KRYPTUS
shaping trusted bonds

ASI-HSM AHX5 KNET Cryptographic Module

Hardware Version 1.0.1, Firmware Version 1.0.1

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.3.2

January 25, 2023

KRYPTUS
shaping trusted bonds

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Scope

This document is the FIPS 140-2 ASI-HSM AHX5 KNET Cryptographic Module Non-Proprietary Security Policy. It describes how the HSM meets the security requirements of FIPS 140-2.

1.2 Overview

The ASI-HSM AHX5 kNET Cryptographic Module (Figure 1.1) is a multi user, multi-chip embedded crypto-module. The FIPS 140-2 cryptographic boundary is the metal case containing the entire ASI-HSM AHX5 kNET Cryptographic Module. The ASI-HSM AHX5 kNET Cryptographic Module is referred to in the remainder of this document as the module.

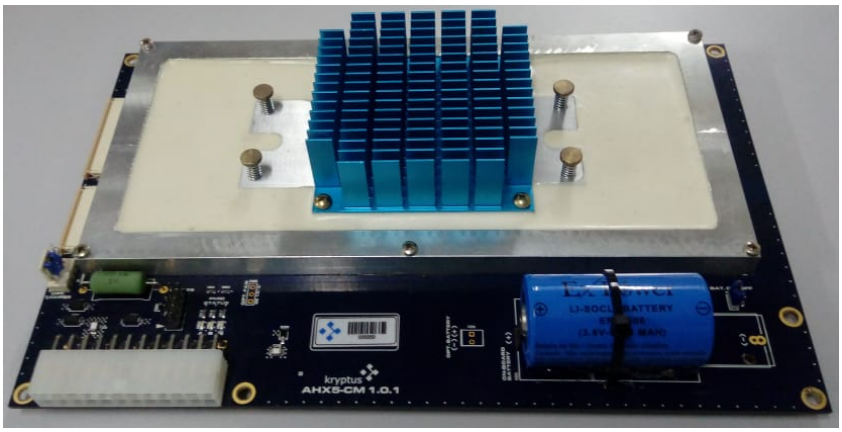

Figure 1.1: ASI-HSM AHX5 kNET Cryptographic Module.

The module exists to provide cryptographic services to applications running on behalf of its users which communicate with it via a standard Ethernet interface using IP protocols. In order to provide these services, the module also requires a power supply.

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

1.3 Acronyms and Abbreviations

AES Advanced Encryption Standard
API Application Programming Interface
CA Certification Authority
CBC Cipher Block Chaining
CPU Central Processing Unit
CSP Critical Security Parameter
CTR Counter
DES Data Encryption Standard
DSA Digital Signature Algorithm
DRBG Deterministic Random Bit Generator

ECB Eletronic Codebook
ECDSA Elliptic Curve Digital Signature Algorithm
EMC Eletromagnetic Compatibility
EMI Eletromagnetic Interference
FIPS Federal Information Processing Standard
GCM Galois/Counter Mode
HMAC Hash-based Message Authentication Code
HSM Hardware Security Module
ID Identifier
IP Internet Protocol
KMIP Key Management Interoperability Protocol
KW Key Wrapping
LED Light-emitting Diode
MAC Message Authentication Code
MD5 Message-Digest algorithm 5
NIST National Institute of Standards and Technology
OAEP Optimal Asymmetric Encryption Padding
OTP One Time Password
PCB Printed Circuit Board
PCO Physical Crypto Officer
PHSM Physical Hardware Securityu Module
PIN Personal Identification Number
RAM Ramdom Access Memory
RNG Random Number Generator
RSA RivestShamirAdleman
RTC Real Time Clock
SEC Standards for Efficient Cryptography
SHA Secure Hash Algorithm
SKMM Secure Key Management Module
SNMP Simple Network Management Protocol
TLS Transport Layer Security
TRNG True Random Number Generator
USB Universal Serial Bus
VCO Virtual Crypto Officer
VHSM Virtual Hardware Security Module
XML eXtensible Markup Language

2 SECURITY LEVEL

The module meets the overall requirements applicable to Level 3 Security for FIPS 140-2. Table 2.1 lists the security level for each requirements section.

Table 2.1: Validation Level by FIPS 140-2 Section

Security Requirements section	**Level**
Cryptographic module specification	3
Cryptographic module ports and interfaces	3
Roles, services, and authentication	3
Finite state model	3
Physical security (multiple-chip embedded)	3
Operational environment	N/A
Cryptographic key management	3
Electromagnetic interference/electromagnetic compatibility (EMI/EMC)	3
Self-tests	3
Design assurance	3
Mitigation of other attacks	N/A
Cryptographic module security policy	3

3 MODES OF OPERATION

The module supports two modes of operation:

- FIPS Mode
- Non-FIPS Mode

When the module is initialized with the Initialize HSM function, the operator can choose the mode of operation to be used. The mode cannot be changed unless the module is reset to the factory state with the Reset HSM function, and reinitialized in the chosen mode.

3.1 FIPS Mode Algorithms

In FIPS Mode, the supported FIPS-Approved algorithms are those listed in Table 3.1:

Table 3.1: Supported FIPS-Approved Algorithms.

CAVP Cert	**Algorithm**	**Standard**	**Mode/Method**	**Key Lengths, Curves or Moduli**	**Use**
A3223	AES	FIPS 197, SP 800-38A	ECB, CBC, CTR	128, 192, 256	Data Encryption/Decryption
A3223	AES	FIPS 197, SP 800-38F	KW	128, 192, 256	Key Wrapping/Unwrapping
A3223	AES	SP 800-38D	GCM	128, 192, 256	Message Authentication, Data Encryption/Decryption
A3223	Triple DES	SP 800-67	ECB, CBC, CTR	Three-Key Triple DES	Data Encryption/Decryption
A3223	SHA	FIPS 180-4	SHA-224, SHA-256, SHA-384, SHA-512		Message Digest, Digital Signature Generation, Digital Signature Verification
A3223	HMAC	FIPS 198-1	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Any	Message Authentication
A3223	DSA	FIPS 186-4		224, 256	Key Pair Generation
A3223	DSA	FIPS 186-4	SHA-224, SHA-256, SHA-384, SHA-512	224, 256	Digital Signature Generation
A3223	DSA	FIPS 186-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	160, 224, 256	Digital Signature Verification

Table 3.1: Supported FIPS-Approved Algorithms (continued).

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
A3223	RSA	FIPS 186-4		2048, 3072, 4096	Key Pair Generation
A3223	RSA	FIPS 186-4	SHA-224, SHA-256, SHA-384, SHA-512 PKCS1 v1.5 and PSS	2048, 3072, 4096	Digital Signature Generation
A3223	RSA	FIPS 186-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 PKCS1 v1.5 and PSS	1024, 2048, 3072, 4096	Digital Signature Verification
A3223	RSA	FIPS 186-2 (Legacy)	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 PKCS1 v1.5 and PSS	1024, 1536, 2048, 3072, 4096	Digital Signature Verification
A3223	ECDSA	FIPS 186-4		P-224, P-256, P-384, P-521	Key Pair Generation
A3223	ECDSA	FIPS 186-4	SHA-224, SHA-256, SHA-384, SHA-512	P-224, P-256, P-384, P-521	Digital Signature Generation
A3223	ECDSA	FIPS 186-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	P-224, P-256, P-384, P-521	Digital Signature Verification
#349	DRBG	SP 800-90A	Hash_DRBG (SHA2-256)	-	Key Generation
Vendor Affimed	CKG	SP 800-133	-	-	Key Generation. Resulting Symmetric keys and seeds used for asymmetric key generation are unmodified output from the module's Approved DRBG.
A3223	CVL (TLS 1.2 KDF)	SP 800-135 Rev 1	SHA2-256	-	Key derivation function used in the TLS protocol.

Table 3.1: Supported FIPS-Approved Algorithms (continued).

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
A3223	KAS	SP-800-56Ar3	Ephemeral Unified	P-256, P-384, P-521	SP 800-56A rev3 KAS-SSC (Cert. #A3223) with SP 800-135 rev 1 TLS 1.2 KDF CVL (Cert. #A3223). Compliant to IG D.8 X1 Option 2, testing the shared secret and separately testing the key derivation function.

KTS (AES Cert. #A3223; key establishment methodology provides between 128 and 256 bits of encryption strength). The module generates cryptographic keys whose strengths are modified by available entropy. The minimum number of bits of entropy generated by the module for use in key generation is 184. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table. At this time, RSA Key Pair generation modulo 4096 and RSA SigGen modulo 4096 cannot be tested. As such, they are not listed on A3223.

Besides, the module supports the non-FIPS 140-2 approved algorithms listed in Table 3.2. Those algorithms may be used in the FIPS-mode of operation.

Table 3.2: Non-Approved but Allowed Cryptographic Algorithms.

Algorithm	Caveat	Use
Brainpool P-224 (r1/t1)	Security Strength: 112 bits	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-256 (r1/t1)	Security Strength: 128 bits	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-320 (r1/t1)	Security Strength: 160 bits	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-384 (r1/t1)	Security Strength: 192 bits	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Brainpool P-512 (r1/t1)	Security Strength: 256 bits	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
SEC P-256 (k1)	Security Strength: 128 bits	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
NDRNG		Seed Approved DRBG

3.2 Non-FIPS Mode Algorithms

When configured in Non-FIPS Mode the algorithms in Table 3.3 are supported as well.

Table 3.3: Supported Non-Approved Algorithms.

Algorithm	**Use**
HMAC-MD5	Message Authentication
RSA	Digital Signature Generation with no padding (raw). Any key size multiple of 16, with a minimum size of 512 bits and maximum of 8192 bits (e.g. 1024, 1984 bits) for Key Pair Generation, Digital Signature Generation and Digital Signature Verification:. Data Encryption and Data Decryption with OAEP or PKCS1 v1.5 padding and with no padding. Key wrapping; key establishment methodology provides 112 bits of security strength.
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
Ed25519	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
Ed448	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
E-521	Key Pair Generation, Digital Signature Generation, Digital Signature Verification
SHAKE256 (with 512-bit output) (non-compliant to FIPS-202)	Hash Computation; Hash parameter in Digital Signature Generation / Verification
MD5	Message Digest

4 IDENTIFICATION AND AUTHENTICATION POLICY

4.1 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 priviledged 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 priviledged 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, altering the virtual module configurations and backup related operations.
- **User**: Created by a VCO, it is responsible for all cryptographic operations and management of cryptographic objects that it has ownership.

4.2 Authentication

The module enforces indentity-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 supports the following authentication schemes:

- **Password-based authentication**: 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 *).
- **Certificate-based authentication**: private key and certificate. 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.
- **Quorum authentication**: 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 quroum. 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.

Table 4.1 summarizes the roles and authentication methods.

Table 4.1: Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
PCO VCO User	Identity-based	Password-based: username and password; Certificate-based: certificate and digitally-signed data (per TLS protocol). Quorum Authentication: one of the above.

Table 4.2 brings the cryptographic strength of the authentication mechanisms.

Table 4.2: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password-based	The worst case scenario is a 6-character password, containing uppercase and lowercase characters, symbols or digits totalling 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 probabilty of 7/782,757,789,696 = 1/111,822,541,385 which is smaller than the required 1/100,000.
Certificate-based	The strength of the mechanism relies on the strength of the digital signature employed. The module will restrict the algorith 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.
Quorum Authentication	The strength of the mechanism relies on the strength of 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.

The module also supports multi-factor authentication mechanisms. One of the mechanisms in Table 4.2 must always be used, but the operator can strengthen the authentication security providing additionally (but not alone), one or more of the mechanisms in Table 4.3.

Table 4.3: Strengths of Additional Authentication Mechanisms

Authentication Mechanism	**Strength of Mechanism**
Time-based OTP	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 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. Sice 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 probabilty 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.
HMAC-based OTP	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 successfull requests done so far using the mechanism. The strength of the mechanism relies on the strength of HMAC-SHA1 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. Sice 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 probabilty of 7/1,000,000 = 1/142,857 which is smaller than the required 1/100,000.
Client token	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 Certificate-based authentication.

5 ACCESS CONTROL POLICY

5.1 Supported Roles

The following roles are supported by this module:

- Physical HSM Cryptographic Officer (PCO)
- Virtual HSM Cryptographic Officer (VCO)
- User

Unauthenticated operators are able to use some of the services. The module distinguishes between operators with and without physical access. Physical access implies access to the frontal board and/or serial interfaces.

5.2 Services Provided

Tables 5.1, 5.2, 5.3, 5.4 and 5.5 list all the services provided by the module, according to which roles they are authorized.

Table 5.1: Services Authorized for PCO Role.

Service	**Description**
Initialize HSM	Initialize the HSM; create first PCO with provisory password (PIN)
Configure Network	Configure network settings (IP, netmask, gateway)
Get Network Configuration	Get network settings
Reset HSM	Reset HSM to factory state
Set Date Time	Set the current date and time
Get Date Time	Get the current date and time
Get HSM Usage	Get CPU, RAM and disk usage
Create User	Create a PCO
Destroy User	Destroy a PCO
List Users	List PCOs
Change Password	Change a PCO password
Reset Password	Reset a PCO password
Register Certificate	Sign a CSR and register the certificate for PCO authentication
Activate Quorum Authentication	Activates quorum authentication for the PHSM
Deactivate Quorum Authentication	Deactivates quorum authentication for the PHSM
Get Quorum Authentication State	Check the quorum authentication state of the PHSM (i.e. activated or not, the minimum quorum)
Get Quorum Authentication Status	Check the quorum authentication status of the PHSM (i.e. number of operations or time left)
Vote Quorum Authentication	Inform the operator's verdict for quorum authentication operations (allow or deny)

Table 5.1: Services Authorized for PCO Role (continued).

Start Quorum Authentication	Request that operators vote to start quorum authentication votes to allow critical operations
Stop Quorum Authentication	Stop quorum authentication, blocking critical operations when quorum authentication is activated (a new start is required)
Create Virtual HSM	Create a Virtual HSM along with its first VCO with provisory password (PIN)
List Virtual HSMs	List all Virtual HSMs
Activate Virtual HSM	Activate a Virtual HSM
Deactivate Virtual HSM	Deactivate a Virtual HSM
Delete Virtual HSM	Delete a Virtual HSM and all of its objects
Edit Virtual HSM	Edit a VHSM configuration
Export VHSM	Export an entire Virtual HSM; its users and objects
Import VHSM	Import an entire Virtual HSM
Export PHSM	Export an entire Physical HSM, its users and VHMs
Import PHSM	Import an entire Physical HSM
Get Requester Type	Get the role of the requester
Update Firmware	Update the module firmware. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.
Get Log Level	Get the current log level
Set Log Level	Set the current log level
Get System Log	Retrieve the PHSM log
Show Status	Get the status of the HSM
Shutdown	Shutdown the HSM
Restart	Restart the HSM and Perform self-tests on demand
Get Device Information	Get device version, status, serial number and other information
Get TLS Certificate	Get the TLS certificate of the PHSM server and the correspoding CA
Renew Server Certificate	Renew the PHSM server TLS certificate
Activate OTP	Activate OTP for the PCO
Manual Activate OTP	Manually activate OTP for the PCO, informing the OTP key
Deactivate OTP	Deactivates OTP for the PCO
Register Authentication Certificate	Register a certificate to be used during PCO authentication
Remove Authentication Certificate	Delete a certificate used for authentication

Table 5.1: Services Authorized for PCO Role (continued).

List Authentication Certificates	List the registered certificates for the PCO
Start Token Authentication	Return a token that the PCO signs to authenticate using one of the registered certificates
Get Session Credential	Retrieves a session token used for further authentications

Table 5.2: Services Authorized for VCO Role.

Service	**Description**
Service	**Description**
Get VHSM Usage	Get VHSM CPU, RAM and disk usage
Create User	Create a VCO or User
Destroy User	Destroy a VCO or User along with all its objects
Reset Password	Reset a VCO's or User's password
Register Certificate	Sign a CSR and register the certificate for VCO authentication
Activate Quorum Authentication	Activates quorum authentication for the VHSM
Deactivate Quorum Authentication	Deactivates quorum authentication for the VHSM
Get Quorum Authentication State	Check the quorum authentication state of the VHSM (i.e. activated or not, the minimum quorum)
Get Quorum Authentication Status	Check the quorum authentication status of the VHSM (i.e. number of operations or time left)
Vote Quorum Authentication	Inform the operator's verdict for quorum authentication operations (allow or deny)
Start Quorum Authentication	Request that operators vote to start quorum authentication votes to allow critical operations
Stop Quorum Authentication	Stop quorum authentication, blocking critical operations when quorum authentication is activated (a new start is required)
Activate User	Activate a User
Deactivate User	Deactivate a User
Get Requester Type	Get the role of the requester
Get Log Level	Get the current log level
Set Log Level	Set the current log level
Get System Log	Retrieve the VHSM log
Get Device Information	Get device version, status, serial number and other information
Get TLS Certificate	Get the TLS certificate of the VHSM server and the correspoding CA
Renew Server Certificate	Renew the VHSM server TLS certificate
Activate OTP	Activate OTP for the VCO

Table 5.2: Services Authorized for VCO Role (continued).

Manual Activate OTP	Manually activate OTP for the VCO, informing the OTP key
Deactivate OTP	Deactivates OTP for the VCO
Register Authentication Certificate	Register a certificate to be used during VCO authentication
Remove Authentication Certificate	Delete a certificate used for authentication
List Authentication Certificates	List the registered certificates for the VCO
Start Token Authentication	Return a token that the VCO signs to authenticate using one of the registered certificates
Get Session Credential	Retrieves a session token used for further authentications

Table 5.3: Services Authorized for User Role

Service	**Description**
Change Password	Change the User password
Register Certificate	Sign a CSR and register the certificate for User authentication
Activate Quorum Authentication	Activates quorum authentication for the usage of an object
Deactivate Quorum Authentication	Deactivates quorum authentication for the usage of an object
Get Quorum Authentication State	Check the quorum authentication state of the usage of an object (i.e. activated or not, the minimum quorum)
Get Quorum Authentication Status	Check the quorum authentication status of the usage of an object (i.e. number of operations or time left)
Vote Quorum Authentication	Inform the operator's verdict for quorum authentication operations (allow or deny)
Start Quorum Authentication	Request that operators vote to start quorum authentication votes to allow critical operations
Stop Quorum Authentication	Stop quorum authentication, blocking critical operations when quorum authentication is activated (a new start is required)
Get System Log	Retrieve the log of operations performed by the user
List Certificates	List certificates registered for User authentication
Delete Certificate	Delete certificate registered for User authentication
Set User Object Permission	Set object permissions for a specific user
Get User Object Permission	Get object permissions for a specific user
Get Requester Type	Get the role of the requester

Table 5.3: Services Authorized for User Role (continued)

Service	Description
Create	KMIP: Create symmetric key
CreateKeyPair	KMIP: Create asymmetric key pair
Register	KMIP: Register an object
Locate	KMIP: Locate a object given its attributes
Check	KMIP: Check usage quota of a object
Get	KMIP: Get an object
GetAttributes	KMIP: Get attribute values of an object
GetAttributeList	KMIP: Get attributes of an object
AddAttribute	KMIP: Add attribute value to an object
ModifyAttribute	KMIP: Modify an attribute value
DeleteAttribute	KMIP: Delete an attribute value from an object
Activate	KMIP: Activate object
Revoke	KMIP: Revoke object
Destroy	KMIP: Destroy object
Query	KMIP: Query for information about the module
DiscoverVersions	KMIP: Query for supported KMIP versions
Encrypt	KMIP: Encrypt data
Decrypt	KMIP: Decrypt data
Sign	KMIP: Sign data
SignVerify	KMIP: Verify signature
Sign XML	Sign data according to XMLDSig standard
Verify XML	Verify XML signature according to XMLDSig standard
MAC	KMIP: Generate MAC of data
MACVerify	KMIP: Verify a MAC
RNGRetrieve	KMIP: Retrieve randomness
RNGSeed	KMIP: Seed RNG
Hash	KMIP: Compute hash
Load Key	Load key in cache
Fast Sign	Faster sign operation with cached key
Validate	KMIP: Validates a digital certificate or certificate chain
Get Session Credential	Retrieves a session token used for further authentications
Get TLS Certificate	Get the TLS certificate of the VHSM server and the correspoding CA
Activate OTP	Activate OTP for the User
Manual Activate OTP	Manually activate OTP for the User, informing the OTP key
Deactivate OTP	Deactivates OTP for the User
Register Authentication Certificate	Register a certificate to be used during User authentication

Table 5.3: Services Authorized for User Role (continued)

Service	Description
Remove Authentication Certificate	Delete a certificate used for authentication
List Authentication Certificates	List the registered certificates for the User
Start Token Authentication	Return a token that the User signs to authenticate using one of the registered certificates
Get Session Credential	Retrieves a session token used for further authentications

Table 5.4: Services Authorized for Unauthenticated Operator without Physical Access

Service	Description
Query	KMIP: Query for information about the module
DiscoverVersions	KMIP: Query for supported KMIP versions

Table 5.5: Services Authorized for Unauthenticated Operator with Physical Access

Service	Description
Initialize HSM	Initialize the HSM; create first PCO with provisory password (PIN)
Configure Network	Configure network settings (IP, netmask, gateway)
Get Network Configuration	Get network settings
Reset HSM	Reset HSM to factory state
Get Date Time	Get the current date and time
Shutdown	Shutdown the HSM
Restart	Restart the HSM

5.3 Cryptographic Keys and Critical Security Parameters (CSPs)

Table 5.6 lists all cryptographic keys and CSPs stored in the module. In this table, "Password" refers to 8 or more alphanumeric characters, which may include both upper and lower case letters, punctuation marks, and symbols (such as @, &, and *).

Table 5.6: Cryptographic Keys and CSPs

Key Name	**Type**	**Generation / Input**	**Output**	**Storage**	**Zeroization**	**Description**
Super Root Key Hash	SHA-256 hash of four RSA Public Keys with at least 2048 bits	Entered during manufacturing	Never	One-time programmable memory	Never	Used to verify boot image (secure boot)
Job Descriptor Key Encryption Key	256-bit AES Key	Generated internally on boot	Never	Temporarily in secure processor memory	Reboot	Encrypts keys in memory while they are being used
PHSM Module Key	3072-bit RSA Private Key	Entered during manufacturing	Never	Obfuscated in disk	Never	Identifies the module; decrypts firmware updates
PHSM Module Certificate	Certificate	Entered during manufacturing	Never	Disk	Never	Certificate of the module; matches PHSM Module Key
Kryptus kNET CA Certificate	Certificate	Entered during manufacturing	Never	Disk	Never	Certificate used to verify firmware updates
PHSM Server CA Key	3072-bit RSA Private Key	Generated internally during setup	Encrypted in backups	Obfuscated in disk	Return to factory state	Key of the PHSM TLS Server CA
PHSM Server CA Certificate	Certificate	Generated internally during setup	Get TLS Certificate operation, encrypted in backups	Disk	Return to factory state	Certificate of the PHSM TLS Server CA; matches PSHM Server CA Key

Table 5.6: Cryptographic Keys and CSPs (continued)

Key Name	Type	Generation / Input	Output	Storage	Zeroization	Description
PHSM Server Key	2048-bit RSA Private Key and/or 256-bit ECC Private Key	Generated internally during setup	Never	Obfuscated in disk	Return to factory state	Authentication during TLS key negotiation
PHSM Server Certificate	Certificate	Generated internally during setup	Get TLS Certificate operation	Disk	Return to factory state	Authentication during TLS key negotiation; matches PSHM Server Key
PHSM Client CA Key	3072-bit RSA Private Key	Generated internally during setup	Encrypted in backups	Obfuscated in disk	Return to factory state	Key of the PHSM TLS Client CA
PHSM Client CA Certificate	Certificate	Generated internally during setup	Get TLS Certificate operation, encrypted in backups	Disk	Return to factory state	Certificate of the PHSM TLS Client CA; matches PHSM Client CA Key
PCOs' Passwords	Password	Generated internally / Provided by user	Provisory password in Initialize HSM operation	Volatile memory	After obfuscation, reboot	PCOs' passwords
PCOs' Obfuscated Passwords	Obfuscated password	Derived from PCOs's Passwords	Encrypted in backups	Disk	When PCO deleted	Obfuscated passwords of PCOs
PCOs' Certificate Fingerprints	SHA-256 hashes	Generated internally	Encrypted in backups	Disk	When PCO deleted	Hashes of certificates authorized for each PCO

Table 5.6: Cryptographic Keys and CSPs (continued)

Key Name	Type	Generation / Input	Output	Storage	Zeroization	Description
PCO's OTP Key	160-bit HMAC-SHA1 key	Generated internally	Activate OTP operation, encrypted in backups	Obfuscated in disk	When PCO deleted or OTP deactivated	Key used for OTP generation
VHSM Server CA Keys	3072-bit RSA Private Key	Generated internally during VHSM creation	Encrypted in backups	Obfuscated in disk	Delete VHSM, return to factory state	Key of the VHSMs TLS Server CAs
VHSM Server CA Certificates	Certificates	Generated internally during VHSM creation	Get TLS Certificate operation, encrypted in backups	Disk	Delete VHSM, return to factory state	Certificates of the VHSMs TLS Server CAs; matches VHSM Server CA Keys
VHSM Server Keys	2048-bit RSA Private Key and/or 256-bit ECC Private Key	Generated internally during VHSM creation	Never	Obfuscated in disk	Delete VHSM, return to factory state	Authentication during TLS key negotiation
VHSM Server Certificates	Certificates	Generated internally during VHSM creation	Get TLS Certificate operation	Disk	Delete VHSM, return to factory state	Authentication during TLS key negotiation; matches VHSM Server Keys
VHSM Client CA Keys	3072-bit RSA Private Key	Generated internally during VHSM creation	Encrypted in backups	Obfuscated in disk	Delete VHSM, return to factory state	Key of the VHSMs TLS Client CAs
VHSM Client CA Certificates	Certificate	Generated internally during VHSM creation	Get TLS Certificate operation, encrypted in backups	Disk	Delete VHSM, return to factory state	Certificates of the TLS Client CAs; matches VHSM Client CA Keys

Table 5.6: Cryptographic Keys and CSPs (continued)

Key Name	**Type**	**Generation / Input**	**Output**	**Storage**	**Zeroization**	**Description**
VCOs' Passwords	Password	Generated internally / Provided by user	Provisory password in Initialize HSM operation	Volatile memory	After obfuscation, reboot	VCOs' Passwords
VCOs' Obfuscated Passwords	Obfuscated password	Derived from VCOs's Passwords	Encrypted in backups	Disk	When VCO deleted	Obfuscated passwords of VCOs
VCOs' Certificate Fingerprints	SHA-256 hashes	Generated internally	Encrypted in backups	Disk	When VCO deleted	Hashes of certificates authorized for each VCO
VCO's OTP Key	160-bit HMAC-SHA1 key	Generated internally	Activate OTP operation, encrypted in backups	Obfuscated in disk	When VCO deleted or OTP deactivated	Key used for OTP generation
Users' Passwords	Password	Generated internally / Provided by user	Provisory password in Create User operation	Volatile memory	After obfuscation, reboot	Users' Passwords
Users' Obfuscated Passwords	Obfuscated password	Derived from Users' Passwords	Encrypted in backups	Disk	When User deleted	Obfuscated passwords of Users
Users' Certificate Fingerprints	SHA-256 hashes	Generated internally	Encrypted in backups	Disk	When User deleted	Hashes of certificates authorized for each User

Table 5.6: Cryptographic Keys and CSPs (continued)

Key Name	Type	Generation / Input	Output	Storage	Zeroization	Description
Users' Objects	RSA, DSA, ECDSA, AES or HMAC Key; Certificate	Generated internally or registered encrypted (wrapped)	Wrapped (encrypted) if allowed, encrypted in backups	Obfuscated in disk	When object is deleted; return to factory state	A cryptographic object generated or imported by a User
User's OTP Key	160-bit HMAC-SHA1 key	Generated internally	Activate OTP operation, encrypted in backups	Obfuscated in disk	When User deleted or OTP deactivated	Key used for OTP generation
ECDH Private Component	Private component of ECDH protocol	Generated internally	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Establishment of TLS session keys
ECDH Public Component	Public component of ECDH protocol	(for the module) Generated internally; (for a peer) Generated externally, entered into the module (in certificate form) in plaintext	(for the module) Exits the module in plaintext form; (for a peer) Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Establishment of TLS session keys

Table 5.6: Cryptographic Keys and CSPs (continued)

Key Name	Type	Generation / Input	Output	Storage	Zeroization	Description
TLS Peer Public Key	2048-bit RSA public key	Generated externally, imported in certificate form in plaintext	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Certificate-based authentication during TLS key negotiation
TLS Pre-Master Secret	(for RSA cipher suites) 384-bit random value; (for ECDH cipher suites) ECDH shared secret	(for RSA cipher suites) Generated externally, imported in encrypted form via RSA key transport; (for ECDH cipher suites) Derived internally via ECDH shared secret computation	(for RSA cipher suites) Never exits the module; (for ECDH cipher suites) Never exits the module	Plaintext in RAM	Upon module reboot; Upon completion of TLS Master Secret computation	Derivation of the TLS Master Secret
TLS Master Secret	384-bit shared secret	Derived internally using the TLS Pre-Master Secret via TLS KDF	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Derivation of the TLS Session Key and TLS Authentication Key

Table 5.6: Cryptographic Keys and CSPs (continued)

Key Name	**Type**	**Generation / Input**	**Output**	**Storage**	**Zeroization**	**Description**
TLS Session Key	128/256-bit AES key	Derived internally using the TLS Master Secret via TLS KDF	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Encryption and decryption of TLS session packets
TLS Authentication Key	160-bit (minimum) HMAC key	Derived internally using the TLS Master Secret via the TLS KDF	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Authentication of TLS session packets
DRBG C and V values	Internal DRBG state value	Generated internally	Never exits the module	Plaintext in secure processor register	Upon module reboot	Generation of random number

GCM IVs can be generated randomly, where an IV is not generated randomly the module supports the importing of GCM IVs. In approved mode, when a GCM IV is generated randomly, the module enforces the use of an approved DRBG in line with Section 8.2.2 of SP 800-38D. In approved mode, importing a GCM IV is non-conformant unless the source of the IV is also FIPS approved for GCM IV generation. Per IG A.5, in case the module's power is lost and then restored, the key used for the AES GCM encryption or decryption shall be redistributed.

The kNET HSM keep a counter of how many bytes a Triple-DES key may be able to encrypt. The kNET HSM does not allow the usage of a key to encrypt more than 2^{16} times. When the counter reaches zero, or when a user tries to protect more bytes than stored in this counter, the kNET HSM blocks the operation. The counter is stored in non-volatile memory, therefore rebooting the HSM won't reset the counter.

5.4 Access Rights

Table 5.7 lists all access rights granted over CSPs in each service. The "Type of Access" column uses letter to specify the following types of access:

R: Read access—the service reads the CSP;
W: Write access—the service writes to the CSP;
G: Generate access—the service generates the CSP;
E: Execute access—the service uses the CSP for a cryptographic operation;
Z: Zeroize access–the service zeorizes the CSP.

Some accesses are common between a all services for a particular role; this is indicated in the table. These access are related to the authentication of the TLS channel between the module and the client.

Some CSPs do not appear in the table. This is because they are accessed either by setup operations (before the module is ready for use) or by autonomous operations (e.g. on boot).

Table 5.7: Access Rights within Services

Service	**Role**	**Type of Access**	**CSPs**
(All PCO Services)	PCO	E	PHSM Server Key
		R	PHSM Server Certificate
		E	PHSM Client CA Certificate
		R	PCO's Certificate Fingerprint
		R	PCO's Password
		R	PCO's Obfuscated Password
		E	Job Descriptor Key Encryption Key
		G,E	TLS Session Keys
Initialize HSM	PCO	G,R	PCO's Password
		W	PCO's Obfuscated Password
Configure Network	PCO		None
Get Network Configuration	PCO		None
Reset HSM	PCO	Z	PHSM Server CA Key
		Z	PHSM Server CA Certificate
		Z	PHSM Server Key
		Z	PHSM Server Certificate

Table 5.7: Access Rights within Services (continued)

Service	Role	Type of Access	CSPs
		Z	PHSM Client CA Key
		Z	PHSM Client CA Certificate
		Z	PCOs' Passwords
		Z	PCOs' Obfuscated Passwords
		Z	PCOs' Certificate Fingerprints
		Z	VHSM Server CA Keys
		Z	VHSM Server CA Certificates
		Z	VHSM Server Keys
		Z	VHSM Server Certificates
		Z	VHSM Client CA Keys
		Z	VHSM Client CA Certificates
		Z	VHSM RNG Seed
		Z	VCOs' Passwords
		Z	VCOs' Obfuscated Passwords
		Z	VCOs' Certificate Fingerprints
		Z	Users' Passwords
		Z	Users' Obfuscated Passwords
		Z	Users' Certificate Fingerprints
		Z	Users' Objects
		Z	TLS Session Keys
Remove from Error State	PCO	R	PCOs' Passwords
Set Date Time	PCO		None
Get Date Time	PCO		None
Get HSM Usage	PCO		None
Create User	PCO	G,R	PCO's Password
	PCO	W	PCO's Obfsucated Password
Destroy User	PCO	Z	PCO's Obfuscated Password
		Z	PCO's Certificate Fingerprints
List Users	PCO		None
Change Password	PCO	R	PCO's Password
		W	PCO's Obfsucated Password
Reset Password	PCO	G,R	PCO's Password
		W	PCO's Obfuscated Password
Register Certificate	PCO	W	PCO's Certificate Fingerprint
List Certificates	PCO	R	PCO's Certificate Fingerprints
Delete Certificate	PCO	Z	PCO's Certificate Fingerprint
Activate Quorum Authentication	PCO		None
Deactivate Quorum Authentication	PCO		None
Get Quorum Authentication State	PCO		None
Get Quorum Authentication Status	PCO		None

Table 5.7: Access Rights within Services (continued)

Service	**Role**	**Type of Access**	**CSPs**
Vote Quorum Authentication	PCO		None
Start Quorum Authentication	PCO		None
Stop Quorum Authentication	PCO		None
Create Virtual HSM	PCO	G	VHSM Server CA Key
		W	VHSM Server CA Certificate
		G	VHSM Server Key
		W	VHSM Server Certificate
		G	VHSM Client CA Key
		W	VHSM Client CA Certificate
		G,R	VCO's Password
		W	VCO's Obfuscated Password
Edit Virtual HSM	PCO		None
List Virtual HSMs	PCO		None
Activate Virtual HSM	PCO		None
Deactivate Virtual HSM	PCO		None
Export VHSM	PCO	R	VHSM Server CA Key
		R	VHSM Server CA Certificate
		R	VHSM Client CA Key
		R	VHSM Client CA Certificate
		R	VCOs' Obfuscated Passwords
		R	VCOs' Certificate Fingerprints
		R	Users' Obfuscated Passwords
		R	Users' Certificate Fingerprints
		R	Users' Objects (Exportable)
Import VHSM	PCO	W	VHSM Server CA Key
		W	VHSM Server CA Certificate
		G	VHSM Server Key
		W	VHSM Server Certificate
		W	VHSM Client CA Key
		W	VHSM Client CA Certificate
		W	VCOs' Obfuscated Passwords
		W	VCOs' Certificate Fingerprints
		W	Users' Obfuscated Passwords
		W	Users' Certificate Fingerprints
		W	Users' Objects

Table 5.7: Access Rights within Services (continued)

Service	Role	Type of Access	CSPs
Export PHSM	PCO	R	PHSM Server CA Key
		R	PHSM Server CA Certificate
		R	PHSM Client CA Key
		R	PHSM Client CA Certificate
		R	PCOs' Obfuscated Passwords
		R	PCOs' Certificate Fingerprints
		R	VHSMs Server CA Keys
		R	VHSMs Server CA Certificates
		R	VHSMs Client CA Keys
		R	VHSMs Client CA Certificates
		R	VCOs' Obfuscated Passwords
		R	VCOs' Certificate Fingerprints
		R	Users' Obfuscated Passwords
		R	Users' Certificate Fingerprints
		R	Users' Objects (Exportable)
Import PHSM	PCO	W	PHSM Server CA Key
		W	PHSM Server CA Certificate
		G	PHSM Server Key
		W	PHSM Server Certificate
		W	PHSM Client CA Key
		W	PHSM Client CA Certificate
		W	PCOs' Obfuscated Passwords
		W	PCOs' Certificate Fingerprints
		W	VHSM Server CA Key
		W	VHSM Server CA Certificate
		G	VHSM Server Key
		W	VHSM Server Certificate
		W	VHSM Client CA Key
		W	VHSM Client CA Certificate
		W	VCOs' Obfuscated Passwords
		W	VCOs' Certificate Fingerprints
		W	Users' Obfuscated Passwords
		W	Users' Certificate Fingerprints
		W	Users' Objects
Update Firmware	PCO	E	PHSM Module Key
		E	Kryptus kNET CA Certificate
Get Log Level	PCO		None
Set Log Level	PCO		None
Get System Log	PCO		None
Show Status	PCO		None
Perform Self-Tests	PCO		None
Shutdown	PCO		None

Table 5.7: Access Rights within Services (continued)

Service	Role	Type of Access	CSPs
Restart	PCO		None
Get Device Information	PCO		None
Get TLS Certificate	PCO	R R	PHSM Server CA Certificate PHSM Server Certificate
Renew Server Certificate	PCO	G	PHSM Server Certificate
Activate OTP	PCO	G,R,E	PCO's OTP Key
Manual Activate OTP	PCO	R,E	PCO's OTP Key
Deactivate OTP	PCO	Z	PCO's OTP Key
Register Authentication Certificate	PCO	R	PCOs Certificate Fingerprints
Remove Authentication Certificate	PCO	Z	PCOs Certificate Fingerprints
List Authentication Certificates	PCO	R	PCOs Certificate Fingerprints
Start Token Authentication	PCO	R	PCOs Certificate Fingerprints
Get Session Credential	PCO		None
(All VCO Services)	VCO	E R E R R R E G,E	VHSM Server Key VHSM Server Certificate VHSM Client CA Certificate VCO's Certificate Fingerprint VCO's Password VCO's Obfuscated Password Job Descriptor Key Encryption Key TLS Session Keys
Get VHSM Usage	VCO		None
Create User (VCO)	VCO VCO	G,R W	VCO's Password VCO's Obfuscated Password
Create User (User)	VCO VCO	G,R W	User's Password User's Obfuscated Password
Destroy User (VCO)	VCO	Z Z	VCO's Obfuscated Password VCO's Certificate Fingerprints
Destroy User (User)	VCO	Z Z	User's Obfuscated Password User's Certificate Fingerprints
Reset Password (VCO)	PCO	G,R W	VCO's Password VCO's Obfuscated Password
Reset Password (User)	PCO	G,R W	User's Password User's Obfuscated Password
List Users	VCO		None
Change Password	VCO	R W	VCO's Password VCO's Obfuscated Password
Register Certificate	VCO	W	VCO's Certificate Fingerprint
List Certificates	VCO	R	VCO's Certificate Fingerprints
Delete Certificate	VCO	Z	VCO's Certificate Fingerprint
Activate Quorum Authentication	VCO		None

Table 5.7: Access Rights within Services (continued)

Service	Role	Type of Access	CSPs
Deactivate Quorum Authentication	VCO		None
Get Quorum Authentication State	VCO		None
Get Quorum Authentication Status	VCO		None
Vote Quorum Authentication	VCO		None
Start Quorum Authentication	VCO		None
Stop Quorum Authentication	VCO		None
Activate User	VCO		None
Deactivate User	VCO		None
Get Requester Type	VCO		None
Get Log Level	VCO		None
Set Log Level	VCO		None
Get System Log	VCO		None
Get TLS Certificate	VCO	R R	VHSM Server CA Certificate VHSM Server Certificate
Renew Server Certificate	VCO	G	VHSM Server Certificate
Activate OTP	VCO	G,R,E	VCO's OTP Key
Manual Activate OTP	VCO	R,E	VCO's OTP Key
Deactivate OTP	VCO	Z	VCO's OTP Key
Register Authentication Certificate	VCO	R	VCOs Certificate Fingerprints
Remove Authentication Certificate	VCO	Z	VCOs Certificate Fingerprints
List Authentication Certificates	VCO	R	VCOs Certificate Fingerprints
Start Token Authentication	VCO	R	VCOs Certificate Fingerprints
Get Session Credential	VCO		None
(All User Services)	User	E R E R R R E G,E	VHSM Server Key VHSM Server Certificate VHSM Client CA Certificate User's Certificate Fingerprint User's Password User's Obfuscated Password Job Descriptor Key Encryption Key TLS Session Keys
Change Password	User	R W	User's Password User's Obfuscated Password
Register Certificate	User	W	User's Certificate Fingerprint
List Certificates	User	R	User's Certificate Fingerprints
Activate Quorum Authentication	User		None
Deactivate Quorum Authentication	User		None
Get Quorum Authentication State	User		None
Get Quorum Authentication Status	User		None

Table 5.7: Access Rights within Services (continued)

Service	Role	Type of Access	CSPs
Vote Quorum Authentication	User		None
Start Quorum Authentication	User		None
Stop Quorum Authentication	User		None
Get System Log	User		None
Delete Certificate	User	Z	User's Certificate Fingerprint
Set User Object Permission	User		None
Get User Object Permission	User		None
Get Requester Type	User		None
Create	User	G	User's Object
CreateKeyPair	User	G	User's Object
Register	User	W	User's Object
Locate	User		None
Check	User		None
Get	User	R	User's Object (Exportable)
GetAttributes	User		None
GetAttributeList	User		None
AddAttribute	User		None
ModifyAttribute	User		None
DeleteAttribute	User		None
Activate	User		None
Revoke	User		None
Destroy	User	Z	User's Object
Query	User		None
Discover Versions	User		None
Encrypt	User	E	User's Object
Decrypt	User	E	User's Object
Sign	User	E	User's Object
SignVerify	User	E	User's Object
SignXML	User	E	User's Object
VerifyXML	User	E	User's Object
MAC	User	E	User's Object
MACVerify	User	E	User's Object
RNGRetrieve	User		None
RNGSeed	User		None
Hash	User		None
Load Key	User		None
Fast Sign	User	E	User's Object
Validate	User	R,E	User's Object
Activate OTP	User	G,R,E	User's OTP Key
Manual Activate OTP	User	R,E	User's OTP Key
Deactivate OTP	User	Z	User's OTP Key

Table 5.7: Access Rights within Services (continued)

Service	**Role**	**Type of Access**	**CSPs**
Register Authentication Certificate	User	R	User's Certificate Fingerprints
Remove Authentication Certificate	User	Z	User's Certificate Fingerprints
List Authentication Certificates	User	R	User's Certificate Fingerprints
Start Token Authentication	User	R	User's Certificate Fingerprints
Get Session Credential	User		None
(All Non-Auth Services)	None	E R G,E	VHSM Server Key VHSM Server Certificate TLS Session Keys
Query	None		None
Discover Versions	None		None

6 OPERATIONAL ENVIRONMENT

The module implements a limited operational environment, hence Section 4.6 of FIPS 140-2 does not apply to the module.

7 PHYSICAL SECURITY

7.1 Physical Security Mechanisms

To prevent physical access to the components of the module, an opaque epoxy resin is applied over its PCB components. The epoxy coating completely conceals the internal components of the cryptographic boundary. Any attempt to physically access the components leads to the destruction of the module. An aluminum frame is used to delimit the resin coating over the PCB, which can be seen on Figure 7.1. Figure 7.2 shows how the resin is spread over the PCB of the module.

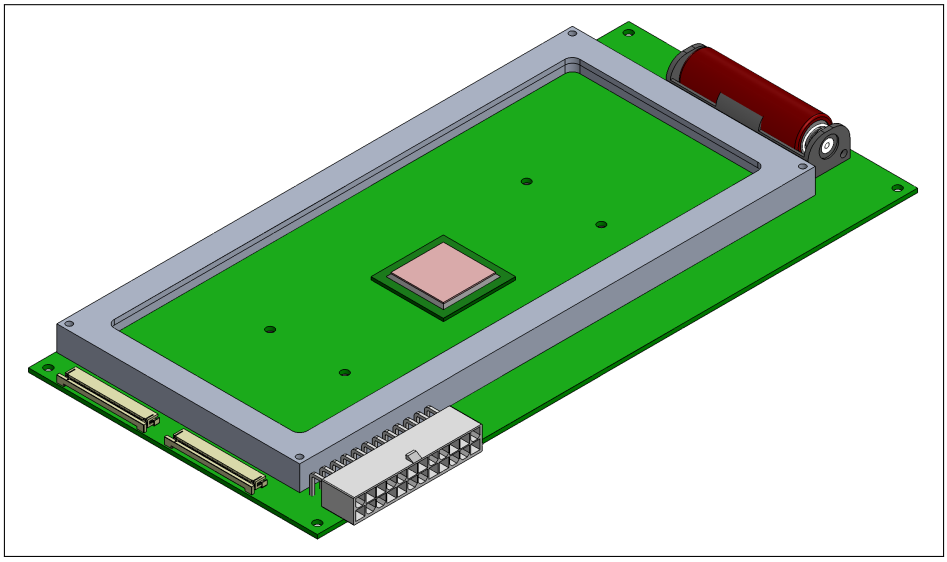

Figure 7.1: Module board with aluminum potting frame.

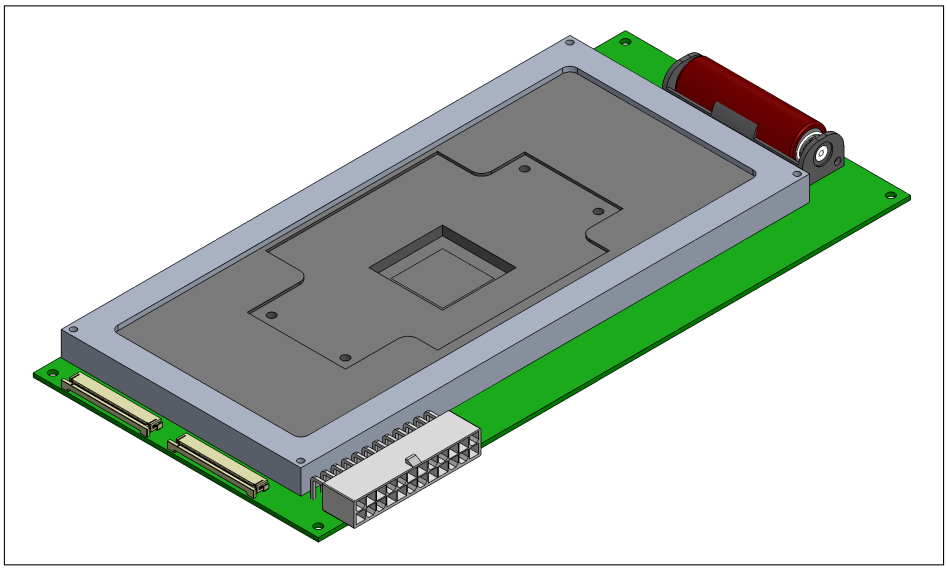

Figure 7.2: Epoxy resin potting of the module.

To allow heat dissipation of the main processor, an aluminum heatsink adapter is placed on top of it and is locked on the resin. This adapter can be seen within the complete module assembly on 7.3 and alone on Figure 7.4.

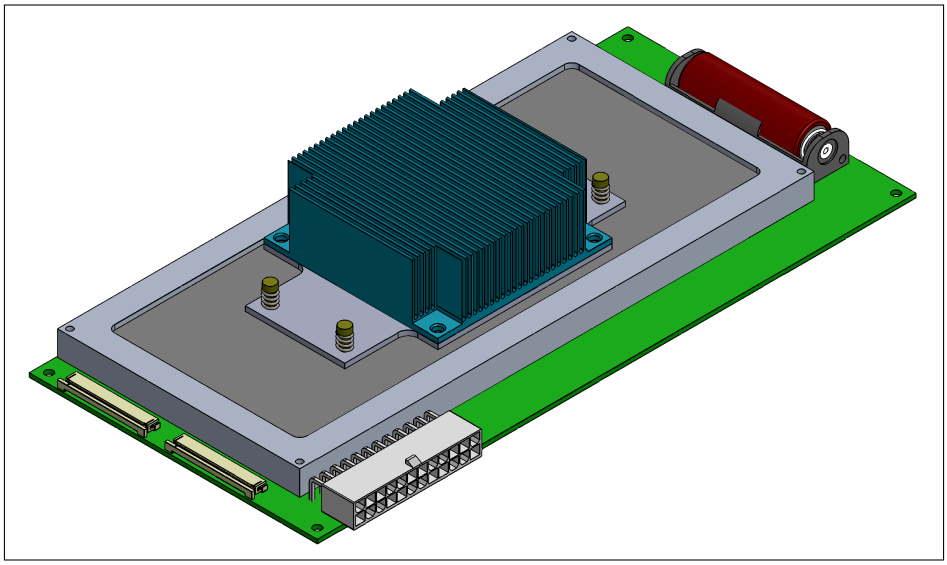

Figure 7.3: Complete assembly of the module.

Besides the use of the epoxy potting, the module monitors environmental parameters to prevent some attacks. An ultra-low-power microcontroller is used to control, sample and analyze the data from the sensors around the PCB. It is also capable of, optionally, holding critical system parameters for the CPU, as it is able to exchange data with it through an internal bus. It is also connected to the real time clock and a dedicated Random Number Generator. A non-removable battery, along with voltage conditioning and a supercapacitor, is used to ensure that all the sensors and the sensors monitor have non-interruptible power at all times.

7.2 Cryptographic Boundary and Interfaces

All the hardware components that will execute security functions are contained in the Cryptographic Boundary, which is completely covered by the epoxy resin potting explained on the Physical Security Mechanisms section. Figure 7.5 illustrates the module's cryptographic boundary and the external interfaces.

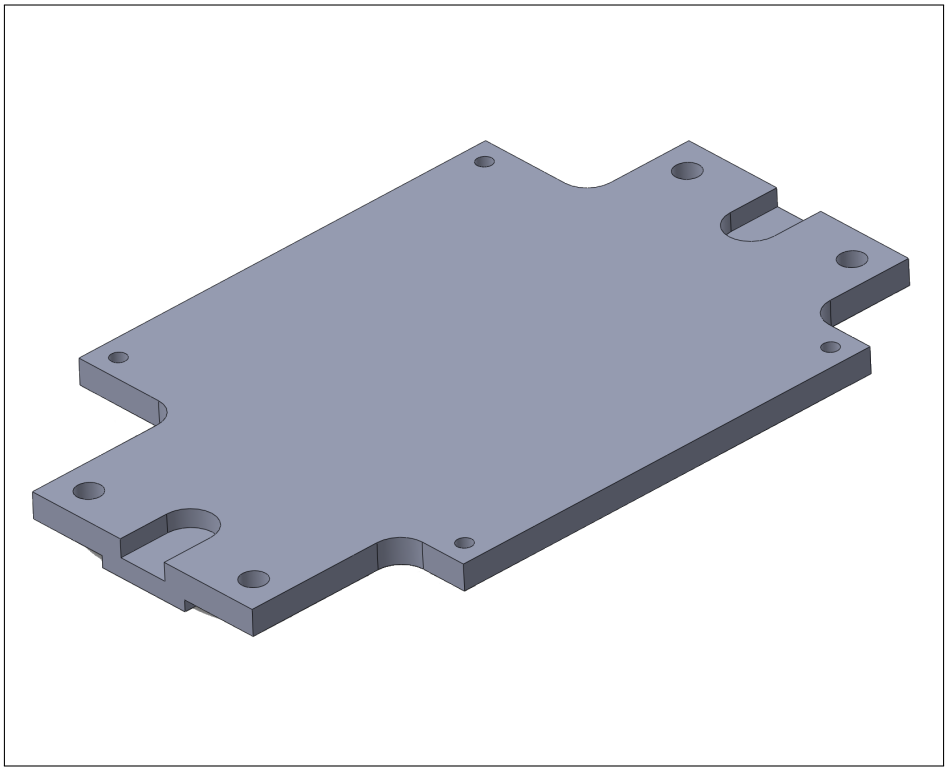

Figure 7.4: Aluminum heatsink adapter.

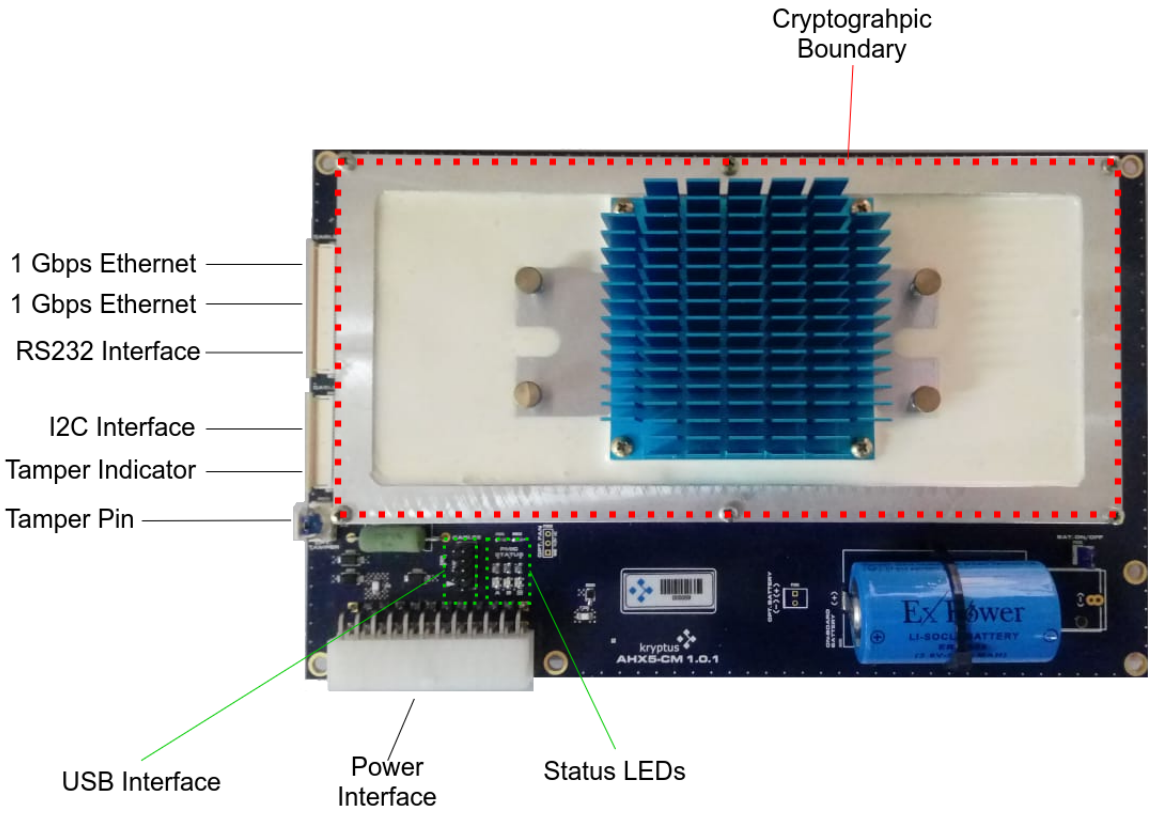

Figure 7.5: Cryptographic Boundary and Interfaces.

Table 7.1 lists the module's external connection interfaces.

Table 7.1: Cryptographic module interfaces.

Interface	Description	FIPS 140-2 Logical Interface
Power Interface	Powers the module.	Power
Status LEDs	Set of pins used to output status.	Status Output
USB Interface	Currently with no function. It will be used in the future to connect external USB devices. No sensitive information is transmitted through this channel.	–
Tamper Pin	Receives a control signal that can be connected to a tamper-evidence device (e.g. tamper switch)	Control Input
Tamper Indicator	Logical part of the I2C interface, indicates if tampering has been detected (either by the Tamper PIN or by the voltage/temperature monitoring)	Status Output
I2C Interface	Used to connect to external devices for module control (e.g. turn off the module). No sensitive information is transmitted through this channel*. Also used to output module status to the frontal board.	Control Input, Status Output
RS232 Interface	Serial interface used for module control (e.g. configure network interface). No sensitive information is transmitted through this channel*. Also used to output module status.	Control Input, Status Output
1 Gbps Ethernet Interfaces	Two sets of pins for Ethernet connection. These interfaces are the main communication channel for the cryptographic module. Sensitive data is always encrypted when transmitted through these pins.	Control Input, Data Input and Output

* When the module is initialized, it outputs the temporary PIN of the crypto officer through the RS232 and I2C interfaces. However, at this moment the module does not contain sensitive user data and

once the crypto officer's password is changed, it cannot be obtained via those interfaces anymore.

The tamper indicator and tamper pin interfaces are used for automatic determination by the module that an attempt has been made to compromise its physical security. Once the attempt is detected, the module reboots and initilizes in an error state, effectively erasing all its sensitive data. To remove the module from this error state, either the Reset HSM or the Remove from Error State services must be used.

7.3 Physical Security Maintenance

The module does not require any physical maintenance.

7.4 EMC/EMI

The module conforms to FCC Part 15 Class B requirements for home use.

8 SELF TESTS

The module performs self-tests according to FIPS140-2. The tests are divided into power-on self-tests and conditional self-tests, explained below.

8.1 Power-On Self-Tests

The power-on self-test are executed when the module initializes, with no operator intervention. If any of the tests fail, the module will not initialize. The power-on self tests are listed in Table 8.1.

Table 8.1: Power-On Self Tests performed.

Test	Description
AES	Encryption and decryption in ECB, CBC and CTR modes. Key size: 128 bits.
AES GCM	Encryption and decryption. Key size: 128 bits.
SHA	SHA-1 and SHA-2 message digest generation with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.
HMAC	Generation and verification with SHA-1*, SHA-224, SHA-256, SHA-384, SHA-512
RSA	Key Pair Generation, Digital Signature Generation and Digital Signature Verification. Key size: 2048 bit.
ECDSA	Key Pair Generation, Digital Signature Generation and Digital Signature Verification. Curve: NIST P-521.
EdDSA*	Key Pair Generation, Digital Signature Generation and Digital Signature Verification. Curve: Ed521.
DSA	Key Pair Generation, Digital Signature Generation and Digital Signature Verification. Key size: 256 bits
DRBG	Known answer test and health tests (instantiate, generate and reseed)
Triple-DES	Encryption and decryption in ECB and CBC modes. Key size: 168 bits.
KAS	Key Agreement Scheme (Primitive "Z" computation using ECDH).
TLS 1.2 KDF	SP800-135 Rev 1 TLS 1.2 KDF
Firmware Integrity Test	Digital Signature Verification with RSA 2048 bits and SHA-256

* When in FIPS mode, only Power-On Self-Tests for the Approved cryptographic algorithms are executed. Therefore, HMAC-SHA1 and EdDSA shall only be executed if the HSM is in non-FIPS mode.

8.2 Conditional Self-Tests

The module performs conditional self-tests during its operation. The self tests are listed in Table 8.2.

Table 8.2: Conditional Self Tests performed.

Test	Description
Pair-wise Consistency Tests	RSA, ECDSA and DSA Key Pair Generation
Continuous RNG test	Continuous DRBG test
Firmware Load Test	Digital Signature Verification with RSA 2048 bits and SHA-256

8.3 Indicators

When the power-on self-tests are run, the frontal board shows the results of each test, as illustrated in Figure 8.1. The same results can be viewed after boot through the frontal board menu.

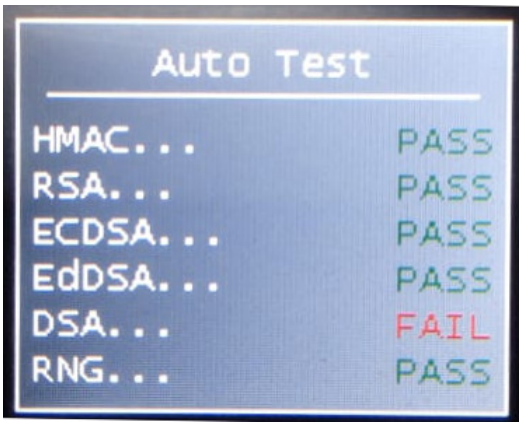

Figure 8.1: Power-on self-test results in frontal board.

Using the frontal board menu, through Settings → Info, it's possible to check if the module is in FIPS mode or not, as illustrated in Figure 8.2.

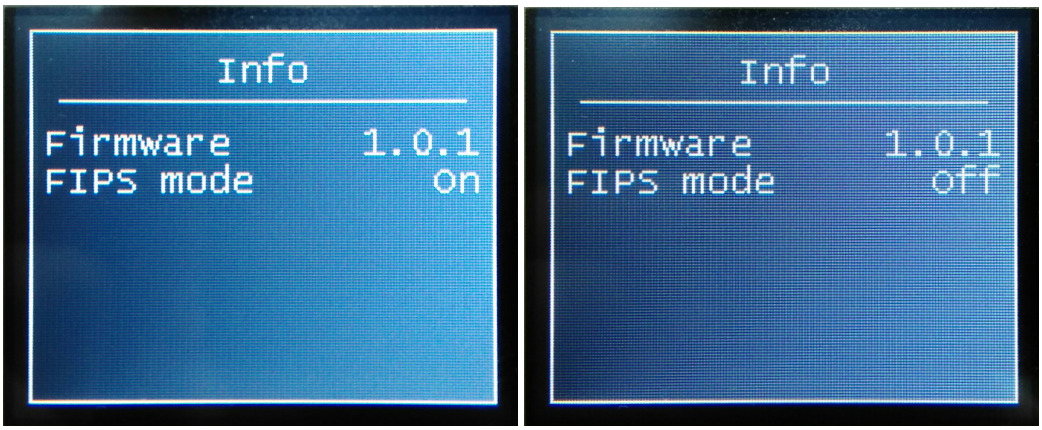

Figure 8.2: FIPS mode indicator in frontal board.

9 MITIGATIONS OF OTHER ATTACKS POLICY

No mitigation of other attacks are implemented on the module.

10 GUIDANCE AND SECURE OPERATION

The module supports FIPS and non-FIPS modes of operation. The mode must be chosen during the module initialization. The initialization is performed by the PCO using the Initialize HSM service (see section 5.2), which will generate the PHSM's CSPs (see section 5.3). All VHSMs created in a FIPS mode PHSM will also operate on FIPS mode.

The mode of operation of the module can only be changed if a factory reset is performed. The Reset HSM service is used for this intent. After a factory reset, all sensitive data of the module's operators will be zeroized. Similarly, if the module is initializes in non-FIPS mode, it can only be changed to FIPS-mode after a factory reset.

10.1 Initial Configuration

1. Turn on the HSM.
2. Configure the network settings (IP, mask, gateway, etc.) through the serial console or the frontal panel. The HSM will reboot. After rebooting, a temporary 6-digit PIN will be shown by the HSM via serial console and frontal panel.
3. Call the Initialize HSM command via the network through a safe connection (e.g. an ethernet cable connected directly to the HSM) in order to initialize the HSM. Use the PIN to authenticate. A new password must be specified along with whether to activate FIPS Mode or not. The HSM creates the first physical officer (PCO) with the given password and returns the Physical HSM (PHSM) certificate which can then be used to authenticate the network connection.
4. Call the Create VHSM command via the network (authenticate with the PCO password and the PHSM certificate) specifying a port number. The HSM creates the VHSM in a uninitialized state and creates its first virtual officer (VCO) with a temporary PIN. The PIN is returned along with a temporary VHSM certificate.
5. Call the Initialize VHSM command via the network on the VHSM port (authenticate with the temporary VCO password and the temporary VHSM certificate), specifying a new password. The HSM changes the VCO password and returns the final VHSM certificate.
6. Call the Create User command via the network on the VHSM port (authenticate with the VCO password and VHSM certificate). The HSM creates the user and returns a temporary password.
7. Call the Change Password command via the network on the VHSM port (authenticate with the temporary user password and the VHSM certificate). The HSM changes the user's password.
8. The user can now create objects and carry out operations using them.

In FIPS Mode the SNMP feature shall not be enabled. Non-approved algorithms listed in Table 3.3 are automatically disabled.