Kryptus

ASI-HSM AHX5 kNET Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 6
1.1 Overview 6
1.2 Security Levels 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 14
2.7 Algorithm Specific Information 19
2.8 RBG and Entropy 20
2.9 Key Generation 20
2.10 Key Establishment 20
2.11 Industry Protocols 21
3 Cryptographic Module Interfaces 22
3.1 Ports and Interfaces 22
3.2 Trusted Channel Specification 23
4 Roles, Services, and Authentication 25
4.1 Authentication Methods 25
4.2 Roles 31
4.3 Approved Services 32
4.4 Non-Approved Services 103
4.5 External Software/Firmware Loaded 104
5 Software/Firmware Security 105
5.1 Integrity Techniques 105
5.2 Initiate on Demand 105
6 Operational Environment 106
6.1 Operational Environment Type and Requirements 106
7 Physical Security 107
7.1 Mechanisms and Actions Required 107
7.2 User Placed Tamper Seals 108
7.3 Filler Panels 108
7.4 Fault Induction Mitigation 108
7.5 EFP/EFT Information 108

7.6 Hardness Testing Temperature Ranges 109
8 Non-Invasive Security 110
8.1 Mitigation Techniques 110
9 Sensitive Security Parameters Management 111
9.1 Storage Areas 111
9.2 SSP Input-Output Methods 111
9.3 SSP Zeroization Methods 114
9.4 SSPs 115
10 Self-Tests 144
10.1 Pre-Operational Self-Tests 144
10.2 Conditional Self-Tests 144
10.3 Periodic Self-Test Information 151
10.4 Error States 158
11 Life-Cycle Assurance 160
11.1 Installation, Initialization, and Startup Procedures 160
11.2 Administrator Guidance 162
11.3 Non-Administrator Guidance 166
11.4 Design and Rules 167
11.5 Maintenance Requirements 167
11.6 End of Life 167
12 Mitigation of Other Attacks 168
12.1 Attack List 168

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 12
Table 5: Vendor-Affirmed Algorithms 13
Table 6: Non-Approved, Not Allowed Algorithms 13
Table 7: Security Function Implementations 19
Table 8: Entropy Certificates 20
Table 9: Entropy Sources 20
Table 10: Ports and Interfaces 22
Table 11: Authentication Methods 30
Table 12: Roles 32
Table 13: Approved Services 103
Table 14: Non-Approved Services 104
Table 15: Mechanisms and Actions Required 107
Table 16: EFP/EFT Information 109
Table 17: Hardness Testing Temperatures 109
Table 18: Storage Areas 111
Table 19: SSP Input-Output Methods 114
Table 20: SSP Zeroization Methods 115
Table 21: SSP Table 1 127
Table 22: SSP Table 2 142
Table 23: Pre-Operational Self-Tests 144
Table 24: Conditional Self-Tests 151
Table 25: Pre-Operational Periodic Information 151
Table 26: Conditional Periodic Information 158
Table 27: Error States 159

List of Figures

Figure 1: Cryptographic module's Physical Perimeter – top view 7
Figure 2: Cryptographic module's Physical Perimeter – bottom view 8
Figure 3: Block Diagram 9
Figure 4: Cryptographic Module Interfaces 23
Figure 5: Top view of the cryptographic module 107
Figure 6: Bottom view of the cryptographic module 108
Figure 7: Installation on the rack 160
Figure 8: Tamper-evident seals 161
Figure 9: Tamper-evident seals – zoom in 161
Figure 10: Label affixed to the back of the device 162
Figure 11: HSM Frontal board after self-tests and not configured 163
Figure 12: HSM Frontal board displaying the Temporary PIN 163
Figure 13: HSM Frontal Board Default Screen 164

1 General

1.1 Overview

The ASI-HSM AHX5 kNET Cryptographic Module is a Hardware Security Module that provides cryptographic services with native implementation of the Key Management Interoperability Protocol to ap-plications. The hardware is optimized for cryptographic operations along with proprietary firmware and software developed exclusively for the module. Its operators communicate with it via a standard Ethernet interface using IP protocols. The module is usually sold embedded within a stand-alone net-work appliance, which is typically used in large-scale cloud infrastructures, where ease of remote configuration and operation is required.

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

The module has an overall security level of 3.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The ASI-HSM AHX5 kNET Cryptographic Module is a multi-user, multi-chip embedded hardware security module. The ASI-HSM AHX5 kNET Cryptographic Module is referred to in the remainder of this document as ‘the module’, ‘kNET HSM’ and ‘kNET’.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The Physical Perimeter of the module is delimited by two aluminum frames, one at the top and other at the bottom of the ASI-HSM AHX5 kNET main board, as depicted in Figure 1 and Figure 2. All the hardware components that execute security functions are contained in the Cryptographic Boundary, which is completely covered by the epoxy resin potting.

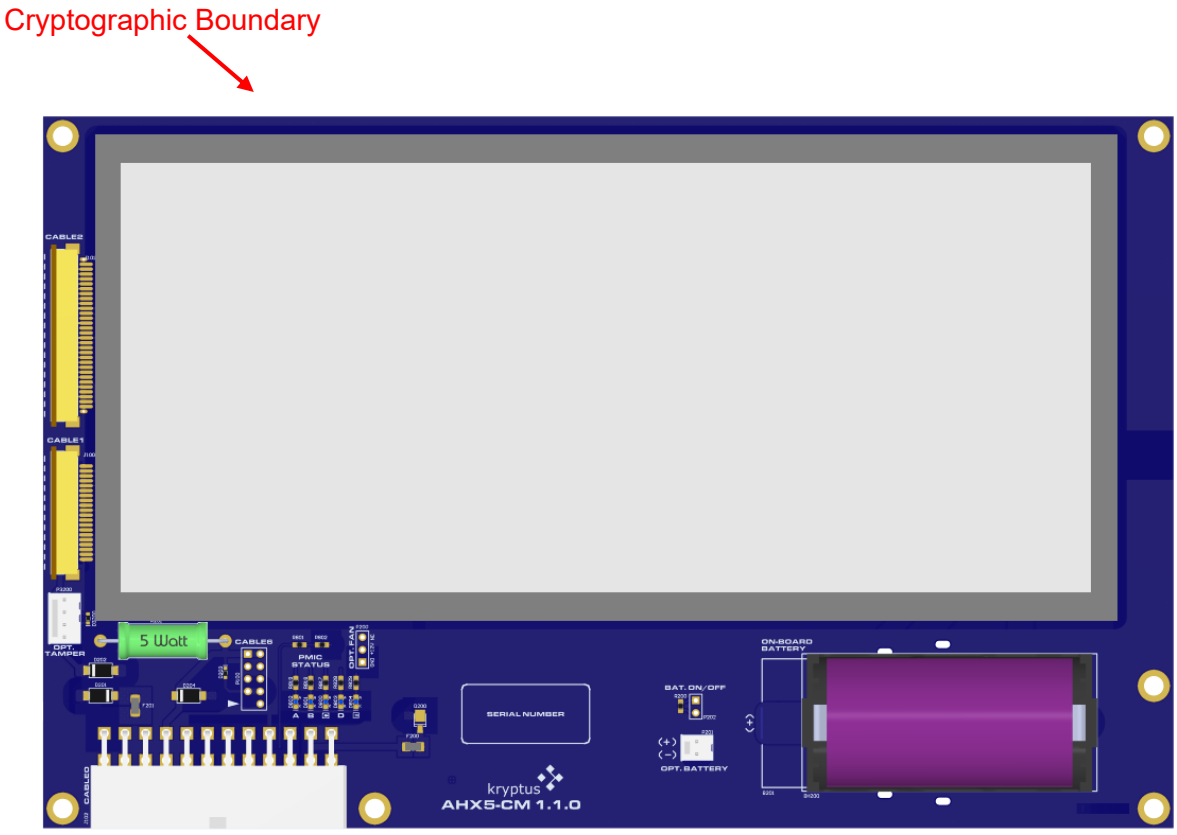

Figure 1: Cryptographic module’s Physical Perimeter – top view

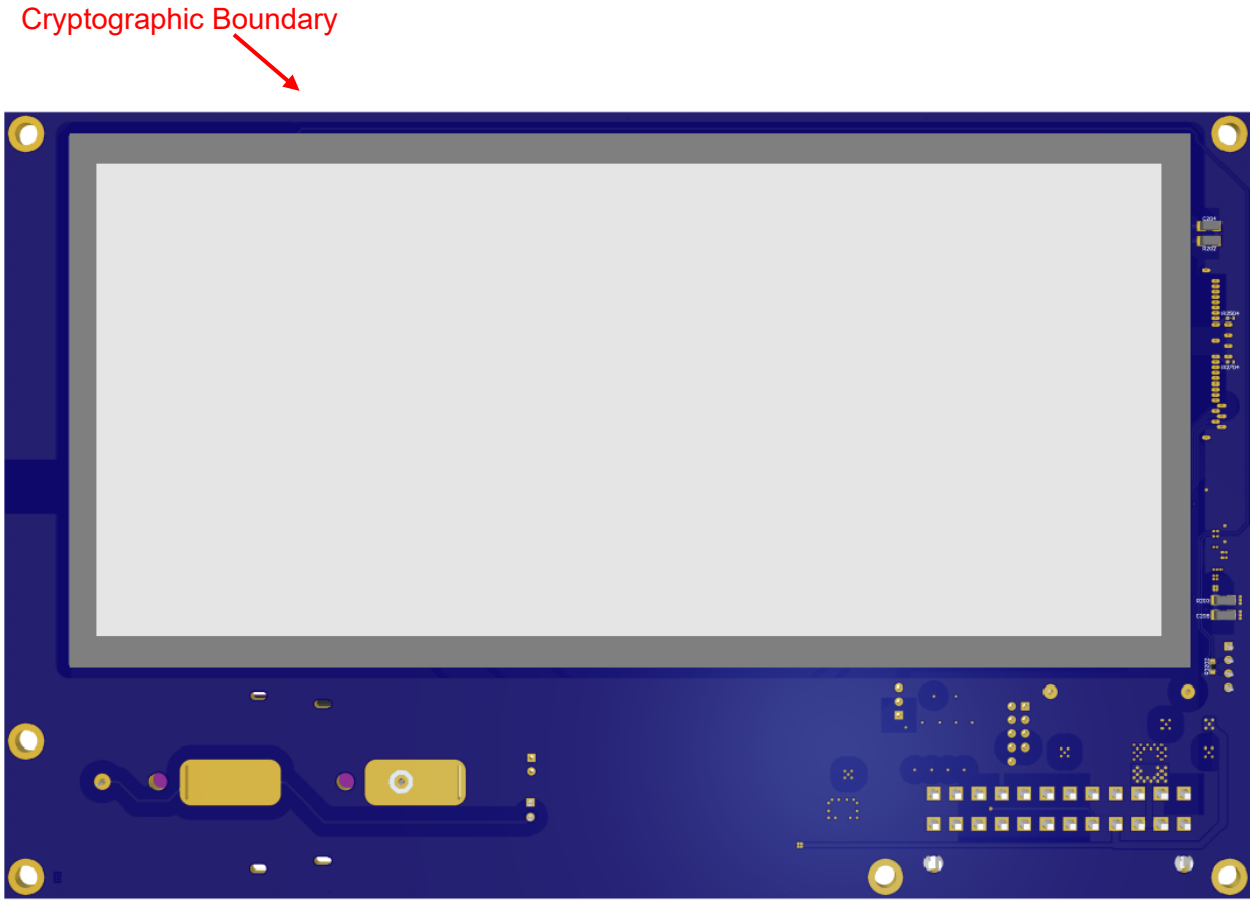

Figure 2: Cryptographic module's Physical Perimeter – bottom view

Tested Operational Environment's Physical Perimeter (TOEPP):

The module is sold embedded within a stand-alone network appliance, which is a 19-inch rackmount case. The appliance is typically used in large-scale cloud infrastructures, where ease of remote configuration and operation is required.

Besides the ASI-HSM AHX5 kNET main board where the module is located, the TOEPP also includes an ATX power supply unit, fans, and the Frontal Board. The latter device contains the external connectors, the graphical display, the interface buttons, and the power button of the appliance.

Figure 3: Block Diagram

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
ASI-HSM AHX5 kNET Cryptographic Module	1.1.0	1.1.0	C293 Crypto Coprocessor	Unique version

Table 2: Tested Module Identification – Hardware

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

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

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

N/A for this module.

2.3 Excluded Components

There are no excluded components within the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
FIPS 140-3	The FIPS 140-3 approved mode of operation	Approved	Frontal Board Display
Legacy FIPS 140-2	Non-approved mode for legacy FIPS 140-2 restrictions	Non-Approved	System Log
Common Criteria	Non-approved mode for Common Criteria restrictions	Non-Approved	System Log
Unrestricted	Non-approved mode for unrestricted usage	Non-Approved	System Log

Table 3: Modes List and Description

When the module is initialized with the Initialize HSM function, the operator can choose the mode of operation to be used.

Mode Change Instructions and Status:

A mode of operations is explicitly selected by an operator during the initialization process. The module enters the approved mode after configuring it as per instructions in Section 11.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6066	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A6066	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A6066	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6066	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6066	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A6066	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
Conditioning Component AES-CBC-MAC SP800-90B	A6066	Key Length - 128, 192, 256	SP 800-90B
ECDSA KeyGen (FIPS186-5)	A6066	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - extra bits	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigGen (FIPS186-5)	A6066	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE-256 Component - Yes	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6066	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE-256	FIPS 186-5
EDDSA KeyGen	A6066	Curve - ED-25519, ED-448	FIPS 186-5
EDDSA SigGen	A6066	Curve - ED-25519, ED-448 PreHash - Yes Pure - Yes	FIPS 186-5
EDDSA SigVer	A6066	Curve - ED-25519, ED-448 PreHash - Yes Pure - Yes	FIPS 186-5
Hash DRBG	A6066	Prediction Resistance - No, Yes Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA-1	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA3-224	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA3-256	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA3-384	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
HMAC-SHA3-512	A6066	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6066	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - responder	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
KDF TLS (CVL)	A6066	TLS Version - v1.2 Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1
ML-DSA KeyGen	A6066	Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87	FIPS 204
ML-DSA SigGen	A6066	Deterministic - No	FIPS 204
ML-DSA SigVer	A6066	-	FIPS 204
ML-KEM EncapDecap	A6066	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768 Functions - Decapsulation, Encapsulation	FIPS 203
ML-KEM KeyGen	A6066	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768	FIPS 203
RSA KeyGen (FIPS186-5)	A6066	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A6066	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6066	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA2-224	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512/224	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512/256	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-224	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-256	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-384	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-512	A6066	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHAKE-256	A6066	Output Length - Output Length: 512	FIPS 202
TDES-CBC	A6066	Direction - Decrypt	SP 800-67 Rev. 2
TDES-ECB	A6066	Direction - Decrypt	SP 800-67 Rev. 2

Table 4: Approved Algorithms

In Approved Mode of operation, the supported Approved algorithms are those listed above.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	SP 800-133r2 Section 4 Example #1, Section 5.1, Section 5.2 and Section 6.1

Table 5: Vendor-Affirmed Algorithms

All vendor-affirmed algorithms are those listed above.

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
Triple DES	Data Encryption
RSA	Data encryption using PKCS#1; Signature Generation using keys less than 2048 bits
MD5	Message Digest
DSA	Key Pair Generation and Signature Generation
Brainpool P-160 (r1/t1)	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-192 (r1/t1)	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-224 (r1/t1)	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-256 (r1/t1)	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-320 (r1/t1)	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-384 (r1/t1)	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-512 (r1/t1)	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Ed521	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
SEC P-256 (k1)	Key Pair Generation, Digital Signature Generation, Digital Signature Verification

Table 6: Non-Approved, Not Allowed Algorithms

When configured in Non-Approved Mode the algorithms in Table 7 are supported as well.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Data Encryption	BC-UnAuthEncrypt	-		AES-CBC: (A6066) Key Length: 256 AES-ECB: (A6066) Key Length: 256 AES-CTR: (A6066) Key Length: 256 RSA KeyGen (FIPS186-5): (A6066) RSA SigGen (FIPS186-5): (A6066)
Data Decryption	BC-UnAuthDecrypt	-		AES-CBC: (A6066) Key Length: 256 AES-ECB: (A6066) Key Length: 256 AES-CTR: (A6066) Key Length: 256 RSA KeyGen (FIPS186-5): (A6066) RSA SigVer (FIPS186-5): (A6066)
Legacy Data Decryption	BC-UnAuthEncrypt	-		TDES-CBC: (A6066) TDES-ECB: (A6066) RSA KeyGen (FIPS186-5): (A6066) RSA SigVer (FIPS186-5): (A6066)
Deterministic Random Number Generator	DRBG	-		Hash DRBG: (A6066)
Digital Signature Generation	DigSig-SigGen	-		SHA2-224: (A6066) SHA2-256:

Name	Type	Description	Properties	Algorithms
				(A6066) SHA2-384: (A6066) SHA2-512: (A6066) SHA2-512/224: (A6066) SHA2-512/256: (A6066) SHA3-224: (A6066) SHA3-256: (A6066) SHA3-384: (A6066) SHA3-512: (A6066) SHAKE-256: (A6066) ML-DSA SigGen: (A6066) ECDSA SigGen (FIPS186-5): (A6066) EDDSA SigGen: (A6066) RSA SigGen (FIPS186-5): (A6066)
Digital Signature Verification	DigSig-SigVer	-		SHA2-224: (A6066) SHA2-256: (A6066) SHA2-384: (A6066) SHA2-512: (A6066) SHA2-512/224: (A6066) SHA2-512/256: (A6066) SHA3-224: (A6066) SHA3-256: (A6066) SHA3-384: (A6066) SHA3-512: (A6066)

Name	Type	Description	Properties	Algorithms
				SHAKE-256: (A6066) ML-DSA SigVer: (A6066) ECDSA SigVer (FIPS186-5): (A6066) EDDSA SigVer: (A6066) RSA SigVer (FIPS186-5): (A6066)
Key Agreement	CKG KAS-135KDF	-	Reference:SP800-56Ar3, SP800-135r1 Caveat:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A6066) KDF TLS: (A6066) CKG: () Key Type: Symmetric and Asymmetric
Key Generation	AsymKeyPair-KeyGen CKG	-		RSA KeyGen (FIPS186-5): (A6066) ECDSA KeyGen (FIPS186-5): (A6066) EDDSA KeyGen: (A6066) ML-DSA KeyGen: (A6066) ML-KEM KeyGen: (A6066) CKG: () Key Type: Symmetric and Asymmetric
Symmetric Key Generation	CKG	-		CKG: () Key Type: Symmetric and Asymmetric
Secure Hash (Message Digest)	SHA	-		SHA2-224: (A6066) SHA2-256: (A6066) SHA2-384:

Name	Type	Description	Properties	Algorithms
				(A6066) SHA2-512: (A6066) SHA2-512/224: (A6066) SHA2-512/256: (A6066) SHA3-224: (A6066) SHA3-256: (A6066) SHA3-384: (A6066) SHA3-512: (A6066)
Message Authentication	MAC	-		AES-GCM: (A6066) AES-CMAC: (A6066) HMAC-SHA-1: (A6066) HMAC-SHA2-224: (A6066) HMAC-SHA2-256: (A6066) HMAC-SHA2-384: (A6066) HMAC-SHA2-512: (A6066) HMAC-SHA2-512/224: (A6066) HMAC-SHA2-512/256: (A6066) HMAC-SHA3-224: (A6066) HMAC-SHA3-256: (A6066) HMAC-SHA3-384: (A6066) HMAC-SHA3-512: (A6066) SHA2-224: (A6066) SHA2-256: (A6066) SHA2-384: (A6066) SHA2-512:

Name	Type	Description	Properties	Algorithms
				(A6066) SHA2-512/224: (A6066) SHA2-512/256: (A6066) SHA3-224: (A6066) SHA3-256: (A6066) SHA3-384: (A6066) SHA3-512: (A6066)
Message Verification	MAC	-		AES-GCM: (A6066) AES-CMAC: (A6066) HMAC-SHA-1: (A6066) HMAC-SHA2-224: (A6066) HMAC-SHA2-256: (A6066) HMAC-SHA2-384: (A6066) HMAC-SHA2-512: (A6066) HMAC-SHA2-512/224: (A6066) HMAC-SHA2-512/256: (A6066) SHA2-224: (A6066) SHA2-256: (A6066) SHA2-384: (A6066) SHA2-512: (A6066) SHA2-512/224: (A6066) SHA2-512/256: (A6066) SHA3-224: (A6066) SHA3-256: (A6066) SHA3-384:

Name	Type	Description	Properties	Algorithms
				(A6066) SHA3-512: (A6066)
Key Encapsulation	KEM-Full	-		ML-KEM EncapDecap: (A6066)
Key Wrapping	KTS-Wrap	-		AES-KW: (A6066) Key length: 256
Key Unwrapping	KTS-Unwrap	-		AES-KW: (A6066) Key Length: 256
Legacy Key Wrapping	KTS-Unwrap	-		TDES-CBC: (A6066) TDES-ECB: (A6066)
Input-Output	BC-UnAuthDecrypt BC-UnAuthEncrypt SHA	-		AES-CBC: (A6066) Key Length: 128 AES-GCM: (A6066) Key Length: 128, 256 SHA2-256: (A6066) SHA2-384: (A6066)
Get Entropy	ENT-ESV	-		Conditioning Component AES-CBC-MAC SP800-90B: (A6066)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

KAS [SP 800-56Ar3] is employed in Ephemeral Unified Mode, using P-256, P-384, P-521 key sizes and strength. [SP 800-56Ar3] KAS-SSC (Cert. #A6066) with [SP 800-135r1] TLS 1.2 KDF CVL (Cert. #A6066). Compliant to IG D.F Scenario 2 Option 2, testing the shared secret and separately testing the key derivation function.

AES-GCM using key sizes of 128, 192, and 256 are employed. The Module supports internal IV generation using the Approved DRBG. The IV is at least 96 bits in length per SP 800-38D Section 8.2.2, and the Approved DRBG generates outputs such that the (key, IV) pair collision probability is less than 2^-32 per SP 800-38D Section 8. AES-GCM IVs shall be used in compliance with IG C.H scenario 1a (TLS/DTLS 1.2, per RFC 5288), The Module is compatible with TLS/DTLS 1.2 protocol and pro-vides the primitives to support the AES GCM cipher suites from SP 800-52 Rev. 1 Section 3.3.1. The Module's implementation of AES-GCM is used

together with one or more applications outside the Module's cryptographic boundary that implement the specified protocols; these protocols have not been reviewed or tested by the CAVP and CMVP.

TDES shall only be used for legacy purposes i.e., for decryption and key unwrapping, in conformance with IG C.M.

2.8 RBG and Entropy

Cert Number	Vendor Name
E11	STMicroelectronics

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
STM32U5x TRNG	Physical	STM32U5x advanced Arm®-based 32-bit MCU	128 bits	Full entropy	AES-CMAC (A1729)

Table 9: Entropy Sources

The entropy source is provided by a microcontroller of the family STM32U5x, from STMicroelectronics, which embeds a validated TRNG entropy source with the certification number #E11. According to STM32U5x TRNG's SP 800-90B Non-Proprietary Public Use Document, its entropy source provides 128 bits of min-entropy per 128 bits output sample, or full entropy.

2.9 Key Generation

The module employs several forms of Key Generation Techniques:

- RSA – Key Pair Generation for 2048, 3072, 4096 bits.
- ECDSA – Key Pair Generation for curves P-224, P-256, P-384, P-521.
- DRBG (HASH_DRBG) – Key Generation.
- EdDSA – Key Pair Generation for curves ED-25519, ED-448.
- ML-DSA [FIPS 204] – Key Generation for ML-DSA-44, ML-DSA-65, ML-DSA-87.
- ML-KEM [FIPS 203] – Key Generation for ML-KEM-512, ML-KEM-768, ML-KEM-1024.

2.10 Key Establishment

The module employs the following Key Agreement Scheme:

- KAS [SP 800-56Ar3] (Ephemeral Unified) – [SP 800-56Ar3] KAS-SSC (Cert. #A6066) with [SP 800-135r1] TLS 1.2 KDF CVL (Cert. #A6066). Compliant to IG D.F Scenario 2 Option 2 for curves P-256, P-384, P-521.

The module employs following Key Transport Schemes:

- AES [SP 800-38F] (KW) – Key Wrapping/Unwrapping for 128, 192, 256 bits.
- ML-KEM [FIPS 203] – Key Encapsulation and Key Decapsulation for ML-KEM-512, ML-KEM-768, ML-KEM-1024.

2.11 Industry Protocols

The module supports TLS v1.2. No parts of this protocol, other than the approved cryptographic algorithms and the KDFs, 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
Ethernet Interfaces	Data Input Data Output Control Input Status Output	Two sets of ports for Ethernet connection are available. These interfaces are the main communication channel for the cryptographic module. Also, encrypted channel with ASI-HSM AHX5 kNET client when using the Trusted Channel (sensitive data is always encrypted when transmitted through these channels)
RS232 Interface	Control Input Status Output	Serial interface used for module configuration (e.g. configure network interface). No sensitive information is transmitted through this channel. Also used to output module status
I2C Interface	Control Input Status Output	Interface with the Frontal Board, which is responsible for power control (e.g. turn off the module) and user interface control (buttons, LCD). Information about the module status is send through this interface, such as temperature and battery voltage. No sensitive information is transmitted through this channel
FLAGx	Status Output	Two output signals (FLAG0 and FLAG1) that inform to the frontal board the current condition of the CM board (normal condition, occurrence of some internal error or environmental failure) and the temperature used at the fans speed control subroutine
Tamper Pin	Control Input	Receives a control signal that can be connected to a tamper-evidence device (e.g. tamper switch)
USB Interface	Data Input Data Output	Currently optionally used for Import/Export Backup Operations. Since backups are encrypted, no sensitive information is transmitted through this channel
ATX Power input	Power	Power input from the ATX power supply unit
Battery Power input	Power	Power input from the battery unit
Status LEDs	Status Output	Indicate the status of the module initialization sequence

Table 10: Ports and Interfaces

Table 11 lists the module's external connection interfaces. The module does not support Control Output interface.

The figure below identifies the physical interfaces of the cryptographic module:

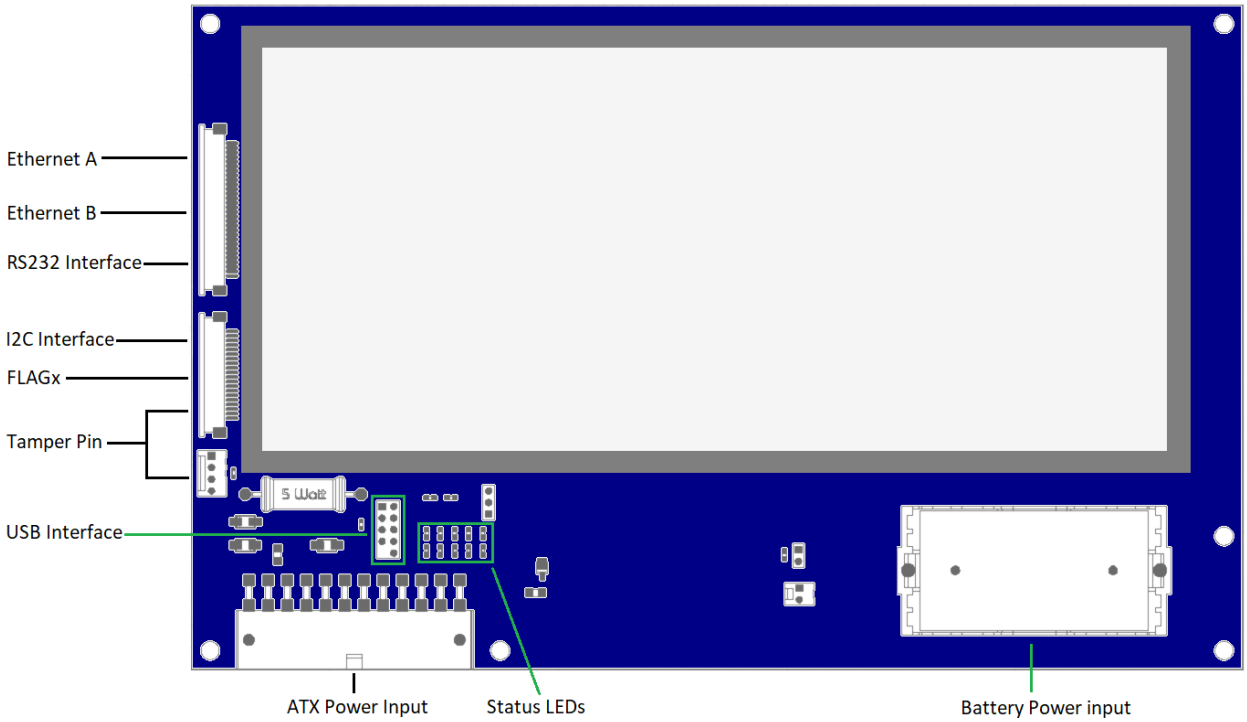

Figure 4: Cryptographic Module Interfaces

3.2 Trusted Channel Specification

The cryptographic module has two Ethernet Interfaces that are used as trusted channel, as identified in Section 3.1 - Ports and Interfaces. The physical path from these interfaces inside the cryptographic boundary is protected by all mechanisms described in Section 7 - Physical Security. The segment outside the cryptographic boundary to the external connector remains inside the equipment external enclosure, which features tamper-evident seals and a lid-open sensor that is monitored by the crypto-graphic module (as described in Section 7.1). The operator can use an ethernet cable directly attached to the connector interface to access the trusted channel.

All communication over the trusted channel is always encrypted and authenticated via the Transport Layer Security (TLS) protocol. The TLS implementation is configured to exclusively use cipher suites constructed from the following approved algorithms:

- Confidentiality: AES-CBC or AES-GCM
- Key Establishment: KAS-ECC-SSC
- Authenticity: RSA SigVer
- Key Derivation: KDF TLS
- Integrity and Hashing: SHA-256 or SHA-384

All services require identity-based authentication from the operator (Section 4) after the secure TLS channel is established.

The module indicates that the trusted channel is in use by the TLS channel establishment and generating a system log for every request, which records the operator's identity, their source address, and the service accessed.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password with KAS-ECC-SSC Sp800-56Ar3	User ID and password. The authentication data is encrypted using the TLS protocol. The password is composed of 6 or more alphanumeric characters, which may include both upper and lower case letters, punctuation marks, and symbols (such as @, &, and *). Each operator follows a Password Policy for its category that can be configured by the Administrators (PCOs and VCOs)	KAS-ECC-SSC Sp800-56Ar3 (A6066)	The worst-case scenario is a 6-character password, containing uppercase and lowercase characters, symbols or digits totaling 96 possibilities (10 digits, 52 letters and 34 symbols); thus, the probability that a random attempt will succeed is 1/96^6 = 1/782,757,789,696, much smaller than the required 1/1,000,000	The password authentication uses an exponential backoff delay on failed attempts for a given operator. After the first failure, a new attempt can be made after 1 s; 2 s after the second failure; 4 s after the third; 8 s after the fourth; and 16 s after the fifth. Therefore, the number of maximum possible attempts during a one-minute period is 7, given a probability of 7/782,757,789,696 = 1/111,822,541,385 which is smaller than the required 1/100,000
Password with KDF TLS	User ID and password. The authentication data is encrypted using the TLS protocol. The password is composed of 6 or more	KDF TLS (A6066)	The worst-case scenario is a 6-character password, containing uppercase and lowercase characters, symbols or digits totaling 96 possibilities (10 digits, 52 letters and	The password authentication uses an exponential backoff delay on failed attempts for a given operator. After the first failure, a new attempt can be made after 1 s; 2 s after the second

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	alphanumeric characters, which may include both upper and lower case letters, punctuation marks, and symbols (such as @, &, and *). Each operator follows a Password Policy for its category that can be configured by the Administrators (PCOs and VCOs)		34 symbols); thus, the probability that a random attempt will succeed is 1/96^6 = 1/782,757,789,696, much smaller than the required 1/1,000,000	failure; 4 s after the third; 8 s after the fourth; and 16 s after the fifth. Therefore, the number of maximum possible attempts during a one-minute period is 7, given a probability of 7/782,757,789,696 = 1/111,822,541,385 which is smaller than the required 1/100,000
mTLS Certificate with KAS-ECC-SSC Sp800-56Ar3	Private key and certificate for mTLS authentication. Both are used to enable client authentication according to the TLS protocol, in which a handshake message is digitally signed using the private key and the signature is sent to the module	KAS-ECC-SSC Sp800-56Ar3 (A6066)	The strength of the mechanism relies on the strength of the digital signature employed. The module will restrict the algorithm to 2048-bit RSA or larger; or 224-bit ECDSA or larger. These provide a 112-bit security level, therefore, the chance that a random attempt will succeed is roughly 1/2^112, much smaller than the required 1/1,000,000	The module is able to execute at most 30,000 verifications per second (less than that in practice, due to software overhead). Being optimistic and assuming 30,000, the chance that random attempts during a one-minute window will succeed is 30,000/2^112, which is roughly equal to 6/10^30 and much smaller than the required 1/100,000
mTLS Certificate with KDF TLS	Private key and certificate for mTLS authentication. Both are used to enable client authentication according to the TLS protocol, in	KDF TLS (A6066)	The strength of the mechanism relies on the strength of the digital signature employed. The module will restrict the algorithm to 2048-bit RSA or larger; or 224-bit	The module is able to execute at most 30,000 verifications per second (less than that in practice, due to software overhead). Being optimistic and assuming 30,000,

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	which a handshake message is digitally signed using the private key and the signature is sent to the module		ECDSA or larger. These provide a 112-bit security level, therefore, the chance that a random attempt will succeed is roughly 1/2^112, much smaller than the required 1/1,000,000	the chance that random attempts during a one-minute window will succeed is 30,000/2^112, which is roughly equal to 6/10^30 and much smaller than the required 1/100,000
Authentication Certificate	The operator must register a certificate in the module and use the corresponding private key to sign a token value provided by the module. The module checks the signature to allow the authentication	Key Generation	The operator must register a certificate in the module and use the corresponding private key to sign a token value provided by the module. The module checks the signature to allow the authentication. The strength of the mechanism is exactly the same as mTLS Certificate method	The strength of the mechanism is exactly the same as mTLS Certificate method
Session Token	The operator can request a session token to the module using another authentication method. Once generated, the token can be used to authenticate the user that requested it. The session token has an expiration time, configurable by the administrator, that is renewed every time the session token is used	Hash DRBG (A6066)	The chance that a random attempt will succeed is roughly 1/2^130, much smaller than the required 1/1,000,000	The timeframe to break the Session Token is similar to the timeframe to break a 128-bit AES Key

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Fastlane Token	The operator can request a fastlane token to the module using another authentication method. Different from session token, the fastlane token is associated with a specific user object and can be used to authenticate the user to use the specific object only	Hash DRBG (A6066)	The chance that a random attempt will succeed is roughly 1/2^128, much smaller than the required 1/1,000,000	The timeframe to break the Session Token is similar to the timeframe to break a 128-bit AES Key
Time-Based OTP	Multi-factor authentication mechanism. The operator must provide a 6-digit time-based OTP value when authenticating. The module checks if the OTP matches the expected value, which is calculated based in the current interval of time	HMAC-SHA-1 (A6066)	The operator must provide a 6-digit time-based OTP value when authenticating. The module checks if the OTP matches the expected value, which is calculated based in the current interval of time. The strength of the mechanism relies on the strength of HMAC-SHA1 with 160-bit key and of the OTP value itself (which changes every 30 seconds). The algorithm provides a 80-bit security level, therefore, the chance that a random attempt of guessing the key will succeed is roughly 1/2^80, much smaller than the required	Since the time-based OTP is subject to the same exponential backoff delay mentioned above, the number of maximum possible attempts during a one-minute period is 7, given a probability of 7/1,000,000 = 1/142,857 which is smaller than the required 1/100,000. In practice, since the code changes every 30 seconds, the odds are even lower

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			1/1,000,000. If the attacker tries to guess the OTP value itself, probability that a random attempt will succeed is the required 1/1,000,000	
HMAC-Based OTP	Multi-factor authentication mechanism. The operator must provide a hash-based OTP value when authenticating. The module checks if the OTP matches the expected value, which is calculated based in the number of successful requests done so far using the mechanism	HMAC-SHA-1 (A6066)	The operator must provide a hash-based OTP value when authenticating. The module checks if the OTP matches the expected value, which is calculated based in the number of successful requests done so far using the mechanism. The strength of the mechanism relies on the strength of HMACSHA1 with 160-bit key and of the OTP value itself (which changes after every successful login). The algorithm provides a 80-bit security level, therefore, the chance that a random attempt of guessing the key will succeed is roughly 1/2^80, much smaller than the required 1/1,000,000. If the attacker tries to guess the OTP value itself, probability that a random attempt will succeed is the required 1/1,000,000	Since the hash-based OTP is subject to the same exponential backoff delay mentioned above the number of maximum possible attempts during a one-minute period is 7, given a probability of 7/1,000,000 = 1/142,857 which is smaller than the required 1/100,000
Quorum	Multi-factor authentication mechanism.	Hash DRBG (A6066)	The strength of the mechanism relies on the strength of the	The strength of the mechanism relies on the strength of

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	The PHSM and the VHSMs can be configured to activate quorum authentication. The quorum authentication activation can be requested by any crypto officer, who defines a number M of crypto officers for the quorum. Then, M out of a total N crypto officers must authenticate themselves (with one of the above schemes) and agree to activate the quorum authentication for the PHSM or VHSM. Once the quorum authentication is activated, critical operations can only be executed if M out of N crypto officers allow it. To do that, the crypto officers must authenticate themselves using one of the methods above and allow the execution of the operation		above mechanisms and on the number M of operators in the quorum. M must always be equal or greater than half of the operators (N), rounded up	the above mechanisms and on the number M of operators in the quorum. M must always be equal or greater than half of the operators (N), rounded up

Table 11: Authentication Methods

The module enforces identity-based authentication, and each identity is mapped to a single role, where the user ID is used as the identification for identity-based authentication. The module also supports multi-factor authentication mechanisms. These mechanisms can't be used alone and must be combined with one more of the authentication methods listed above to authenticate the user. Similar to the authentication methods, it's the Crypto Officers that define which multi-factor mechanisms are mandatory. The module supports the following authentication methods.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Physical HSM Crypto Officer	Identity	Crypto Officer	Password with KAS-ECC-SSC Sp800-56Ar3 Password with KDF TLS mTLS Certificate with KAS-ECC-SSC Sp800-56Ar3 mTLS Certificate with KDF TLS Authentication Certificate Session Token Time-Based OTP HMAC-Based OTP Quorum
Virtual HSM Crypto Officer	Identity	Crypto Officer	Password with KAS-ECC-SSC Sp800-56Ar3 Password with KDF TLS mTLS Certificate with KAS-ECC-SSC Sp800-56Ar3 mTLS Certificate with KDF TLS Authentication Certificate Session Token Time-Based OTP HMAC-Based OTP Quorum
User	Identity	User	Password with KAS-ECC-SSC Sp800-56Ar3 Password with KDF TLS mTLS Certificate with KAS-ECC-SSC Sp800-56Ar3 mTLS Certificate with KDF TLS Authentication Certificate Session Token Fastlane Token Time-Based OTP

Name	Type	Operator Type	Authentication Methods
			HMAC-Based OTP Quorum

Table 12: Roles

The module supports three different roles: the Physical HSM Crypto Officer (PCO), the Virtual HSM Crypto Officer (VCO), and the User. A Virtual HSM (VHSM) is a logical security module implemented in the physical module. The physical module is referred as the Physical HSM (PHSM). Multiple VHSMs can be created in the PHSM and each VHSM has its own users and data, which cannot be accessed by other VHSMs.

- Physical HSM Crypto Officer (PCO): The most privileged role on the physical HSM; created when the physical HSM is initialized or by another PCO. It is responsible for the physical module management, which includes creation and deletion of virtual HSMs and firmware updates.
- Virtual HSM Crypto Officer (VCO): The most privileged role on the virtual HSM; created when the virtual HSM is initialized or by another VCO. It is responsible for the virtual HSM management, which includes the creation of users and altering the virtual module configurations.
- User: Created by a VCO, it is responsible for all cryptographic operations and management of cryptographic objects that it has ownership.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialize HSM	Initialize the HSM; create first PCO with provisory password (PIN)	IND-1	Temporary PIN and arguments	Initialization status	Digital Signature Generation Input-Output	Physical HSM Crypto Officer - Job Descriptor Key Encryption Key: G - PCO Initialization Password: W,E,Z - PCOs' Passwords: W,E,Z - PHSM Server CA Key: G - Master Key: E - PHSM Server

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G - PHSM Server CA Certificate: G - PHSM Client CA Key: G - PHSM Client CA Certificate: G Virtual HSM Crypto Officer - Job Descriptor Key Encryption Key: G - VCO Initialization Password: W,E,Z - VCOs' Passwords: W,E,Z - VCOs' Hashed Passwords: G,Z - VHSM Server CA Certificate: G - VHSM Client CA Certificates: G
Configure Network	Configure network settings (IP, netmask, gateway (optional), DNS (optional))	IND-1	Network arguments	Configured network settings	None	Physical HSM Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Network Configuration	Get network setting	IND-1	-	Network Configuration	None	Physical HSM Crypto Officer
Reset HSM	Reset HSM to factory state	IND-1	-	HSM in Factory State	None	Physical HSM Crypto Officer - Job Descriptor Key Encryption Key: Z - PHSM Server CA Key: Z - PHSM Server CA Certificate: Z - PCO Initialization Password: Z - PCOs' Temporary Password: Z - PCOs' Hashed Passwords: Z - PCOs' Certificate Fingerprints: Z - PCO's OTP Key: Z - PCO's OTP: Z - VHSM Server CA Key: Z - VHSM Server CA Certificate: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- VHSM Server Keys: Z - VHSM Server Certificates: Z - VHSM Client CA Keys: Z - VHSM Client CA Certificates: Z - VCO Initialization Password: Z - VCOs' Passwords: Z - VCOs' Hashed Passwords: Z - VCOs' Certificate Fingerprints: Z - VCO's OTP Key: Z - VCO's OTP: Z - Users' Temporary Password (Pin): Z - Users' Passwords: Z - Users' Hashed Passwords: Z - Users' Certificate Fingerprint

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						s: Z - User's OTP Key: Z - User's OTP: Z - Users' RSA Private Key: Z - Users' RSA Public Key: Z - Users' ECDSA Private Key: Z - Users' ECDSA Public Key: Z - Users' EDDSA Private Key: Z - Users' EDDSA Public Key: Z - Users' ML-DSA Private Key: Z - Users' ML-DSA Public Key: Z - Users' ML-KEM Private Key: Z - Users' ML-KEM Public Key: Z - Users' AES Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Users' HMAC Key: Z - Users' Certificate: Z - ECDH Private Component (ephemeral): Z - ECDH Public Component (ephemeral): Z - TLS Peer Public Key: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - TLS Session Key: Z - TLS Authentication Key: Z - DRBG C and V values: Z - Disk Encryption Key: Z - Cluster TLS CA Private Key: Z - Cluster TLS CA Certificate: Z - Cluster TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Server Private Key: Z - Cluster TLS Server Certificate: Z - Cluster TLS Client Private Key: Z - Cluster TLS Client Certificate: Z - Cluster Secret: Z - Authentication Certificate: Z - Authentication Certificate Challenge: Z - Authentication Certificate Response: Z - Session Token: Z - Fastlane ID: Z - Fastlane Secret: Z - Quorum Secret: Z - Quorum Secret Share: Z - DRBG Entropy Input: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed: Z - PHSM Server Key: Z - PHSM Server Certificate: Z - PHSM Client CA Key: Z - PHSM Client CA Certificate: Z
Set Date Time	Set the current date and time	IND-1	Date, time and arguments	Set Date Time	None	Physical HSM Crypto Officer
Get Date Time	Get the current date and time	IND-1	Get Date Time arguments	Current Date Time	None	Physical HSM Crypto Officer
Get HSM Usage	Get CPU, RAM and disk usage	IND-1	Get HSM Usage arguments	Current HSM Usage	None	Physical HSM Crypto Officer
Create User	Create a PCO, VCO or User	IND-1	New user information and arguments	New User Temporary Password	Deterministic Random Number Generator Input-Output	Physical HSM Crypto Officer - PCOs' Temporary Password: G - Users' Temporary Password (Pin): G Virtual HSM Crypto Officer - VCOs' Temporary Password: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Users' Temporary Password (Pin): G
Delete User	Destroy a PCO, VCO or User	IND-1	User Unique Identifier and arguments	Deleted User	None	Physical HSM Crypto Officer - PCOs' Hashed Passwords: Z - PCOs' Certificate Fingerprints: Z - PCO's OTP: Z - Users' Hashed Passwords: Z - Users' Certificate Fingerprints: Z - User's OTP Key: Z - Authentication Certificate: Z - Quorum Secret Share: Z Virtual HSM Crypto Officer - VCOs' Hashed Passwords: Z - VCOs' Certificate Fingerprints: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- VCO's OTP: Z - Users' Hashed Passwords: Z - Users' Certificate Fingerprints: Z - User's OTP Key: Z - Users' RSA Private Key: Z - Users' RSA Public Key: Z - Users' ECDSA Private Key: Z - Users' ECDSA Public Key: Z - Users' EDDSA Private Key: Z - Users' EDDSA Public Key: Z - Users' ML-DSA Private Key: Z - Users' ML-DSA Public Key: Z - Users' ML-KEM Private Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Users' ML-KEM Public Key: Z - Users' AES Key: Z - Users' HMAC Key: Z - Users' Certificate: Z - Authentication Certificate: Z - Quorum Secret Share: Z
List Users	List PCOs, VCOs or Users	IND-1	List User Arguments	List of PCOs, VCOs or Users	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Change Password	Change a PCO, VCO or User's password. It's used to activate the user in its first time performing this operation	IND-1	Temporary Password and arguments	Status return	Digital Signature Verification Input-Output	Physical HSM Crypto Officer - PCOs' Temporary Password: W,E,Z - PCOs' Passwords: W,E,Z - PCOs' Hashed Passwords: W,E,Z - Users' Temporary Password (Pin):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E,Z - Users' Passwords: W,E,Z - Users' Hashed Passwords: G,E,Z Virtual HSM Crypto Officer - VCOs' Temporary Password: W,E,Z - VCOs' Passwords: W,E,Z - VCOs' Hashed Passwords: G,E,Z - Users' Temporary Password (Pin): W,E,Z - Users' Passwords: W,E,Z - Users' Hashed Passwords: E,Z User - Users' Temporary Password (Pin): W,E,Z - Users' Passwords: W,E,Z - Users' Hashed Passwords: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Reset Password	Reset a PCO, VCO or User's password. When a User's password is reset, it deactivates the user, until their password is set again	IND-1	Reset arguments	Temporary Password	Deterministic Random Number Generator Secure Hash (Message Digest) Input-Output	Physical HSM Crypto Officer - PCOs' Temporary Password: G,R - Users' Temporary Password (Pin): G,R - PCOs' Hashed Passwords: G,Z - PCOs' Certificate Fingerprints: Z - PCO's OTP Key: Z - Users' Hashed Passwords: G,Z - Users' Certificate Fingerprints: Z - User's OTP Key: Z - Authentication Certificate: Z - Quorum Secret Share: Z Virtual HSM Crypto Officer - VCOs' Temporary Password:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,R - Users' Temporary Password (Pin): G,R - VCOs' Hashed Passwords: G,Z - VCOs' Certificate Fingerprints: Z - VCO's OTP Key: Z - Users' Hashed Passwords: Z - Users' Certificate Fingerprints: Z - User's OTP Key: Z - Users' RSA Private Key: Z - Users' RSA Public Key: Z - Users' ECDSA Private Key: Z - Users' ECDSA Public Key: Z - Users' EDDSA Private Key: Z - Users' EDDSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: Z - Users' ML-DSA Private Key: Z - Users' ML-DSA Public Key: Z - Users' ML-KEM Private Key: Z - Users' ML-KEM Public Key: Z - Users' AES Key: Z - Users' HMAC Key: Z - Users' Certificate: Z - Authentication Certificate: Z - Quorum Secret Share: Z User - Users' Temporary Password (Pin): G,R - Users' Hashed Passwords: G,Z - Users' Certificate Fingerprints: Z - User's

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						OTP Key: Z
Register Certificate	Sign a CSR and register the certificate for PCO, VCO or User authentication	IND-1	Certificate and arguments	Registered Certificate	Digital Signature Generation	Physical HSM Crypto Officer - PCOs' Certificate Fingerprints: W,Z - Users' Certificate Fingerprints: W,Z - PHSM Client CA Key: E - PHSM Client CA Certificate: E Virtual HSM Crypto Officer - VCOs' Certificate Fingerprints: W,Z - Users' Certificate Fingerprints: W,Z User - Users' Certificate Fingerprints: W,Z
Activate Quorum Authentication	Activates quorum authentication for the PHSM, VHSM or a Object	IND-1	Activate Quorum Authentication arguments	Activated Quorum Authentication	Deterministic Random Number Generator	Physical HSM Crypto Officer - Quorum Secret: G - Quorum Secret Share: G Virtual HSM

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Crypto Officer - Quorum Secret: G - Quorum Secret Share: G User - Quorum Secret: G - Quorum Secret Share: G
Deactivate Quorum Authentication	Deactivates quorum authentication for the PHSM	IND-1	Deactivate Quorum Authentication arguments	Deactivated Quorum Authentication	Data Decryption	Physical HSM Crypto Officer - Quorum Secret: Z - Quorum Secret Share: Z Virtual HSM Crypto Officer - Quorum Secret: Z - Quorum Secret Share: Z User - Quorum Secret: Z - Quorum Secret Share: Z
Get Quorum Authentication State	Check the quorum authentication state of the PHSM (i.e. activated or not, the minimum quorum)	IND-1	Get Quorum Authentication State arguments	Quorum Authentication State	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Quorum Authentication Status	Check the quorum authentication status of the PHSM (i.e. number of operations or time left)	IND-1	Get Quorum Authentication Status arguments	Quorum Authentication Status	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Vote Quorum Authentication	Inform the operator's verdict for quorum authentication operations (allow or deny)	IND-1	Vote Quorum Authentication arguments	Voted Quorum Authentication	Data Encryption Data Decryption Input-Output	Physical HSM Crypto Officer - PCOs' Passwords: W,E,Z - Users' Passwords: W,E,Z - Quorum Secret: W - Quorum Secret Share: G,E Virtual HSM Crypto Officer - VCOs' Passwords: W,E,Z - Users' Passwords: W,E,Z - Quorum Secret: W - Quorum Secret Share: G,E User - Users' Passwords: W,E,Z - Quorum Secret: W - Quorum Secret

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Share: G,E
Start Quorum Authentication	Request that operators vote to start quorum authentication votes to allow critical operations	IND-1	Start Quorum Authentication arguments	Started Quorum Authentication	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Stop Quorum Authentication	Stop quorum authentication, blocking critical operations when quorum authentication is activated (a new start is required)	IND-1	Stop Quorum Authentication	Stopped Quorum Authentication	None	Physical HSM Crypto Officer - Quorum Secret: Z Virtual HSM Crypto Officer - Quorum Secret: Z User - Quorum Secret: Z
Create Virtual HSM	Create a Virtual HSM along with its first VCO with provisory password (PIN)	IND-1	Virtual HSM information and arguments	Created Virtual HSM information	Deterministic Random Number Generator Input-Output	Physical HSM Crypto Officer - VCO Initialization Password: G,R,Z
List Virtual HSMs	List all Virtual HSMs	IND-1	List Virtual HSMs arguments	List of Virtual HSMs	None	Physical HSM Crypto Officer
Activate Virtual HSM	Activate a Virtual HSM	IND-1	Activate Virtual HSM arguments	Activated Virtual HSM	None	Physical HSM Crypto Officer
Deactivate Virtual HSM	Deactivate a Virtual HSM	IND-1	Deactivate Virtual HSM arguments	Deactivated Virtual HSM	None	Physical HSM Crypto Officer - VCO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Initialization Password: Z - VCOs' Temporary Password: Z - VCOs' Passwords: Z - VCO's OTP: Z - Users' Temporary Password (Pin): Z - Users' Passwords: Z - User's OTP: Z - ECDH Private Component (ephemeral): Z - ECDH Public Component (ephemeral): Z - TLS Peer Public Key: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - TLS Session Key: Z - TLS Authentication Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Authentication Certificate Challenge: Z - Authentication Certificate Response: Z - Session Token: Z - Fastlane ID: Z - Fastlane Secret: Z - Quorum Secret: Z
Delete Virtual HSM	Delete a Virtual HSM and all of its objects	IND-1	Delete Virtual HSM arguments	Deleted Virtual HSM	None	Physical HSM Crypto Officer - VHSM Server CA Key: Z - VHSM Server CA Certificate: Z - VHSM Server Keys: Z - VHSM Server Certificates: Z - VHSM Client CA Keys: Z - VHSM Client CA Certificates: Z - VCOs' Hashed Passwords: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- VCOs' Certificate Fingerprints: Z - VCO's OTP Key: Z - Users' Hashed Passwords: Z - Users' Certificate Fingerprints: Z - User's OTP Key: Z - Users' RSA Private Key: Z - Users' RSA Public Key: Z - Users' ECDSA Private Key: Z - Users' ECDSA Public Key: Z - Users' EDDSA Private Key: Z - Users' EDDSA Public Key: Z - Users' ML-DSA Private Key: Z - Users' ML-DSA Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - Users' ML-KEM Private Key: Z - Users' ML-KEM Public Key: Z - Users' AES Key: Z - Users' HMAC Key: Z - Users' Certificate: Z - Authentication Certificate: Z - Quorum Secret Share: Z
Edit Virtual HSM	Edit a VHSM configuration	IND-1	Edit Virtual HSM arguments	Edited Virtual HSM	None	Physical HSM Crypto Officer
Export VHSM	Export an entire Virtual HSM; its users and objects	IND-1	Export VHSM arguments	Exported VHSM encrypted package	Data Encryption Deterministic Random Number Generator Digital Signature Generation Input-Output	Physical HSM Crypto Officer - VHSM Server CA Key: R - VHSM Server CA Certificate: R - VHSM Server Keys: R - VHSM Server Certificates: R - VHSM

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Client CA Keys: R - VHSM Client CA Certificates: R - VCOs' Hashed Passwords: R - VCOs' Certificate Fingerprints: R - VCO's OTP Key: R - Users' Hashed Passwords: R - Users' Certificate Fingerprints: R - User's OTP Key: R - Users' RSA Private Key: R - Users' RSA Public Key: R - Users' ECDSA Private Key: R - Users' ECDSA Public Key: R - Users' EDDSA Private Key: R - Users'

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						EDDSA Public Key: R - Users' ML-DSA Private Key: R - Users' ML-DSA Public Key: R - Users' ML-KEM Private Key: R - Users' ML-KEM Public Key: R - Users' AES Key: R - Users' HMAC Key: R - Users' Certificate: R - Authentication Certificate: R - Quorum Secret Share: R - Disk Encryption Key: E - Kryptus kNET CA Certificate: E - PHSM Module Key: E - PHSM Module

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Certificate: E
Import VHSM	Import an entire Virtual HSM	IND-1	Import VHSM encrypted package and arguments	Status return	Data Decryption Digital Signature Generation Input-Output	Physical HSM Crypto Officer - VHSM Server CA Key: W - VHSM Server CA Certificate: W - VHSM Server Keys: W - VHSM Server Certificates: W - VHSM Client CA Keys: W - VHSM Client CA Certificates: W - VCOs' Hashed Passwords: W - VCOs' Certificate Fingerprints: W - VCO's OTP Key: W - Users' Hashed Passwords: W - Users' Certificate Fingerprints: W - User's OTP Key: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Users' RSA Private Key: W - Users' RSA Public Key: W - Users' ECDSA Private Key: W - Users' ECDSA Public Key: W - Users' EDDSA Private Key: W - Users' EDDSA Public Key: W - Users' ML-DSA Private Key: W - Users' ML-DSA Public Key: W - Users' ML-KEM Private Key: W - Users' ML-KEM Public Key: W - Users' AES Key: W - Users' HMAC Key: W - Users' Certificate: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Authentication Certificate: W - Quorum Secret Share: W - PHSM Module Key: E - PHSM Module Certificate: E - Disk Encryption Key: E - Kryptus kNET CA Certificate: E
Export PHSM	Export an entire Physical HSM, its users and VHMs	IND-1	Export PHSM arguments	Exported PHSM encrypted package	Data Encryption Deterministic Random Number Generator Digital Signature Generation Input-Output	Physical HSM Crypto Officer - PHSM Module Key: R,E - PHSM Module Certificate: E - Quorum Secret Share: R - Authentication Certificate: R - Cluster TLS CA Certificate: R - Cluster TLS Server Certificate:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						R - Cluster TLS Client Certificate: R - Cluster Secret: R - VHSM Client CA Keys: R - VHSM Client CA Certificates: R - VHSM Server CA Certificate: R - PHSM Server CA Certificate: R - PHSM Server CA Key: R - PCOs' Hashed Passwords: R - PCOs' Certificate Fingerprints: R - PCO's OTP Key: R - VHSM Server CA Key: R - VHSM Server Keys: R - Users' Hashed Passwords: R - Users' Certificate Fingerprint

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						s: R - User's OTP Key: R - Users' RSA Private Key: R - Users' RSA Public Key: R - Users' ECDSA Private Key: R - Users' ECDSA Public Key: R - Users' EDDSA Private Key: R - Users' EDDSA Public Key: R - Users' ML-DSA Private Key: R - Users' ML-DSA Public Key: R - Users' ML-KEM Private Key: R - Users' ML-KEM Public Key: R - Users' AES Key: R - Users' HMAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: R - Users' Certificate: R - Disk Encryption Key: R - Cluster TLS CA Private Key: R - Cluster TLS Server Private Key: R - Cluster TLS Client Private Key: R
Import PHSM	Import an entire Physical HSM	IND-1	Import PHSM encrypted package and arguments	Status return	Data Decryption Digital Signature Verification Input-Output	Physical HSM Crypto Officer - Kryptus kNET CA Certificate: E - PHSM Module Key: E - PHSM Module Certificate: W,E - PHSM Server CA Key: W - PHSM Server CA Certificate: W - PCOs' Hashed Passwords: W - PCOs' Certificate Fingerprint

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						s: W - PCO's OTP Key: W - VHSM Server CA Key: W - VHSM Server CA Certificate: W - VHSM Server Keys: W - VHSM Server Certificates: W - VCOs' Hashed Passwords: W - VCOs' Certificate Fingerprints: W - VCO's OTP Key: W - Cluster TLS CA Private Key: W - Cluster TLS CA Certificate: W - Cluster TLS Server Private Key: W - Cluster TLS Server Certificate: W - Cluster TLS Client

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: W - Cluster TLS Client Certificate: W - Cluster Secret: W - Disk Encryption Key: W - Authentication Certificate: W - Quorum Secret Share: W - Users' Hashed Passwords: W - Users' Certificate Fingerprints: W - User's OTP Key: W - Users' RSA Private Key: W - Users' RSA Public Key: W - Users' ECDSA Private Key: W - Users' ECDSA Public Key: W - Users' EDDSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W - Users' EDDSA Public Key: W - Users' ML-DSA Private Key: W - Users' ML-DSA Public Key: W - Users' ML-KEM Private Key: W - Users' ML-KEM Public Key: W - Users' AES Key: W - Users' HMAC Key: W - Users' Certificate: W - Master Key: E
Get Requester Type	Get the role of the requester	IND-1	Get Requester Type arguments	Requester Type	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Update Firmware	Update the module firmware. Any firmware loaded into this module that is not	IND-1	Update Firmware encrypted package and arguments	Status return; Updated Firmware	Digital Signature Generation Secure Hash (Message Digest)	Physical HSM Crypto Officer - PHSM Module Key: E - PHSM

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140- 3 validation					Module Certificate: E
Get Log Level	Get the current log level	IND-1	Get Log Level arguments	Log Level	None	Physical HSM Crypto Officer
Set Log Level	Set the current log level	IND-1	Set Log Level arguments	Log Level set	None	Physical HSM Crypto Officer
Get System Log	Retrieve the PHSM log	IND-1	Get System Log arguments	System Log file	Digital Signature Generation Secure Hash (Message Digest)	Physical HSM Crypto Officer - PHSM Module Key: E
Show Status	Get the status of the HSM	IND-1	Show Status arguments	Status	None	Physical HSM Crypto Officer
Shutdown	Shutdown the HSM	IND-1	Shutdown arguments	-	None	Physical HSM Crypto Officer - PCO Initialization Password: Z - PCOs' Temporary Password: Z - PCOs' Passwords: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PCO's OTP: Z - VCO Initialization Password: Z - VCOs' Temporary Password: Z - VCOs' Passwords: Z - VCO's OTP: Z - Users' Temporary Password (Pin): Z - Users' Passwords: Z - User's OTP: Z - ECDH Private Component (ephemeral): Z - ECDH Public Component (ephemeral): Z - TLS Peer Public Key: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - TLS Session Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Authentication Key: Z - Authentication Certificate Challenge: Z - Authentication Certificate Response: Z - Session Token: Z - Fastlane ID: Z - Fastlane Secret: Z - Quorum Secret: Z
Restart	Restart the HSM and Perform self-tests on demand	IND-1	Restart arguments	-	Data Decryption Deterministic Random Number Generator Digital Signature Verification Key Generation	Physical HSM Crypto Officer - Job Descriptor Key Encryption Key: G - PCO Initialization Password: G - DRBG C and V values: G - Super Root Key Hash: E - PCOs' Temporary Password: Z - PCOs' Passwords

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						: Z - PCO's OTP: Z - VCO Initialization Password: Z - VCOs' Temporary Password: Z - VCOs' Passwords : Z - VCO's OTP: Z - Users' Temporary Password (Pin): Z - Users' Passwords : Z - User's OTP: Z - ECDH Private Component (ephemeral): Z - ECDH Public Component (ephemeral): Z - TLS Peer Public Key: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - TLS Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - TLS Authentication Key: Z - Authentication Certificate Challenge: Z - Authentication Certificate Response: Z - Session Token: Z - Fastlane ID: E - Fastlane Secret: E - Quorum Secret: E - DRBG Entropy Input: G - DRBG Seed: G
Boot	Boot process before main services are available	IND-1	-	-	Data Decryption Deterministic Random Number Generator Digital Signature Verification Key Generation	Physical HSM Crypto Officer - Job Descriptor Key Encryption Key: G - PCO Initialization Password: G - DRBG C and V values: G - Super Root Key Hash: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Entropy Input: G - DRBG Seed: G - Master Key: E
Get Device Information	Get device version, status, serial number and other information	IND-1	Get Device Information arguments	Device Information	None	Physical HSM Crypto Officer
Get TLS Certificate	Get the TLS certificate of the PHSM server and the corresponding CA	IND-1	Get TLS Certificate arguments	TLS Certificate	Input-Output	Physical HSM Crypto Officer - PHSM Server CA Key: R - PHSM Server CA Certificate: R - PHSM Server Certificate: R Virtual HSM Crypto Officer - VHSM Server CA Key: R - VHSM Server CA Certificate: R
Renew Server Certificate	Renew the PHSM server TLS certificate	IND-1	Renew Server Certificate arguments	Renewed Server Certificate	Key Generation Input-Output	Physical HSM Crypto Officer - PHSM Server CA Certificate: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PHSM Server Certificate: G Virtual HSM Crypto Officer - VHSM Server Certificates: G,R,Z
Activate OTP	Activate OTP for the PCO, VCO or User	IND-1	Activate OTP arguments	Activated OTP	Key Generation Message Authentication Input-Output	Physical HSM Crypto Officer - PCO's OTP Key: G,R - PCO's OTP: G,W - User's OTP Key: G,R - User's OTP: G,W - DRBG C and V values: E - DRBG Entropy Input: E - DRBG Seed: E Virtual HSM Crypto Officer - VCO's OTP Key: G,R - VCO's OTP: G,W - User's OTP Key: G,R - User's OTP: G,W - DRBG C

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						and V values: E - DRBG Entropy Input: E - DRBG Seed: E User - User's OTP Key: G,R - User's OTP: G,W - DRBG C and V values: E - DRBG Entropy Input: E - DRBG Seed: E
Manual Activate OTP	Manually activate OTP for the PCO, VCO or User informing the OTP key	IND-1	Manual Activate OTP arguments	Manually Activated OTP	Message Authentication	Physical HSM Crypto Officer - PCO's OTP Key: W - PCO's OTP: G,W - User's OTP Key: W - User's OTP: G,W Virtual HSM Crypto Officer - VCO's OTP Key: W - VCO's OTP: G,W - User's OTP Key: W - User's OTP: G,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						User - User's OTP Key: W - User's OTP: G,W
Deactivate OTP	Deactivates OTP for the PCO, VCO or User	IND-1	Deactivate OTP arguments	Deactivated OTP	None	Physical HSM Crypto Officer - PCO's OTP Key: Z - User's OTP Key: Z Virtual HSM Crypto Officer - VCO's OTP Key: Z - User's OTP Key: Z User - User's OTP Key: Z
Register Authentication Certificate	Register a certificate to be used during PCO, VCO or User authentication	IND-1	Register Authentication Certificate arguments	Registered Authentication Certificate	Digital Signature Verification Input-Output	Physical HSM Crypto Officer - Authentication Certificate: W Virtual HSM Crypto Officer - Authentication Certificate: W User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Authentication Certificate: W
Remove Authentication Certificate	Delete a certificate used for authentication	IND-1	Remove Authentication Certificate arguments	Removed Authentication Certificate	None	Physical HSM Crypto Officer - Authentication Certificate: Z Virtual HSM Crypto Officer - Authentication Certificate: Z User - Authentication Certificate: Z
List Authentication Certificates	List the registered certificates for the PCO, VCO or User	IND-1	List Authentication Certificates arguments	List of Authentication Certificates	None	Physical HSM Crypto Officer - Authentication Certificate: R Virtual HSM Crypto Officer - Authentication Certificate: R User -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Certificate: R
Get Session Credential	Retrieves a session token used for further authentications	IND-1	Get Session Credential arguments	Session Credential	Input-Output	Physical HSM Crypto Officer - Session Token: R Virtual HSM Crypto Officer - Session Token: R User - Session Token: R
Upload Logo Image	Uploads a logo image for the kNET frontal board	IND-1	Upload Logo Image arguments	Uploaded Logo Image	None	Physical HSM Crypto Officer
Get SNMP Data	Retrieves SNMP Data	IND-1	Get SNMP Data arguments	SNMP Data	None	Physical HSM Crypto Officer
Set SNMP Data	Sets up the kNET SNMP Agent as well as some information it provides	IND-1	Set SNMP Data arguments	Set SNMP Data	None	Physical HSM Crypto Officer
Delete Session Credential	Deletes the user session credential cached on server	IND-1	Delete Session Credential arguments	Deleted Session Credential	None	Physical HSM Crypto Officer - Session Token: Z Virtual HSM Crypto Officer - Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Token: Z User - Session Token: Z
Start Token Authentication	Starts a token authentication	IND-1	Start Token Authentication arguments	Started Token Authentication	Input-Output	Physical HSM Crypto Officer - Authentication Certificate Challenge: R Virtual HSM Crypto Officer - Authentication Certificate Challenge: R User - Authentication Certificate Challenge: R
Set Password Policy	Changes authentication restrictions	IND-1	Set Password Policy arguments	Password Policy set	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer
Get Password Policy	Retrieves the current password policy for a specific user	IND-1	Get Password Policy arguments	Password Policy information	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Activate NTP Service	Activates the NTP service	IND-1	Activate NTP Service arguments	Activated NTP Service	None	Physical HSM Crypto Officer
Deactivate NTP Service	Deactivates the NTP service	IND-1	Deactivate NTP Service arguments	Deactivated NTP Service	None	Physical HSM Crypto Officer
Get NTP Service Info	Retrieves the current status of the NTP Service in the HSM	IND-1	Get NTP Service Info arguments	NTP Service Info	None	Physical HSM Crypto Officer
Activate Remote Syslog	Activates the Remote System Log	IND-1	Activate Remote Syslog arguments	Activated Remote Syslog	None	Physical HSM Crypto Officer
Deactivate Remote Syslog	Deactivates the Remote System Log	IND-1	Deactivate Remote Syslog arguments	Deactivated Remote Syslog	None	Physical HSM Crypto Officer
Get Remote Syslog	Retrieves the current status of the Remote System Log in the HSM	IND-1	Get Remote Syslog arguments	Remote Syslog status	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Set Unauthenticated Get System Log Permission	Updates the permission for unauthenticated execution of the Get System Log operation	IND-1	Set Unauthenticated Get System Log Permission arguments	Unauthenticated Get System Log Permission set	Data Encryption None	Physical HSM Crypto Officer Virtual HSM Crypto Officer
Get Unauthenticated Get System Log Permission	Retrieves the current status of the permission for unauthenticated execution of	IND-1	Get Unauthenticated Get System Log Permission arguments	Unauthenticated Get System Log Permission status	None	Physical HSM Crypto Officer Virtual HSM Crypto

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the Get System Log operation					Officer User
Optimize Database	Drops and recreates all tables to reclaim disk space remnant from delete operations	IND-1	Optimize Database arguments	Optimized Database	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer
Query Operation	Retrieves information about the HSM	IND-1	Query Operation arguments	Queried Operation	None	Physical HSM Crypto Officer - PHSM Module Certificate: R Virtual HSM Crypto Officer User
Get Firmware Update Status	Retrieves the current status of an ongoing firmware update operation	IND-1	Get Firmware Update Status arguments	Firmware Update Status	None	Physical HSM Crypto Officer
Get Requester Info	Retrieves information about the requester from the system	IND-1	Get Requester Info arguments	Requester Info	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Set Authentication Policy	Sets the authentication policy for Users, VCOs and PCOs	IND-1	Set Authentication Policy arguments	Authentication Policy set	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Authentication Policy	Retrieves the authentication policy for Users, VCOs and PCOs	IND-1	Get Authentication Policy arguments	Authentication Policy	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Create Cluster	Initializes a database synchronization cluster	IND-1	Create Cluster arguments	Created Cluster	Digital Signature Generation Key Generation	Physical HSM Crypto Officer - Cluster TLS CA Private Key: G - Cluster TLS CA Certificate: G - Cluster TLS Server Private Key: G - Cluster TLS Server Certificate: G - Cluster TLS Client Private Key: G - Cluster TLS Client Certificate: G - Cluster Secret: G
Prepare Join Cluster	Prepares a node to join in the cluster	IND-1	Prepare Join Cluster arguments	Join Cluster encrypted package	Data Encryption Digital Signature Generation Input-Output	Physical HSM Crypto Officer - Cluster TLS CA Private Key: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Cluster TLS CA Certificate: R - Cluster TLS Server Private Key: R - Cluster TLS Server Certificate: R - Cluster TLS Client Private Key: R - Cluster TLS Client Certificate: R - Cluster Secret: R
Join Cluster	Allows a HSM to join an existing cluster	IND-1	Join encrypted package and arguments	Joined Cluster	Data Decryption Digital Signature Verification Input-Output	Physical HSM Crypto Officer - Cluster TLS CA Private Key: W - Cluster TLS CA Certificate: W - Cluster TLS Server Private Key: W - Cluster TLS Server Certificate: W - Cluster TLS Client Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W - Cluster TLS Client Certificate: W - Cluster Secret: W
Get Session Timeout	Retrieves the current session timeout	IND-1	Get Session Timeout arguments	Session Timeout	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Set Session Timeout	Sets the session timeout with minutes precision	IND-1	Set Session Timeout arguments	Session Timeout set	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer
Leave Cluster	Leaves the existing cluster	IND-1	Leave Cluster arguments	The HSM is no longer part of the cluster	None	Physical HSM Crypto Officer - Kryptus kNET CA Certificate: Z - PHSM Module Key: Z - PHSM Server CA Certificate: Z - VHSM Server CA Certificate: Z - VHSM Server Certificates: Z - VHSM

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Client CA Certificates: Z - Cluster TLS CA Certificate: Z - Cluster TLS Server Certificate: Z - Cluster TLS Client Certificate: Z - Cluster Secret: Z - Authentication Certificate: Z - Quorum Secret Share: Z - PCO Initialization Password: Z - PCOs' Temporary Password: Z - PCOs' Passwords: Z - PCO's OTP: Z - VCO Initialization Password: Z - VCOs' Temporary Password: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- VCOs' Passwords: Z - VCO's OTP: Z - Users' Temporary Password (Pin): Z - Users' Passwords: Z - User's OTP: Z - ECDH Private Component (ephemeral): Z - ECDH Public Component (ephemeral): Z - TLS Peer Public Key: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - TLS Session Key: Z - TLS Authentication Key: Z - Authentication Certificate Challenge: Z - Authentica

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						tion Certificate Response: Z - Session Token: Z - Fastlane ID: Z - Fastlane Secret: Z - Quorum Secret: Z
Get Cluster Status	Retrieves the cluster status	IND-1	Get Cluster Status arguments	Cluster Status	None	Physical HSM Crypto Officer Virtual HSM Crypto Officer User
Configure Cluster	Updates the cluster configuration	IND-1	Configure Cluster arguments	Configured Cluster	None	Physical HSM Crypto Officer
Cancel Backup	Stops the execution of any ongoing Import Physical HSM	IND-1	Cancel Backup arguments	-	None	Physical HSM Crypto Officer
Change kNET State	Updates the state of the HSM	IND-1	Change kNET State arguments	Changed kNET State	None	Physical HSM Crypto Officer
Get Virtual HSM Usage	Get VHSM CPU, RAM and disk usage	IND-1	Get Virtual HSM Usage arguments	Virtual HSM Usage information	None	Virtual HSM Crypto Officer
Activate User	Activate a User (This is embedded in Change Password Operation)	IND-1	Activate User arguments	Activated User	None	Virtual HSM Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Deactivate User	Deactivate a User (This is embedded in Reset Password Operation)	IND-1	Deactivate User arguments	Deactivated User	None	Virtual HSM Crypto Officer
Change Operator Permission	This operation changes the permissions of a user	IND-1	Change Operator Permission arguments	Changed Operator Permission	None	Virtual HSM Crypto Officer
Approve Backup Import	This operation approves an imported Virtual HSM to enter the Operational State	IND-1	Approve Backup Import arguments	Backup Import approved	None	Virtual HSM Crypto Officer
Discover Versions	Determine a list of supported protocol versions by the server	IND-1	Discover Versions arguments	Discovered Versions	None	Virtual HSM Crypto Officer User
Create	Create a symmetric key within the VHSM	IND-1	Create arguments	Key UID	Symmetric Key Generation	User - Users' AES Key: G - Users' HMAC Key: G
Create Key Pair	Create asymmetric key pair in the VHSM	IND-1	Create Key Pair arguments	Key Pair UIDs	Key Generation	User - Users' RSA Private Key: G - Users' RSA Public Key: G - Users' ECDSA Private Key: G - Users' ECDSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: G - Users' EDDSA Private Key: G - Users' EDDSA Public Key: G - Users' ML-DSA Private Key: G - Users' ML-DSA Public Key: G - Users' ML-KEM Private Key: G - Users' ML-KEM Public Key: G
Add Attribute	Add a single attribute to an object	IND-1	Add Attribute arguments	Attribute added	None	User
Get Attributes	Retrieve attribute values of an object	IND-1	Get Attributes arguments	List of Attributes values	None	User
Get Attributes List	Retrieve attributes of an object	IND-1	Get Attributes List arguments	List of Attributes names	None	User
Modify Attribute	Modify an attribute value	IND-1	Modify Attribute arguments	Modified Attribute	None	User
Delete Attribute	Delete an attribute value of an object	IND-1	Delete Attribute arguments	Deleted attribute	None	User
Revoke	Revoke object	IND-1	Revoke arguments	Revoked object UID	None	User
Activate	Activate object	IND-1	Activate arguments	Activated object UID	None	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Destroy	Destroy object	IND-1	Destroy arguments	Destroyed object UID	None	User - Users' RSA Private Key: Z - Users' RSA Public Key: Z - Users' ECDSA Private Key: Z - Users' ECDSA Public Key: Z - Users' EDDSA Private Key: Z - Users' EDDSA Public Key: Z - Users' ML-DSA Private Key: Z - Users' ML-DSA Public Key: Z - Users' ML-KEM Private Key: Z - Users' ML-KEM Public Key: Z - Users' AES Key: Z - Users' HMAC Key: Z - Users'

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Certificate: Z
Locate	Locate an object given its attributes	IND-1	Locate arguments	Located object(s) UIDs	None	User
Check	Check usage quota of an object	IND-1	Check arguments	Checked object	None	User
Register	Register an object	IND-1	Register arguments	Object's UID	Key Unwrapping Legacy Key Wrapping Input-Output	User - Users' RSA Private Key: W - Users' RSA Public Key: W - Users' ECDSA Private Key: W - Users' ECDSA Public Key: W - Users' EDDSA Private Key: W - Users' EDDSA Public Key: W - Users' ML-DSA Private Key: W - Users' ML-DSA Public Key: W - Users' ML-KEM Private Key: W - Users' ML-KEM Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W - Users' AES Key: W - Users' HMAC Key: W - Users' Certificate: W
Get	Get an object	IND-1	Get arguments	Wrapped object	Key Wrapping	User - Users' RSA Private Key: R - Users' RSA Public Key: R - Users' ECDSA Private Key: R - Users' ECDSA Public Key: R - Users' EDDSA Private Key: R - Users' EDDSA Public Key: R - Users' ML-DSA Private Key: R - Users' ML-DSA Public Key: R - Users' ML-KEM Private Key: R - Users' ML-KEM

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: R - Users' AES Key: R,E - Users' HMAC Key: R - Users' Certificate: R
Encrypt	Encrypt data	IND-1	Encrypt arguments	Encrypted data	Data Encryption	User - Users' RSA Public Key: E - Users' ECDSA Public Key: E - Users' EDDSA Public Key: E - Users' AES Key: E
Decrypt	Decrypt data	IND-1	Decrypt arguments	Decrypted data	Data Decryption Legacy Data Decryption	User - Users' RSA Private Key: E - Users' ECDSA Private Key: E - Users' EDDSA Private Key: E - Users' AES Key: E
Sign	Sign data	IND-1	Sign arguments	Signed data	Digital Signature Generation	User - Users' RSA Private Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Users' ECDSA Private Key: E - Users' EDDSA Private Key: E - Users' ML-DSA Private Key: E
Signature verify	Verify signature	IND-1	Signature verify arguments	Signature verification result	Digital Signature Verification	User - Users' RSA Public Key: E - Users' ECDSA Public Key: E - Users' EDDSA Public Key: E - Users' ML-DSA Public Key: E
RNG Retrieve	Retrieve randomness	IND-1	RNG Retrieve arguments	RNG Retrieved	Deterministic Random Number Generator	User - DRBG C and V values: E - DRBG Entropy Input: E - DRBG Seed: E
RNG Seed	Seed RNG	IND-1	RNG Seed arguments	RNG Seeded	Get Entropy	User
Hash	Compute hash	IND-1	Hash arguments	Computed hash	None	User
MAC	Generate MAC of data	IND-1	MAC arguments	Generated MAC	Message Authentication	User - DRBG C and V values: E - DRBG Entropy

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Input: E - DRBG Seed: E
MAC Verify	Verify a MAC	IND-1	MAC Verify arguments	Verified MAC	Message Verification	User - DRBG C and V values: E - DRBG Entropy Input: E - DRBG Seed: E
Set User Object Permission	Set object permissions for a specific user	IND-1	Set User Object Permission arguments	User Object Permission set	None	User
Get User Object Permission	Get object permissions for a specific user	IND-1	Get User Object Permission arguments	User Object Permission	None	User
Load Key	Load key in cache	IND-1	Load Key arguments	Loaded Key UID	Deterministic Random Number Generator Input-Output	User - Fastlane ID: G,R - Fastlane Secret: W
Validate	Validate a digital certificate or certificate chain	IND-1	Validate arguments	Validity Indicator	Data Decryption	User - Users' Certificate: E
Sign XML	Sign data according to XMLDSig standard	IND-1	Sign XML arguments	Signed XML	Digital Signature Generation Secure Hash (Message Digest)	User - Users' RSA Private Key: E - Users' ECDSA Private Key: E
Generate CSR	Generate a Signing Certificate Request	IND-1	Generate CSR arguments	Generated CSR	Digital Signature Generation	User - Users' RSA Private Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Users' RSA Public Key: R - Users' ECDSA Private Key: E - Users' ECDSA Public Key: R - Users' EDDSA Private Key: E - Users' EDDSA Public Key: R
Generate Timestamp	Generate a time stamp for the given hash, and signs it	IND-1	Generate Timestamp arguments	Generated Timestamp	Digital Signature Generation	User - Users' RSA Private Key: E - Users' ECDSA Private Key: E
Derive Key	Derive a new key from a pre-existing key	IND-1	Derive Key arguments	Derived Key UID; and/or Derivation Data	Key Generation Symmetric Key Generation Key Encapsulation Key Wrapping	User - Users' ECDSA Private Key: E - Users' ML-DSA Private Key: E - Users' AES Key: G,E - Users' HMAC Key: G - Users' ML-KEM Private Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Secret Share	Request the user respective encrypt-ed share for quor-um activation for given Object	IND-1	Get Secret Share arguments	Secret Share (encrypted)	Data Encryption Digital Signature Generation Input-Output	User - Quorum Secret Share: R
Reformat Clear PIN	Take a PIN Block and reformats it to the desired format	IND-1	Reformat Clear Pin arguments	Reformatted Clear Pin	None	User
Create Split Key	Create a key in different parts and save each part as one key in the HSM	IND-1	Create Split Key arguments	Split Key UIDs	Symmetric Key Generation	User - Users' AES Key: G,E - Users' HMAC Key: G,E
Join Split Key	Join different parts of a split key into only one key in the HSM	IND-1	Join Split Key arguments	Joined Split Key UID	Symmetric Key Generation	User - Users' AES Key: G,E - Users' HMAC Key: G,E
Prepare Fast Red Blob Sign	Prepare the HSM to perform Fast Red Blob Sign operation	IND-1	Prepare Fast Red Blob Sign arguments	Red Blob UID	Deterministic Random Number Generator	User - Fastlane ID: G,R - Fastlane Secret: W
Sign Authentication Package	Sign a Token Authentication Pack-age generated by the Start Token Authentication Operation	IND-1	Sign Authentication Package arguments	Signed Authentication Package	Digital Signature Generation	User - PHSM Module Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Decrypt Secret Share	Decrypt a Packaged Secret Share retrieved from the Get Secret Share Operation	IND-1	Decrypt Secret Share arguments	Decrypted Secret Share	Data Decryption	User - Users' RSA Private Key: E - Users' ECDSA Private Key: E - Users' EDDSA Private Key: E
Generate EMV Cryptogram	Generate an EMV (Europay, MasterCard and Visa) Cryptogram	IND-1	Generate EMV Cryptogram arguments	Generated EMV Cryptogram	Data Encryption	User - Users' AES Key: E
Authentication	The operator authentication process, using one or more of the authentication methods	IND-1	Authentication	-	Digital Signature Verification Secure Hash (Message Digest) Message Authentication Input-Output	Physical HSM Crypto Officer - PCO Initialization Password: W,E,Z - PCOs' Temporary Password: W,E,Z - PCOs' Passwords: W,E,Z - PCOs' Hashed Passwords: E - PCOs' Certificate Fingerprints: E - PCO's OTP: E - Users' Temporary Password (Pin):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E,Z - Users' Passwords: W,E,Z - Users' Hashed Passwords: E - Users' Certificate Fingerprints: E - User's OTP Key: E - User's OTP: W,E,Z - Authentication Certificate: E - Authentication Certificate Challenge: W,E,Z - Authentication Certificate Response: W,E,Z - Fastlane ID: W,E - Fastlane Secret: W,E,Z Virtual HSM Crypto Officer - VCO Initialization Password: W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- VCOs' Temporary Password: W,E,Z - VCOs' Passwords: W,E,Z - VCOs' Hashed Passwords: E - VCOs' Certificate Fingerprints: E - VCO's OTP Key: E - VCO's OTP: W,E,Z - Users' Temporary Password (Pin): W,E,Z - Users' Passwords: W,E,Z - Users' Hashed Passwords: E - Users' Certificate Fingerprints: E - User's OTP Key: E - User's OTP: W,E,Z - Authentication Certificate: E -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Certificate Challenge: W,E,Z - Authentication Certificate Response: W,E - Fastlane ID: W,E - Fastlane Secret: W,E,Z User - Users' Temporary Password (Pin): W,E,Z - Users' Passwords: W,E,Z - Users' Hashed Passwords: E - Users' Certificate Fingerprints: E - User's OTP Key: E - User's OTP: W,E,Z - Authentication Certificate: E - Authentication Certificate Challenge:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E,Z - Authentication Certificate Response: W,E,Z - Fastlane ID: W,E - Fastlane Secret: W,E,Z
TLS Establishment	The process to establish the TLS connection between the module and the external entity (operator, process, etc.)	IND-1	TLS Establishment arguments	TLS Established	Key Agreement Key Generation	Physical HSM Crypto Officer - ECDH Private Component (ephemeral): G,R,W,E,Z - ECDH Public Component (ephemeral): G,R,W,E,Z - TLS Peer Public Key: W,E - TLS Pre-Master Secret: G,E,Z - TLS Master Secret: G,E,Z - TLS Session Key: G,E,Z - TLS Authentication Key: G,E,Z - PHSM

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Server CA Key: E - PHSM Server CA Certificate: E - PHSM Server Key: E - PHSM Server Certificate: E - PHSM Client CA Key: E - PHSM Client CA Certificate: E Virtual HSM Crypto Officer - ECDH Private Component (ephemeral): G,R,W,E,Z - ECDH Public Component (ephemeral): G,R,W,E,Z - TLS Peer Public Key: W,E - TLS Pre-Master Secret: G,E,Z - TLS Master Secret: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Session Key: G,E,Z - TLS Authentication Key: G,E,Z - VHSM Server CA Key: E - VHSM Server CA Certificate: E - VHSM Client CA Keys: E - VHSM Client CA Certificates: E User - ECDH Private Component (ephemeral): G,R,W,E,Z - ECDH Public Component (ephemeral): G,R,W,E,Z - TLS Peer Public Key: W,E - TLS Pre-Master Secret: G,E,Z - TLS Master Secret: G,E,Z - TLS Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,E,Z - TLS Authentication Key: G,E,Z

Table 13: Approved Services

All services listed in this section can be accessed in approved mode. Services that give access to cryptographic algorithms provide only FIPS 140-3 approved algorithms.

Notes

- Indicator
How to identify if the requested service is approved.
IND-1: The HSM is in Approved Mode (See 11.2 Administrator Guidance). KMIP operations will return “Illegal Operation” if not approved.

- Access Rights to Keys and/or SSPs
The following definition will be used when listing access rights for each SSP (Sensitive Security Parameter):

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g. the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroise: The module zeroises the SSP.

- KMIP Operations
All services that are identified as KMIP Operations use a TLS connection to send requests and receive responses from the module. They also require the authentication of the requester via one or more of the authentication methods. Because of that, all KMIP Operations are executed together with “TLS Establishment” and “Authentication” services.

- HSM Reset
After the HSM Reset service execution, to zeroise the SSPs stored in the non-volatile memory, the Restart service is executed automatically, doing the zeroization of all SSPs stored in the volatile memory.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Register SEApp	The kNET HSM enables the user to execute Python applications with access to cryptographic objects stored on that device. These applications may be uploaded, controlled and monitored on the device via custom KMIP requests. These requests, although use the KMIP protocol, are not commands from the KMIP specification, but were added by Kryptus to its own KMIP server to offer extended	Triple DES RSA MD5 DSA Brainpool P-160 (r1/t1) Brainpool P-	User

Name	Description	Algorithms	Role
	functionalities. This document provides a brief explanation on how the kNET HSM Secure Execution feature works. For instructions on commands to manage Secure Execution Applications, please refer to the Command Line Interface manual. Important: The user of the SE App is responsible for its security and enforcing the desired security rules upon its connections	192 (r1/t1) Brainpool P-224 (r1/t1) Brainpool P-256 (r1/t1) Brainpool P-320 (r1/t1) Brainpool P-384 (r1/t1) Brainpool P-512 (r1/t1) Ed521 SEC P-256 (k1)	

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

The operational environment is limited and, therefore, is designed to accept only controlled firmware changes that successfully pass the software/firmware load test. The software/firmware is generated and validated by Kryptus Segurança da Informação S.A, no data is output until the software/firmware is loaded during the update process and all of the required tests are executed prior first use, including the integrity test.

5 Software/Firmware Security

5.1 Integrity Techniques

The firmware of the kNET HSM is stored in an encrypted format inside the device using AES 256 CBC. During the boot process, the device decrypts the firmware image and check the integrity with digital signature verification (RSA 2048 bits with SHA2-256). If the decryption fails or the decrypted image is invalid, the device will not boot, ensuring that only trusted and unmodified firmware is executed.

5.2 Initiate on Demand

If the Operator needs to perform the kNET HSM tests, they can restart the HSM and then, all the self-tests will be performed.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Epoxy resin	N/A	N/A
EFP	N/A	N/A

Table 15: Mechanisms and Actions Required

The module is a multi-chip embedded hardware and meets the physical security level 3. The crypto-graphic boundary is completely coated by epoxy resin, so that any attempt to physically gain access to the module's circuitry is highly likely to cause its destruction. Two aluminum frames are used to delimit the resin area that is applied over the PCB, which can be seen in Figure 5 and Figure 6. The resin is opaque inhibiting visual inspection and, moreover, providing tamper-evidence. Besides the epoxy resin, the module implements environmental failure protection (EFP), forcing the equipment to shut down in case any voltage or temperature monitored do not meet the module's operating range.

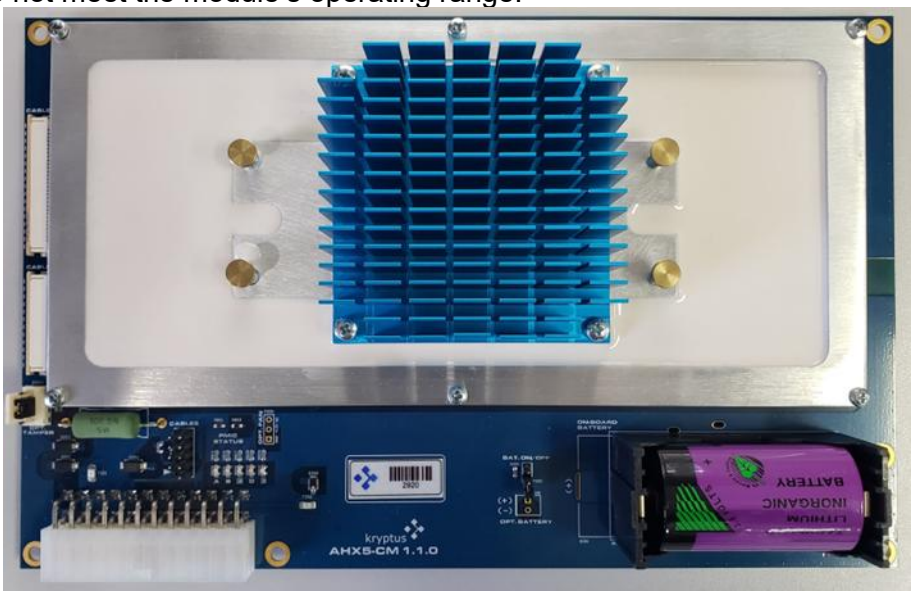

Figure 5: Top view of the cryptographic module

Figure 6: Bottom view of the cryptographic module

Furthermore, the module was designed with an input interface for the monitoring of an external event. In the scope of the TOEPP, this interface is connected to the kNET cover opening sensor. The response to this event is the same as that applied to the EFP.

7.2 User Placed Tamper Seals

The module is completely covered by epoxy resin, hence, there is no cover or opening that allows internal access. As a result, no tamper evident seal is used over the module.

7.3 Filler Panels

The module is completely covered by epoxy resin, hence, there is no cover or opening that allows internal access. As a result, no filler is used over the module.

7.4 Fault Induction Mitigation

Not Applicable.

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-25°C (storage); -2°C (installed)	EFP	Shutdown
HighTemperature	+85°C (storage); +70°C (installed)	EFP	Shutdown
LowVoltage	10.20 V (+12V ATX); 2.80 V (+3.3V ATX); 1.96 V (Battery)	EFP	Shutdown

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
HighVoltage	13.80 V (+12V ATX); 3.80 V (+3.3V ATX); 5.75 V (+5V Standby ATX); 4.08 V (Battery)	EFP	Shutdown

Table 16: EFP/EFT Information

The module uses ultra-low-power microcontroller and sensors to constantly monitor the environmental parameters, even when the appliance is not plugged to the mains electricity. A non-removable battery, along with voltage conditioning and a supercapacitor, are used to ensure that the sensors have non-interruptible power.

The module monitors the voltage of the power inputs and the temperature, triggering an EFP response in case any parameter is outside the operating range. After the module recovers from an EFP event, it switches to Intrusion State.

Regarding the voltage inputs, +12V ATX, +3.3V ATX, +5V Standby ATX and Battery are monitored and trigger the environmental failure response.

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-25°C
HighTemperature	+85°C

Table 17: Hardness Testing Temperatures

The hardness tested temperature considers the temperature range for an appliance at storage.

8 Non-Invasive Security

8.1 Mitigation Techniques

Non-invasive security is non-applicable since there are currently no requirement in [SP 800-140F].

9 Sensitive Security Parameters Management

The Database Encryption Key encrypts all other private SSP (CSPs) stored in the disk. The Database Encryption Key itself is stored in the disk encrypted by the Master Key. The Master Key is stored in-side the main CPU enclosure and never leaves it. The usage of the Master Key and Database Key Encryption Key is controlled by the KMIP server and are never used to encrypt arbitrary data (i.e.: they can't be used directly by any user).

The integrity of all public SSPs (PSPs) stored in the disk are protected by the KMIP server. The KMIP server integrity is verified by the Bootloader. The Bootloader integrity is verified by the Super Root Key. The Super Root Key integrity is verified by the main CPU, using the Super Root Key Hash stored in a read-only memory inside the CPU enclosure.

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
One-time Programmable Memory	Read-only, non-volatile memory, internal to the CPU encapsulation	Static
Non-volatile Memory	Non-volatile memory, external to the CPU, but internal to the cryptographic boundary	Dynamic
Encrypted Non-volatile Memory	Non-volatile Memory where encrypted data is stored	Dynamic
Volatile Memory	Volatile memory, external to the CPU, but internal to the cryptographic boundary	Dynamic
Encrypted Volatile Memory	Volatile Memory where encrypted data is stored	Dynamic
CPU Registers	CPU registers, internal to the CPU encapsulation	Dynamic

Table 18: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
ACTIVATE OTP 1	Volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
ACTIVATE OTP 2	External	Encrypted Volatile Memory	Encrypted	Manual	Electronic	Input-Output
AUTHENTICATION	External	Volatile Memory	Encrypted	Manual	Electronic	Input-Output
CHANGE PASSWORD	External	Encrypted Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
CREATE USER	Volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
CREATE VHSM	Volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
ESTABLISH TLS SESSION 1	Volatile Memory	External	Plaintext	Manual	Electronic	Key Agreement
ESTABLISH TLS SESSION 2	External	Volatile Memory	Plaintext	Manual	Electronic	Key Agreement
EXPORT PHSM 1	Encrypted Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
EXPORT PHSM 2	Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
EXPORT VHSM 1	Encrypted Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
EXPORT VHSM 2	Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
FACTORY INPUT 1	External	Non-volatile Memory	Plaintext	Manual	Direct	
FACTORY INPUT 2	External	Non-volatile Memory	Plaintext	Manual	Direct	
GET	Encrypted Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
GET SECRET SHARE	Encrypted Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
GET SESSION CREDENTIAL	Volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
GET TEMPORARY PIN	Volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
GET TLS CERTIFICATE	Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
IMPORT PHSM 1	External	Encrypted Non-	Encrypted	Manual	Electronic	Input-Output

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
		volatile Memory				
IMPORT PHSM 2	External	Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output
IMPORT VHSM 1	External	Encrypted Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output
IMPORT VHSM 2	External	Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output
INITIALIZE HSM	External	Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output
JOIN CLUSTER	External	Encrypted Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output
LCD DISPLAY	Volatile Memory	External	Plaintext	Manual	Direct	
LOAD KEY	Encrypted Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
PREPARE JOIN CLUSTER	Encrypted Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
QUERY	Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
REGISTER	External	Encrypted Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output
REGISTER AUTHENTICATION CERTIFICATE	External	Encrypted Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output
RENEW SERVER CERTIFICATE	External	Non-volatile Memory	Encrypted	Manual	Electronic	Input-Output
RESET PASSWORD	Non-volatile Memory	External	Encrypted	Manual	Electronic	Input-Output

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
START TOKEN AUTHENTICATION	Volatile Memory	External	Encrypted	Manual	Electronic	Input-Output
VOTE QUORUM AUTHENTICATION	External	Volatile Memory	Encrypted	Manual	Electronic	Input-Output

Table 19: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
AFTER USE ZEROISATION	It is the zeroisation processes executed when a unprotected SSP is the volatile memory is not required anymore	The zeroisation is applied in order to make the SSP irretrievable and not reusable	No
PHSM ZEROISATION	It is the zeroisation of all PHSM SSPs	Since the PHSM represents all the information of the module, the zeroisation is applied in order to make the PHSM SSPs irretrievable and not reusable when the process is initiated by the Operator	Yes
VHSM ZEROISATION	It is the zeroisation of all SSPs of a VHSM	Since the VHSM represents part of the information of the module, the zeroisation is applied in order to make the VHSM SSPs irretrievable and not reusable when the process is initiated by the Operator. When the PHSM ZEROISATION is applied, the VHSM ZEROISATION is applied as a consequence	Yes
USER ZEROISATION	It is the zeroisation of all SSPs of a USER	Since the USER's SSPs reside in the module, the zeroisation is applied in order to make the USER SSPs irretrievable and not reusable when the process is initiated by the Operator. When the PHSM ZEROISATION or VHSM ZEROISATION is applied, the USER ZEROISATION is applied as a consequence	Yes
OBJECT ZEROISATION	It is the zeroisation of all SSPs of an OBJECT	Since the OBJECT is a USER's SSPs, the zeroisation is applied in order to make the OBJECT SSPs irretrievable and not reusable when the process is	Yes

Zeroization Method	Description	Rationale	Operator Initiation
		initiated by the Operator. When the PHSM ZEROISATION, VHSM ZEROISATION or USER ZEROISATION is applied, the OBJECT ZEROISATION is applied as a consequence	
SHUTDOWN ZEROISATION	It is the zeroisation of all SSPs stored in the Volatile Memory and Encrypted Volatile Memory	Since the SSPs stored in the volatile memory are not stored in the disk, the SHUTDOWN ZEROISATION guarantees that the SSPs are irretrievable and not reusable. The SHUTDOWN ZEROISATION process can be initiated either by the Operator or Automatically: if the module enters in Intrusion State, the shutdown is applied	Yes

Table 20: SSP Zeroization Methods

All SSPs and key components within the module are physically and logically protected. Most of the SSPs within the module are encrypted. All temporarily stored SSPs within the module are kept in the volatile memory and zeroised when they are no longer needed. A zeroised SSP are not retrievable or reusable.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Super Root Key Hash	Hash of the Public Key used to verify the Bootloader image (secure boot)	256-bit - 128-bit	Message Digest - Neither			
Master Key	Device's master key, used to encrypt the Disk Encryption Key. The access to this key is hardware restricted to the CPU (no other hardware or process have access to it)	256-bit - 256-bit	Symmetric Key - CSP			Key Wrapping Key Unwrapping

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Job Descriptor Key Encryption Key	Key used to keep keys protected by the Master Key encrypted in memory while they are being used	256-bit - 256-bit	Symmetric Key - CSP	Symmetric Key Generation		Key Wrapping Key Unwrapping
Kryptus kNET CA Certificate	X.509 Certificate used to verify firmware update packages	4096-bit - 140-bit	X.509 Certificate - PSP			Digital Signature Verification
PHSM Module Key	Private Key that identifies the module. It is used to decrypt firmware update packages, sign backup packages and decrypt backup packages	3072-bit - 128-bit	Private Key - CSP			Data Decryption Digital Signature Generation
PHSM Module Certificate	X.509 Certificate that identifies a module. It is used to verify backup packages signatures and to encrypt backup packages	3072-bit - 128-bit	X.509 Certificate - PSP			Digital Signature Verification
PHSM Server CA Key	Private Key used during the PHSM TLS Server authentication	3072-bit - 128-bit	Private Key - CSP	Key Generation		Digital Signature Generation
PHSM Server CA Certificate	Certificate of the PHSM TLS Server CA, used to sign TLS Server certificates. Matches PSHM Server CA Key	3072-bit - 128-bit	X.509 Certificate - PSP	Key Generation		Digital Signature Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PHSM Server Key	Private Key used during the PHSM TLS Server authentication	3072-bit - 128-bit	Private Key - CSP	Key Generation		Digital Signature Verification
PHSM Server Certificate	X.509 Certificate used during the PHSM TLS Server authentication. Matches the PHSM Server Key	3072-bit - 128-bit	X.509 Certificate - PSP	Key Generation Secure Hash (Message Digest)		Digital Signature Verification
PHSM Client CA Key	Private Key of the PHSM TLS Client CA, used to sign TLS Client certificates	3072-bit - 128-bit	Private Key - CSP	Key Generation		Digital Signature Generation
PHSM Client CA Certificate	Certificate of the PHSM TLS Client CA, used to sign TLS Server certificates. Matches PSHM Client CA Key	3072-bit - 128-bit	X.509 Certificate - PSP	Key Generation Secure Hash (Message Digest)		Digital Signature Verification
PCO Initialization Password	Password used to initialize the PHSM when it is in factory state	6 characters - 6 characters	Password - CSP	Deterministic Random Number Generator		Secure Hash (Message Digest)
PCOs' Temporary Password	Temporary password generated when the PCO is created. It can be used only in the CHANGE PASSWORD operation	12 characters - 12 characters	Password - CSP	Deterministic Random Number Generator		Secure Hash (Message Digest)
PCOs' Passwords	PCO's password, used for authentication	6 characters - 6 characters	Password - CSP			Secure Hash (Message Digest)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PCOs' Hashed Passwords	PCO's hashed passwords, used for authentication	256-bit - 128-bit	Hashed Password - CSP	Deterministic Random Number Generator Secure Hash (Message Digest)		
PCOs' Certificate Fingerprints	PCO's mTLS certificate fingerprint, used for authentication	256-bit - 128-bit	Message Digest - PSP	Secure Hash (Message Digest)		
PCO's OTP Key	PCO's OTP secret, used to generate the OTP	160-bit - 80-bit	Symmetric Key - CSP	Symmetric Key Generation		Message Authentication
PCO's OTP	PCO's one-time password, used for authentication	6 characters - 6 characters	One-time Password - CSP	Message Authentication		Message Verification
VHSM Server CA Key	Private Key of the VHSM TLS Server CA, used to sign TLS Server certificates	3072-bit - 128-bit	Private Key - CSP	Key Generation		Digital Signature Generation
VHSM Server CA Certificate	Certificate of the VHSM TLS Server CA, used to sign TLS Server certifi-cates. Matches VHSM Server CA Key	3072-bit - 128-bit	X.509 Certificate - PSP	Key Generation		Digital Signature Verification
VHSM Server Keys	Private Key used during the VHSM TLS Server authentication	3072-bit - 128-bit	Private Key - CSP	Key Generation		Digital Signature Generation
VHSM Server Certificates	X.509 Certificate used during the VHSM TLS Server authentication.	3072-bit - 128-bit	X.509 Certificate - PSP	Key Generation		Digital Signature Verification

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Matches the VHSM Server Key					
VHSM Client CA Keys	Internally when re-quested: INITIALIZE HSM	3072-bit - 128-bit	Private Key - CSP	Key Generation		Digital Signature Generation
VHSM Client CA Certificates	Certificate of the VHSM TLS Client CA, used to sign TLS Server certifi-cates. Matches VHSM Client CA Key	3072-bit - 128-bit	X.509 Certificate - PSP	Key Generation		Digital Signature Verification
VCO Initialization Password	Password used to initialize the VHSM after its creation	12 characters - 12 characters	Password - CSP	Deterministic Random Number Generator		Secure Hash (Message Digest)
VCOs' Temporary Password	Temporary password generated when the VCO is created. It can be used only in the CHANGE PASSWORD operation	12 characters - 12 characters	Password - CSP	Deterministic Random Number Generator		Secure Hash (Message Digest)
VCOs' Passwords	VCO's password, used for authentication	12 characters - 79-bit	Password - CSP			Secure Hash (Message Digest)
VCOs' Hashed Passwords	VCO's hashed passwords, used for authentication	256-bit - 128-bit	Hashed Password - CSP	Deterministic Random Number Generator Secure Hash (Message Digest)		
VCOs' Certificate Fingerprints	VCO's mTLS certificate fingerprint, used for authentication	256-bit - 128-bit	Message Digest - PSP	Secure Hash (Message Digest)		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
VCO’s OTP Key	VCO's OTP secret, used to generate the OTP	160-bit - 80-bit	HMAC OTP Key - CSP	Symmetric Key Generation		Message Authentication
VCO's OTP	VCO's one-time password, used for authentication	6 characters - 6 characters	One-Time Password - CSP	Message Authentication		Message Verification
Users' Temporary Password (Pin)	Temporary password generated when the User is created. It can be used only in the CHANGE PASSWORD operation	12 characters - 12 characters	Password - CSP	Deterministic Random Number Generator		Secure Hash (Message Digest)
Users’ Passwords	User's password, used for authentication	8 characters - 8 characters	Password - CSP			Secure Hash (Message Digest)
Users’ Hashed Passwords	User's hashed passwords, used for authentication	256-bit - 128-bit	Hashed Password - CSP	Deterministic Random Number Generator Secure Hash (Message Digest)		
Users’ Certificate Fingerprints	User's mTLS certifi-cate fingerprint, use for authentication	256-bit - 128-bit	Message Digest - PSP	Secure Hash (Message Digest)		
User’s OTP Key	User's OTP secret, used to generate the OTP	160-bit - 80-bit	HMAC OTP Key - CSP	Symmetric Key Generation		Message Authentication
User’s OTP	User's one-time password, used for authentication	6 characters - 6 characters	One-Time Password - CSP	Message Authentication		Message Verification

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Users' RSA Private Key	User's RSA private keys	2048-bit, 3072-bit, 4096-bit - 112-bit, 128-bit, 140-bit	Private Key - CSP	Key Generation		Data Decryption Digital Signature Generation
Users' RSA Public Key	User's RSA public keys	2048-bit, 3072-bit, 4096-bit - 112-bit, 128-bit, 140-bit	Public Key - PSP	Key Generation		Data Encryption Digital Signature Verification
Users' ECDSA Private Key	User's ECDSA private keys	P-224, P-256, P-384, P-521 - 112-bit, 128-bit, 192-bit, 256-bit	Private Key - CSP	Key Generation		Digital Signature Generation Key Agreement
Users' ECDSA Public Key	User's ECDSA public keys	P-224, P-256, P-384, P-521 - 112-bit, 128-bit, 192-bit, 256-bit	Public Key - PSP	Key Generation		Digital Signature Verification Key Agreement
Users' EDDSA Private Key	User's EDDSA private keys	ED-25519, ED-448 - 128-bit, 224-bit	Private Key - CSP	Key Generation		Digital Signature Generation
Users' EDDSA Public Key	User's EDDSA public keys	ED-25519, ED-448 - 128-bit, 224-bit	Public Key - PSP	Key Generation		Digital Signature Verification

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Users' ML-DSA Private Key	User's ML-DSA private keys	ML-DSA-44, ML-DSA-65, ML-DSA-87 - 128-bit, 192-bit, 256-bit	Private Key - CSP	Key Generation		Digital Signature Generation
Users' ML-DSA Public Key	User's ML-DSA public keys	ML-DSA-44, ML-DSA-65, ML-DSA-87 - 128-bit, 192-bit, 256-bit	Public Key - PSP	Key Generation		Digital Signature Verification
Users' ML-KEM Private Key	User's ML-KEM private keys	ML-KEM-512, ML-KEM-768, ML-KEM-1024 - 128-bit, 192-bit, 256-bit	Private Key - CSP	Key Generation		Key Encapsulation
Users' ML-KEM Public Key	User's ML-KEM public keys	ML-KEM-512, ML-KEM-768, ML-KEM-1024 - 128-bit, 192-bit, 256-bit	Public Key - PSP	Key Generation		Key Encapsulation
Users' AES Key	User's AES symmetric keys	128-bit, 192-bit, 256-bit -	Symmetric Key - CSP	Symmetric Key Generation		Data Encryption Data

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128-bit, 192-bit, 256-bit				Decryption Message Authentication Message Verification Key Wrapping Key Unwrapping
Users' HMAC Key	User's HMAC symmetric keys	224-bit, 256-bit, 384-bit, 512-bit - 112-bit, 128-bit, 192-bit, 256-bit	Symmetric Key - CSP	Symmetric Key Generation Secure Hash (Message Digest)		Message Authentication Message Verification
Users' Certificate	User's public key certificates	RSA: 2048-bit, 3072-bit, 4096-bit; ECDSA: P-224, P-256, P-384, P-521 - RSA: 112-bit, 128-bit, 140-bit, ECDSA: 112-bit, 128-bit, 192-bit, 256-bit	X.509 Certificate - PSP			Digital Signature Verification
ECDH Private Component (ephemeral)	Ephemeral ECDH private component used during the TLS session key Establishment	P-256, P-384, P-521 - 128-bit, 192-bit, 256-bit	Private Key - CSP	Key Generation		Key Agreement

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ECDH Public Component (ephemeral)	Ephemeral ECDH public component used during the TLS session key Establishment	P-256, P-384, P-521 - 128-bit, 192-bit, 256-bit	Public Key - PSP	Key Generation		Key Agreement
TLS Peer Public Key	Certificate-based authentication during TLS session key Establishment	2048-bit - 112-bit	Public Key - PSP			Digital Signature Verification
TLS Pre-Master Secret	Derivation of the TLS Master Secret	256-bit, 384-bit, 521-bit - 256-bit, 384-bit, 521 bit	Shared Secret - CSP		Key Agreement	Key Agreement
TLS Master Secret	Derivation of the TLS Session Key and TLS Authentication Key	384-bit - 384-bit	Shared Secret - CSP		Key Agreement	Key Agreement
TLS Session Key	Encryption and decryption of TLS session packets	128-bit, 256-bit - 128-bit, 256-bit	AES Session Key - CSP		Key Agreement	Data Encryption Data Decryption
TLS Authentication Key	Authentication of TLS session packets	256-bit - 128-bit	HMAC-Key - CSP		Key Agreement	Message Authentication Message Verification
DRBG Entropy Input	Generation of random number	384-bit - 256-bit	Entropy Input - CSP	Get Entropy		Deterministic Random Number Generator
DRBG Seed	Generation of random number	384-bit - 256-bit	DRBG Seed - CSP	Get Entropy		Deterministic Random Number Generator
DRBG C and V values	Generation of random number	256-bit - 256-bit	DRBG Internal State - CSP	Get Entropy		Deterministic Random Number Generator

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Disk Encryption Key	Encryption and de-cryption of SSPs stored in the non-volatile memory	256-bit - 256-bit	Symmetric Key - CSP	Symmetric Key Generation		Data Encryption Data Decryption Key Wrapping Key Unwrapping
Cluster TLS CA Private Key	TLS key used to establish the TLS session between kNETs in the cluster	2048-bit - 112-bit	Private Key - CSP	Key Generation		Digital Signature Generation
Cluster TLS CA Certificate	TLS certificate used to establish the TLS session between kNETs in the cluster	2048-bit - 112-bit	X.509 Certificate - PSP	Key Generation		Digital Signature Verification
Cluster TLS Server Private Key	TLS key used to establish the TLS session between kNETs in the cluster	2048-bit - 112-bit	Private Key - CSP	Key Generation		Digital Signature Generation
Cluster TLS Server Certificate	TLS certificate used to establish the TLS session between kNETs in the cluster	2048-bit - 112-bit	X.509 Certificate - PSP	Key Generation		Digital Signature Verification
Cluster TLS Client Private Key	TLS key used to establish the TLS session between kNETs in the cluster	2048-bit - 112-bit	Private Key - CSP			Digital Signature Generation
Cluster TLS Client Certificate	TLS certificate used to establish the TLS session between kNETs in the cluster	2048-bit - 112-bit	X.509 Certificate - PSP	Key Generation		Digital Signature Verification
Cluster Secret	Use to authenticate kNETs in the cluster	16 characters - 16 characters	Secret - CSP	Deterministic Random Number Generator		Secure Hash (Message Digest)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Authentication Certificate	X.509 Certificate used in non-TLS authentication schemes	RSA: 2048-bit, 3072-bit, 4096-bit; ECDSA: 224-bit, 256-bit, 384-bit, 521-bit - RSA: 112-bit, 128-bit, 140-bit; ECDSA: 112-bit, 128-bit, 192-bit, 256-bit	X.509 Certificate - PSP			Digital Signature Verification
Authentication Certificate Challenge	The challenge of the challenge-response protocol used to authenticate the user based on its AUTHENTICATION CERTIFICATE	800-bit - 128-bit	Other - CSP	Deterministic Random Number Generator		
Authentication Certificate Response	The response of the challenge-response protocol used to authenticate the user based on its AUTHENTICATION CERTIFICATE	RSA: 2048-bit, 3072-bit, 4096-bit; ECDSA: P-224, P-256, P-384, P-521 - RSA: 112-bit, 128-bit, 140-bit;	Other - CSP			Digital Signature Verification

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		ECDSA: 112-bit, 128-bit, 192-bit, 256-bit				
Session Token	Session token, used for authentication	20 characters - 20 characters	Other - CSP	Deterministic Random Number Generator		
Fastlane ID	Fastlane ID, used for authentication	128-bit - 128-bit	Other - CSP	Deterministic Random Number Generator		
Fastlane Secret	Fastlane Secret, used for authentication	128-bit - 128-bit	Other - CSP			Secure Hash (Message Digest)
Quorum Secret	Quorum secret used to encrypt a User Object protected by quorum authentication	256-bit - 128-bit	Other - CSP	Deterministic Random Number Generator		Key Wrapping Key Unwrapping
Quorum Secret Share	Quorum secret share used to reconstitute the quorum secret	256-bit - 128-bit	Other - CSP	Deterministic Random Number Generator		

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Super Root Key Hash	FACTORY INPUT 2	One-time Programmable Memory:Encrypted	Permanent	N/A	Master Key:Derived From
Master Key	FACTORY INPUT 2	One-time Programmable Memory:Encrypted	Permanent	N/A	
Job Descriptor Key Encryption Key		CPU Registers:Plaintext	Until Reboot	PHSM ZEROISATION SHUTDOWN	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				ZEROISATION	
Kryptus kNET CA Certificate	FACTORY INPUT 1	Non-volatile Memory:Plaintext	Permanent	N/A	PHSM Module Certificate:Signs
PHSM Module Key	FACTORY INPUT 1	Non-volatile Memory:Plaintext	Permanent	N/A	PHSM Module Key:Paired With
PHSM Module Certificate	EXPORT PHSM 2 FACTORY INPUT 1 IMPORT PHSM 1 IMPORT PHSM 2 QUERY	Non-volatile Memory:Plaintext	Permanent	N/A	PHSM Module Key:Paired With Kryptus kNET CA Certificate:Signed by
PHSM Server CA Key	EXPORT PHSM 1 IMPORT PHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION	PHSM Server CA Certificate:Paired With
PHSM Server CA Certificate	EXPORT PHSM 2 IMPORT PHSM 2	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION	PHSM Server CA Key:Paired With
PHSM Server Key	EXPORT VHSM 1 IMPORT PHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION	PHSM Server Certificate:Paired With
PHSM Server Certificate	EXPORT PHSM 2 IMPORT PHSM 2	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION	PHSM Server Key:Paired With
PHSM Client CA Key	EXPORT PHSM 1 IMPORT PHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION	PHSM Client CA Certificate:Paired With
PHSM Client CA Certificate	EXPORT PHSM 2 IMPORT PHSM 2	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION	PHSM Client CA Key:Paired With
PCO Initialization Password	AUTHENTICATION GET TEMPORARY PIN INITIALIZE	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	HSM LCD DISPLAY			ZEROISATION	
PCOs' Temporary Password	AUTHENTICATION CHANGE PASSWORD CREATE USER RESET PASSWORD	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
PCOs' Passwords	AUTHENTICATION CHANGE PASSWORD	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
PCOs' Hashed Passwords	EXPORT PHSM 1 IMPORT PHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	PCOs' Passwords:Derived From
PCOs' Certificate Fingerprints	EXPORT PHSM 1 IMPORT PHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
PCO's OTP Key	ACTIVATE OTP 1 ACTIVATE OTP 2 EXPORT PHSM 1 IMPORT PHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
PCO's OTP	ACTIVATE OTP 2 AUTHENTICATION	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	PCO's OTP Key:Derived From
VHSM Server CA Key	EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1 IMPORT VHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION	VHSM Server CA Certificate:Paired With
VHSM Server CA Certificate	EXPORT PHSM 2 EXPORT VHSM 2 IMPORT PHSM 2 IMPORT VHSM 2	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION	VHSM Server CA Key:Paired With
VHSM Server Keys	EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1 IMPORT VHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION	VHSM Server Certificates:Paired With
VHSM Server Certificates	EXPORT PHSM 2 EXPORT VHSM 2 GET TLS CERTIFICATE IMPORT PHSM 2 IMPORT VHSM 2 RENEW SERVER CERTIFICATE	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION OBJECT ZEROISATION	VHSM Server Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
VHSM Client CA Keys	EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1 IMPORT VHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION	VHSM Client CA Certificates:Paired With
VHSM Client CA Certificates	EXPORT PHSM 2 EXPORT VHSM 2 IMPORT PHSM 2 IMPORT VHSM 2	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION	VHSM Client CA Keys:Paired With
VCO Initialization Password	AUTHENTICATION CREATE VHSM INITIALIZE HSM	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
VCOs' Temporary Password	AUTHENTICATION CHANGE PASSWORD CREATE USER RESET PASSWORD	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
VCOs' Passwords	AUTHENTICATION CHANGE PASSWORD	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
VCOs' Hashed Passwords	EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER	VCOs' Passwords:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	IMPORT VHSM 1			ZEROISATION OBJECT ZEROISATION	
VCOs' Certificate Fingerprints	EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1 IMPORT VHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
VCO's OTP Key	ACTIVATE OTP 2 EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1 IMPORT VHSM 1	Encrypted Volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
VCO's OTP	ACTIVATE OTP 2 AUTHENTICATION	Encrypted Non-volatile Memory:Encrypted	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	VCO's OTP Key:Derived From
Users' Temporary Password (Pin)	AUTHENTICATION CHANGE PASSWORD CREATE USER RESET PASSWORD	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Users' Passwords	AUTHENTICATION CHANGE PASSWORD	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
Users' Hashed Passwords	EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1 IMPORT VHSM 1	Volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	Users' Passwords:Derived From
Users' Certificate Fingerprints	EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1 IMPORT VHSM 1	Encrypted Volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
User's OTP Key	ACTIVATE OTP 1 ACTIVATE OTP 2 EXPORT PHSM 1 EXPORT VHSM 1 IMPORT PHSM 1 IMPORT VHSM 1	Encrypted Volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
User's OTP	ACTIVATE OTP 2	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATI	User's OTP Key:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AUTHENTICATION			ON SHUTDOWN ZEROISATION	
Users' RSA Private Key	EXPORT PHSM 1 EXPORT VHSM 1 GET IMPORT PHSM 1 IMPORT VHSM 1 REGISTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' RSA Public Key	EXPORT PHSM 2 EXPORT VHSM 2 GET IMPORT PHSM 2 IMPORT VHSM 2 REGISTER	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' ECDSA Private Key	EXPORT PHSM 1 EXPORT VHSM 1 GET IMPORT PHSM 1 IMPORT VHSM 1 REGISTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' ECDSA Public Key	EXPORT PHSM 2 EXPORT VHSM 2 GET IMPORT PHSM	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	2 IMPORT VHSM 2 REGISTER			USER ZEROISATION OBJECT ZEROISATION	
Users' EDDSA Private Key	EXPORT PHSM 1 EXPORT VHSM 1 GET IMPORT PHSM 1 IMPORT VHSM 1 REGISTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' EDDSA Public Key	EXPORT PHSM 2 EXPORT VHSM 2 GET IMPORT PHSM 2 IMPORT VHSM 2 REGISTER	Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' ML-DSA Private Key	EXPORT PHSM 1 EXPORT VHSM 1 GET IMPORT PHSM 1 IMPORT VHSM 1 REGISTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' ML-DSA Public Key	EXPORT PHSM 2 EXPORT VHSM 2 GET	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATI	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	IMPORT PHSM 2 IMPORT VHSM 2 REGISTER			ON USER ZEROISATION OBJECT ZEROISATION	
Users' ML-KEM Private Key	EXPORT PHSM 1 EXPORT VHSM 1 GET IMPORT PHSM 1 IMPORT VHSM 1 REGISTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' ML-KEM Public Key	EXPORT PHSM 2 EXPORT VHSM 2 GET IMPORT PHSM 2 IMPORT VHSM 2 REGISTER	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' AES Key	EXPORT PHSM 1 EXPORT VHSM 1 GET IMPORT PHSM 1 IMPORT VHSM 1 REGISTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' HMAC Key	EXPORT PHSM 1 EXPORT VHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION VHSM	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	GET IMPORT PHSM 1 IMPORT VHSM 1 REGISTER			ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Users' Certificate	EXPORT PHSM 2 EXPORT VHSM 2 GET IMPORT PHSM 2 IMPORT VHSM 2 REGISTER	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
ECDH Private Component (ephemeral)		Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	ECDH Public Component (ephemeral):Paired With
ECDH Public Component (ephemeral)	ESTABLISH TLS SESSION 1 ESTABLISH TLS SESSION 2	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	ECDH Private Component (ephemeral):Paired With
TLS Peer Public Key	ESTABLISH TLS SESSION 1	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	TLS Pre-Master Secret:Encrypts
TLS Pre-Master Secret		Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATI	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				ON SHUTDOWN ZEROISATION	
TLS Master Secret		Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION ON SHUTDOWN ZEROISATION	TLS Pre-Master Secret:Derived From
TLS Session Key		Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION ON SHUTDOWN ZEROISATION	TLS Master Secret:Derived From
TLS Authentication Key		Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION ON SHUTDOWN ZEROISATION	TLS Master Secret:Derived From
DRBG Entropy Input		CPU Registers:Plaintext	Until zeroization	SHUTDOWN ZEROISATION	DRBG Seed:Used With DRBG C and V values:Used With
DRBG Seed		CPU Registers:Plaintext	Until zeroization	SHUTDOWN ZEROISATION	DRBG Entropy Input:Used With DRBG C and V values:Used With
DRBG C and V values		CPU Registers:Plaintext	Until zeroization	SHUTDOWN ZEROISATION	DRBG Entropy Input:Used With DRBG Seed:Used With
Disk Encryption Key	EXPORT PHSM 1 IMPORT PHSM 1	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION	PHSM Server CA Key:Encrypts PCOs' Hashed Passwords:Encry

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	JOIN CLUSTER PREPARE JOIN CLUSTER				pts PCOs' Certificate Fingerprints:Encrypts PCO's OTP Key:Encrypts VHSM Server CA Key:Encrypts VHSM Server Keys:Encrypts VHSM Client CA Keys:Encrypts VCOs' Hashed Passwords:Encrypts VCOs' Certificate Fingerprints:Encrypts VCO's OTP Key:Encrypts Users' Hashed Passwords:Encrypts Users' Certificate Fingerprints:Encrypts User's OTP Key:Encrypts Users' RSA Private Key:Encrypts Users' ECDSA Private Key:Encrypts Users' EDDSA Private Key:Encrypts Users' ML-DSA Private Key:Encrypts Users' ML-KEM Private Key:Encrypts Users' AES Key:Encrypts Users' HMAC Key:Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					PHSM Client CA Key:Encrypts
Cluster TLS CA Private Key	EXPORT PHSM 1 IMPORT PHSM 1 JOIN CLUSTER PREPARE JOIN CLUSTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION	Cluster TLS CA Certificate:Paired With Cluster TLS Server Certificate:Signs
Cluster TLS CA Certificate	EXPORT PHSM 2 IMPORT PHSM 2 JOIN CLUSTER PREPARE JOIN CLUSTER	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION	Cluster TLS CA Private Key:Paired With
Cluster TLS Server Private Key	EXPORT PHSM 1 IMPORT PHSM 1 JOIN CLUSTER PREPARE JOIN CLUSTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION	Cluster TLS Server Certificate:Paired With
Cluster TLS Server Certificate	EXPORT PHSM 2 IMPORT PHSM 2 JOIN CLUSTER PREPARE JOIN CLUSTER	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION	Cluster TLS Server Private Key:Paired With Cluster TLS CA Private Key:Signed by
Cluster TLS Client Private Key	EXPORT PHSM 1 IMPORT PHSM 1 JOIN CLUSTER PREPARE JOIN CLUSTER	Encrypted Non-volatile Memory:Encrypted	Until zeroization	PHSM ZEROISATION	Cluster TLS Client Certificate:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Cluster TLS Client Certificate	EXPORT PHSM 2 IMPORT PHSM 2 JOIN CLUSTER PREPARE JOIN CLUSTER	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION	Cluster TLS Client Private Key:Paired With
Cluster Secret	EXPORT PHSM 2 IMPORT PHSM 2 JOIN CLUSTER PREPARE JOIN CLUSTER	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION	
Authentication Certificate	EXPORT PHSM 2 EXPORT VHSM 2 IMPORT PHSM 2 IMPORT VHSM 2 REGISTER AUTHENTICATION CERTIFICATE	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	
Authentication Certificate Challenge	START TOKEN AUTHENTICATION	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
Authentication Certificate Response	AUTHENTICATION	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Session Token	AUTHENTICATION GET SESSION CREDENTIAL	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
Fastlane ID	AUTHENTICATION LOAD KEY	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
Fastlane Secret	AUTHENTICATION LOAD KEY	Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	Fastlane ID:Encrypts
Quorum Secret		Volatile Memory:Plaintext	Until zeroization	AFTER USE ZEROISATION SHUTDOWN ZEROISATION	
Quorum Secret Share	EXPORT PHSM 2 EXPORT VHSM 2 GET SECRET SHARE IMPORT VHSM 2 VOTE QUORUM AUTHENTICATION	Non-volatile Memory:Plaintext	Until zeroization	PHSM ZEROISATION VHSM ZEROISATION USER ZEROISATION OBJECT ZEROISATION	

Table 22: SSP Table 2

Note: For Reset HSM Service and Leave Cluster services, all SSPs have Z permissions, except:
Super Root Key Hash, Master Key, Kryptus kNET CA, Certificate, PHSM Module Key, PHSM Module.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-5) (A6066)	Digital Signature Verification with RSA 2048 bits and SHA-256	KAT	SW/FW Integrity	Frozen in “Initializing” screen on the frontal board in case of failure, otherwise, the device will enter the Conditional Self-Tests stage	Digital Signature

Table 23: Pre-Operational Self-Tests

Pre-Operational Self-Tests are run during the power-on process and after a reboot. The system image is decrypted, and its integrity is checked. If this test fails, the device does not boot and cannot receive requests through the Ethernet interface.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG (A6066)	SHA2-256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Hash-based Deterministic Random Number Generation: Instantiate, Reseed, Generate and Uninstantiate	Prior to the first operational use of any cryptographic algorithm
AES-ECB Encrypt (A6066)	Encryption ECB mode. Key size: 128, 256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Encryption	Prior to the first operational use of any cryptographic algorithm
AES-ECB Decrypt (A6066)	Decryption ECB mode. Key size: 128, 256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Decryption	Prior to the first operational use of any cryptographic algorithm

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt (A6066)	Encryption in CBC mode. Key size: 128, 256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Encryption	Prior to the first operational use of any cryptographic algorithm
AES-CBC Decrypt (A6066)	Decryption in CBC mode. Key size: 128, 256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Decryption	Prior to the first operational use of any cryptographic algorithm
AES-CTR Encrypt (A6066)	Encryption in CTR mode. Key size: 128, 256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Encryption	Prior to the first operational use of any cryptographic algorithm
AES-CTR Decrypt (A6066)	Decryption in CTR mode. Key size: 128, 256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Decryption	Prior to the first operational use of any cryptographic algorithm
AES-GCM Encrypt (A6066)	Encryption in GCM mode. Key size: 128, 256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Encryption	Prior to the first operational use of any cryptographic algorithm
AES-GCM Decrypt (A6066)	Decryption in GCM mode. Key size: 128, 256	KAT	CAST	“PASS” or “FAIL” on the frontal board	Decryption	Prior to the first operational use of any cryptographic algorithm
SHA2-224 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any cryptographic algorithm
SHA2-256 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						cryptographic algorithm
SHA2-384 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any cryptographic algorithm
SHA2-512 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any cryptographic algorithm
SHA2-512/224 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any cryptographic algorithm
SHA2-512/256 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any cryptographic algorithm
SHA3-224 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any cryptographic algorithm
SHA3-256 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any cryptographic algorithm
SHA3-384 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on the frontal board	Message Digest	Prior to the first operational use of any cryptographic algorithm
SHA3-512 (A6066)	N/A	KAT	CAST	“PASS” or “FAIL” on	Message Digest	Prior to the first operational

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				the frontal board		use of any cryptographic algorithm
HMAC-SHA-1 (A6066)	SHA-1	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm
HMAC-SHA2-224 (A6066)	SHA2-224	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm
HMAC-SHA2-256 (A6066)	SHA2-256	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm
HMAC-SHA2-384 (A6066)	SHA2-384	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm
HMAC-SHA2-512 (A6066)	SHA2-512	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm
HMAC-SHA3-224 (A6066)	SHA3-224	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm
HMAC-SHA3-256 (A6066)	SHA3-256	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-384 (A6066)	SHA3-384	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm
HMAC-SHA3-512 (A6066)	SHA3-512	KAT	CAST	“PASS” or “FAIL” on the frontal board	MAC Generation	Prior to the first operational use of any cryptographic algorithm
RSA SigGen (FIPS186-5) (A6066)	Digital Signature Generation. SHA-256. Key size: 2048 bit	KAT	CAST	“PASS” or “FAIL” on the frontal board	Digital Signature Generation	Prior to the first operational use of any cryptographic algorithm
RSA SigVer (FIPS186-5) (A6066)	Digital Signature Verification. Key size: 2048 bit	KAT	CAST	“PASS” or “FAIL” on the frontal board	Digital Signature Verification	Prior to the first operational use of any cryptographic algorithm
ECDSA SigGen (FIPS186-5) (A6066)	Digital Signature Generation. Curve: NIST P-521	KAT	CAST	“PASS” or “FAIL” on the frontal board	Digital Signature Generation	Prior to the first operational use of any cryptographic algorithm
ECDSA SigVer (FIPS186-5) (A6066)	Digital Signature Verification. Curve: NIST P-521	KAT	CAST	“PASS” or “FAIL” on the frontal board	Digital Signature Verification	Prior to the first operational use of any cryptographic algorithm
EDDSA SigGen (A6066)	Digital Signature Generation. Curve Ed25519	KAT	CAST	“PASS” or “FAIL” on the frontal board	Digital Signature Generation	Prior to the first operational use of any cryptographic algorithm
EDDSA SigVer (A6066)	Digital Signature Verification. Curve Ed25519	KAT	CAST	“PASS” or “FAIL” on the frontal board	Digital Signature Verification	Prior to the first operational use of any

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						cryptographic algorithm
ML-KEM Encapsulation (A6066)	Encapsulation. Parameters Set: ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	“PASS” or “FAIL” on the frontal board	Key Encapsulation	Prior to the first operational use of any cryptographic algorithm
ML-KEM Decapsulation (A6066)	Decapsulation. Parameters Set: ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	“PASS” or “FAIL” on the frontal board	Key Decapsulation	Prior to the first operational use of any cryptographic algorithm
ML-DSA SigGen (A6066)	Digital Signature Generation. Parameters Set: ML-DSA-44, ML-DSA-65, ML-DSA-87	KAT	CAST	“PASS” or “FAIL” on the frontal board	Digital Signature Generation	Prior to the first operational use of any cryptographic algorithm
ML-DSA SigVer (A6066)	Digital Signature Verification. Parameters Set: ML-DSA-44, ML-DSA-65, ML-DSA-87	KAT	CAST	“PASS” or “FAIL” on the frontal board	Digital Signature Verification	Prior to the first operational use of any cryptographic algorithm
KAS-ECC-SSC Sp800-56Ar3 (A6066)	Key Agreement Scheme (Primitive “Z” computation using ECDH). Curve: P-256, P-384, P-512	KAT	CAST	“PASS” or “FAIL” on the frontal board	Shared Secret Computation	Prior to the first operational use of any cryptographic algorithm
KDF TLS (A6066)	[SP800-135 Rev 1] TLS 1.2 KDF. SHA-256, SHA-384	KAT	CAST	“PASS” or “FAIL” on the frontal board	Key Derivation Function	Prior to the first operational use of any cryptographic algorithm

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TDES-CBC (A6066)	Key Option: 1	KAT	CAST	“PASS” or “FAIL” on the frontal board	Decryption	Prior to the first operational use of any cryptographic algorithm
TDES-ECB (A6066)	Key Option: 1	KAT	CAST	“PASS” or “FAIL” on the frontal board	Decryption	Prior to the first operational use of any cryptographic algorithm
Firmware Load Test	Digital Signature Verification and AES Decryption: RSA 2048 bits and SHA-256	KAT	SW/FW Load	Frontal board frozen in “Initializing” screen	Decryption, Digital Signature Verification	Prior to the first operational use of any cryptographic algorithm
Entropy 90 Repetition Count Test (RCT)	N/A	RCT	CAST	System Log	Continuous Health Test	Continuous during the entropy source operation
Entropy 90 Adaptive Proportion Test (APT)	N/A	APT	CAST	System Log	Continuous Health Test	Continuous during the entropy source operation
ECDSA KeyGen (FIPS186-5) (A6066)	N/A	PCT	PCT	System Log	Key Pair Generation and Verification	Prior to the first operational use of any cryptographic algorithm and on-demand
RSA KeyGen (FIPS186-5) (A6066)	N/A	PCT	PCT	System Log	Key Pair Generation and Verification	Prior to the first operational use of any cryptographic algorithm and on-demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
EDDSA KeyGen (A6066)	N/A	PCT	PCT	System Log	Key Pair Generation and Verification	Prior to the first operational use of any cryptographic algorithm and on-demand
ML-DSA KeyGen (A6066)	N/A	PCT	PCT	System Log	Key Pair Generation and Verification	Prior to the first operational use of any cryptographic algorithm and on-demand
ML-KEM KeyGen (A6066)	N/A	PCT	PCT	System Log	Key Pair Generation and Verification	Prior to the first operational use of any cryptographic algorithm and on-demand

Table 24: Conditional Self-Tests

The module performs conditional self-tests prior to the first operational use of the cryptographic algorithm.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A6066)	KAT	SW/FW Integrity	On-demand	On-demand (power-on process and after a reboot)

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG (A6066)	KAT	CAST	On-demand	On-demand (after boot process, triggered by

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				power-on or reboot)
AES-ECB Encrypt (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
AES-ECB Decrypt (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
AES-CBC Encrypt (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
AES-CBC Decrypt (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
AES-CTR Encrypt (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
AES-CTR Decrypt (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
AES-GCM Encrypt (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process,

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				triggered by power-on or reboot)
AES-GCM Decrypt (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA2-224 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA2-256 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA2-384 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA2-512 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA2-512/224 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA2-512/256 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				process, triggered by power-on or reboot)
SHA3-224 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA3-256 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA3-384 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
SHA3-512 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
HMAC-SHA-1 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
HMAC-SHA2-224 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
HMAC-SHA2-256 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				(after boot process, triggered by power-on or reboot)
HMAC-SHA2-384 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
HMAC-SHA2-512 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
HMAC-SHA3-224 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
HMAC-SHA3-256 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
HMAC-SHA3-384 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
HMAC-SHA3-512 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-5) (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
RSA SigVer (FIPS186-5) (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
ECDSA SigGen (FIPS186-5) (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
ECDSA SigVer (FIPS186-5) (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
EDDSA SigGen (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
EDDSA SigVer (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
ML-KEM Encapsulation (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				power-on or reboot)
ML-KEM Decapsulation (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
ML-DSA SigGen (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
ML-DSA SigVer (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
KAS-ECC-SSC Sp800-56Ar3 (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
KDF TLS (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
TDES-CBC (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process, triggered by power-on or reboot)
TDES-ECB (A6066)	KAT	CAST	Every 24h	Automatically or on-demand (after boot process,

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				triggered by power-on or reboot)
Firmware Load Test	KAT	SW/FW Load	On-demand	On-demand (on SW/FW load or after boot process)
Entropy 90 Repetition Count Test (RCT)	RCT	CAST	On-demand	On-demand (continuous during the entropy source operation)
Entropy 90 Adaptive Proportion Test (APT)	APT	CAST	On-demand	On-demand (continuous during the entropy source operation)
ECDSA KeyGen (FIPS186-5) (A6066)	PCT	PCT	On-demand	On-demand (for Key Pair Generation)
RSA KeyGen (FIPS186-5) (A6066)	PCT	PCT	On-demand	On-demand (for Key Pair Generation)
EDDSA KeyGen (A6066)	PCT	PCT	On-demand	On-demand (for Key Pair Generation)
ML-DSA KeyGen (A6066)	PCT	PCT	On-demand	On-demand (for Key Pair Generation)
ML-KEM KeyGen (A6066)	PCT	PCT	On-demand	On-demand (for Key Pair Generation)

Table 26: Conditional Periodic Information

The module performs Periodic Self-Tests every 24 hours.

The execution of the Periodic Self-Tests is not affected by or affects other uses of the HSM, then there is no current operation listed above that could interrupt or delay the HSM performance and vice-versa.

Note: The execution and the results from the periodic routine are not displayed in the frontal panel. It can be checked getting the module's log.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	Failure of any Self-Test	Failure of any Pre-Operational Self-tests. Failure of any Conditional Self-tests. Failure of any Periodic Self-Test Information	Click on MENU to restart the module or click on OK to proceed. If the latter option is chosen, the only services available will be: “Get System Log”, “Restart” and “Shutdown”. Power cycle or re-start the module to recover it from this state	Right after test execution, the test will be tagged as “FAIL” on the frontal display. After the completion of the FIPS tests, the device switches to Error State. This condition is indicated on the frontal display by the message “Auto Test has failed”. Also, it can be checked by getting the log file
Start Failures	Failures at the hardware	Failures at the hardware of the module detected during the boot, preventing its operation	Click on MENU to restart the module or click on OK to proceed. If the latter option is chosen, the only services available will be: “Get System Log”, “Restart” and “Shutdown”. Power cycle or restart the module to recover it from this state	The frontal display shows the message “Failure” and one of the following conditions: · “Cryptographic Module Start Failure” · “CPU start Failure” After the message has been displayed for 10 seconds, the module is restarted, and if the failure persists, the kNET switches to Power Off State

Table 27: Error States

Errors are indicated on the frontal display.

Besides the screen that informs the occurrence of an EFP event, in case of hardware malfunction preventing the module operation, the screen “Failure” will be shown before the module is power cycled in an attempt to recover it from this state. If this error persists after the power cycle, the kNET switches to Power Off State.

In case the same behavior is seen after the operator power cycles the kNET, contact Kryptus’ support.

On completion of the auto-tests, if any test has failed, the display will show the following message:

“WARNING: Auto Test has failed.”

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Installation

11.1.1.1 Secure Location

The module shall operate in a protected environment that limits physical access to the appliance to authorized PCOs. The equipment must be installed and maintained by PCOs in a secure state that mitigates against the following risks:

- Protection against loss or theft of the module.
- Inspection to deter and detect tampering (Ref. 11.1.2.2 Detecting Modifications and Tampering).
- Protection against changes on the hardware appliance.

11.1.1.2 Installation on the rack

Figure 7: Installation on the rack

11.1.2 Initialization

11.1.2.1 Secure Initialization

During device initialization, a test suite is executed to ensure the integrity of the module. This suite verifies that no algorithm tampering has occurred. If any of the power-on self-tests fail, the module will be considered insecure and will not initialize, entering an error state. The Frontal Board Interface visually indicates the success or failure of the self-tests, providing assurance to the operator and preventing any potential malicious hardware intervention.

11.1.2.2 Detecting Modifications and Tampering

Following setup, it is highly advisable to extract logs from the acquired devices prior to initiating any cryptographic operations. In the event of tampering attempts occurring between shipment and receipt, these logs will provide comprehensive details regarding any such incidents and the nature of tampering detected. It is imperative to verify the absence of any such log entries before proceeding with routine operations using the module, ensuring the utmost safety and security. In addition, as a physical security measure, it is strongly recommended that the tamper-evident seal of the TOEPP be verified.

Figure 8: Tamper-evident seals

Figure 9: Tamper-evident seals – zoom in

11.1.2.3 Serial Number Validation

After extracting the log in the previous step, the header of the log file should include information about the device's serial. Please check that the serial number therein informed is equal to the serial number printed on the label affixed to the back of the device.

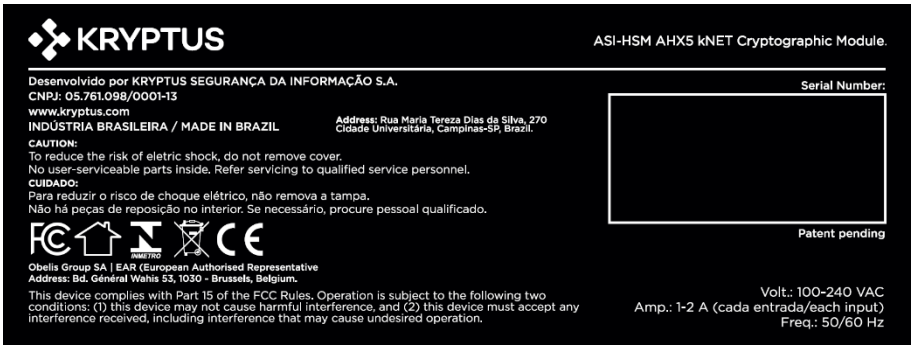

Figure 10: Label affixed to the back of the device

11.1.2.4 Software Validation

Software validation occurs automatically upon boot-up by the module during the decryption of the system image. If the decryption process fails, the device will reject the boot-up sequence.

11.1.3 Startup Procedure

The startup process is fully described in sections 11.2.1 HSM Initial Configuration and 11.2.2 Get Device Status.

11.2 Administrator Guidance

11.2.1 HSM Initial Configuration

Before proceeding, it is crucial to configure the device network, initialize the HSM, set and confirm the mode of operation, verify the hardware and software versions, and ensure that the module has passed all tests and is fully operational. These steps are listed below:

1. HSM Network Configuration:

    a. When a factory state kNET HSM is turned on, the frontal panel informs that the HSM is not configured yet. Tap the CONFIRM button to proceed with the initialization according with [Kryptus FIPS 140-3 Mode Manual].

Figure 11: HSM Frontal board after self-tests and not configured

2. HSM Initialization in Approved Mode:
   a. T The Temporary PIN should be displayed in the frontal panel after configuring the network interface:

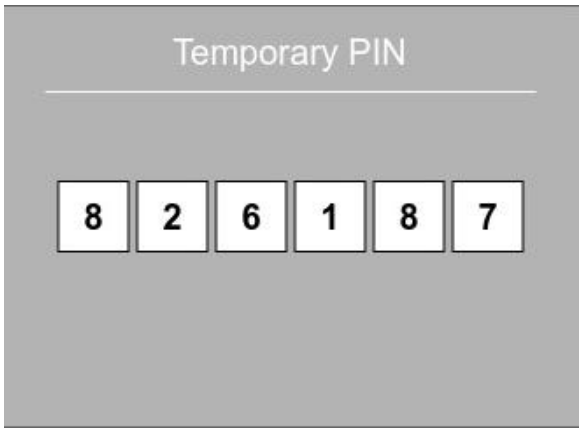

Figure 12: HSM Frontal board displaying the Temporary PIN

   b. Initialize PHSM operation through the CLI (Command Line Client) is used to complete the HSM initialization process using the command below:
      - ./command_line_client man initialize-phsm
        --username DEFAULT_PCO
        --password <TEMP_PIN>
        --host <kNET-IP-ADDRESS>
        --port 60000
        --old-password <TEMP_PIN>
        --new-password <NEW_PASSWORD>
        --hostname <HOSTNAME>
        --country <COUNTRY>
        --state-or-province <STATE_OR_PROVINCE>
        --locality <LOCALITY>
        --organization <ORGANIZATION>
        --organizational-unit <OU>

--hsm-name <HSM_NAME>
--use-system-date-time
--out-cert <OUTPUT_CERT_PATH>
--hsm-policy fips140_3
--insecure

The Approved mode of operation is strictly enforced by specifying the *--hsm-policy fips140_3* flag.

IMPORTANT: Once this policy is committed during initialization, the module cannot revert to a non-Approved policy without a **full factory reset** (zeroization) of the module.

Note: The flag –insecure indicates that the SSL verification is disabled. In other words, the client trusts the CA certificate provided by the server when the communication is established instead of verifying it, which could be exploited by man-in-the-middle attacks, hence the “insecure” name. However, the exchange of information between client and server still happens in an encrypted channel secured by the TLS key exchange. Besides testing purposes, we strongly recommend using the CA Certificate instead.

For additional information regarding the CLI usage, consult the instructions stated in [Kryptus FIPS 140-3 Mode Manual]

3. Check the Frontal Panel:
   a. If the initialization process is completed successfully, the CLI operation will return with no errors and the HSM’s frontal panel will display the screen:

Figure 13: HSM Frontal Board Default Screen

11.2.2 Get Device Status

Getting the device status can be achieved by using the following command:

- ./command_line_client man get-device-information --username DEFAULT_PCO --interactive-password --host <kNET-IP-ADDRESS> --port 60000 –insecure

Specifying the username and password as well as the host and port.

Note: The flag –insecure indicates that the SSL verification is disabled. In other words, the client trusts the CA certificate provided by the server when the communication is established instead of verifying it, which could be exploited by man-in-the-middle attacks, hence the “insecure”

name. However, the exchange of information between client and server still happens in an encrypted channel secured by the TLS key exchange. Besides testing purposes, we strongly recommend using the CA Certificate instead.
The command returns status information about the device temperature, battery voltage, monitor state, intrusion state, device state, Approved Mode, firmware version, serial number and SNMP Configurations.
Below is an example of the output of the command

```
kNET Status:
   Temperature (Millidegree Celsius ): 38250
   Battery Voltage (millivolts): 3651
        Monitor State: Nominal
        Intrusion State: Nominal
        KNET State: Operational
        Approved Mode: On

kNET Version: 1.1.0

kNET Serial Number: 000000000000XXXX

SNMP Configuration:
        SNMP v1 is enabled
        SNMP v2c is enabled
        SNMP v3 is disabled
        SNMP traps are disabled
        SNMP System Description: Network HSM - kNET
        SNMP System Contact: contact@knet.com
        SNMP System Name: kNET production 1
        SNMP System Location: Department 3
```

The kNET Version in the output of this command is the firmware version, which should be in version **1.1.0**.
The Approved Mode should be **ON**, indicating the correct mode.

11.2.3 Get Software Version
Getting the device's software version can be achieved by using the following command:

- ./command_line_client man get-knet-server-version --username DEFAULT_PCO --interactive-password --insecure --host <kNET-IP-ADDRESS> --port 60000

This command will return only the version of the software in a single line, which should be in version **1.50.0**.
The same information can be double checked in the next command.
Note: The flag –insecure indicates that the SSL verification is disabled. In other words, the client trusts the CA certificate provided by the server when the communication is established instead of verifying it, which could be exploited by man-in-the-middle attacks, hence the "insecure" name. However, the exchange of information between client and server still happens in an encrypted channel secured by the TLS key exchange. Besides testing purposes, we strongly recommend using the CA Certificate instead.

11.2.4 Get Approved Mode
Checking if the HSM is correctly set in the Approved Mode, using the following command:

- ./command_line_client man get-log --username DEFAULT_PCO --interactive-password --insecure --host <kNET-IP-ADDRESS> --port 60000 --startdate <DATE> --outfile /tmp/outfile.txt

This command will generate an output file, in the header of this output file will be the information about the software version, device serial number and policy, which is supposed to be set as FIPS 140-3.
The *startdate* parameter should be just one hour before the command is executed, this will get just some logs instead of every log entry, since we are interested only on the header and not in the log entries.
Note: The flag –insecure indicates that the SSL verification is disabled. In other words, the client trusts the CA certificate provided by the server when the communication is established instead of verifying it, which could be exploited by man-in-the-middle attacks, hence the “insecure” name. However, the exchange of information between client and server still happens in an encrypted channel secured by the TLS key exchange. Besides testing purposes, we strongly recommend using the CA Certificate instead.
Below is an example of the output file of the command:

```
-------------------------------------
kNET Version: 1.50.0
Device serial number: 0000000000000000
Policy name: FIPS 140-3
-------------------------------------
2024-08-16T17:00:53.508864+00:00 ahx5 PHSM[17796]:       [Info] [IPC-JSON]
[17886:0:0] [] REQUEST [] [] [GetSNMPData] [] []
2024-08-16T17:00:53.629664+00:00 ahx5 PHSM[17796]:       [Info] [IPC-JSON]
[17886:0:0] [] RESPONSE [] [] [GetSNMPData] [] [] [Success] []
```

11.2.5 Checking the Hardware Version
Getting the device's hardware version can be achieved by using the following SNMP command:

- snmpwalk -v 2c -t 5 -c public 172.30.203.54 iso.3.6.1.4.1.44588.1.1.1.3

This command will return only the kNET's hardware version in a single line, which should be in version **1.1.0**.
Note: The OID 3.6.1.4.1.44588.1.1.1.3 is equivalent of the device’s hardware.

11.3 Non-Administrator Guidance

The module makes a clear separation between Administrators and Users. Access to management operations in the module is exclusive to administrator operators: the PCO and the VCO. The former has rights to manage the whole device, while the latter can only manage its respective VHSM. Meanwhile the User type does not have the same management capabilities as the previous two but is the only one that can execute cryptographic operations and own cryptographic objects.

All possible operations are detailed in the kNET Operations Document, which outlines the full range of HSM functions for both Administrators (PHSM and VSHM) and Users. The CLI Manual provides guidance on executing these operations, including all necessary parameters.

11.4 Design and Rules

Not applicable for this module.

11.5 Maintenance Requirements

The module does not require any periodic maintenance besides the physical inspection of the TOEPP for signs of tamper, as described in Section 11.1.2.2 Detecting Modifications and Tampering.

11.6 End of Life

The recommended processes for the secure sanitization and secure destruction of the module are reported in a proprietary document. For further information, request the above-mentioned document.

12 Mitigation of Other Attacks

12.1 Attack List

N/A. No mitigation of other attacks is implemented on the module.