS-IFC KATs in conditional self-test.	The Module enters the KTS-RSA error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:KTS-RSA][result]:[1]"indicates KTS-RSA error; "[alg]:KTS-RSA][result]:[0]"indicates KTS-RSA success.
KTS-AES Error	The Module fails in one of the KTS-AES KATs in conditional self-test.	The Module enters the KTS-AES error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:KTS-AES][result]:[1]"indicates KTS-AES error; "[alg]:KTS-AES][result]:[0]"indicates KTS-AES success.
KAS-SSC Error	The Module fails in one of the KAS-SSC KATs in conditional self-test.	The Module enters the KAS-SSC error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:KAS-SSC][result]:[1]"indicates KAS-SSC error; "[alg]:KAS-SSC][result]:[0]"indicates KAS-SSC success.

Name	Description	Conditions	Recovery Method	Indicator
TLS-KDF Error	The Module fails in one of the TLS KDF KATs in conditional self-test.	The Module enters the TLS KDF error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:TLS-KDF][result]:[1]"indicates TLS-KDF error; "[alg]:TLS-KDF][result]:[0]"indicates TLS-KDF success.
Random Error	The Module fails in one of the DRBG KATs in conditional self-test.	The Module enters the DRBG error state	Reboot/Power cycle the module	LCD Outputs status: "[alg]:DRBG][result]:[1]"indicates SRBG error; "[alg]:DRBG][result]:[0]"indicates DRBG success.
RSA PCT Error	The Module fails in the PCT performed after a RSA key generation	The Module enters the RSA PCT error state	Reboot/Power cycle the module	Outputs status of RSA PCT error, otherwise it indicates successful completion by RSA PCT success.
ECDSA PCT Error	The Module fails in the PCT performed after an ECDSA key generation.	The Module enters the ECDSA PCT error state	Reboot/Power cycle the module	Return 1 indicates ECDSA PCT error, return 0 indicates ECDSA PCT success.
ML-DSA PCT Error	The Module fails in the PCT performed after an ML-DSA key generation.	The Module enters the ML-DSA PCT error state	Reboot/Power cycle the module	Return 1 indicates MLDSA PCT error, return 0 indicates MLDSA PCT success.
ML-KEM PCT Error	The Module fails in the PCT performed after an ML-KEM key generation.	The Module enters the ML-KEM PCT error state	Reboot/Power cycle the module	Return 1 indicates MLKEM PCT error, return 0 indicates MLKEM PCT success.
SLH-DSA PCT Error	The Module fails in the PCT performed after an SLH-DSA	The Module enters the SLH-DSA PCT error state	Reboot/Power cycle the module	Return 1 indicates SLHDSA PCT error, return 0 indicates SLHDSA PCT success.

Name	Description	Conditions	Recovery Method	Indicator
	key generation.			
VSM initialization Error	The Module fails in VSM initialization	The Module enters the VSM initialization error state	Reinitialize VSM	VSM management service Outputs status of initialization error, otherwise it indicates successful completion by initialization success.
CO authentication error	The Module fails in VSM CO authentication	The Module enters the CO authentication error state	Re-authenticate	VSM management service Outputs status of authentication error, otherwise it indicates successful completion by authentication success.
vsm csp entry error	The Module fails in entry csp to VSM.	The Module enters the vsm csp entry error state	Re-entry	VSM management service Outputs status of csp entry error, otherwise it indicates successful completion by csp entry success.
vsm calling cryptographic service error	The Module fails in VSM calling cryptographic service in user state	The Module enters the vsm cryptographic service error state	Re-calling cryptographic service	No data outputs when cryptographic service error and record log, otherwise it return data when success.

Table 30: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Installation and Initialization:

The following steps must be performed in order to securely install, initialize, and start up the Sansec HSM cryptographic module in FIPS 140-3 approved mode of operation:

1. Module Install:
1) Open the packaging of the cryptographic device, compare it with the "Installation List", and check if the equipment accessories are complete.
2) Remove the cryptographic device from the packaging box and secure it in the installation position.
3) Connect the power module cable.
4) Turn on the power switch of the cryptographic device, start the cryptographic device.
5) When managing cryptographic devices through serial ports, use a cable to connect the serial port of the cryptographic device to the USB interface of the management terminal.
6) Enter the management program.

2. Module Initialization:

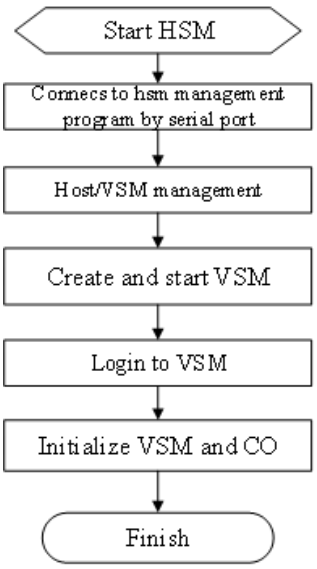
Cryptographic module initialization is a necessary process before a new cryptographic module can be used.

When HSM is authentication for the first time, the default username and password need to be used for serial login, and the default password needs to be forcibly modified during the first login.

When VSM is initialized the first time, the default password also needs to be entered and forcibly modified before it can be executed.

HSM default username and password, VSM default login password and USB token PIN are required to be obtained by referring to user manual.

Through this process, you can set the cryptographic module status, create and start VSM, establish multi-level permission mechanisms, and generate keys. The process steps are as follows:



HSM is only used for vsm management, so it does not require dedicated initialization operation, when VSM is created and VSM's ip is set by HSM management service, detailed initialization process is as follows:

1)Access the VSM management program, enter the default password and modify the password as prompted.

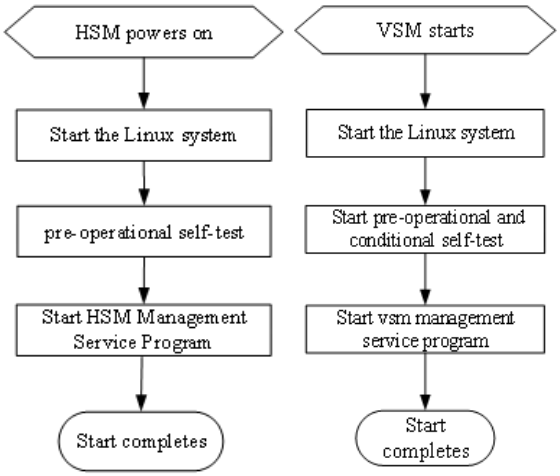
2)Select "Installation guide"->initialize the VSM, initialization will erase all the keys and CO/user accounts in the VSM.

3) Initialize administrator, add three new administrators with USB token in sequence. In this step, SPK is generated and component (encrypted by USB token's public key, use KTS IFC #A6703) is exported to the USB token.

When vsm initialization is completed, other operation can be performed. For example, add operator and auditor, generate keys, configure and start service.

The module can enter approved mode either after first-time use and initialization, or after switching and initializing via the VSM management program by selecting "Set Approved Mode"; When in approved mode, the module can enter non-approved mode after switching and initializing by selecting "Set non-Approved Mode" through the VSM management program.

3. Module Startup:
The main steps of the power on startup workflow include：



Delivery:

The following steps must be performed in order to securely deliver the Sansec HSM cryptographic module to the authorized operator:
During the production, installation, delivery, and initialization process of the cryptographic module, it does not contain any sensitive data. All sensitive data will be generated and configured by the user on-site.
The cryptographic module is pre-configured with information such as the Part Number (P/N) and Serial Number (S/N) at the factory. Both the product and its outer packaging are labeled with barcode identifiers. The P/N is the standardized code for the product, while the S/N is the unique identifier for each individual unit.

The cryptographic module has measures to ensure its integrity during delivery, installation, and initialization, used to detect whether it has been disassembled.

After the production of the cryptographic module is completed, there are tamper-evident seals attached to the cover to protect the cryptographic module; During delivery, the cryptographic module is packaged in a packaging box, and the packaging box is sealed using company customized tape and packaging tape to package the external packaging box, ensuring the integrity of the cryptographic module during the delivery process.

Before installing and initializing the cryptographic module, users can first check whether the packaging tape and adhesive tape of the outer packaging box have been damaged to determine whether the cryptographic module packaging has been opened during the delivery process. They can also determine whether the cryptographic module has been disassembled by observing whether the tamper-evident seals at the cover of the cryptographic module have been damaged. If the packaging box or cryptographic module shows signs of being opened or disassembled, the user should promptly contact and provide feedback.

Products with tamper-evident seals will leave evidence of disassembly.

11.2 Administrator Guidance

Please refer to the “Sansec HSM Cryptographic Module Administrator guidance for VSM Management”.

11.3 Non-Administrator Guidance

Please refer to the document “Sansec HSM Cryptographic Module Non-administrator guidance”.

11.4 Design and Rules

Rules of Operation

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
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. All self-tests do not require any operator action.
7. Data output is 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 no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not enter or output plaintext CSPs.
15. The Module does not store any plaintext CSPs
16. The Module does not output intermediate key values.
17. The Module does not provide bypass services or ports/interfaces.

11.6 End of Life

When the module reaches the end of its lifecycle, it needs to be secure destruction.
Please refer to section 2.6 “Zeroization and destruction” of the “Sansec HSM Cryptographic Module Non-administrator guidance” for details.

12 Mitigation of Other Attacks

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

References and Definitions

The following standards are referred to in this Security Policy.

Table 31 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, September 2, 2025*
[108]	*NIST Special Publication 800-108 rev1, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), August 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 (2023) Digital Signature Standard (DSS). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 186-5. February 3, 2023*
[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*

Abbreviation*	Full Specification Name
[203]	*National Institute of Standards and Technology, Module-Lattice-Based Key-Encapsulation Mechanism Standard, Federal Information Processing Standards Publication 203, August 2024*
[204]	*National Institute of Standards and Technology, Module-Lattice-Based Digital Signature Standard, Federal Information Processing Standards Publication 204, August 2024*
[205]	*National Institute of Standards and Technology, Stateless Hash-Based Digital Signature Standard, Federal Information Processing Standards Publication 205, August 2024*
[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*
[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 800-67, May 2004*
[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.*

Abbreviation*	Full Specification Name
[ISO14888-3]	*International Standard, ISO/IEC 14888-3:2018, Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms, Third edition, April 2018*
[ISO18033-3]	*International Standard, ISO/IEC 18033-3:2010, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers, First edition, December 2010*
[ISO10118-3]	*International Standard, ISO/IEC 10118-3:2018, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions, Third edition, March 2018*

Table 32 Acronyms and Definitions

Acronym*	Definition
AES	Advanced Encryption Standard
APT	Adaptative Proportion Test
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CMAC	Cipher-based Message Authentication Code
CN	Common Name
CO	Cryptographic Officer
CSP	Critical Security Parameter
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
EFP/EFT	Environmental Failure Protection/ Environmental Failure Test
ENT	Approved SP800-90B Entropy Source
ESV	Entropy Source Validation

Acronym*	Definition
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
KAS	Key Agreement Scheme
KAT	Know Answer Test
KAT	Know Answer Test
KBKDF	Key-Based Key Derivation Functions
KDF	Key Derivation Function
KTS	Key Transport Methods
KVM	Kernel-based Virtual Machine
LMK	Local master key
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key Encapsulation Mechanism
MS	Master Secret
NIST	National Institute of Standards and Technology
OAEP	Optimal Asymmetric Encryption Padding
OFB	Output Feedback
PBKDF	Password-Based Key Derivation Function
PCT	Pairwise Consistency Test
PKCS	Public-Key Cryptography Standards
PMS	Pre-Master Secret/Shared Secret
PQC	Post-Quantum Cryptography
PR	Prediction Resistance
PSP	Public Security Parameter
RAM	Random Access Memory
RCT	Repetition Count Test
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm

Acronym*	Definition
SHS	Secure Hash Standard
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SM2	Chinese Elliptic Curve Digital Signature Algorithm
SM3	Chinese Message Digest algorithm
SM4	Chinese Block Cipher Symmetric algorithm
SPK	System Protection Key
SSP	Sensitive Security Parameter
TLS	Transport Layer Security
Triple-DES	Triple Data Encryption Standard
VSM	Virtual Security Module
XTS	XEX-based Tweaked Codebook with CipherText Stealing