Beijing JN TASS Technology Co., Ltd.

TASS Crypto Engine

FIPS 140-3 Non-Proprietary Security Policy

1 Table of Contents

1 Table of Contents 2
1. General 6
1.1 Overview 6
1.2 Security Levels 6
1.3 Additional Information 6
2 Cryptographic Module Specification 7
2.1 Description 7
2.2 Tested and Vendor Affirmed Module Version and Identification 9
2.3 Excluded Components 9
2.4 Modes of Operation 10
2.5 Algorithms 10
2.6 Security Function Implementations 16
2.7 Algorithm Specific Information 24
2.7.1 AES GCM IV (IG C.H) 24
2.7.2 AES XTS 24
2.7.3 Key Derivation using SP 800-132 PBKDF2 24
2.7.4 SP 800-56Ar3 Assurances 24
2.7.5 RSA Signatures (IG C.F) 25
2.7.6 ML-KEM 25
2.8 RBG and Entropy 25
2.9 Key Generation 26
2.10 Key Establishment 26
2.11 Industry Protocols 26
3 Cryptographic Module Interfaces 27
3.1 Ports and Interfaces 27
3.2 Trusted Channel Specification 28
4 Roles, Services, and Authentication 29
4.1 Authentication Methods 29
4.1.1 Manager, Operator, Auditor 29
4.1.2 User Application 29
4.1.3 Authentication Strength 30
4.2 Roles 30
4.3 Approved Services 30
4.4 Non-Approved Services 48
4.5 External Software/Firmware Loaded 51
5 5 Software/Firmware Security 52
5.1 Integrity Techniques 52
5.2 Initiate on Demand 52
6 Operational Environment 53
6.1 Operational Environment Type and Requirements 53
7 Physical Security 54
7.1 Mechanisms and Actions Required 54
7.2 EFP/EFT Information 56
7.3 Hardness Testing Temperature Ranges 56

8 Non-Invasive Security 57
9 Sensitive Security Parameters Management 58
9.1 Storage Areas 58
9.2 SSP Input-Output Methods 58
9.3 SSP Zeroization Methods 59
9.4 SSPs 60
9.5 Transitions 77
10 Self-Tests 78
10.1 Pre-Operational Self-Tests 78
10.2 Conditional Self-Tests 78
10.3 Periodic Self-Test Information 86
10.4 Error States 89
10.5 Operator Initiation of Self-Tests 89
11 Life-Cycle Assurance 90
11.1 Installation, Initialization, and Startup Procedures 90
11.2 Administrator Guidance 95
11.3 Non-Administrator Guidance 95
11.4 End of Life 96
12 Mitigation of Other Attacks 97
Appendix A. Glossary and Abbreviations 98
Appendix B. References 100

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Hardware 9
Table 3: Modes List and Description 10
Table 4: Approved Algorithms 15
Table 5: Vendor-Affirmed Algorithms 15
Table 6: Non-Approved, Not Allowed Algorithms 16
Table 7: Security Function Implementations 23
Table 8: Entropy Certificates 25
Table 9: Entropy Sources 25
Table 10: Ports and Interfaces 27
Table 11: Authentication Methods 29
Table 12: Roles 30
Table 13: Approved Services 47
Table 14: Non-Approved Services 51
Table 15: Mechanisms and Actions Required 54
Table 16: EFP/EFT Information 56
Table 17: Hardness Testing Temperatures 56
Table 18: Storage Areas 58
Table 19: SSP Input-Output Methods 59
Table 20: SSP Zeroization Methods 59
Table 21: SSP Table 1 66
Table 22: SSP Table 2 77
Table 23: Pre-Operational Self-Tests 78
Table 24: Conditional Self-Tests 86
Table 25: Pre-Operational Periodic Information 86
Table 26: Conditional Periodic Information 89
Table 27: Error States 89

List of Figures

Figure 1: Application scenario of the module 7
Figure 2: Front panel of the module 8
Figure 3: Back panel of the module 8
Figure 4: Hardware block diagram of the module 9
Figure 5: Physical ports (front panel) 27
Figure 6: Physical ports (back panel) 28
Figure 7: Tamper evidence seals 55
Figure 8: Initialize – 1 91
Figure 9: Initialize - 2 92
Figure 10: User Management – Crypto Officer 92
Figure 11: Network Configuration 93
Figure 12: Device Configuration – Host Service Property 93
Figure 13: User Management – White List 94
Figure 14: Key Management – Symmetric Key 94
Figure 15: Packing of the module 95

1. General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for TASS Crypto Engine. 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.
This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

1.2 Security Levels

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

1.3 Additional Information

In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing. The vendor reviewed the intermediate and final Security Policy and approved all of its content.

2 Cryptographic Module Specification

2.1 Description

The TASS Crypto Engine (hereafter referred to as the “module”) is a hardware security module (HSM) with physical security protection measures, key management mechanisms and security functions to provide secure application-level cryptographic services for customer systems. The security functionalities include key wrapping, message authentication code (MAC), message digest, data encryption and decryption, digital signature generation and verification, among others.

Purpose and Use:
An application server (host) connects to the module over a network using the TCP/IP protocol and authenticates to the module via the mutually authenticated TLS channel using its digital certificate. Once authentication is successful, the host invokes cryptographic services from the module, which processes the requests and returns the corresponding results.
In addition, authorized users may access the module’s management functions through a management interface either via a serial console connection or through a web-based interface.
A typical application scenario is shown in Figure 1.

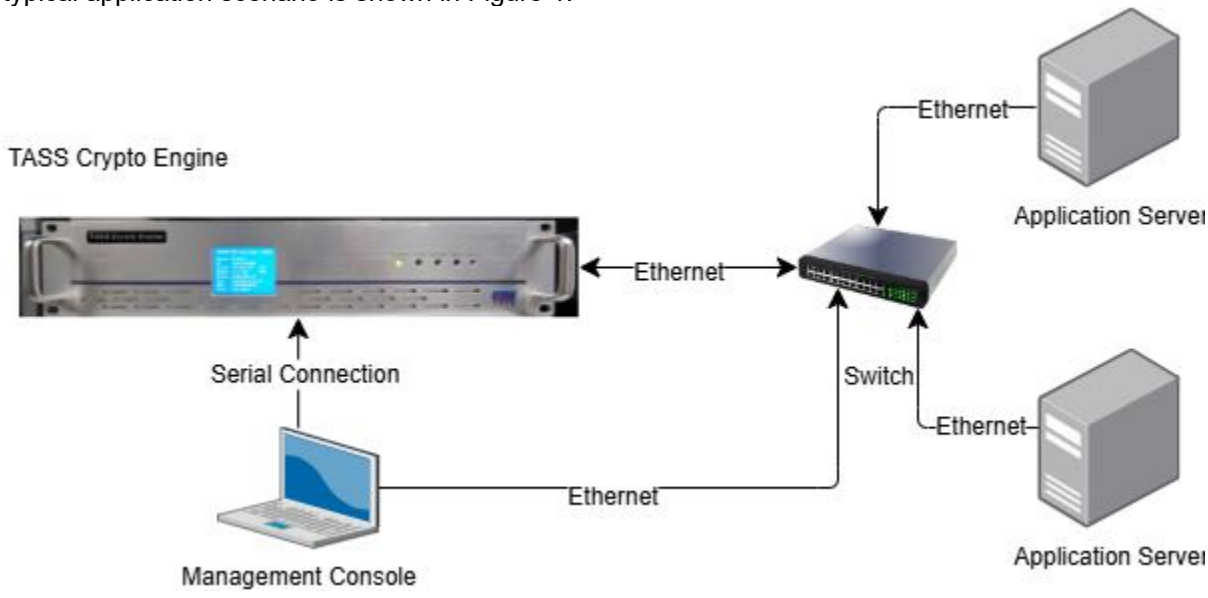


Figure 1: Application scenario of the module

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:
The cryptographic boundary (red dotted line in Figure 4: Hardware block diagram of the module) of the module is defined as the entire hardware security module (HSM).
The physical dimensions of the module are 465 mm x 88.8 mm x 557.5 mm (width x height x length).

The block diagram below shows the module, its interfaces with the operational environment and the delimitation of its cryptographic boundary. Figure 4: Hardware block diagram of the module also depicts the flow of status output (SO), control input (CI), data input (DI) and data output (DO). Description of the ports and interfaces can be found in Table 8: Ports and Interfaces. The entropy source used by the module is located within the module’s cryptographic boundary (see Figure 4).

Diagram, Photograph



Figure 2: Front panel of the module



Figure 3: Back panel of the module

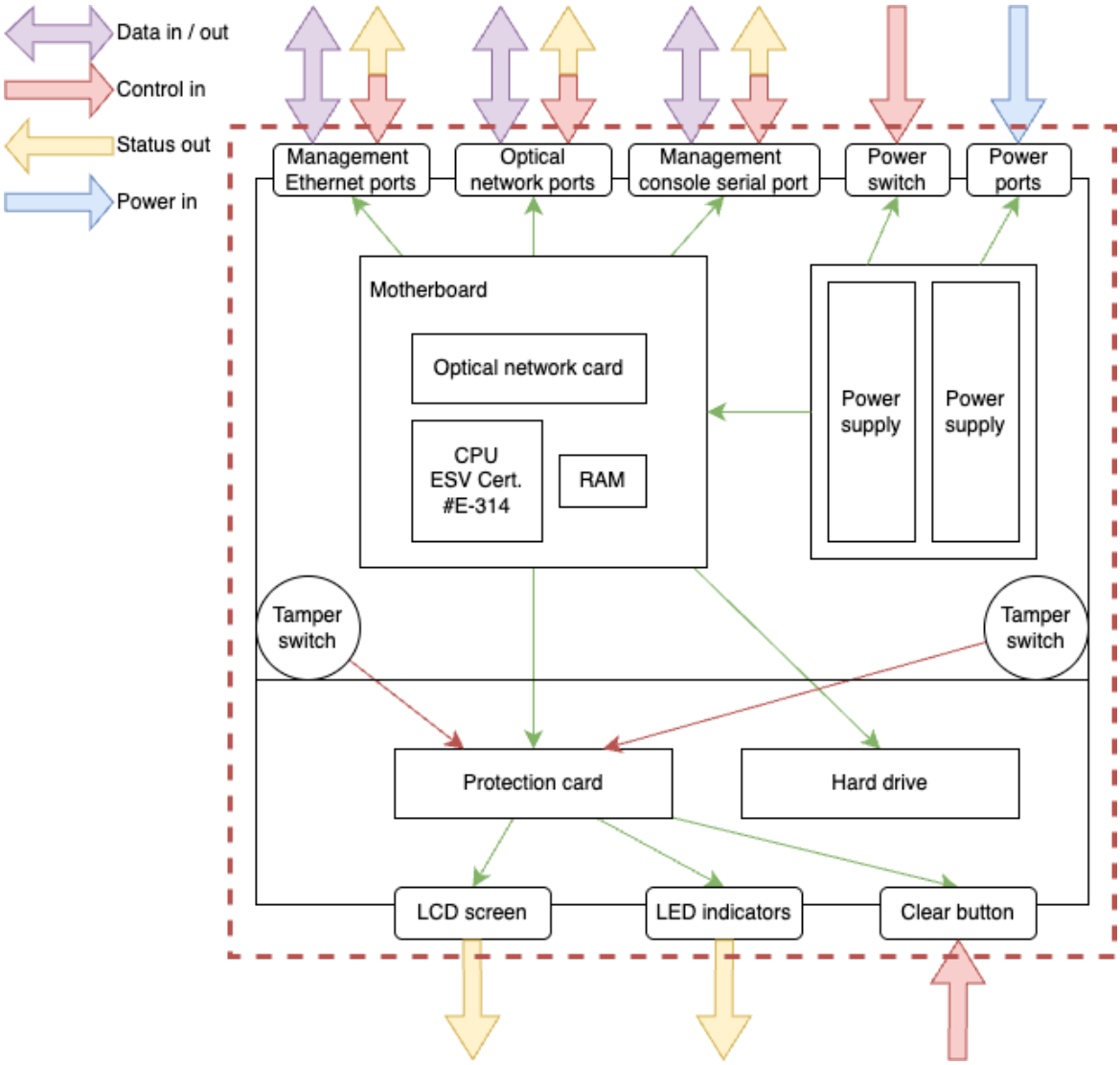


Figure 4: Hardware block diagram of the module

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
TASS Crypto Engine	S10000-II-B V2.00	H2.00.00	Intel® Xeon® E-2334 Rocket Lake	

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

There are no components excluded from the requirements of the FIPS 140-3 standard.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved mode	The module is configured with an Approved DMK algorithm and executes an Approved service.	Approved	'FIPS: YES' is displayed, and the service indicator returns 1.
Non-approved mode	The module operates in non-Approved mode when either (1) a non-Approved DMK algorithm is configured during installation, or (2) a non-Approved service is invoked while the module is configured with an Approved DMK algorithm.	Non-Approved	The service indicator returns 0. The status indicator displays 'FIPS: NO' for a non-Approved DMK configuration and 'FIPS: YES' otherwise.

Table 3: Modes List and Description

After successfully completing all pre-operational self-tests and cryptographic algorithm self-tests during start-up, the module automatically enters the operational mode. No operator intervention is required.

Mode Change Instructions and Status:

If the module is installed with an Approved DMK algorithm (status indicator "FIPS: YES"), the service indicator returns 1 when an Approved service is invoked and 0 when a non-Approved service is invoked. The status indicator remains "FIPS: YES" in both cases.

If the module is installed with a non-Approved DMK algorithm (status indicator "FIPS: NO"), it operates exclusively in non-Approved mode, with the service indicator returning 0 for all services. The module must be reinstalled with an Approved DMK algorithm to enable Approved operation.

Each SSP stored by the module is associated with a unique index and contextual information (e.g., mode of operation), ensuring that SSPs are not shared between approved and non-approved modes.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC, AES-CFB128, AES-ECB, AES-OFB	A6945	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A6945	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 AAD Length - AAD Length: 0-2048 Increment 8	SP 800-38C
AES-CMAC	A6945	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 0-65536 Increment 8	SP 800-38B

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A6945	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 - Yes Counter Tests Performed - Yes	SP 800-38A
AES-GCM	A6945	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, 128 Payload Length - Payload Length: 8-65536 Increment 8 AAD Length - AAD Length: 0-2048 Increment 8	SP 800-38D
AES-KW	A6945	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 128	SP 800-38F
AES-KWP	A6945	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 8-4096 Increment 8	SP 800-38F
AES-XTS Testing Revision 2.0	A6945	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 8 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
Counter DRBG	A6956	Prediction Resistance - Yes Supports Reseed - Yes Mode - AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 384 Entropy Input - Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 384 Returned Bits - 256	SP 800-90A Rev. 1
cSHAKE-128	A6958	Message Length - Message Length: 0-65536 Increment 8 Output Length - Output Length: 256-512 Increment 8 Hex Customization - Yes	SP 800-185
ECDSA KeyGen (FIPS186-5)	A6946	Curve - B-283, B-409, B-571, K-283, K-409, K-571, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6946	Curve - B-283, B-409, B-571, K-283, K-409, K-571, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6946	Curve - B-283, B-409, B-571, K-283, K-409, K-571, P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512,	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
		SHA2-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE-128, SHAKE-256 Component - No, Yes	
ECDSA SigVer (FIPS186-5)	A6946	Component - No Curve - B-283, B-409, B-571, K-283, K-409, K-571, P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512, SHA2-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE-128, SHAKE-256	FIPS 186-5
EDDSA KeyGen, EDDSA KeyVer	A6947	Curve - ED-25519, ED-448	FIPS 186-5
EDDSA SigGen	A6947	Curve - ED-25519, ED-448 Context Length - Context Length: 0-255 Increment 1 PreHash - No Pure - Yes	FIPS 186-5
EDDSA SigVer	A6947	Curve - ED-25519, ED-448 PreHash - No Pure - Yes	FIPS 186-5
HMAC-SHA2-256, HMAC-SHA2-512/256, HMAC-SHA3-256	A6955	MAC - MAC: 256 Key Length - Key Length: 128-256 Increment 8	FIPS 198-1
HMAC-SHA2-384, HMAC-SHA3-384	A6955	MAC - MAC: 384 Key Length - Key Length: 128-256 Increment 8	FIPS 198-1
HMAC-SHA2-512, HMAC-SHA3-512	A6955	MAC - MAC: 512 Key Length - Key Length: 128-256 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6953	Domain Parameter Generation Methods - B-283, B-409, B-571, K-283, K-409, K-571, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A6954	Fixed Info Pattern - uPartyInfo||vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 256-16384 Increment 8 HMAC Algorithm - SHA2-256, SHA2-384, SHA2-512, SHA2-512/256, SHA3-256, SHA3-384, SHA3-512 Perform Multiple Expansion Tests - No Uses Hybrid Shared Secret - No	SP 800-56C Rev. 2
KDF ANS 9.63 (CVL)	A6951	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512, SHA2-512/256, SHA3-256, SHA3-384, SHA3-512 Field Size - 256, 571 Shared Info Length - Shared Info Length: 0-1024 Increment 8 Key Data Length - Key Data Length: 128-256 Increment 8	SP 800-135 Rev. 1
KDF SP800-108	A6949	KDF Mode - Counter MAC Mode - HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512 Supported Lengths - Supported Lengths: 128-256	SP 800-108 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Increment 8 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - Yes Requires Empty IV - No Custom Key In Length - 0	
KMAC-128	A6958	Message Length - Message Length: 0-65536 Increment 8 MAC Length - MAC Length: 256-512 Increment 8 Key Data Length - Key Data Length: 128-256 Increment 8 Hex Customization - Yes Supports eXtendable-Output Functions - No, Yes	SP 800-185
LMS KeyGen, LMS SigGen, LMS SigVer	A6960	LMS Modes - LMS_SHA256_M32_H10, LMS_SHA256_M32_H15, LMS_SHA256_M32_H20, LMS_SHA256_M32_H25, LMS_SHA256_M32_H5 LMOTS Modes - LMOTS_SHA256_N32_W1, LMOTS_SHA256_N32_W2, LMOTS_SHA256_N32_W4, LMOTS_SHA256_N32_W8	SP 800-208
ML-DSA KeyGen	A6959	Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87	FIPS 204
ML-DSA SigGen	A6959	Signature Interfaces - external, internal Pre Hash - preHash 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, SHA3-512, SHAKE-256 Context Length - Context Length: 0-1024 Increment 8	FIPS 204
ML-DSA SigVer	A6959	Signature Interfaces - external, internal Pre Hash - preHash 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, SHA3-512, SHAKE-256 Context Length - Context Length: 0-1024 Increment 8	FIPS 204
ML-KEM EncapDecap	A6959	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768 Functions - Decapsulation, Encapsulation	FIPS 203
ML-KEM KeyGen	A6959	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768	FIPS 203
PBKDF	A6950	Iteration Count - Iteration Count: 1000-10000000 Increment 1 HMAC Algorithm - SHA2-256, SHA2-384, SHA2-512, SHA2-512/256, SHA3-256, SHA3-384, SHA3-512 Password Length - Password Length: 8-128	SP 800-132

Algorithm	CAVP Cert	Properties	Reference
		Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-256 Increment 8	
RSA Decryption Primitive Sp800-56Br2 (CVL)	A6948	Modulo - 2048, 3072, 4096 Key Format - Chinese Remainder Theorem (CRT) Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A6948	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096, 8192 p mod 8 - 0 Primality Tests - 2powSecStr q mod 8 - 0 Fixed Public Exponent - 010001 Info Generated By Server - Yes Private Key Format - crt Public Exponent Mode - fixed	FIPS 186-5
RSA SigGen (FIPS186-5)	A6948	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5
RSA Signature Primitive (CVL)	A6948	Modulo - 2048, 3072, 4096 Private Key Format - crt Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-5
RSA SigVer (FIPS186-5)	A6948	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
SHA2-256, SHA2-384, SHA2-512, SHA2-512/256	A6957	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA3-256, SHA3-384, SHA3-512	A6957	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHAKE-128, SHAKE-256	A6957	Supports Bit-Oriented Messages - No Supports Empty Message - Yes Supports Bit-Oriented Output - No Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SLH-DSA KeyGen	A6959	Parameter Sets - 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	A6959	Deterministic - No, Yes Signature Interfaces - external, internal Pre Hash - preHash, pure Parameter Sets - SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-	FIPS 205

Algorithm	CAVP Cert	Properties	Reference
		SHAKE-256s Message Length - Message Length: 8-65536 Increment 8 Context Length - Context Length: 0-1024 Increment 8 Hash Algorithms - SHA2-512, SHA3-512, SHAKE-256	
SLH-DSA SigVer	A6959	Signature Interfaces - external, internal Pre Hash - preHash, pure Parameter Sets - 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 Context Length - Context Length: 0-1024 Increment 8 Hash Algorithms - SHA2-512, SHA3-512, SHAKE-256	FIPS 205
TLS v1.2 KDF RFC7627 (CVL)	A6952	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A6952	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	Random bit strings required for generating the cryptographic keys is compliant with [SP 800-133Rev2] section 4 example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
SM2	Key generation; Digital signature generation and verification; Asymmetric encryption and decryption; Key agreement
SM3	Message digest
SM4	Symmetric algorithm for data encryption and decryption

Name	Use and Function
SM9	Key generation; Digital signature generation and verification; Asymmetric encryption and decryption; Key agreement; key encapsulation and decapsulation
ZUC	Symmetric algorithm for data encryption and decryption
DES	Symmetric algorithm for data encryption and decryption
TDES	Symmetric algorithm for data encryption and decryption
AES with non-SP800-38F use	Symmetric algorithm for data encryption and decryption with non-SP800-38F format
RSA (1024bits)	Key generation; Digital signature generation and verification; Asymmetric encryption and decryption
ECC (K-283, K-409, K-571, B-283, B-409, B-571, NISTP192v1, NISTP192v2, NISTP192v3, BRAINPOOLP192R1, BRAINPOOLP224R1, BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1, BRAINPOOLP192T1, BRAINPOOLP224T1, BRAINPOOLP256T1, BRAINPOOLP320T1, BRAINPOOLP384T1, BRAINPOOLP512T1, SECP192K1, SECP256K1, SECP224R1, SECT233K1, SECT233R1, frp256v1)	Key generation; Digital signature generation and verification; Key agreement
X25519/X448	Key generation; Key agreement
SHA-1, SHA-224, SHA3-224, MD5	Message digest
HMAC (SHA-1, SHA-224, SHA3-224, MD5, SM3)	Message Authentication Code
GMAC	Message Authentication Code
HKDF (SHA-1, SHA-224, SHA3-224, MD5, SM3)	Key Derivation
XMSS	Key generation; Digital signature generation and verification

Table 6: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric Encryption with AES	BC-UnAuth	Symmetric encryption using AES		AES-ECB: (A6945) AES-CBC: (A6945) AES-OFB: (A6945) AES-CFB128: (A6945) AES-CTR: (A6945) AES-XTS Testing Revision 2.0: (A6945)

Name	Type	Description	Properties	Algorithms
Symmetric Decryption with AES	BC-UnAuth	Symmetric decryption using AES		AES-ECB: (A6945) AES-CBC: (A6945) AES-OFB: (A6945) AES-CFB128: (A6945) AES-CTR: (A6945) AES-XTS Testing Revision 2.0: (A6945)
KTS-Wrap with AES-KW and AES-KWP	KTS-Wrap	Key wrapping using AES KW and AES-KWP	Standard:SP 800-38F IG D.G:approved method from IG D.G Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-KW: (A6945) AES-KWP: (A6945)
KTS-Unwrap with AES-KW and AES-KWP	KTS-Unwrap	Key unwrapping using AES KW and AES-KWP	Standard:SP 800-38F IG D.G:approved method from IG D.G Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-KW: (A6945) AES-KWP: (A6945)
Key Derivation with HKDF	KAS-56CKDF	Key Derivation using HKDF		KDA HKDF SP800-56Cr2: (A6954)
Key Derivation with KBKDF	KBKDF	Generate secret keys from a pre-existing key-derivation-key		KDF SP800-108: (A6949)
Password-based Key Derivation	PBKDF	Derive keys for use in storage applications		PBKDF: (A6950)
Random Number Generation	DRBG	Generate random bytes		Counter DRBG: (A6956)
Signature Generation	DigSig-SigGen	Generate a digital signature		ECDSA SigGen (FIPS186-5): (A6946) RSA SigGen (FIPS186-5): (A6948) EDDSA SigGen: (A6947) Counter

Name	Type	Description	Properties	Algorithms
				DRBG: (A6956)
Signature Verification	DigSig-SigVer	Verify a digital signature		ECDSA SigVer (FIPS186-5): (A6946) RSA SigVer (FIPS186-5): (A6948) EDDSA SigVer: (A6947)
Message Authentication Code	MAC	Message authentication code		HMAC-SHA2-256: (A6955) HMAC-SHA2-384: (A6955) HMAC-SHA2-512: (A6955) HMAC-SHA2-512/256: (A6955) HMAC-SHA3-256: (A6955) HMAC-SHA3-384: (A6955) HMAC-SHA3-512: (A6955) AES-CMAC: (A6945)
Message Digest	SHA XOF	Compute a message digest		SHA2-256: (A6957) SHA2-384: (A6957) SHA2-512: (A6957) SHA2-512/256: (A6957) SHA3-256: (A6957) SHA3-384: (A6957) SHA3-512: (A6957) SHAKE-128: (A6957) SHAKE-256:

Name	Type	Description	Properties	Algorithms
				(A6957) cSHAKE-128: (A6958) KMAC-128: (A6958)
Authenticated Symmetric Encryption	BC-Auth	Authenticated symmetric encryption		AES-CCM: (A6945) AES-GCM: (A6945)
Authenticated Symmetric Decryption	BC-Auth	Authenticated symmetric decryption		AES-CCM: (A6945) AES-GCM: (A6945)
KTS-Wrap with AES-CCM and AES-GCM	KTS-Wrap	Key wrapping with AES CCM and AES-GCM	Standard:SP 800-38F IG D.G:approved method from IG D.G Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-CCM: (A6945) AES-GCM: (A6945)
KTS-Unwrap with AES-CCM and AES-GCM	KTS-Unwrap	Key unwrapping with AES CCM and AES-GCM	Standard:SP 800-38F IG D.G:approved method from IG D.G Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-CCM: (A6945) AES-GCM: (A6945)
Symmetric key generation	CKG	Generate a symmetric key		CKG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A6956)
Key Pair Generation	AsymKeyPair-KeyGen CKG	Generate an ECDSA, ECDH, RSA, EdDSA key pair		CKG: () Key Type: Symmetric and Asymmetric ECDSA KeyGen (FIPS186-5): (A6946) RSA KeyGen (FIPS186-5): (A6948) EDDSA KeyGen: (A6947) Counter DRBG: (A6956)
Key Pair Verification	AsymKeyPair-KeyVer	Verify an ECDSA,		ECDSA KeyVer (FIPS186-5):

Name	Type	Description	Properties	Algorithms
		EdDSA key pair		(A6946) EDDSA KeyVer: (A6947)
Key agreement with ECDH and ANS X9.63 KDF	KAS-Full	Shared Secret Computation followed by KDF with ANS X9.63	IG:IG D.F. Scenario 2 (path 2), end-to-end Key confirmation":no Key derivation:IG 2.4.B ANS X9.63 KDF Caveat:Key establishment methodology provides between 128 and 256 bits of key strength	KAS-ECC-SSC Sp800-56Ar3: (A6953) KDF ANS 9.63: (A6951)
Key Encapsulation with ML-KEM	KEM-Encap	Key Encapsulation with ML-KEM	IG:IG D.S Scenario 1	ML-KEM EncapDecap: (A6959) SHA3-256: (A6957) SHA3-512: (A6957) SHAKE-128: (A6957) SHAKE-256: (A6957)
Key Decapsulation with ML-KEM	KEM-Decap	Key Decapsulation with ML-KEM	IG:IG D.S Scenario 1	ML-KEM EncapDecap: (A6959) SHA3-256: (A6957) SHA3-512: (A6957) SHAKE-128: (A6957) SHAKE-256: (A6957)
Asymmetric Decryption with RSA	AsymKeyPair-Decap	Asymmetric Decryption with RSA	Standard:SP 800-56Brev2 IG D.G:approved method from IG D.G Caveat:Key establishment methodology provides between 112 and 128 bits of security strength	RSA Decryption Primitive Sp800-56Br2: (A6948)
Signature Generation Primitive	DigSig-SigGen	Signature Generation Primitive with RSA		RSA Signature Primitive: (A6948)
TLS Handshake KAS	KAS-Full	Key agreement	IG D.F:Scenario 2 (path 2), end-to-end Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL and KDA (separately tested) Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A6953) TLS v1.2 KDF RFC7627: (A6952) TLS v1.3 KDF:

Name	Type	Description	Properties	Algorithms
				(A6952) KDA HKDF SP800-56Cr2: (A6954)
ML-DSA key pair generation	AsymKeyPair-KeyGen	Generate an ML-DSA key pair	Parameter Sets:ML-DSA-44, ML-DSA-65, ML-DSA-87	CKG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A6956) ML-DSA KeyGen: (A6959) SHAKE-128: (A6957) SHAKE-256: (A6957)
ML-KEM key pair generation	AsymKeyPair-KeyGen	Generate an ML-KEM key pair	Parameter Sets:ML-KEM-1024, ML-KEM-512, ML-KEM-768	CKG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A6956) ML-KEM KeyGen: (A6959) SHA3-256: (A6957) SHA3-512: (A6957) SHAKE-128: (A6957) SHAKE-256: (A6957)
SLH-DSA key pair generation	AsymKeyPair-KeyGen	Generate an SLH-DSA key pair	Parameter Sets:SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s	CKG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A6956) SLH-DSA KeyGen: (A6959) SHAKE-256: (A6957)
LMS key pair generation	AsymKeyPair-KeyGen	Generate an LMS key pair	LMS Modes:LMS_SHA256_M32_H10,	CKG: () Key Type:

Name	Type	Description	Properties	Algorithms
			LMS_SHA256_M32_H15, LMS_SHA256_M32_H20, LMS_SHA256_M32_H25, LMS_SHA256_M32_H5 LMOTS Modes:LMOTS_SHA256_N32_W1, LMOTS_SHA256_N32_W2, LMOTS_SHA256_N32_W4, LMOTS_SHA256_N32_W8	Symmetric and Asymmetric Counter DRBG: (A6956) LMS KeyGen: (A6960) SHA2-256: (A6957)
Signature Generation ML-DSA External Deterministic	DigSig-SigGen	Signature generation with ML-DSA External Deterministic	ML-DSA SigGen (FIPS 204):ML-DSA-44, ML-DSA-65, ML-DSA-87	Counter DRBG: (A6956) ML-DSA SigGen: (A6959) SHA2-512: (A6957) SHA3-512: (A6957) SHAKE-256: (A6957) SHAKE-128: (A6957)
Signature Generation ML-DSA External Hedged	DigSig-SigGen	Signature generation with ML-DSA External Hedged	ML-DSA SigGen (FIPS 204):ML-DSA-44, ML-DSA-65, ML-DSA-87	Counter DRBG: (A6956) ML-DSA SigGen: (A6959) SHA2-512: (A6957) SHA3-512: (A6957) SHAKE-256: (A6957) SHAKE-128: (A6957)
Signature Verification ML-DSA External	DigSig-SigVer	Signature verification with ML-DSA External	ML-DSA SigVer (FIPS 204):ML-DSA-44, ML-DSA-65, ML-DSA-87	ML-DSA SigVer: (A6959) SHA2-512: (A6957) SHA3-512: (A6957) SHAKE-256: (A6957) SHAKE-128: (A6957)
Signature Generation SLH-DSA External Pure	DigSig-SigGen	Signature generation with SLH-DSA External Pure	SLH-DSA SigGen (FIPS 205):SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-	Counter DRBG: (A6956) SLH-DSA

Name	Type	Description	Properties	Algorithms
			DSA-SHAKE-256f, SLH-DSA-SHAKE-256s Deterministic:Yes, No	SigGen: (A6959) SHAKE-256: (A6957)
Signature Generation SLH-DSA External PreHash	DigSig-SigGen	Signature generation with SLH-DSA External PreHash	SLH-DSA SigGen (FIPS 205): SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s Deterministic : :Yes, No	Counter DRBG: (A6956) SLH-DSA SigGen: (A6959) SHA2-512: (A6957) SHA3-512: (A6957) SHAKE-256: (A6957)
Signature Verification SLH-DSA External Pure	DigSig-SigVer	Signature verification with SLH-DSA External Pure	SLH-DSA SigVer (FIPS 205):SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s	SLH-DSA SigVer: (A6959) SHAKE-256: (A6957)
Signature Verification SLH-DSA External PreHash	DigSig-SigVer	Signature verification with SLH-DSA External PreHash	SLH-DSA SigVer (FIPS 205): SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s	SLH-DSA SigVer: (A6959) SHA2-512: (A6957) SHA3-512: (A6957) SHAKE-256: (A6957)
Signature Generation LMS	DigSig-SigGen	Signature verification with LMS	LMS Siggen (SP 800-208):LMS parameters: SHA256_M32_H5, SHA256_M32_H10, SHA256_M32_H15, SHA256_M32_H20, SHA256_M32_H25; LMOTS parameters: SHA256_N32_W1, SHA256_N32_W2, SHA256_N32_W4, SHA256_N32_W8	Counter DRBG: (A6956) LMS SigGen: (A6960) SHA2-256: (A6957)
Signature Verification LMS	DigSig-SigVer	Signature Verification with LMS	LMS Siggen (SP 800-208):LMS parameters: SHA256_M32_H5, SHA256_M32_H10, SHA256_M32_H15, SHA256_M32_H20, SHA256_M32_H25; LMOTS parameters: SHA256_N32_W1, SHA256_N32_W2, SHA256_N32_W4, SHA256_N32_W8	LMS SigVer: (A6960) SHA2-256: (A6957)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV (IG C.H)

The module implements AES GCM algorithm with two IV generation options:
Compliant to IG C.H scenario 1: In this case, the module generates GCM IV in the context of TLS 1.2 and 1.3 protocol. The IV is 96 bits with 32 bits of implicit field and 64 bits of explicit field (i.e. counter portion) For TLS 1.2 module supports acceptable AES-GCM cipher suites from section 3.3.1 of SP 800-52r2 and the mechanism for IV generation is compliant with RFC 5288. For TLS 1.3 module supports acceptable AES-GCM cipher suites from section 3.3.1 of SP 800-52r2 and the mechanism for IV generation is compliant with RFC 8446.
The design of the TLS protocol implicitly ensures that the counter does not exhaust the maximum number of possible values for a given session key. In the event the module's power is lost and restored, the entire TLS connection is closed, and the module ensures that a new key is established under new TLS session for use with the AES GCM key encryption or decryption.
Compliant to IG C.H scenario 2: In this case a 96 bit IV is generated using approved DRBG implemented by the module.

2.7.2 AES XTS

The length of a single data unit encrypted or decrypted with AES XTS shall not exceed 2^{20} AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E.
To meet the requirement stated in IG C.I, two AES keys are independently generated using an Approved DRBG compliant with SP 800-90A. The module implements a check that ensures, before performing any cryptographic operation, that the two AES keys used in AES XTS mode are not identical.
The XTS mode shall only be used for the cryptographic protection of data on storage devices. It shall not be used for other purposes, such as the encryption of data in transit.

2.7.3 Key Derivation using SP 800-132 PBKDF2

The module provides password-based key derivation (PBKDF2), compliant with SP 800-132. The module supports option 1a from Section 5.4 of SP 800-132, in which the Master Key (MK) or a segment of it is used directly as the Data Protection Key (DPK). In accordance with SP 800-132 and FIPS 140-3 IG D.N, the following requirements are met:

- Derived keys shall be used only for storage applications and shall not be used for any other purposes. The length of the MK or DPK is 112 bits or more.
- Passwords or passphrases, used as an input for the PBKDF2, shall not be used as cryptographic keys.
- The minimum length of the password or passphrase accepted by the module is 8 characters. The probability of guessing the value, assuming a worst-case scenario of all digits, is estimated to be at most 10^8. Combined with the minimum iteration count as described below, this provides an acceptable trade-off between user experience and security against brute-force attacks.
- The salt is generated randomly using the SP 800-90Ar1 DRBG provided by the module. The minimum length required is 128 bits.
- The iteration count shall be selected as large as possible, as long as the time required to generate the key using the entered password is acceptable for the users. The minimum value accepted by the module is 1000.

2.7.4 SP 800-56Ar3 Assurances

To comply with the assurances found in Section 5.6.2 of SP 800-56Ar3, the keys for KAS-ECC must be generated using the approved key generation services specified in Section 2.9 or the key pairs must be obtained from another FIPS-validated module.
The module performs full public key validation on the generated public keys. Additionally, the module performs full public key validation on the received public keys, complying with Sections 5.6.2.2.1 and 5.6.2.2.2 of SP 800-56A Rev. 3.
The module implements key agreement compliant to IG D.F following scenario 2 path (2). The key agreement scheme used is One-Pass Diffie-Hellman scheme (1e, 1s, ECDH) where the module's key is static and the other party acts as the Initiator that provides the ephemeral key. The CAVP testing was performed end-to-end with a KAS-ECC CAVP certificate issued (without key confirmation).

The following is a list of applicable sections from SP800-56Arev3 section 5.6.2 and how the respective shall requirements are met.

- Assurance that the key pair was generated correctly is met as specified 5.6.2.1.1 item a, since the module generates the key pair for ECDH using NIST curves from SP 800-186.
- Assurance of private key validity is met as specified 5.6.2.1.2 item a, since the owner uses the module to generate the key pair as specified above.
- Assurance of public key validity is met as specified 5.6.2.1.3 item a, since the module performs full public key validation.
- Assurance of pair-wise consistency is met as specified 5.6.2.1.4 item a, since the module generates the key pair as specified above.
- Assurance of possession of the private key is met as specified in 5.6.2.1.5 item a, since the module generates the key pair as specified above.
- Assurance of public-key validity is met as specified in 5.6.2.2.2, since the module performs public key validation on the received public key.
- Assurance of private-key possession: As explained above the module only allows use of ephemeral keys from other peer so assurance of private-key possession is not mandatory when using ephemeral keys.

2.7.5 RSA Signatures (IG C.F)

The module implements the approved modulus sizes of 2048, 3072, and 4096 bits for signature generation and signature verification. Each algorithm was tested, and corresponding certificates can be found detailed in Section 2.5 Table Approved Algorithms.

2.7.6 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 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
E314	tass

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
CPU Time Jitter RNG Entropy Source	Non-Physical	TASS Crypto Engine	256 bits	Full entropy	SHA3-256 Cert. #A7532

Table 9: Entropy Sources

The module employs the Deterministic Random Bit Generator (DRBG) implementations based on SP 800-90Ar1. In addition to the DRBG algorithms provided to the operator, the module internally uses two dedicated DRBG instances based on SP 800-90A Rev. 1 to generate seeds for asymmetric key pairs and random numbers for security functions. The DRBG is automatically reseeded whenever the module transitions from a non-Approved service to an Approved service that requires random number generation. The following parameters are used:

- Private DRBG: AES-256 CTR_DRBG without derivation function. This DRBG is used to generate secret random values (e.g. during asymmetric key pair generation). It can be accessed using RAND_priv_bytes.
- Public DRBG: AES-256 CTR_DRBG without derivation function. This DRBG is used to generate general purpose random values that do not need to remain secret (e.g. initialization vectors). It can be accessed using RAND_bytes.

2.9 Key Generation

The module implements asymmetric key generation methods according to SP 800-133r2 section 5.1, which maps to FIPS 186-5.
The module implements symmetric key generation with the "Symmetric key generation" service.
In addition, the HMAC and AES symmetric keys are derived from shared secrets by applying [SP 800-135] as part of the TLS, ANSI X9.63-2001 protocols and standards. The scenario maps to the [SP 800-133r2] section 6.2.1 *Symmetric keys generated using Key Agreement Scheme*.

The key generation methods are specified in the Security Function Implementations table in section 2.6.
The cryptographic module performs Cryptographic Key Generation (CKG) included in table Vendor-Affirmed Algorithms in section 2.5.

2.10 Key Establishment

The module implements SSP agreement and SSP transport methods as specified in the Security Function Implementations table in section 2.6.
The module offers ML-KEM as a service to the operator of the module but does not establish module SSPs to be used by the module for cryptographic protection.

2.11 Industry Protocols

No parts of the TLS protocols, other than those mentioned above, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Management Ethernet ports	Data Input	Import backup archive for key restore. Authentication information. Configuration information.
Optical network ports	Data Input	User service request messages.
Management console serial port	Data Input	Command line management information. Configuration information.
Management Ethernet ports	Data Output	Export backup archive for key backup.
Optical network ports	Data Output	User service response messages.
Management console serial port	Data Output	Command line management information. Configuration information.
Management Ethernet ports	Control Input	Configuration information.
Optical network ports	Control Input	Configuration information.
Management console serial port	Control Input	Command line management information. Configuration information.
Power switch	Power	Power on/off the module.
Clear button	Control Input	Clear keys stored in the module (if pressed for 10 seconds).
Management Ethernet ports	Status Output	Display module information and business functions of operation.
Optical network ports	Status Output	Display module information and business functions of operation.
Management console serial port	Status Output	Display module information and business functions of operation.
LCD screen	Status Output	Display module information and business functions of operation.
LED indicators (power, work, alarm, fault)	Status Output	Indicate power on/off, work activity, alarm, fault states.
Buzzer/audible alarm	Status Output	Indicate that only one power cable is plugged in.
Power connectors	Power	Two power cables used for power redundancy.

Table 10: Ports and Interfaces

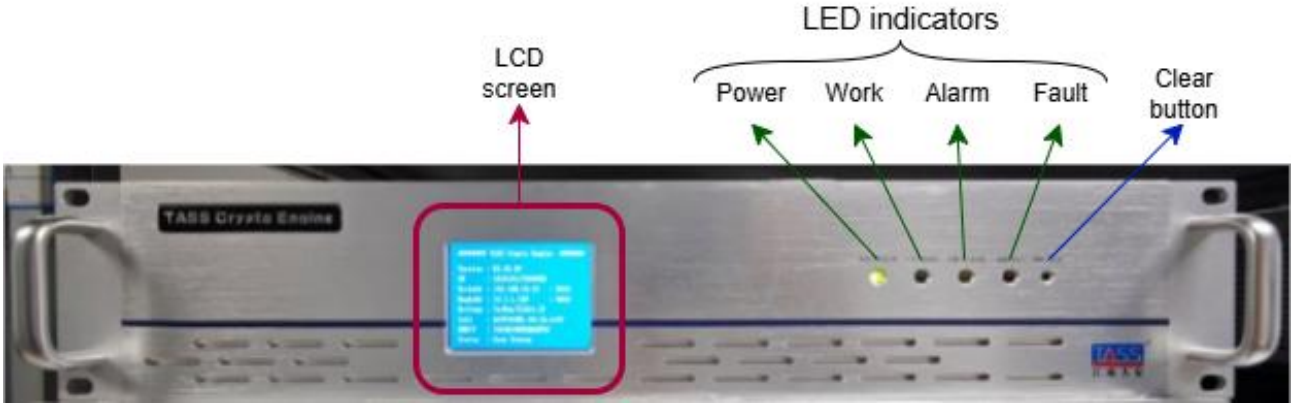


Figure 5: Physical ports (front panel)

Indicators include a power light, a work light (if the HSM is performing some cryptographic operations from a command), an alarm light (if no DMK – Device Master Key- is present and no Manager is registered), and a fault light.

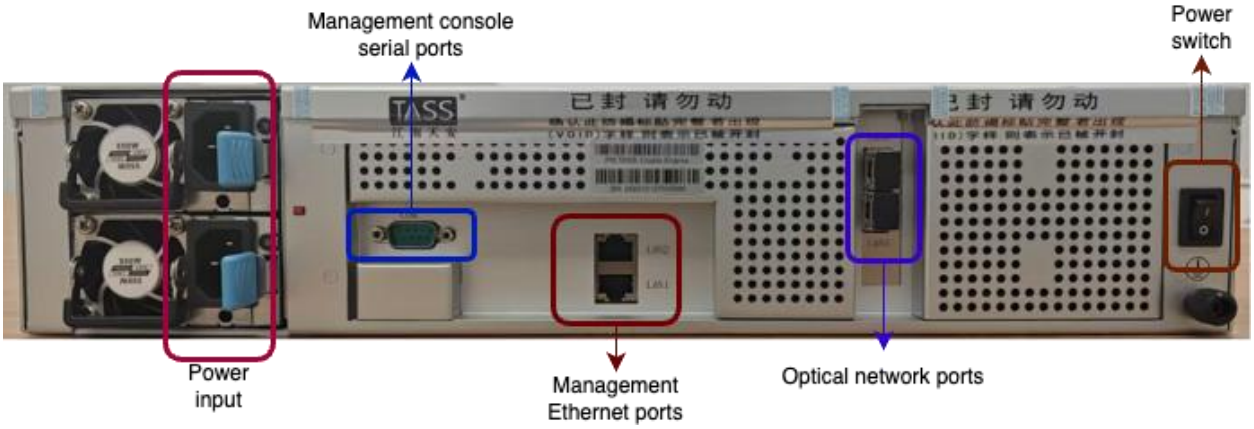


Figure 6: Physical ports (back panel)

If one of the power supplies fails or is not connected, the module emits an alarm, also indicated with the alarm light. Application servers connect to the module via the two service optical network ports. These two optical ports operate in IEEE 802.3ad Link Aggregation mode.
A management console is connected to the management serial port for command-line input and output of management services (e.g., network configuration, Module initialization). Two RJ-45 Ethernet ports and two optical ports provide connection to management and user services.
The module does not implement a control output interface.

3.2 Trusted Channel Specification

The module does not support trusted channel. All the SSPs are transmitted over TLS channel with authenticated encryption.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Crypto Officer Authentication	COs with the Manager, Operator and Auditor roles	RSA signature verification	10^-33	6*10^-33
User Authentication	External applications with the User role	RSA signature verification	10^-33	100*10^-33

Table 11: Authentication Methods

The module employs identity-based authentication to identify and authenticate crypto-officers and users of the module.
The operator belonging to Crypto Officer (CO) type is identified by a username and authenticated using a challenge-response mechanism based on RSA-2048 signature verification. The corresponding public key is stored in plaintext within the module.
The operator belonging to User type (external application servers) is identified by an RSA-2048 key pair and digital certificate used for TLS authentication. The public key is stored in plaintext within the module, while the private key is retained by the User. Additionally, if the IP whitelist is configured, the module enforces access control using an IP address whitelist, which is stored in plaintext.
The module does not maintain authenticated sessions upon power cycling. Power-cycling the system requires the authentication credentials to be re-entered. No service has access to this authentication data except Authentication and Module Initialization services.

4.1.1 Manager, Operator, Auditor

The operator type CO includes Manager, Operator and Auditor roles and are authenticated in the following manner:

- The CO connects to the module via the management web interface (through the configured management ports) using a management computer and browser, and establishing a TLS (via HTTPS) connection between the browser and the module's web interface. The TLS connection uses server authentication only (using the module's certificate).
- Once the TLS connection is established, the CO sends its username to the module, and the module verifies the username against the database stored within the module.
- If username verification is successful, module sends a challenge to the CO in the form of 256 bits random value R.
- Upon receiving the challenge, the CO generates a signature of R and the signature is sent to the module.
- The module verifies the received signature. If the signature verifies successfully, the CO is authenticated.

The 2048-bit RSA key used by the CO for challenge response, is generated during initialization of the CO as explained in section 11.1.

4.1.2 User Application

The operator type User includes the User Application role and are authenticated in the following manner:

- The CO (Operator) imports the User Application's digital certificate. The User Application subsequently connects to the module via the service optical or Ethernet network ports.
- The module verifies the peer's IP address against the configured whitelist (optional) to determine whether the peer is authorized to connect to the module. If the IP address is not authorized, the module rejects the connection.
- If the IP address is authorized, the module establishes a mutually authenticated TLS channel using the User Application's digital certificate. Successful establishment of the TLS session authenticates the User; otherwise, authentication fails.

User Application credentials are managed (added or deleted) by Operator or Manager role. The certificate containing RSA public key is stored in the module's hard disk in plaintext format. The User Application entity remains authenticated to the module only for the duration of the TLS session, or until the module is powered off.

4.1.3 Authentication Strength

For the CO operator, the user authentication mechanism uses a 2048-bit RSA key for signature verification. According to SP800-57, such a key length in the aforementioned mechanism provides a security strength of 112 bits. Therefore, the probability of a successful authentication by guessing the private key, is $2^{-112} \approx 10^{-33}$. The module permits a maximum of six consecutive failed authentication attempts. Upon exceeding this limit, the associated username is locked for one minute.
For the User operator, the user authentication mechanism uses at least the 2048-bit RSA key for mutual TLS channel establishment. According to SP800-57, such a key length in the aforementioned mechanism provides a security strength of 112 bits. Therefore, the probability of a successful authentication by guessing the private key is $2^{-112} \approx 10^{-33}$. The module permits a maximum of 100 consecutive failed authentication attempts. Upon exceeding this limit, the associated IP address is locked for one minute.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Manager	Identity	CO	Crypto Officer Authentication
Operator	Identity	CO	Crypto Officer Authentication
Auditor	Identity	CO	Crypto Officer Authentication
User Application	Identity	User	User Authentication

Table 12: Roles

The module supports two types of operators, Crypto Officer and User.

- The Crypto Officer includes Manager role (3 to 9), Operator role (1 to 6), and Auditor role (1 to 3). These roles are assigned to operators of the module who perform management operations. When the module is initialized for the first time, as there are no registered operators provided by default, the Manager role is assigned to the operator who accesses the module via the management interface to initialize it.
- The User operator represents application server roles (external entities) that connect to the module to invoke cryptographic services. The module supports up to 2048 user applications.

The module allows concurrent Crypto Officers (Manager, Operator, Auditor) to log in.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show module name and version	Show module name and version on LCD screen	Last byte of the return value is '1' for Approved Mode	N/A	Name and version information	None	Unauthenticated
Display IP address	Show IP address on LCD screen	Last byte of the return	N/A	IP address	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		value is '1' for Approved Mode				
Show status	Show module status information on LCD screen	Last byte of the return value is '1' for Approved Mode	N/A	Module status, including the current operation function and working state.	None	Unauthenticated
Zeroization and Factory rest	Factory reset of the module that also serve as end of life service for the module. All SSPs will be zeroized.	None	N/A	Pass/fail result	None	Unauthenticated - DMK: Z - KBK: Z - CO authentication public key: Z - App symmetric key: Z - App asymmetric private key: Z - Entropy input: Z - DRGB seed: Z - DRBG internal state (V value, Key): Z - Intermediate key generation value: Z - LMK: Z - ML-DSA private key: Z - ML-DSA public key: Z - ML-KEM decapsulation key: Z - ML-KEM encapsulation key: Z - SLH-DSA private key: Z - SLH-DSA public key: Z - LMS private key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- LMS public key: Z - User Application Digital Certificate: Z - ML-DSA seed: Z - ML-KEM seed: Z - ML-KEM shared secret key: Z - SLH-DSA seed: Z - LMS seed: Z - TLS ECDH private key: Z - TLS ECDH public key: Z - TLS RSA private key: Z - TLS RSA public key: Z - TLS premaster secret: Z - TLS master secret: Z - TLS encryption key: Z
Module initialization	Reinitializing the module after Factory reset	None	N/A	Pass/fail result	Random Number Generation Signature Generation Signature Verification TLS Handshake KAS	Manager - DMK: G,R,W,E - LMK: G - CO authentication public key: E - KBK: G,R,W,E - App symmetric key: G,W - App asymmetric private key: G,W - App asymmetric public key: G,W - ML-DSA private key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,W - ML-DSA public key: G,W - ML-KEM decapsulation key: G,W - ML-KEM encapsulation key: G,W - SLH-DSA private key: G,W - SLH-DSA public key: G,W - LMS private key: G,W - LMS public key: G,W Operator - CO authentication public key: E Auditor - CO authentication public key: E
Random number generation	Generate random bytes	Last byte of the return value is '1' for Approved Mode	Output length	Random bytes	Random Number Generation	Manager - Entropy input: G,E - DRGB seed: G,E - DRBG internal state (V value, Key): G,W,E User Application - Entropy input: G,E - DRGB seed: G,E - DRBG internal state (V value, Key): G,W,E
Symmetric key generation	Generate symmetric key using the DRBG via web management portal or via	Last byte of the return value is '1' for	N/A	AES key ID, HMAC key ID	Symmetric key generation	Manager - App symmetric key: G User Application - App

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the API call. The keys are stored within the module with the associated information identifying the operator.	Approved Mode				symmetric key: G
Asymmetric key pair generation	Generate an asymmetric key pair with the associated information identifying the operator.	Last byte of the return value is '1' for Approved Mode	Group; Curve; Modules bits	Key pair ID	Key Pair Generation Key Pair Verification	Manager - App asymmetric private key: G - App asymmetric public key: G - Intermediate key generation value: G,E,Z User Application - App asymmetric private key: G - App asymmetric public key: G - Intermediate key generation value: G,E,Z
PQC key pair generation	Generate an PQC key pair with the associated information identifying the operator.	Last byte of the return value is '1' for Approved Mode	Algorithm; Parameters	Key pair ID	ML-DSA key pair generation ML-KEM key pair generation SLH-DSA key pair generation LMS key pair generation	Manager - Intermediate key generation value: G,E,Z - ML-DSA private key: G - ML-DSA public key: G - ML-KEM decapsulation key: G - ML-KEM encapsulation key: G - SLH-DSA private key: G - SLH-DSA public key: G - LMS private key: G - LMS public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key: G - ML-DSA seed: G - ML-KEM seed: G - SLH-DSA seed: G - LMS seed: G User Application - Intermediate key generation value: G,E,Z - ML-DSA private key: G - ML-DSA public key: G - ML-KEM decapsulation key: G - ML-KEM encapsulation key: G - SLH-DSA private key: G - SLH-DSA public key: G - LMS private key: G - LMS public key: G - ML-DSA seed: G - ML-KEM seed: G - SLH-DSA seed: G - LMS seed: G
Symmetric encryption	Encrypt a plaintext	Last byte of the return value is '1' for Approved Mode	Plaintext, AES key ID, IV	Ciphertext, Tag	Symmetric Encryption with AES	User Application - App symmetric key: W,E
Symmetric decryption	Decryption a ciphertext	Last byte of the return value is '1' for	Ciphertext, AES key ID, IV	Plaintext	Symmetric Decryption with AES	User Application - App symmetric key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		Approved Mode				
Authenticated Symmetric Encryption	Encrypt a plaintext with autentication	Last byte of the return value is '1' for Approved Mode	Plaintext, AES key ID, IV, AAD	Ciphertext, Tag	Authenticated Symmetric Encryption	User Application - App symmetric key: W,E
Authenticated Symmetric Decryption	Decryption a ciphertext with authentication	Last byte of the return value is '1' for Approved Mode	Ciphertext, AES key ID, IV, AAD, Tag	Plaintext	Authenticated Symmetric Decryption	User Application - App symmetric key: W,E
Key wrapping	Perform AES based key wrapping	Last byte of the return value is '1' for Approved Mode	Key ID to be wrapped, AES key ID	Wrapped key	KTS-Wrap with AES-KW and AES-KWP	Manager - App symmetric key: W,E User Application - App symmetric key: W,E
Key unwrapping	Perform AES based key unwrapping	Last byte of the return value is '1' for Approved Mode	Wrapped key, AES key ID	Unwrapped key ID	KTS-Unwrap with AES-KW and AES-KWP	Manager - App symmetric key: W,E User Application - App symmetric key: W,E
Decapsulation	SP800-56B RSA-based decapsulation using the private key of the operator stored in the module.	Last byte of the return value is '1' for Approved Mode	Encapsulated key, RSA private key ID	Decapsulated key ID	Asymmetric Decryption with RSA	User Application - App asymmetric private key: E
Signature generation	Generate a digital signature on a message	Last byte of the return value is '1' for Approved Mode	Message, message digest algorithm, private key ID	Signature	Signature Generation	User Application - App asymmetric private key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Signature generation primitive	Generate a digital signature on a hashed message	Last byte of the return value is '1' for Approved Mode	Message digest, private key ID	Signature	Signature Generation Primitive	User Application - App asymmetric private key: W,E
Signature verification	Verify a digital signature	Last byte of the return value is '1' for Approved Mode	Message, signature, public key ID	Pass/fail result	Signature Verification	User Application - App asymmetric public key: W,E
PQC Signature generation	Generate a digital signature on a message with PQC algorithms	Last byte of the return value is '1' for Approved Mode	Message, context string, ML-DSA private key ID, SLH-DSA private key ID, LMS private key ID	Signature	Signature Generation ML-DSA External Deterministic Signature Generation ML-DSA External Hedged Signature Generation SLH-DSA External Pure Signature Generation SLH-DSA External PreHash Signature Generation LMS	User Application - ML-DSA private key: W,E - SLH-DSA private key: W,E - LMS private key: W,E
PQC Signature verification	Verify a digital signature with PQC algorithms	Last byte of the return value is '1' for Approved Mode	Message, signature, context string, ML-DSA public key ID, SLH-DSA public key ID, LMS public key ID	Pass/fail result	Signature Verification ML-DSA External Signature Verification SLH-DSA External Pure Signature Verification SLH-DSA External PreHash	User Application - ML-DSA public key: W,E - SLH-DSA public key: W,E - LMS public key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Signature Verification LMS	
KAS with ANS X9.63 KDF	Compute a shared secret followed by X9.63 KDF	Last byte of the return value is '1' for Approved Mode	Public key, AES key ID	Pass/fail result	Key agreement with ECDH and ANS X9.63 KDF	User Application - App asymmetric public key: W,E - Shared secret: G,Z - ANS X9.63 derived Key: G,R
ML-KEM encapsulation	Encapsulation with ML-KEM	Last byte of the return value is '1' for Approved Mode	ML-KEM encapsulation key ID	ML-KEM shared secret key, ciphertext	Key Encapsulation with ML-KEM	User Application - ML-KEM encapsulation key: W,E - ML-KEM shared secret key: G,R
ML-KEM decapsulation	Decapsulation with ML-KEM	Last byte of the return value is '1' for Approved Mode	ML-KEM decapsulation key ID, ciphertext	ML-KEM shared secret key	Key Decapsulation with ML-KEM	User Application - ML-KEM decapsulation key: E - ML-KEM shared secret key: G,R
Message digest	Message digest	Last byte of the return value is '1' for Approved Mode	Message	Message digest	Message Digest	User Application
Message authentication code	Compute a MAC tag	Last byte of the return value is '1' for Approved Mode	Message, AES Key ID or HMAC key ID	Mac tag	Message Authentication Code	User Application - App symmetric key: W,E
Key derivation	Derive a key	Last byte of the return value is '1' for	User input data	Derived key ID	Key Derivation with HKDF Password-based Key Derivation Key	User Application - App symmetric key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		Approved Mode			Derivation with KBKDF	
Key management	Support the generation of AES keys for finalcial use (such as KEK, ZPK, PVK, and other keys in different financial schemes). (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	Financial schemes	LMK wapped AES key as key block	Random Number Generation Symmetric Encryption with AES Message Authentication Code	User Application - App symmetric key: G,E
PIN security administration with key ID	Card PIN related operations. (such as PIN encryption; Digital / Character PIN conversion encryption; PINOFFSET; PVV; Translate a PIN from BDK to ZPK/ BDK Encrypt (DUKPT)). (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	AES key ID, PIN, PAN	PINBLOCK / PINOFFSET / PVV	Symmetric Encryption with AES Message Authentication Code	User Application - App symmetric key: E
PIN security administration with wrapped key	Card PIN related operations. (such as PIN encryption; Digital / Character PIN conversion encryption; PINOFFSET; PVV; Translate a PIN from BDK to ZPK/ BDK Encrypt (DUKPT)). (Service	Last byte of the return value is '1' for Approved Mode	LMK wapped AES key as key block, PIN, PAN	PINBLOCK / PINOFFSET / PVV	Symmetric Decryption with AES Symmetric Encryption with AES Message Authentication Code	User Application - App symmetric key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	available in Financial mode only)					
Verification of weak PIN	Verifying if the provided PIN is weak based on the input rules. (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	AES key ID or LMK wapped AES key as key block, PIN, PAN, set of weak PINs	Pass/fail result	Symmetric Decryption with AES	User Application - App symmetric key: E
EMV/VISA regulates the trading function with key ID	Financial related operations (such as ARQC/TC/AAC; ARPC; Script safety message/PIN modification). (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	AES key ID, trading data	Ciphertext data, MAC value, ARPC data	Key Derivation with KBKDF Symmetric Encryption with AES Message Authentication Code	User Application - App symmetric key: G,E
EMV/VISA regulates the trading function with wrapped key	Financial related operations (such as ARQC/TC/AAC; ARPC; Script safety message/PIN modification). (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	LMK wapped AES key as key block, trading data	Ciphertext data, MAC value, ARPC data	Key Derivation with KBKDF Symmetric Decryption with AES Symmetric Encryption with AES Message Authentication Code	User Application - App symmetric key: G,E
GP specification for data operation with key ID	GP data operation with vendor AES keys (Specially KMC keys). (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	AES key ID, Plaintext data	Ciphertext data, MAC	Key Derivation with KBKDF Symmetric Encryption with AES Message Authentication Code	User Application - App symmetric key: G,E
GP specification for data operation with wrapped key	GP data operation with vendor AES keys (Specially KMC keys).	Last byte of the return value is '1' for	LMK wapped AES key as key block, Plaintext data	Ciphertext data, MAC	Key Derivation with KBKDF Symmetric Decryption with AES	User Application - App symmetric key: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	(Service available in Financial mode only)	Approved Mode			Symmetric Encryption with AES Message Authentication Code	
OTP dynamic password	Generate or verify OTP. (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	HMAC key, Token seed	OTP code	Message Authentication Code Message Digest	User Application - App symmetric key: E
Deriving keys or generating session keys (DUKPT) with key ID	Derive DUKPT keys. (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	AES key ID, financial schemes, derived factors	AES key ID	Key Derivation with KBKDF	User Application - App symmetric key: G,E
Deriving keys or generating session keys (DUKPT) with wrapped key	Derive DUKPT keys. (Service available in Financial mode only)	Last byte of the return value is '1' for Approved Mode	LMK wapped AES key as key block, financial schemes, derived factors	AES key ID	Symmetric Decryption with AES Key Derivation with KBKDF	User Application - App symmetric key: G,E
Configure IP addresses white-listing	Configure module's IP addresses and add white-list of application servers	Last byte of the return value is '1' for Approved Mode	IP address	Module status	None	Operator - CO authentication public key: E
Review audit log	Review audit log	Last byte of the return value is '1' for Approved Mode	N/A	Audit logs	None	Manager - CO authentication public key: E Operator - CO authentication public key: E Auditor - CO authentication public key: E
Keystore backup	Backup the keystore, all keys stored in	Last byte of the	N/A	Wrapped keys	KTS-Wrap with AES-	Manager - KBK: E - CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the module are wrapped using KBK.	return value is '1' for Approved Mode			KW and AES-KWP	authentication public key: R - App symmetric key: R - App asymmetric private key: R - App asymmetric public key: R - ML-DSA private key: R - ML-DSA public key: R - ML-KEM decapsulation key: R - ML-KEM encapsulation key: R - SLH-DSA private key: R - SLH-DSA public key: R - LMS public key: R - User Application Digital Certificate: R
Keystore restore	Restore the keystore, all keys unwrapped with KBK are stored in the module	Last byte of the return value is '1' for Approved Mode	Wrapped keys	Pass/fail result	KTS-Unwrap with AES-KW and AES-KWP	Manager - KBK: E - CO authentication public key: W - App symmetric key: W - App asymmetric private key: W - App asymmetric public key: W - ML-DSA private key: W - ML-DSA public key: W - ML-KEM encapsulation key: W - ML-KEM decapsulation

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key: W - SLH-DSA private key: W - SLH-DSA public key: W - LMS public key: W - User Application Digital Certificate: W
DMK export	Export DMK XORed with randomly generated value	Last byte of the return value is '1' for Approved Mode	N/A	DMK Components	Random Number Generation	Manager - DMK Components: E
KBK export	Export KBK as key components	Last byte of the return value is '1' for Approved Mode	N/A	KBK Components	None	Manager - KBK Components: E
DMK reconstruct	Reconstruct DMK	Last byte of the return value is '1' for Approved Mode	DMK Components	Pass/fail result	None	Manager - DMK: W
KBK reconstruct	Reconstruct KBK	Last byte of the return value is '1' for Approved Mode	KBK Components	Pass/fail result	None	Manager - KBK: W
Add CO	Add Crypto Officers	Last byte of the return value is '1' for Approved Mode	CO authentication public key	Pass/fail result	Random Number Generation Signature Verification TLS Handshake KAS	Manager - CO authentication public key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Modify USB token PIN	Modify the PIN of CO's USB token	Last byte of the return value is '1' for Approved Mode	Original PIN	Pass/fail result	Random Number Generation Signature Verification TLS Handshake KAS	Manager - CO authentication public key: E Operator - CO authentication public key: E Auditor - CO authentication public key: E
Establish TLS session	Establish TLS session between the module and client	Last byte of the return value is '1' for Approved Mode	Address / algorithms	Confirmation of digital signature verification of TLS session, Confirmation of establishment of TLS session	TLS Handshake KAS	Manager - Intermediate key generation value: E - TLS ECDH private key: G,E,Z - TLS ECDH public key: G,E,Z - TLS RSA private key: E - TLS RSA public key: E - TLS premaster secret: G,E,Z - TLS master secret: G,E - TLS encryption key: G,E Operator - Intermediate key generation value: E - TLS ECDH private key: G,E,Z - TLS ECDH public key: G,E,Z - TLS RSA private key: E - TLS RSA public key: E - TLS premaster secret: G,E,Z - TLS master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						secret: G,E - TLS encryption key: G,E Auditor - Intermediate key generation value: E - TLS ECDH private key: G,E,Z - TLS ECDH public key: G,E,Z - TLS RSA private key: E - TLS RSA public key: E - TLS premaster secret: G,E,Z - TLS master secret: G,E - TLS encryption key: G,E User Application - Intermediate key generation value: E - TLS ECDH private key: G,E,Z - TLS ECDH public key: G,E,Z - TLS RSA private key: E - TLS RSA public key: E - TLS premaster secret: G,E,Z - TLS master secret: G,E - TLS encryption key: G,E
Maintain TLS session	Maintain TLS session between the	None	TLS Derived Session key	TLS session information	Authenticated Symmetric Encryption	Manager - Intermediate key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	module and client				Authenticated Symmetric Decryption KTS-Wrap with AES-CCM and AES-GCM KTS-Unwrap with AES-CCM and AES-GCM	generation value: E - TLS master secret: E - TLS encryption key: E Operator - Intermediate key generation value: E - TLS master secret: E - TLS encryption key: E Auditor - Intermediate key generation value: E - TLS master secret: E - TLS encryption key: E User Application - Intermediate key generation value: E - TLS master secret: E - TLS encryption key: E
Close TLS session	Close TLS session between the module and client	None	N/A	Confirmation of TLS session closure	None	Manager - Intermediate key generation value: Z - TLS master secret: Z - TLS encryption key: Z Operator - Intermediate key generation value: Z - TLS master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						secret: Z - TLS encryption key: Z Auditor - Intermediate key generation value: Z - TLS master secret: Z - TLS encryption key: Z User Application - Intermediate key generation value: Z - TLS master secret: Z - TLS encryption key: Z
Self-test	Perform pre-operational and conditional self-tests	Success: LCD screen shows "User Status"	N/A	Pass/fail result	None	Operator
Add User Application	Import the User Application's certificates	Last byte of the return value is '1' for Approved Mode	User Application's digital certificate	Pass/fail result	Signature Verification TLS Handshake KAS	Operator - User Application Digital Certificate: W,E

Table 13: Approved Services

The module provides services to operators that assume the available role. All services are described in detail in the User's Guidance document. The convention below applies when specifying the access permissions (types) that the service has for each SSP.

- Generate (G): The module generates or derives the SSP.
- Read (R): The SSP is read from the module (e.g. the SSP is output).
- Write (W): The SSP is updated, imported, or written to the module.
- Execute (E): The module uses the SSP in performing a cryptographic operation.
- Zeroize (Z): The module zeroizes the SSP.
- N/A: The module does not access any SSP or key during its operation.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Symmetric key generation	Generate a symmetric key	SM4 ZUC TDES	Manager, User Application
Symmetric encryption	Encrypt a plaintext	SM4 ZUC TDES	User Application
Symmetric decryption	Decrypt a ciphertext	SM4 ZUC TDES	User Application
Asymmetric key generation	Generate an asymmetric key	SM2 SM9 RSA (1024bits) ECC (K-283, K-409, K-571, B-283, B-409, B-571, NISTP192v1, NISTP192v2, NISTP192v3, BRAINPOOLP192R1, BRAINPOOLP224R1, BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1, BRAINPOOLP192T1, BRAINPOOLP224T1, BRAINPOOLP256T1, BRAINPOOLP320T1, BRAINPOOLP384T1, BRAINPOOLP512T1, SECP192K1, SECP256K1, SECP224R1, SECT233K1, SECT233R1, frp256v1) X25519/X448 XMSS	Manager, User Application
Asymmetric encryption	Encrypt a plaintext	SM2 SM9 RSA (1024bits)	User Application
Asymmetric decryption	Decrypt a ciphertext	SM2 SM9 RSA (1024bits)	User Application
Signature generation	Sign a message	SM2 SM9 RSA (1024bits) ECC (K-283, K-409, K-571, B-283, B-409, B-571, NISTP192v1, NISTP192v2, NISTP192v3, BRAINPOOLP192R1, BRAINPOOLP224R1, BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1, BRAINPOOLP192T1, BRAINPOOLP224T1, BRAINPOOLP256T1, BRAINPOOLP320T1, BRAINPOOLP384T1,	User Application

Name	Description	Algorithms	Role
		BRAINPOOLP512T1, SECP192K1, SECP256K1, SECP224R1, SECT233K1, SECT233R1, frp256v1) X25519/X448 XMSS	
Signature verification	Verify a message	SM2 SM9 RSA (1024bits) ECC (K-283, K-409, K-571, B-283, B-409, B-571, NISTP192v1, NISTP192v2, NISTP192v3, BRAINPOOLP192R1, BRAINPOOLP224R1, BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1, BRAINPOOLP192T1, BRAINPOOLP224T1, BRAINPOOLP256T1, BRAINPOOLP320T1, BRAINPOOLP384T1, BRAINPOOLP512T1, SECP192K1, SECP256K1, SECP224R1, SECT233K1, SECT233R1, frp256v1) X25519/X448 XMSS	User Application
Key agreement	Generate a shared secret	SM2 SM9 ECC (K-283, K-409, K-571, B-283, B-409, B-571, NISTP192v1, NISTP192v2, NISTP192v3, BRAINPOOLP192R1, BRAINPOOLP224R1, BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1, BRAINPOOLP192T1, BRAINPOOLP224T1, BRAINPOOLP256T1, BRAINPOOLP320T1, BRAINPOOLP384T1, BRAINPOOLP512T1, SECP192K1, SECP256K1, SECP224R1, SECT233K1, SECT233R1, frp256v1) X25519/X448	User Application
Message digest	Generate a message digest	SM3 SHA-1, SHA-224, SHA3-224, MD5	User Application
Message authentication code	Generate a message authentication code	HMAC (SHA-1, SHA-224, SHA3-224, MD5, SM3) GMAC	User Application
Blockchain protocol algorithm	Generate root key; The root key derives the subkey; Perform correlation operations	ECC (K-283, K-409, K-571, B-283, B-409, B-571, NISTP192v1, NISTP192v2, NISTP192v3, BRAINPOOLP192R1, BRAINPOOLP224R1,	User Application

Name	Description	Algorithms	Role
		BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1, BRAINPOOLP192T1, BRAINPOOLP224T1, BRAINPOOLP256T1, BRAINPOOLP320T1, BRAINPOOLP384T1, BRAINPOOLP512T1, SECP192K1, SECP256K1, SECP224R1, SECT233K1, SECT233R1, frp256v1)	
Key derivation	Derive a key	HKDF (SHA-1, SHA-224, SHA3-224, MD5, SM3)	User Application
Key encapsulation	Key encapsulation	SM9	User Application
Key decapsulation	Key decapsulation	SM9	User Application
Key variant	Generate symmetric or asymmetric key as variant. (Service available in Financial mode only)	SM2 SM4 SM9 ZUC TDES RSA (1024bits) ECC (K-283, K-409, K-571, B-283, B-409, B-571, NISTP192v1, NISTP192v2, NISTP192v3, BRAINPOOLP192R1, BRAINPOOLP224R1, BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1, BRAINPOOLP192T1, BRAINPOOLP224T1, BRAINPOOLP256T1, BRAINPOOLP320T1, BRAINPOOLP384T1, BRAINPOOLP512T1, SECP192K1, SECP256K1, SECP224R1, SECT233K1, SECT233R1, frp256v1) X25519/X448 XMSS	User Application
Key block	Generate TR31 key block in non-SP800-38F format. (Service available in Financial mode only)	SM4 ZUC TDES AES with non-SP800-38F use	User Application
Card Verification	Generate and verify Card Verification Codes for different finalcial schemes (such as CVV, iCVV, dCVV). (Service available in Financial mode only)	TDES	User Application

Name	Description	Algorithms	Role
EMV/VISA regulates the trading function	Financial related operations in non-SP800-38F format (such as ARQC/TC/AAC; ARPC; Script safety message/PIN modification). (Service available in Financial mode only)	DES TDES	User Application
PBOC regulates the trading function	Financial related operations in non-SP800-38F format (such as ARQC/TC/AAC; ARPC; Script safety message/PIN modification). (Service available in Financial mode only)	TDES AES with non-SP800-38F use SM4	User Application
GP specification for data operation	Data operation with vendor AES or TDES keys in non-SP800-38F format. (Service available in Financial mode only)	TDES AES with non-SP800-38F use	User Application
OTP dynamic password	Generate or verify OTP. (Service available in Financial mode only)	SM3 SM4 SHA-1, SHA-224, SHA3-224, MD5	User Application

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

5 5 Software/Firmware Security

5.1 Integrity Techniques

The module's firmware component consists of one OS image, two service images and a configuration file package. The module's integrity test routine verifies the OS image by validating an RSA-4096 digital signature using SHA-512. The OS image includes all the programs, libraries, web pages and the core components of the operating system. If the OS integrity test succeeds, the OS loads the service images and verifies their integrity with ECDSA P-521 with SHA-512 digital signature. Lastly the configuration file is integrity verified using HMAC-SHA-256.
If all integrity tests succeed, the service images become fully operational and proceed to perform the cryptographic algorithm self-tests (CASTs) for remaining algorithms. The CAST for RSA, ECDSA, HMAC and SHA algorithms is performed before the integrity test.
The public keys used to verify the digital signatures of OS and service images, as well as the HMAC key and the pre-computed HMAC value are stored within the module. The private keys used to sign the OS and the service images always reside outside of the module.

5.2 Initiate on Demand

Integrity tests are performed as part of the pre-operational self-tests, which are executed when the module is initialized. The integrity test may be invoked on-demand by manually performing a power cycle of the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

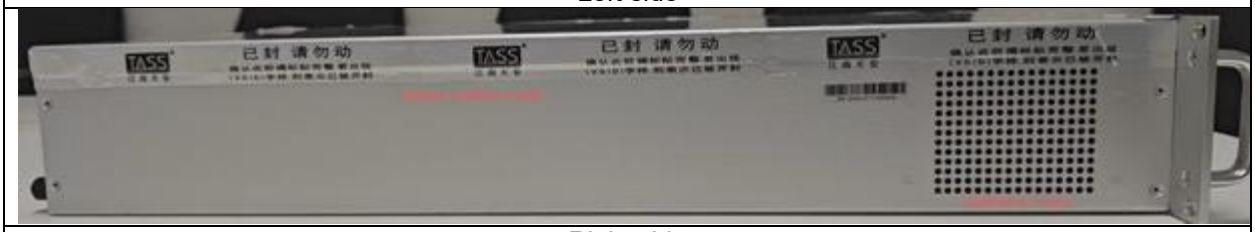
Type of Operational Environment: Non-Modifiable
The module is a hardware validated at a Security Level 3 in Physical Security.
Once the module is operational, it does not allow the loading of any additional firmware.
There are no further requirements for this security area.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper evident seals	At least once a month by CO role.	Unique tamper seals are produced and factory installed by the vendor, including: (a). 11 Labels are surrounding the whole chassis to cover all the gaps; The label is printed with the information: Sealed, please do not touch. Make sure the tamper-resistant label is intact. If the word "VOID" appears, it means that the label has been tampered; (b). 3 labels are on the left side of the chassis, covering the joint gap between the upper cover and the chassis; (c). 3 labels are on the right side of the chassis, covering the joint gap between the upper cover and the chassis; (d). 2 labels are on the rear panel of the chassis, covering the joint with the upper cover; (e). 3 labels are on the top upper cover of the chassis, covering the upper cover and the top panel. CO role shall verify that the tamper seals remain intact and remain in the original location as shown in Figure 7. In case evidence of tampering is found, the CO shall immediately cease operation of the module and shall perform the Module initialization service. Next, the CO shall contact the manufacturer to return the module for repair and maintenance. At the factory, new tamper-evidence labels shall be applied as specified. Upon receiving the restored module, the CO shall follow the guidance as applicable to the new module.
Tamper switches	Immediately after the tampering event is detected. Otherwise at least once a month by CO role.	The module contains a removable top cover, which is protected by two tamper switches. Removing the top cover causes the module to zeroize the DMK stored in the Protection Card and powers-off the module.
production grade material and Opacity	At least once a month by CO role.	The module is enclosed entirely within an opaque secure steel and aluminium chassis. The ventilation holes are filled with mesh to protect from direct probing.

Table 15: Mechanisms and Actions Required

Left side

Right side



Rear



Top



Figure 7: Tamper evidence seals

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	0 °C	EFP	Shut down
HighTemperature	45 °C	EFP	Shut down
LowVoltage	190 V	EFP	Shut down
HighVoltage	250 V	EFP	Shut down

Table 16: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	Operational: 0 °C, Storage: 0 °C, Distribution: 0 °C
HighTemperature	Operational: 45 °C, Storage: 45 °C, Distribution: 45 °C

Table 17: Hardness Testing Temperatures

8 Non-Invasive Security

This module does not implement any non-invasive security mechanism, and therefore this section is not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Protection card	Protection card is used to store the DMK	Static
Internal hard drive	Internal hard drive of the module is used to store all SSPs in authenticated encryption format by DMK.	Static
RAM	Temporary storage for SSPs used by the module as part of service execution. SSPs are stored until they are zeroized by the operator (using a zeroization call or removing power from the module) or zeroized automatically	Dynamic

Table 18: Storage Areas

The module protects SSPs using key wrapping algorithms compliant with SP800-38F by the DMK. The computed integrity value is stored with the encrypted SSP.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Protection card import (DMK)	Crypto Officer Management Console	Protection card	Encrypted	Manual	Electronic	KTS-Unwrap with AES-KW and AES-KWP
Protection card export (DMK)	Protection card	Crypto Officer Management Console	Encrypted	Manual	Electronic	KTS-Wrap with AES-KW and AES-KWP
Hard drive encrypted import (SSPs other than DMK)	Application	Internal hard drive	Encrypted	Automated	Electronic	KTS-Unwrap with AES-KW and AES-KWP
Hard drive encrypted export (SSPs other than DMK)	Internal hard drive	Application	Encrypted	Automated	Electronic	KTS-Wrap with AES-KW and AES-KWP
HSM hard drive import (KBK)	Crypto Officer Management Console	Internal hard drive	Encrypted	Manual	Electronic	KTS-Unwrap with AES-KW and AES-KWP
HSM hard drive export (KBK)	Internal hard drive	Crypto Officer Management Console	Encrypted	Manual	Electronic	KTS-Wrap with AES-KW and AES-KWP
Input unwrapped	Application	RAM	Encrypted	Automated	Electronic	KTS-Unwrap with

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
by AES (SSPs other than DMK)						AES-CCM and AES-GCM
Output wrapped by AES (SSPs other than DMK)	RAM	Application	Encrypted	Automated	Electronic	KTS-Wrap with AES-CCM and AES-GCM

Table 19: SSP Input-Output Methods

Note that all keys or key components (in case of DMK and KBK) entered or output to or from the module are encrypted using either AES-GCM or AES-CCM over a TLS channel for the Crypto Officers or User Application.

Additionally, cryptographic services requested by User role may involve input of keys in the request message or output of keys in the response message. In this case, the input or output keys are separately wrapped using SP800-38F AES KW or KWP as the key transport mechanism even though the command and response is sent over TLS channel.

The module does not support intermediate key generation and does not accept entry or output of keys in plaintext format from outside its cryptographic boundary.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Automatic	Automatically zeroized by the module when no longer needed	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable.	N/A
Module initialization (Zeroization)	Automatically zeroized by the module when performing Module initialization service	Module is switched off immediately and overwrites DMK with zeroes in Protection Card	By calling Module initialization service
Tamper response switches	Automatically zeroized by the module when performing Module initialization service	Module is switched off immediately and overwrites DMK with zeroes in Protection Card	N/A
Clear button in the front panel	Automatically zeroized by the module when performing Module initialization service	Module is switched off immediately and overwrites DMK with zeroes in Protection Card	By pressing the Clear button for 10 seconds

Table 20: SSP Zeroization Methods

While the module is executing the zeroization, data output (via the data output interface) is inhibited until the zeroization is successfully completed.
The fault LED of the front panel lights up to indicate that the zeroization is completed.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DMK	Derives LMK to protect the secure storage of other CSPs	Length: 256 - 256 bits	Symmetric - CSP	Random Number Generation		Key Derivation with KBKDF
DMK Components	Used for reconstructing DMK via XOR method	Length: 256 - 256 bits	Symmetric - CSP			
LMK	Protect the secure storage of other CSPs	Length: 256 - 256 bits	Symmetric - CSP	Key Derivation with KBKDF		
KBK	Used for encrypting and protecting internal CSP during device backup	Length: 256 - 256 bits	Symmetric - CSP	Random Number Generation		KTS-Wrap with AES-KW and AES-KWP KTS-Unwrap with AES-KW and AES-KWP
KBK Components	Used for reconstructing KBK via Shamir method	Length: 256 - 256 bits	Symmetric - CSP			
CO authentication public key	Used for CO login authentication. Only the public key is stored in the module, and the private key always resides in the USB token.	Modulus: 2048 - 112 bits	Asymmetric-PSP - PSP			Signature Verification
App symmetric key	Encrypt / decrypt user data and perform MAC calculations	Length: 128, 192, 256 - 128, 192, 256 bits. XTS-AES-128 has 128-bit security strength even if	Symmetric - CSP	Random Number Generation		Symmetric Encryption with AES Symmetric Decryption with AES KTS-Wrap with AES-KW and AES-KWP KTS-Unwrap with AES-KW and AES-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		the 2 keys add up to 256 bits of random while XTS-AES-256 has 256-bit security strength even if the 2 keys add up to 512 bits of random				KWP Message Authentication Code Authenticated Symmetric Encryption Authenticated Symmetric Decryption Symmetric key generation
App asymmetric private key	Encrypt, decrypt, and sign user data	RSA modulus: 2048, 3072, 4096; ECDSA: curves P-256, P-384, P-521; EdDSA curves: Ed448, Ed25519 - RSA: 112, 128, 149 bits; ECDSA: 128, 192, 256 bits; EdDSA: 128, 224 bits	Asymmetric-CSP - CSP	Key Pair Generation		Signature Generation Key agreement with ECDH and ANS X9.63 KDF Asymmetric Decryption with RSA
App asymmetric public key	Encrypt, decrypt, and sign user data	RSA modulus: 2048, 3072, 4096; ECDSA curve: P-256,	Asymmetric-PSP - PSP	Key Pair Generation		Signature Verification Key agreement with ECDH and ANS X9.63 KDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		P-384, P-521; EdDSA curves: Ed448, Ed25519 - RSA: 112, 128, 149 bits; ECDSA: 128, 192, 256 bits; EdDSA: 128, 224 bits				
ML-DSA private key	Private key used for ML-DSA	2,560 bytes, 4,032 bytes, 4,896 bytes - 128, 192, 256 bits	Asymmetric-CSP - CSP	ML-DSA key pair generation		Signature Generation SLH-DSA External Pure Signature Generation SLH-DSA External PreHash
ML-DSA public key	Public key used for ML-DSA	1,312 bytes, 1,952 bytes, 2,592 bytes - 128, 192, 256 bits	Asymmetric-PSP - PSP	ML-DSA key pair generation		Signature Verification ML-DSA External
ML-KEM decapsulation key	Decapsulation key used for ML-KEM	1,632 bytes, 2,400 bytes, 3,168 bytes - 128, 192, 256 bits	Asymmetric-CSP - CSP	ML-KEM key pair generation		Key Decapsulation with ML-KEM
ML-KEM encapsulation key	Encapsulation key used for ML-KEM	800 bytes, 1,184 bytes, 1,568 bytes - 128,	Asymmetric-PSP - PSP	ML-KEM key pair generation		Key Encapsulation with ML-KEM

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		192, 256 bits				
SLH-DSA private key	Private key used for SLH-DSA	64 bytes, 96 bytes, 128 bytes - 128, 192, 256 bits	Asymmetric-CSP - CSP	SLH-DSA key pair generation		Signature Generation SLH-DSA External Pure Signature Generation SLH-DSA External PreHash
SLH-DSA public key	Public key used for SLH-DSA	32 bytes, 48 bytes, 64 bytes - 128, 192, 256 bits	Asymmetric-PSP - PSP	SLH-DSA key pair generation		Signature Verification SLH-DSA External Pure Signature Verification SLH-DSA External PreHash
LMS private key	Private key used for LMS	min of 60 bytes - 256 bits	Asymmetric-CSP - CSP	LMS key pair generation		Signature Generation LMS
LMS public key	Public key used for LMS	56 bytes - 256 bits	Asymmetric-PSP - PSP	LMS key pair generation		Signature Verification LMS
Shared secret	Shared secret	Length: 128, 192, 256 - 128, 192, 256 bits	Symmetric - CSP		Key agreement with ECDH and ANS X9.63 KDF	Key agreement with ECDH and ANS X9.63 KDF
Entropy input	Entropy input string used to seed the DRBG (IG D.L compliant)	384 bits - 384 bits	Entropy Input - CSP			Random Number Generation
DRGB seed	DRBG seed derived from entropy input (IG D.L compliant)	384 bits - 256 bits	Seed - CSP	Random Number Generation		Random Number Generation
DRBG internal state (V value, Key)	Internal state of the CTR_DRBG (IG D.L compliant)	348 bits - 256 bits	Internal state - CSP	Random Number Generation		Random Number Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Intermediate key generation value	Intermediate key pair generation value generated during key generation and key derivation services (SP 800- 133r2 Section 4, 5.1, and 5.2)	112 ~ 256 - 112 ~ 256 bits	Intermediate value - CSP	Key Pair Generation		Key Pair Generation
User Application Digital Certificate	Used for User Application authentication	RSA modulus: 2048, 3072, 4096; ECDSA: curves P-256, P-384, P-521 - RSA: 112, 128, 149 bits; ECDSA: 128, 192, 256 bits	Asymmetric -PSP - PSP			Signature Verification
ML-DSA seed	Seed used in ML-DSA keypair generation	256 bits - 256 bits	N/A - CSP	Random Number Generation		ML-DSA key pair generation
ML-KEM seed	Seed used in ML-KEM keypair generation	512 bits - 256 bits	N/A - CSP	Random Number Generation		ML-KEM key pair generation
ML-KEM shared secret key	Shared secret key established by ML-KEM. Output to the calling application for external usage.	256 bits - 128, 192, 256 bits	Symmetric - CSP	Key Encapsulation with ML-KEM	Key Decapsulation with ML-KEM	
SLH-DSA seed	Seed used in SLH-DSA keypair generation, including	384, 576, 768 bits - 256 bits	N/A - CSP	Random Number Generation		SLH-DSA key pair generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	PK.seed, SK.seed, and SK.prf					
LMS seed	Seed used in LMS keypair generation	256 bits - 256 bits	N/A - CSP	Random Number Generation		LMS key pair generation
TLS ECDH private key	TLS session private key	P-256, P-384, P-521 - 128, 192, 256 bits	Asymmetric -CSP - CSP	Key Pair Generation		TLS Handshake KAS
TLS ECDH public key	TLS session public key	P-256, P-384, P-521 - 128, 192, 256 bits	Asymmetric -PSP - PSP	Key Pair Generation		TLS Handshake KAS
TLS RSA private key	TLS server host private key	RSA 2048, 3072, 4096 - 112, 128, 149 bits	Asymmetric -CSP - CSP	Key Pair Generation		Signature Generation
TLS RSA public key	TLS server host public key	RSA 2048, 3072, 4096 - 112, 128, 149 bits	Asymmetric -PSP - PSP	Key Pair Generation		Signature Verification
TLS premaster secret	TLS premaster secret	384 bits - 128 bits	Symmetric - CSP		TLS Handshake KAS	TLS Handshake KAS
TLS master secret	TLS master secret	384 bits - 128 bits	Symmetric - CSP	TLS Handshake KAS		TLS Handshake KAS
TLS encryption key	TLS session encryption key	128, 192, 256 bits - 128, 192, 256 bits	Symmetric - CSP	TLS Handshake KAS		Authenticated Symmetric Encryption Authenticated Symmetric Decryption KTS-Wrap with AES-CCM and AES-GCM KTS-Unwrap with AES-CCM and AES-GCM

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ANS X9.63 derived Key	Key derived using ANS X9.63 KDF	128, 192, 256 bits - 128, 192, 256 bits	Symmetric - CSP		Key agreement with ECDH and ANS X9.63 KDF	Key agreement with ECDH and ANS X9.63 KDF

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DMK	Protection card import (DMK) Protection card export (DMK)	Protection card:Plaintext		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	
DMK Components	Protection card import (DMK) Protection card export (DMK)			Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:XOR method
LMK		RAM:Plaintext		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Derived From
KBK	HSM hard drive import (KBK) HSM hard drive export (KBK)	RAM:Plaintext		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	
KBK Components	HSM hard drive import			Automatic Module	KBK:Shamir method

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	(KBK) HSM hard drive export (KBK)			initialization (Zeroization) Tamper response switches Clear button in the front panel	
CO authentication public key		Internal hard drive:Plaintext		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	
App symmetric key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by
App asymmetric private key	Hard drive encrypted import (SSPs other than DMK) Hard drive	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches	DMK:Encrypted by KBK:Encrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)			Clear button in the front panel	
App asymmetric public key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by
ML-DSA private key	Hard drive encrypted import	Internal hard drive:Encrypted		Automatic Module initialization	DMK:Encrypted by KBK:Encrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	(SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)			(Zeroization) Tamper response switches Clear button in the front panel	ML-DSA public key:Paired With
ML-DSA public key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by ML-DSA private key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	other than DMK)				
ML-KEM decapsulation key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by ML-KEM encapsulation key:Paired With
ML-KEM encapsulation key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by ML-KEM decapsulation key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	DMK) Output wrapped by AES (SSPs other than DMK)				
SLH-DSA private key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by SLH-DSA public key:Paired With
SLH-DSA public key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by SLH-DSA private key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)				
LMS private key		Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	KBK:Encrypted by LMS public key:Paired With
LMS public key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK) Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by LMS private key:Paired With
Shared secret	Input unwrapped by AES (SSPs	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper	ANS X9.63 derived Key:Dervies

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	other than DMK)			response switches Clear button in the front panel	
Entropy input		RAM:Plaintext	From generation until DRBG seed is created	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	
DRGB seed		RAM:Plaintext	While the DRBG is instantiated	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	Entropy input:Derived From
DRBG internal state (V value, Key)		RAM:Plaintext	From DRBG instantiation until DRBG termination	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DRGB seed:Derived From
Intermediate key generation value		RAM:Plaintext	From service invocation until cipher handle is freed	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	
User Application Digital Certificate		Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				in the front panel	
ML-DSA seed		RAM:Plaintext	For the duration of the service	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	ML-DSA private key:Derived From ML-DSA public key:Derived From
ML-KEM seed		RAM:Plaintext	For the duration of the service	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	ML-KEM decapsulation key:Derived From ML-KEM encapsulation key:Derived From
ML-KEM shared secret key	Input unwrapped by AES (SSPs other than DMK) Output wrapped by AES (SSPs other than DMK)	RAM:Plaintext	For the duration of the service	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	
SLH-DSA seed		RAM:Plaintext	For the duration of the service	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	SLH-DSA private key:Derived From SLH-DSA public key:Derived From
LMS seed		RAM:Plaintext	For the duration of the service	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	LMS private key:Derived From LMS public key:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS ECDH private key		RAM:Plaintext	For the duration of the service	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	TLS ECDH public key:Paired With TLS premaster secret:Derives
TLS ECDH public key		RAM:Plaintext	For the duration of the service	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	TLS ECDH private key:Paired With TLS premaster secret:Derives
TLS RSA private key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard drive export (KBK)	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by TLS RSA public key:Paired With
TLS RSA public key	Hard drive encrypted import (SSPs other than DMK) Hard drive encrypted export (SSPs other than DMK) HSM hard drive import (KBK) HSM hard	Internal hard drive:Encrypted		Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	DMK:Encrypted by KBK:Encrypted by TLS RSA private key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	drive export (KBK)				
TLS premaster secret		RAM:Plaintext	Until the generation of master secret is completed in TLS handshake	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	TLS ECDH private key:Derived From TLS ECDH public key:Derived From TLS master secret:Derives
TLS master secret		RAM:Plaintext	Until TLS session is completed	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	TLS premaster secret:Derived From TLS encryption key:Derives
TLS encryption key		RAM:Plaintext	Until TLS session is completed	Automatic Module initialization (Zeroization) Tamper response switches Clear button in the front panel	TLS master secret:Derived From DMK Components:Encrypts KBK Components:Encrypts App symmetric key:Encrypts App asymmetric private key:Encrypts App asymmetric public key:Encrypts ML-DSA private key:Encrypts ML-DSA public key:Encrypts ML-KEM decapsulation key:Encrypts ML-KEM encapsulation key:Encrypts SLH-DSA private key:Encrypts SLH-DSA public key:Encrypts LMS private key:Encrypts LMS public key:Encrypts User Application Digital

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Certificate:Encrypts DMK Components:Decrypts KBK Components:Decrypts App symmetric key:Decrypts App asymmetric private key:Decrypts App asymmetric public key:Decrypts ML-DSA private key:Decrypts ML-DSA public key:Decrypts ML-KEM decapsulation key:Decrypts ML-KEM encapsulation key:Decrypts SLH-DSA private key:Decrypts SLH-DSA public key:Decrypts LMS private key:Decrypts LMS public key:Decrypts User Application Digital Certificate:Decrypts
ANS X9.63 derived Key	Output wrapped by AES (SSPs other than DMK)	RAM:Plaintext	Until service is completed	Module initialization (Zeroization) Tamper response switches Clear button in the front panel	Shared secret:Derived From

Table 22: 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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA 4096	4096 with SHA-512	Digital signature verification	SW/FW Integrity	Module becomes operational and services are available for use	Integrity of the OS images is verified by verifying the 4096 bit RSA signature stored in the module that was computed during the production process.
ECDSA P-521	P-521 with SHA-512	Digital signature verification	SW/FW Integrity	Module becomes operational and services are available for use	Integrity of the service images is verified by verifying the curve P-521 ECDSA signature stored in the module, that was computed during the production process.
HMAC	SHA-256	HMAC verification	Critical Function	Module becomes operational and services are available for use	Firmware calls HMAC verification on configuration file

Table 23: Pre-Operational Self-Tests

The pre-operational integrity tests are performed automatically when the module is initialized, before the module transitions into the operational state. The algorithms listed in Section Integrity Techniques are self-tested before the pre-operational firmware integrity and the critical function test starts.
While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the tests are successfully completed. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A6957)	32-byte message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on after the integrity test
SHA2-384 (A6957)	32-byte message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on after the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
SHA2-512 (A6957)	32-byte message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on after the integrity test
SHA3-256 (A6957)	32-byte message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on after the integrity test
SHA3-384 (A6957)	32-byte message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on after the integrity test
SHA3-512 (A6957)	32-byte message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on after the integrity test
RSA SigVer (FIPS186-5) (A6948)	PKCS#1 v1.5, SHA-256 and 2048-bit key / SHA-512 and 4096-bit key	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6948)	PKCS#1 v1.5, SHA-256 and 2048-bit key / SHA-512 and 4096-bit key	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-5) (A6946)	SHA-256 and P-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
ECDSA SigGen (FIPS186-5) (A6946)	SHA-256 and P-224, P-256, P-384, and P-521	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on after the integrity test
EDDSA SigVer (A6947)	Ed448 with SHAKE-256, Ed25519 with SHA-512	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on after the integrity test
EDDSA SigGen (A6947)	Ed448 with SHAKE-256, Ed25519 with SHA-512	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on after the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A6953)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on after the integrity test
AES-CBC (A6945) Encrypt	128 bits, 32-byte message	KAT	CAST	Module becomes operational	Encryption	Test runs at power-on after the integrity test
AES-CBC (A6945) Decrypt	128 bits, 32-byte message	KAT	CAST	Module becomes operational	Decryption	Test runs at power-on after the integrity test
AES-CCM (A6945) Encrypt	128bits, 32-byte message	KAT	CAST	Module becomes operational	Authenticated encryption	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A6945) Decrypt	128bits, 32-byte message	KAT	CAST	Module becomes operational	Authenticated decryption	Test runs at power-on after the integrity test
AES-GCM (A6945) Encrypt	128bits, 32-byte message	KAT	CAST	Module becomes operational	Authenticated encryption	Test runs at power-on after the integrity test
AES-GCM (A6945) Decrypt	128bits, 32-byte message	KAT	CAST	Module becomes operational	Authenticated decryption	Test runs at power-on after the integrity test
AES-KW (A6945) wrapping	128bits	KAT	CAST	Module becomes operational	Key wrapping	Test runs at power-on after the integrity test
AES-KW (A6945) unwrapping	128bits	KAT	CAST	Module becomes operational	Key unwrapping	Test runs at power-on after the integrity test
AES-KWP (A6945) wrapping	128bits	KAT	CAST	Module becomes operational	Key wrapping	Test runs at power-on after the integrity test
AES-KWP (A6945) unwrapping	128bits	KAT	CAST	Module becomes operational	Key unwrapping	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ML-KEM EncapDecap (A6959) encapsulation	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Module becomes operational	ML-KEM encapsulation	Test runs at power-on after the integrity test
ML-KEM EncapDecap (A6959) decapsulation	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Module becomes operational	ML-KEM decapsulation	Test runs at power-on after the integrity test
ML-DSA SigVer (A6959)	ML-DSA-44 and deterministic; all rejection paths are covered; internal (Algorithm 7 with the pre-computed hash M′) and external (Algorithm 2 with the actual message M)	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on after the integrity test
ML-DSA SigGen (A6959)	ML-DSA-44 and deterministic; all rejection paths are covered; internal (Algorithm 8 with the pre-computed hash M′) and external (Algorithm 3 with the actual message M)	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on after the integrity test
SLH-DSA SigVer (A6959)	SLH-DSA-SHAKE-128s; internal (Algorithms 20 with the pre-computed hash M′) and external (Algorithms 24 with the raw message M)	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on after the integrity test
SLH-DSA SigGen (A6959)	SLH-DSA-SHAKE-128s; internal (Algorithms 19 with the pre-computed hash M′) and external (Algorithms 22 with the raw message M)	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on after the integrity test
LMS SigVer (A6960)	LMSOTS_SHA256_N32_W2/LMS_SHA256_M32_H5	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
LMS SigGen (A6960)	LMSOTS_SHA256_N32_W2/LMS_SHA256_M32_H5	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A6955)	32-byte message	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
KDA HKDF SP800-56Cr2 (A6954)	SHA-512	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on after the integrity test
KDF ANS 9.63 (A6951)	SHA-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on after the integrity test
KDF SP800-108 (A6949)	Counter mode; HMAC-SHA-256; 128-bit input key	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on after the integrity test
PBKDF (A6950)	SHA-256, 128 character password; 3072-bit salt; Iteration count: 55208	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on after the integrity test
TLS v1.2 KDF RFC7627 (A6952)	SHA-256; 384-bit input secret	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TLS v1.3 KDF (A6952)	Extract and expand modes; SHA-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on after the integrity test
Counter DRBG (A6956)	AES-256 with prediction resistance	KAT	CAST	Module becomes operational	Instantiate; Generate; Reseed; Health test (compliant to SP 800-90Arev1 Section 11.3)	Test runs at power-on after the integrity test
cSHAKE-128 (A6958)	32-byte message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on after the integrity test
RSA KeyGen (FIPS186-5) (A6948)	PKCS#1 v1.5 with SHA-256 and requested modulus size	PCT	PCT	Key pair generation is successful	Calculation and verification of a digital signature	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6946)	SHA-256 and requested curve size	PCT	PCT	Key pair generation is successful	Calculation and verification of a digital signature	Key pair generation
EDDSA KeyGen (A6947)	Ed448 with SHAKE-256, Ed25519 with SHA-512	PCT	PCT	Key pair generation is successful	Calculation and verification of a digital signature	Key pair generation
ML-KEM KeyGen (A6959) PCT	ML-KEM-512, ML-KEM-768, ML-KEM-1024	PCT	PCT	Key pair generation is successful	Calculation and verification of a shared secret	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					computation	
ML-DSA KeyGen (A6959) PCT	ML-DSA-44, ML-DSA-65, ML-DSA-87	PCT	PCT	Key pair generation is successful	Calculation and verification of a digital signature	Key pair generation
SLH-DSA KeyGen (A6959) PCT	SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s	PCT	PCT	Key pair generation is successful	Calculation and verification of a digital signature	Key pair generation
LMS KeyGen (A6960) PCT	LMS parameters: SHA256_M32_H5, SHA256_M32_H10, SHA256_M32_H15, SHA256_M32_H20, SHA256_M32_H25; LMOTS parameters: SHA256_N32_W1, SHA256_N32_W2, SHA256_N32_W4, SHA256_N32_W8	PCT	PCT	Key pair generation is successful	Key pair generation	Key pair generation
LMS KeyGen (A6960) KAT	LMSOTS_SHA256_N32_W2/LMS_SHA256_M32_H5	KAT	CAST	Module becomes operational	Key pair generation	Test runs at power-on after the integrity test
ML-DSA KeyGen (A6959) KAT	ML-DSA-44, ML-DSA-65, ML-DSA-87	KAT	CAST	Module becomes operational	Key pair generation	Test runs at power-on after the integrity test
ML-KEM KeyGen (A6959) KAT	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Module becomes operational	Key pair generation	Test runs at power-on after the integrity test
SLH-DSA KeyGen (A6959) KAT	SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s	KAT	CAST	Module becomes operational	Key pair generation	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ESV - Repetition Count Test (Startup)	Startup test with 1124 samples; Cutoff value = 91	Fault detection test	CAST	Successful seeding of SP 800-90A DRBG	SP 800-90B 4.4.1 Repetition Count Test	Upon seeding or reseeding SP 800-90A DRBG
ESV - Adaptive Proportional Test (Startup)	Startup test with 1124 samples; Cutoff value = 459	Fault detection test	CAST	Successful seeding of SP 800-90A DRBG	SP 800-90B 4.4.2 Adaptive Proportion Test	Upon seeding or reseeding SP 800-90A DRBG
ESV - Repetition Count Test (Continuous)	Cutoff value = 181	Fault detection test	CAST	Successful seeding of SP 800-90A DRBG	SP 800-90B 4.4.1 Repetition Count Test	Upon seeding or reseeding SP 800-90A DRBG
ESV - Adaptive Proportional Test (Continuous)	Cutoff value = 479	Fault detection test	CAST	Successful seeding of SP 800-90A DRBG	SP 800-90B 4.4.2 Adaptive Proportion Test	Upon seeding or reseeding SP 800-90A DRBG

Table 24: Conditional Self-Tests

Data output through the data output interface is inhibited during the conditional self-tests. The module does not return control to the calling application until the tests are completed. If any of these tests fail, the module transitions to the error state (Section 10.4 Error States).

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA 4096	Digital signature verification	SW/FW Integrity	Programmatically	Every 12 hours
ECDSA P-521	Digital signature verification	SW/FW Integrity	Programmatically	Every 12 hours
HMAC	HMAC verification	Critical Function	Programmatically	Every 12 hours

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A6957)	KAT	CAST	Programmatically	Every 12 hours
SHA2-384 (A6957)	KAT	CAST	Programmatically	Every 12 hours
SHA2-512 (A6957)	KAT	CAST	Programmatically	Every 12 hours
SHA3-256 (A6957)	KAT	CAST	Programmatically	Every 12 hours
SHA3-384 (A6957)	KAT	CAST	Programmatically	Every 12 hours
SHA3-512 (A6957)	KAT	CAST	Programmatically	Every 12 hours
RSA SigVer (FIPS186-5) (A6948)	KAT	CAST	Programmatically	Every 12 hours
RSA SigGen (FIPS186-5) (A6948)	KAT	CAST	Programmatically	Every 12 hours
ECDSA SigVer (FIPS186-5) (A6946)	KAT	CAST	Programmatically	Every 12 hours
ECDSA SigGen (FIPS186-5) (A6946)	KAT	CAST	Programmatically	Every 12 hours
EDDSA SigVer (A6947)	KAT	CAST	Programmatically	Every 12 hours
EDDSA SigGen (A6947)	KAT	CAST	Programmatically	Every 12 hours
KAS-ECC-SSC Sp800-56Ar3 (A6953)	KAT	CAST	Programmatically	Every 12 hours
AES-CBC (A6945) Encrypt	KAT	CAST	Programmatically	Every 12 hours
AES-CBC (A6945) Decrypt	KAT	CAST	Programmatically	Every 12 hours
AES-CCM (A6945) Encrypt	KAT	CAST	Programmatically	Every 12 hours
AES-CCM (A6945) Decrypt	KAT	CAST	Programmatically	Every 12 hours
AES-GCM (A6945) Encrypt	KAT	CAST	Programmatically	Every 12 hours
AES-GCM (A6945) Decrypt	KAT	CAST	Programmatically	Every 12 hours
AES-KW (A6945) wrapping	KAT	CAST	Programmatically	Every 12 hours
AES-KW (A6945) unwrapping	KAT	CAST	Programmatically	Every 12 hours
AES-KWP (A6945) wrapping	KAT	CAST	Programmatically	Every 12 hours
AES-KWP (A6945) unwrapping	KAT	CAST	Programmatically	Every 12 hours
ML-KEM EncapDecap (A6959) encapsulation	KAT	CAST	Programmatically	Every 12 hours
ML-KEM EncapDecap (A6959) decapsulation	KAT	CAST	Programmatically	Every 12 hours
ML-DSA SigVer (A6959)	KAT	CAST	Programmatically	Every 12 hours

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ML-DSA SigGen (A6959)	KAT	CAST	Programmatically	Every 12 hours
SLH-DSA SigVer (A6959)	KAT	CAST	Programmatically	Every 12 hours
SLH-DSA SigGen (A6959)	KAT	CAST	Programmatically	Every 12 hours
LMS SigVer (A6960)	KAT	CAST	Programmatically	Every 12 hours
LMS SigGen (A6960)	KAT	CAST	Programmatically	Every 12 hours
HMAC-SHA2-256 (A6955)	KAT	CAST	Programmatically	Every 12 hours
KDA HKDF SP800-56Cr2 (A6954)	KAT	CAST	Programmatically	Every 12 hours
KDF ANS 9.63 (A6951)	KAT	CAST	Programmatically	Every 12 hours
KDF SP800-108 (A6949)	KAT	CAST	Programmatically	Every 12 hours
PBKDF (A6950)	KAT	CAST	Programmatically	Every 12 hours
TLS v1.2 KDF RFC7627 (A6952)	KAT	CAST	Programmatically	Every 12 hours
TLS v1.3 KDF (A6952)	KAT	CAST	Programmatically	Every 12 hours
Counter DRBG (A6956)	KAT	CAST	Programmatically	Every 12 hours
cSHAKE-128 (A6958)	KAT	CAST	Programmatically	Every 12 hours
RSA KeyGen (FIPS186-5) (A6948)	PCT	PCT	Programmatically	Every 12 hours
ECDSA KeyGen (FIPS186-5) (A6946)	PCT	PCT	Programmatically	Every 12 hours
EDDSA KeyGen (A6947)	PCT	PCT	Programmatically	Every 12 hours
ML-KEM KeyGen (A6959) PCT	PCT	PCT	Programmatically	Every 12 hours
ML-DSA KeyGen (A6959) PCT	PCT	PCT	Programmatically	Every 12 hours
SLH-DSA KeyGen (A6959) PCT	PCT	PCT	Programmatically	Every 12 hours
LMS KeyGen (A6960) PCT	PCT	PCT	Programmatically	Every 12 hours
LMS KeyGen (A6960) KAT	KAT	CAST	Programmatically	Every 12 hours
ML-DSA KeyGen (A6959) KAT	KAT	CAST	Programmatically	Every 12 hours
ML-KEM KeyGen (A6959) KAT	KAT	CAST	Programmatically	Every 12 hours
SLH-DSA KeyGen (A6959) KAT	KAT	CAST	Programmatically	Every 12 hours
ESV - Repetition Count Test (Startup)	Fault detection test	CAST	Programmatically	Every 12 hours

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ESV - Adaptive Proportional Test (Startup)	Fault detection test	CAST	Programmatically	Every 12 hours
ESV - Repetition Count Test (Continuous)	Fault detection test	CAST	Programmatically	Every 12 hours
ESV - Adaptive Proportional Test (Continuous)	Fault detection test	CAST	Programmatically	Every 12 hours

Table 26: Conditional Periodic Information

The periodic self-test is performed automatically every 12 hours, and the self-test will run synchronously in the background at a low priority if the system is under high load.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Halt Error	Module is no longer operational. The data output is inhibited.	Integrity test failure CAST failure PCT failure APT/ RCT failure	Module initialization	LCD display shows error message: "Error: (OS SelfTest)","Error: (Service SelfTest)","Error: (Config SelfTest)","Error: (Entropy SelfTest)","Error: (Random SelfTest)","Error: (AES SelfTest)","Error: (ECDSA SelfTest)","Error: (ECDH SelfTest)","Error: (RSA SelfTest)","Error: (HASH SelfTest)","Error: (KDF SelfTest)","Error: (LMS SelfTest)","Error: (MLKEM SelfTest)","Error: (MLDSA SelfTest)","Error: (SLHDSA SelfTest)"; LED indicator "Alarm" flashes

Table 27: Error States

In the error state, the module immediately stops functioning and ends the application process. Consequently, the data output interface is inhibited, and the module no longer accepts inputs or requests (as the module is no longer running).

10.5 Operator Initiation of Self-Tests

Both conditional and pre-operational self-tests can be executed on-demand by rebooting the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is shipped to the operator without any initialization of SSPs, or authentication information. The operator function (general purpose mode or financial mode) and the operational mode (FIPS YES and FIPS No) can be selected during this initialization routine and can only be changed to another mode by re-initializing the module which zeroizes all SSPs.

Before starting the module installation, the operator needs to have access to the following peripheral devices:

- Management console which is a computer that acts on behalf of the operator.
- USB token that is used by the operator for storing RSA private key.

The first task for the operator is to connect the USB token to the management console and run the ad-hoc utility shipped with the management console. Using the utility, the operator must generate an RSA key pair, which is stored on the USB. The operator must also set an eight-digit PIN to access the USB device. These steps complete the USB initialization process.

At a later point the corresponding public key is installed in the module during operator initialization and is thereafter used as for Operator authentication. The module never has access to the RSA private key. Also note that the Management console and USB are not part of the module.

Following are the number of USB devices required per the operator role:

1. One USB token for each Manager, one USB token for the Operator, one USB token for the Auditor.
2. Minimum three USB tokens are needed for exporting the KBK components with “DMK and KBK export” service.
3. Minimum two USB tokens are needed for exporting the DMK with “DMK and KBK export” service.

After the preparation above, the operator must perform the initialization of the module following the instructions listed below.

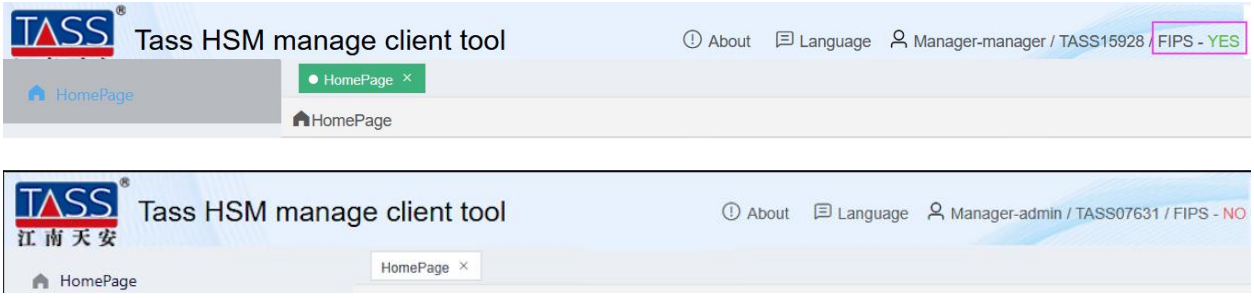
1. Verify that the external condition of the package per Figure 15 to see if there are signs of damage, or if the package has been opened during transit.
2. Open the package and verify with the content list that the HSM and all accessories are included.
3. Verify that the eleven tamper evidence seals are intact and located at the expected positions (see Section 7.1).
4. Connect the module’s power supplies and turn on the module.
5. Connect the management console as shown in Figure 1 to the module through the management serial port. The management
6. Power-up the module.
7. Login into the management console and run the management program.
8. Verify that the product model and version provided in the “View Device Basic Information” menu option matches the following information:
    - Operation functions: “General Purpose Mode”.
    - Firmware Version: H2.00.00.
9. Use the Installation Wizard to perform the following activities:
    a. Initialize the module following the below two steps:

        Choose the “DMK Algorithm” and “DMK Method” (which defines the DMK generation mode).



Figure 8: Initialize – 1

- The DMK algorithm configured during installation is reflected with “FIPS: YES” or “FIPS: NO” status as shown in right corner of the screenshots below. “FIPS: YES” indicates an Approved DMK algorithm, allowing Approved services (service indicator 1) and non-Approved services (service indicator 0). “FIPS: NO” indicates a non-Approved DMK algorithm, in which case all services are non-Approved (service indicator 0). Please see section 2.2 for details.



- The next screen allows the operator to register the first CO role. The operator shall type “Manager” as the CO name. The Ukey drop down allows the operator to select the serial number of the connected USB token and operator must enter the eight digit PIN for the selected USB. Once the USB successfully verifies the provided PIN, it outputs the stored RSA public key to the management console which then transfers this key along with Ukey and CO name to the module in order to register the first Manager.

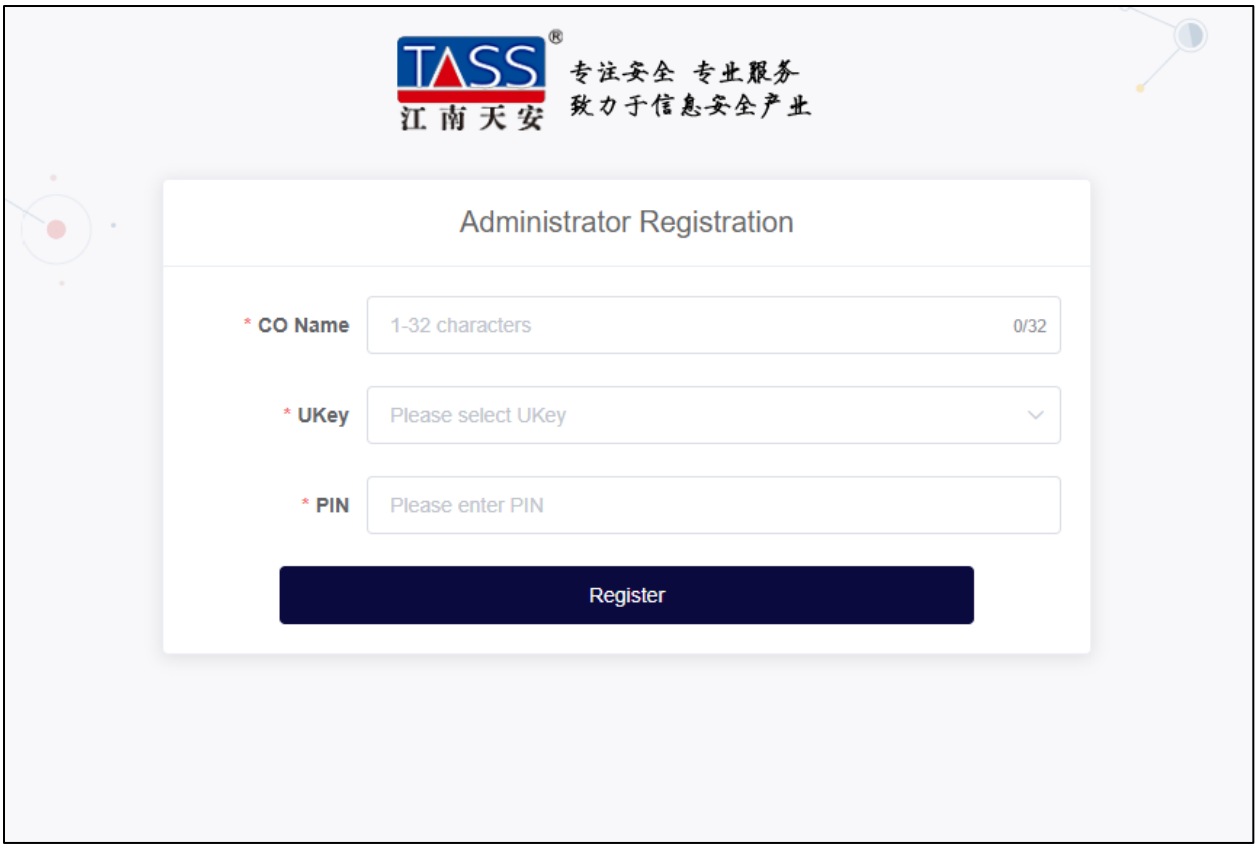


Figure 9: Initialize - 2

b. After the first Manager role logs in, the Manager can create additional operators with type CO using “Add CO” service for other COs. (Managers, Operator, Auditor). The RSA public key and UKey ID for each of the operator is stored in the module as part of operator registration. As below:

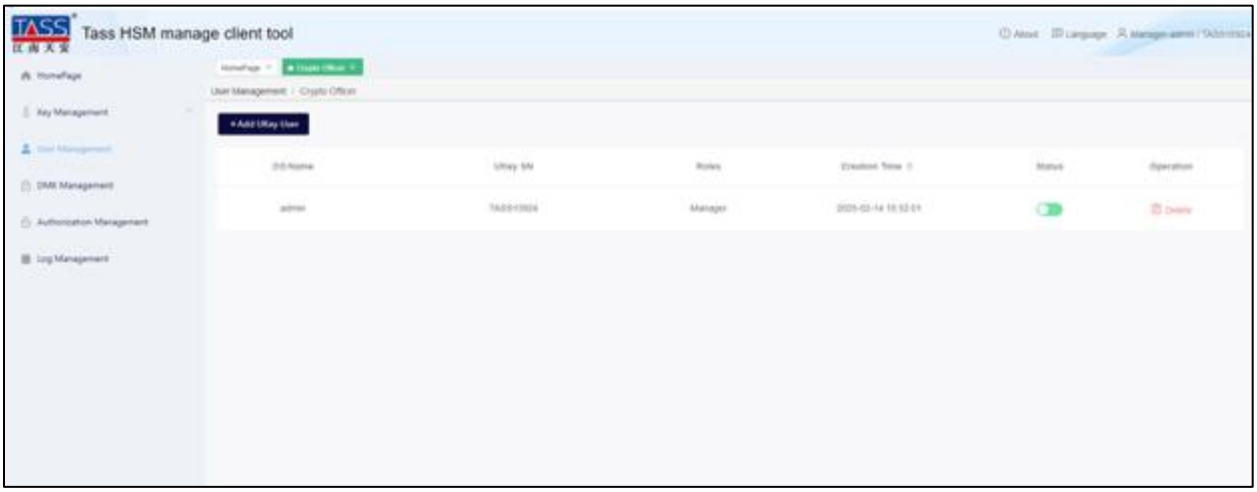


Figure 10: User Management – Crypto Officer

c. After operator login, Configure the network. As below:

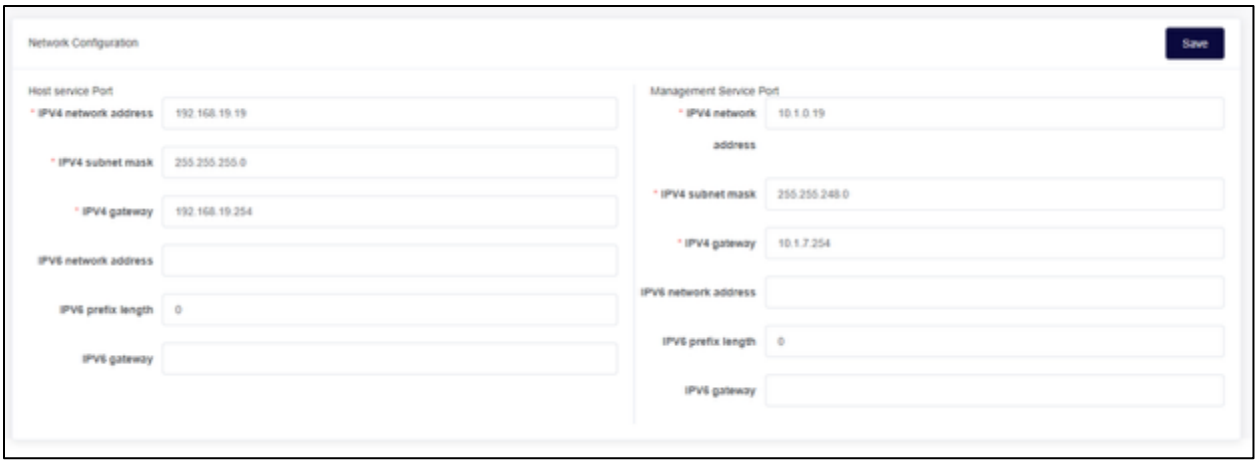


Figure 11: Network Configuration

d. Configure the device configuration, includes Host Service Property and Communication Configuration. As below:

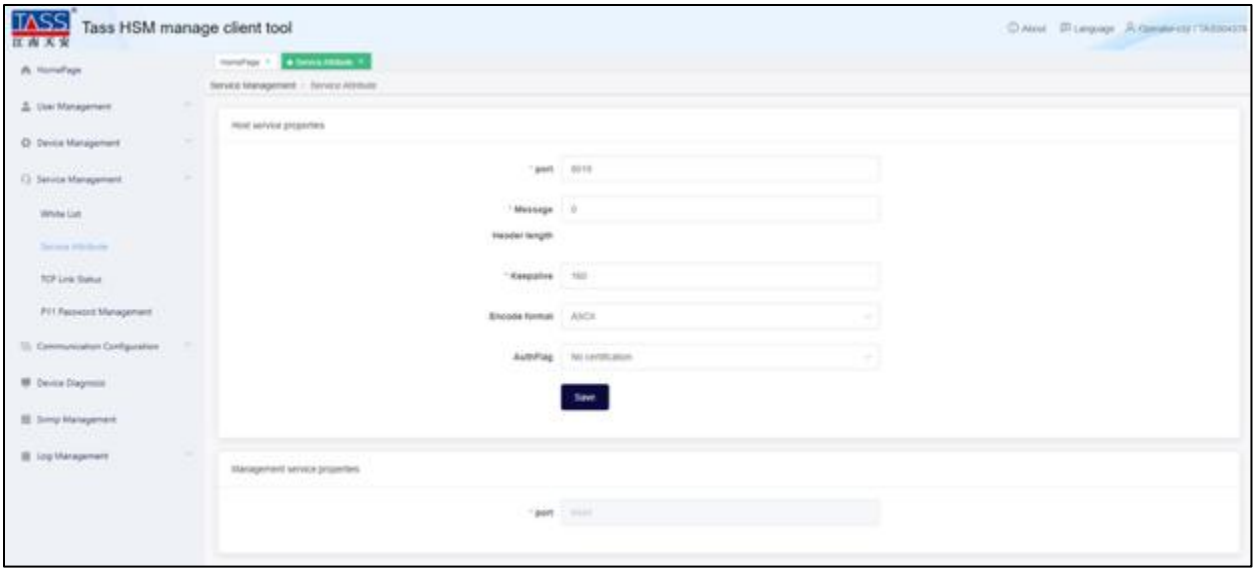


Figure 12: Device Configuration – Host Service Property

e. (Optional) Configure the IP address whitelist with “Configure IP addresses white-listing” service with Operator identity role. As below:

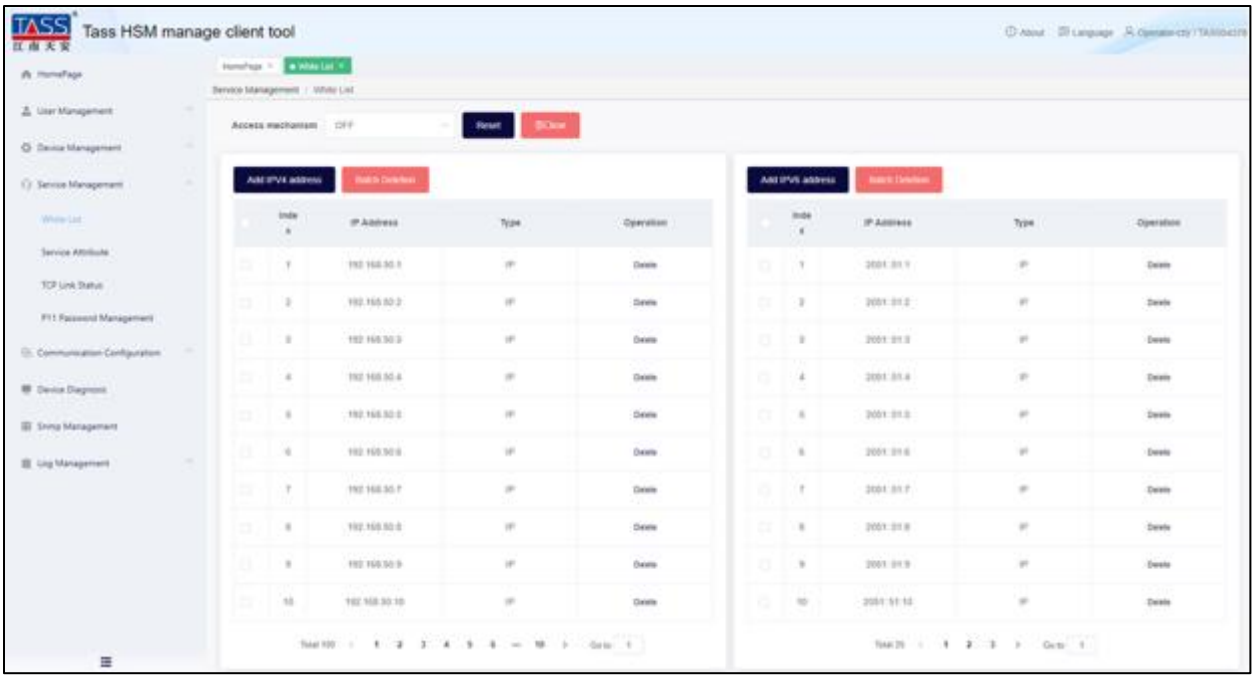


Figure 13: User Management – White List

10. (Optional) Once the installation is done, the Manager could log in to the module by performing challenge response as explained in section 4.3 and generate or import symmetric keys or asymmetric key pairs to be used by the User Application role later point of time. As below:

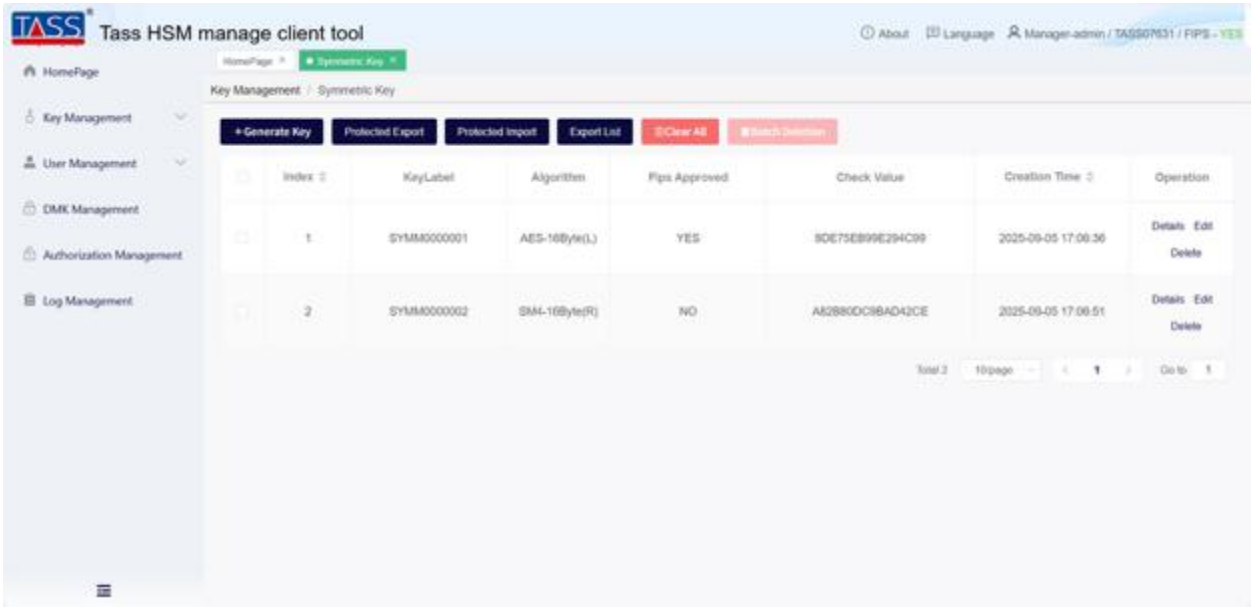


Figure 14: Key Management – Symmetric Key

11.2 Administrator Guidance

Crypto Officer Manager role must visually verify that the tamper evidence seals are intact and located in the expected positions of the chassis once a month. In case evidence of tampering is found, the Manager identity role shall immediately cease operation of the module and shall perform the Module Initialization service. Next, the Manager identity role shall contact the manufacturer to return the module for repair and maintenance. At the factory, new tamper-evidence labels shall be applied as specified. Upon receiving the restored module, the Manager identity role shall follow the guidance as applicable to a new module.

11.3 Non-Administrator Guidance

The whole equipment and accessories are first packed into the inner packing box, and the foam plastic is cushioning in the packing box. The module is firmly wrapped, and then packed into the outer packing box together with the inner packing box, and TASS is used. The transparent tape of logo pastes the joint of the carton; in addition, one side of the outer packing box is pasted with the model and serial number of the equipment in the package; finally, the packing box is bound with the automatic packer, as shown in the following figure:



Figure 15: Packing of the module

Express delivery (SF) is chosen for delivery. The express sheet is pasted on the transparent tape at the joint of the outer package, and then delivered by the express company.
Each express bill has a unique order number. From the delivery to the courier, you can query and track the logistics situation through the express official website.
In addition, the manufacturer will inform the receiving party of the express bill number, equipment model and serial number by e-mail.

After receiving the package, the receiving party needs to check: the express bill, packing strap and the transparent tape at the joint are complete, and the express bill number, equipment model and equipment serial number are consistent with the contents of the mail, then the package shall be signed for acceptance; if there is any abnormality, the package shall be rejected.

The ESV Public Use Document (PUD) reference for non-physical entropy source is as follows:
https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/314

11.4 End of Life

When the module is no longer in use, the COs need to perform the “Module initialization” to ensure that all SSPs and user data on the module are zeroized. And then the module can be removed from the rack or working location and placed in an appropriate environment for storage.

12 Mitigation of Other Attacks

This module does not implement any mitigation of other attacks, and therefore this section is not applicable.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
DF	Derivation Function
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
KW	AES Key Wrap
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OFB	Output Feedback
PSP	Public Security Parameter
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
DMK	Device Master Key
LMK	Local Master Key
KBK	Key Backup Key
PIN	Personal Identification Number
PAN	Personal Account Number
CVV	Card Verification Value
DUKPT	Derived Unique Key Per Transaction
BDK	Base Derivation Key
EMV	Europay, MasterCard, Visa
ZPK	Zone PIN Key
PVK	PIN Verification Key
PBOC	People’s Bank of China
OTP	One Time Password
GP	Global Platform

KMC	Issuing Master Key
KDEK	Data Encryption Key
KMAC	Static Secure Channel Message Authentication Code Key
KENC	Static Secure Channel Encryption Key
SDEK	Session Key for encrypting secret card data
SENC	Secure Channel command and response encryption key
SCMAC	Secure Channel C-MAC session key
SRMAC	Secure Channel R-MAC session key
ARQC	Authorization Request Cryptogram
ARPC	Authorization Response Cryptogram
TC	Transaction Certificate
AAC	Application Authentication Cryptogram

Appendix B. References

FIPS140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
FIPS140-3_IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS180-4	**Secure Hash Standard (SHS)** August 2015 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS186-4	**Digital Signature Standard (DSS)** July 2013 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS186-5	Digital Signature Standard (DSS) February 2023 https://doi.org/10.6028/NIST.FIPS.186-5
FIPS197	**Advanced Encryption Standard** November 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography** Specifications Version 2.1 February 2003 http://www.ietf.org/rfc/rfc3447.txt
RFC3394	**Advanced Encryption Standard (AES) Key Wrap Algorithm** September 2002 http://www.ietf.org/rfc/rfc3394.txt
RFC5649	**Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm** September 2009 http://www.ietf.org/rfc/rfc5649.txt
SP 800-38A	**NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 http://csrc.nist.gov/publications/nistpubs/800-38a/SP 800-38a.pdf
SP 800-38B	**NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

SP 800-38C	**NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality** May 2004 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf
SP 800-38D	**NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** November 2007 http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
SP 800-38E	**NIST Special Publication 800-38E - Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices** January 2010 http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf
SP 800-38F	**NIST Special Publication 800-38F - Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** December 2012 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf
SP 800-38G	**NIST Special Publication 800-38G - Recommendation for Block Cipher Modes of Operation: Methods for Format - Preserving Encryption** March 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf
SP 800-56Ar3	**NIST Special Publication 800-56A Revision 3 - Recommendation for Pair Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** April 2018 https://doi.org/10.6028/NIST.SP.800-56Ar3
SP 800-56Cr2	**Recommendation for Key Derivation through Extraction-then-Expansion** August 2020 https://doi.org/10.6028/NIST.SP.800-56Cr2
SP 800-57	**NIST Special Publication 800-57 Part 1 Revision 4 - Recommendation for Key Management Part 1: General** January 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
SP 800-67	**NIST Special Publication 800-67 Revision 1 - Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher** January 2012 http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf
SP 800-90Ar1	**NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 http://dx.doi.org/10.6028/NIST.SP.800-90Ar1
SP 800-90B	**NIST Special Publication 800-90B - Recommendation for the Entropy Sources Used for Random Bit Generation** January 2018 https://doi.org/10.6028/NIST.SP.800-90B
SP 800-131r2	**Transitioning the Use of Cryptographic Algorithms and Key Lengths** March 2019 https://doi.org/10.6028/NIST.SP.800-131Ar2

SP 800-132	**NIST Special Publication 800-132 - Recommendation for Password-Based Key Derivation - Part 1: Storage Applications** December 2010 http://csrc.nist.gov/publications/nistpubs/800-132/nist-SP 800-132.pdf
SP 800-133r2	**NIST Special Publication 800-133 - Recommendation for Cryptographic Key Generation** June 2020 https://doi.org/10.6028/NIST.SP.800-133r2
SP 800-135r1	**NIST Special Publication 800-135 Revision 1 - Recommendation for Existing Application-Specific Key Derivation Functions** December 2011 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
SP 800-140Br1	**NIST Special Publication 800-140B - CMVP Security Policy Requirements** November 2023 https://doi.org/10.6028/NIST.SP.800-140Br1