YUBICO, INC.

YubiHSM 2 Cryptographic Module

# FIPS 140-3 Non-Proprietary Security Policy

Version 1.0

# TABLE OF CONTENTS

# List of Tables

## List of Figures

# 1 GENERAL

## 1.1 OVERVIEW

This document defines the Security Policy for the Yubico, Inc. (Yubico) YubiHSM 2 Cryptographic Module, hereafter "the module".

The physical form of the module is depicted in Figure 1. The module is a single-chip embodiment as defined by FIPS 140-3 and conforms to Security Level 3.

## 1.2 SECURITY LEVELS

The module meets the overall requirements of FIPS 140-3 Security Level 3.

| Section | Title | Security Level |
|---|---|---|
| 1 | General | 3 |
| 2 | Cryptographic module specification | 3 |
| 3 | Cryptographic module interfaces | 3 |
| 4 | Roles, services, and authentication | 3 |
| 5 | Software/Firmware security | 3 |
| 6 | Operational environment | N/A |
| 7 | Physical security | 3 |
| 8 | Non-invasive security | N/A |
| 9 | Sensitive security parameter management | 3 |
| 10 | Self-tests | 3 |
| 11 | Life-cycle assurance | 3 |
| 12 | Mitigation of other attacks | N/A |
| | Overall Level | 3 |

Table 1: Security Levels

# 2 CRYPTOGRAPHIC MODULE SPECIFICATION

## 2.1 DESCRIPTION

The YubiHSM 2 Cryptographic Module (the module) is a single-chip module validated at FIPS 140-3 Security Level 3.


Figure 1 - YubiHSM 2 Cryptographic Module

**Purpose and Use:**

The module is the core component of the Yubico YubiHSM 2 product and is a dedicated hardware security module that offers superior protection for private keys against theft and misuse.

**Module Type**: Hardware

**Module Embodiment**: Single Chip

**Module Characteristics:**

The critical components within the module are encapsulated inside a single, integrated circuit.

**Cryptographic Boundary:**

The cryptographic boundary is defined as the IC package that comprises the Infineon Technologies SLE 78CLUFX5000P.

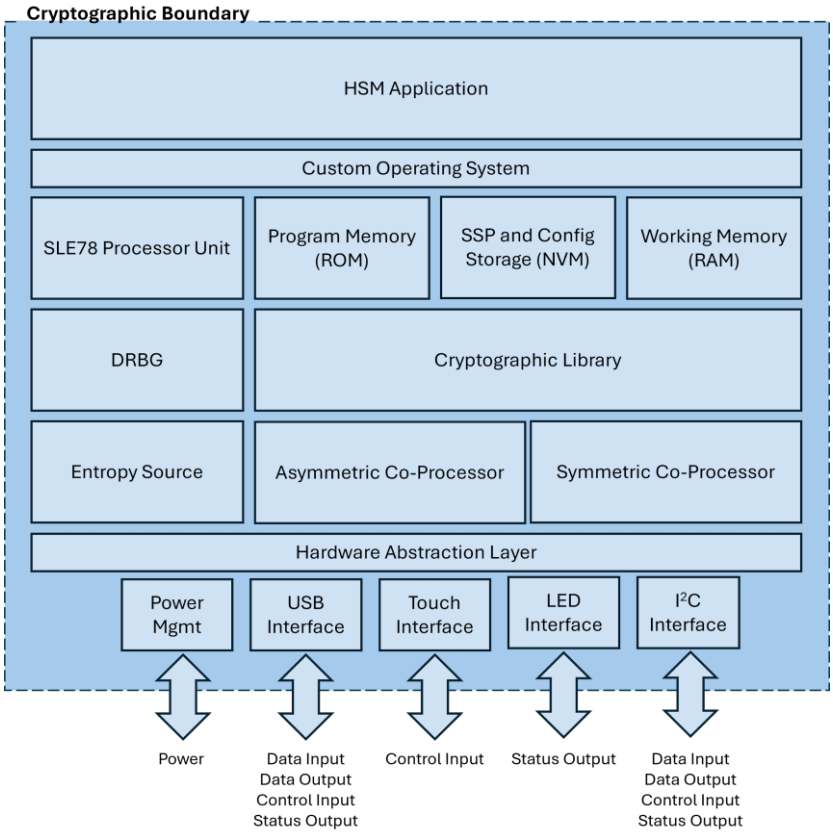


**Figure 2 - Block Diagram**

## 2.2 TESTED AND VENDOR AFFIRMED MODULE VERSION AND IDENTIFICATION

The YubiHSM 2 Cryptographic Module is designed to meet the requirements of FIPS 140-3 Security Level 3 (refer to Table 1). The module is available in the following configuration (refer to Table 2):

**Tested Module Identification – Hardware:**

| Model and/or Part Number | Hardware Version | Firmware Version | Processors | Features |
|---|---|---|---|---|
| SLE78CLUFX5000P | SLE78CLUFX5000P | 2.4.1 | SLE78CLUFX5000P | Single-Chip |

**Table 2: Tested Module Identification – Hardware**

*N.B. The module returns the hardware identifier '78CLUFX5000P' and firmware version '2.4.1' when queried*

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

N/A for this module.

## 2.3 EXCLUDED COMPONENTS

The module does not exclude any components from the requirements of FIPS 140-3.

## 2.4 MODES OF OPERATION

**Modes List and Description:**

The module supports an Approved mode and a non-Approved mode of operation. The Approved mode must be initialized per the instructions in this Security Policy. The module does not support a degraded mode of operation or a maintenance interface. The module requires zeroisation prior to changing the mode of operation. The mode of operation cannot be changed if any SSPs are present. The operator must update the default Authentication Key upon authenticating to the module for the first time.

| Mode Name | Description | Type | Status Indicator |
|---|---|---|---|
| Approved | Only Approved algorithms are available. | Approved | 01 |
| Non-Approved | Both Approved and non-Approved algorithms are available. | Non-Approved | 00 |

Table 3: Modes List and Description

**Mode Change Instructions and Status:**

The module requires zeroisation prior to changing the mode of operation. The mode of operation cannot be changed if any SSPs are present. The operator must update the default Authentication Key upon authenticating to the module for the first time. Section 11.1 provides mode change instructions.

## 2.5 ALGORITHMS

The YubiHSM 2 Cryptographic Module supports the approved cryptographic algorithms shown in Table 4.

**Approved Algorithms:**

The module supports the following approved cryptographic algorithms.

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CBC | A5891 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CCM | A5891 | Key Length - 128, 192, 256 | SP 800-38C |
| AES-CMAC | A5891 | Direction - Generation, Verification<br>Key Length - 128, 192, 256 | SP 800-38B |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-ECB | A5891 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-KWP | A5891 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38F |
| Counter DRBG | A5891 | Prediction Resistance - No<br>Mode - AES-256<br>Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| ECDSA KeyGen (FIPS186-5) | A5891 | Curve - P-224, P-256, P-384, P-521<br>Secret Generation Mode - testing candidates | FIPS 186-5 |
| ECDSA SigGen (FIPS186-5) | A5891 | Curve - P-224, P-256, P-384, P-521<br>Hash Algorithm - SHA2-256, SHA2-384, SHA2-512<br>Component - Yes | FIPS 186-5 |
| ECDSA SigVer (FIPS186-5) | A5891 | Curve - P-224, P-256, P-384, P-521<br>Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 | FIPS 186-5 |
| EDDSA KeyGen | A5891 | Curve - ED-25519 | FIPS 186-5 |
| EDDSA SigGen | A5891 | Curve - ED-25519<br>PreHash - No<br>Pure - Yes | FIPS 186-5 |
| EDDSA SigVer | A5891 | Curve - ED-25519 | FIPS 186-5 |
| HMAC-SHA-1 | A5891 | Key Length - Key Length: 112-512 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-256 | A5891 | Key Length - Key Length: 112-512 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-384 | A5891 | Key Length - Key Length: 112-1024 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-512 | A5891 | Key Length - Key Length: 112-1024 Increment 8 | FIPS 198-1 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| KAS-ECC-SSC Sp800-56Ar3 | A5891 | Domain Parameter Generation Methods - P-224, P-256, P-384, P-521<br>Scheme -<br>fullUnified -<br>KAS Role - initiator, responder<br>onePassDh -<br>KAS Role - initiator, responder<br>onePassUnified -<br>KAS Role - initiator, responder | SP 800-56A Rev. 3 |
| KDF ANS 9.63 (CVL) | A5891 | Hash Algorithm - SHA2-256<br>Key Data Length - Key Data Length: 512, 640 | SP 800-135 Rev. 1 |
| KDF SP800-108 | A5891 | KDF Mode - Counter<br>Supported Lengths - Supported Lengths: 8-2040 Increment 8 | SP 800-108 Rev. 1 |
| KTS-IFC | A5891 | Modulo - 2048, 3072, 4096<br>Key Generation Methods - rsakpg1-crt<br>Scheme -<br>KTS-OAEP-basic -<br>KAS Role - initiator, responder<br>Key Transport Method -<br>Key Length - 1024 | SP 800-56B Rev. 2 |
| RSA Decryption Primitive Sp800-56Br2 (CVL) | A5891 | Modulo - 2048, 3072, 4096 | SP 800-56B Rev. 2 |
| RSA KeyGen (FIPS186-5) | A5891 | Key Generation Mode - probable<br>Modulo - 2048, 3072, 4096<br>Primality Tests - 2powSecStr<br>Private Key Format - crt | FIPS 186-5 |
| RSA SigGen (FIPS186-5) | A5891 | Modulo - 2048, 3072, 4096<br>Signature Type - pkcs1v1.5 | FIPS 186-5 |
| RSA Signature Primitive (CVL) | A5891 | Modulo - 2048, 3072, 4096 | FIPS 186-4 |
| RSA SigVer (FIPS186-5) | A5891 | Modulo - 2048, 3072, 4096<br>Signature Type - pkcs1v1.5 | FIPS 186-5 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| SHA-1 | A5891 | Message Length - Message Length: 0-65528 Increment 8 | FIPS 180-4 |
| SHA2-256 | A5891 | Message Length - Message Length: 0-65528 Increment 8 | FIPS 180-4 |
| SHA2-384 | A5891 | Message Length - Message Length: 0-65528 Increment 8 | FIPS 180-4 |
| SHA2-512 | A5891 | Message Length - Message Length: 0-65528 Increment 8 | FIPS 180-4 |

Table 4: Approved Algorithms

**Vendor-Affirmed Algorithms:**

The module supports the following vendor affirmed algorithms:

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| CKG | Key Type:Symmetric and Asymmetric | Yubico Common Cryptographic Library | NIST SP 800-133r2, Section 4 example 1, Sections 5.1, 5.2, and 6.1 |

Table 5: Vendor-Affirmed Algorithms

**Non-Approved, Allowed Algorithms:**

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| ECDSA | Curve:brainpool256r1, brainpool384r1, brainpool512r1, secp256k1 | Yubico Common Cryptographic Library | IG C.A |
| KAS | Curve:brainpool256r1, brainpool384r1, brainpool512r1 | Yubico Common Cryptographic Library | IG C.A |

Table 6: Non-Approved, Allowed Algorithms

**Non-Approved, Allowed Algorithms with No Security Claimed:**

| Name | Caveat | Use and Function |
|---|---|---|
| DES | No security claimed | For internal integrity checking use only |

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed

**Non-Approved, Not Allowed Algorithms:**

| Name | Use and Function |
|---|---|
| ECDSA Signature Primitive with SHA-1 | Non-Approved signature generation |
| RSA PKCS#1 v1.5 Signature Primitive with SHA-1 | Non-Approved signature generation |
| RSA PSS Signature Primitive with SHA-1 | Non-Approved signature generation |
| secp256k1 (ECDSA and KAS) - Currently not included as part of IG C.A for key agreement | Non-Approved key agreement and signature generation with non-Approved curve |
| Decrypt PKCS#1 | Decryption |

Table 8: Non-Approved, Not Allowed Algorithms

## 2.6 SECURITY FUNCTION IMPLEMENTATIONS

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| AKG | AsymKeyPair-KeyGen<br>CKG | RSA 2048, 3072, 4096, ECDSA P-224, P-256, P-384, P-521 | Standard:NIST FIPS 186-5 | CKG: ()<br>Key Type: Asymmetric<br>Counter DRBG: (A5891)<br>RSA KeyGen (FIPS186-5): (A5891)<br>Modulo: 2048, 3072, 4096<br>ECDSA KeyGen (FIPS186-5): (A5891)<br>Curve: P-224, P-256, P-384, P-521, brainpool256r1, brainpool384r1, brainpool512r1<br>EDDSA KeyGen: (A5891)<br>Curve: ed25519 |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| AKV | AsymKeyPair-KeyVer | | Standards:NIST SP 800-56Ar3, FIPS 186-5 | ECDSA KeyGen (FIPS186-5): (A5891)<br>EDDSA KeyGen: (A5891)<br>KAS-ECC-SSC Sp800-56Ar3: (A5891)<br>RSA KeyGen (FIPS186-5): (A5891) |
| ECSP | UNK | Signature Generation Primitive | Standard:NIST FIPS 186-5 | ECDSA SigGen (FIPS186-5): (A5891)<br>Curve: P-224, P-256, P-384, P-521, brainpool256r1, brainpool384r1, brainpool512r1<br>Counter DRBG: (A5891) |
| ENC | BC-Auth | Symmetric Encryption | Standard:NIST FIPS 197 | AES-CBC: (A5891)<br>Key Size: 128, 192, 256<br>AES-ECB: (A5891)<br>Key Size: 128, 192, 256 |
| ENC-A | BC-Auth | Authenticated Symmetric Encryption | Standard:NIST FIPS 197 | AES-CCM: (A5891)<br>Key Size: 128, 192, 256 |
| DEC | BC-UnAuth | Symmetric Decryption | Standard:NIST FIPS 197 | AES-CBC: (A5891)<br>Key Size: 128, 192, 256<br>AES-ECB: (A5891)<br>Key Size: 128, 192, 256 |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| DEC-A | BC-UnAuth | Authenticated Symmetric Decryption | Standard:NIST FIPS 197 | AES-CCM: (A5891) Key Size: 128, 192, 256 |
| ESV | ENT-ESV | NIST SP 800-90B Physical Entropy Source | Standard:NIST SP 800-90B | |
| KAS-SC | KAS-Full | Secure Channel, which provides data protection and integrity using NIST SP 800-135r1 ANSI X9.63 KDF | Standard:NIST SP 800-56Ar3 IG:IG D.F Scenario 2 path (2), split Key confirmation:No Key Derivation:KDA (separately tested) Caveat:Key establishment methodology provides 128 bits of security strength | KAS-ECC-SSC Sp800-56Ar3: (A5891) Curve: P-256 KDF ANS 9.63: (A5891) |
| KAS-KG | KAS-KeyGen | Key Generation | Standard:NIST SP 800-56Ar3 | KAS-ECC-SSC Sp800-56Ar3: (A5891) Curve: P-224, P-256, P-384, P-521 |
| KBKDF | KBKDF | Key-Based Key Derivation CMAC-AES128 (Secure Channel). Only used as part of session establishment. | Standard:NIST SP 800-108 | KDF SP800-108: (A5891) |
| KTS-CBC-CMAC | KTS-Unwrap KTS-Wrap | Key Wrapping using Secure Channel Session Keys | Standard:NIST SP 800-38F IG D.G:Approved method from IG D.G Caveat:Key establishment methodology 128 | AES-CBC: (A5891) Key Size: 128 AES-CMAC: (A5891) Key Size: 128 |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | bits of security strength | |
| KTS-CCM | KTS-Unwrap<br>KTS-Wrap | Key Wrapping using AES-CCM Wrap Key | Standards:NIST SP 800-38F, SP 800-108, Global Platform GPC 2.3 Amendment D v1.2 SCP03<br>IG D.G:Approved method from IG D.G<br>Caveat:Key establishment methodology provides between 128 and 256 bits of security strength | AES-CCM: (A5891)<br>Key Size: 128, 192, 256 |
| KTS-IFC | KTS-Unwrap<br>KTS-Wrap | Key Encapsulation | Standard:NIST SP 800-56Br2<br>IG D.G:Approved method from IG D.G<br>Key confirmation:no<br>Caveat:Key establishment methodology provides between 112 and 150 bits of security strength | KTS-IFC: (A5891)<br>Modulo: 2048, 3072, 4096 |
| KTS-KWP | KTS-Unwrap<br>KTS-Wrap | Key Wrapping using AES-KWP Wrap Key | Standard:NIST SP 800-38F<br>IG D.G:Approved method from IG D.G<br>Caveat:Key establishment methodology provides between 128 and 256 bits of security strength | AES-KWP: (A5891)<br>Key Size: 128, 192, 256 |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| MAC | MAC | Keyed MAC | Standard:NIST FIPS 198-2 | AES-CMAC: (A5891) Key Size: 128, 192, 256<br>HMAC-SHA-1: (A5891)<br>HMAC-SHA2-256: (A5891)<br>HMAC-SHA2-384: (A5891)<br>HMAC-SHA2-512: (A5891)<br>SHA-1: (A5891)<br>SHA2-256: (A5891)<br>SHA2-384: (A5891)<br>SHA2-512: (A5891) |
| RAND | DRBG | Random Number Generation | Standard:NIST SP 800-90Ar1 | Counter DRBG: (A5891) |
| PKV | AsymKeyPair-PubKeyVal | Public key validation | Standards:NIST SP 800-56Ar3, FIPS 186-5, SP 800-56Br2 | ECDSA KeyGen (FIPS186-5): (A5891)<br>Curve: P-224, P-256, P-384, P-521<br>KAS-ECC-SSC Sp800-56Ar3: (A5891)<br>Curve: P-224, P-256, P-384, P-521<br>KTS-IFC: (A5891)<br>Modolo: 2048, 3078, 4096 |
| RSADP | UNK | RSA Decryption Primitive | Standard:NIST SP 800-56Br2 | RSA Decryption Primitive Sp800-56Br2: (A5891)<br>Modulo: 2048, 3072, 4096 |
| RSASP | UNK | RSA Signature Primitive | Standard:NIST FIPS 186-5 | RSA Signature Primitive: (A5891) |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | Modulo: 2048, 3072, 4096 |
| SigGen | DigSig-SigGen | Signature Generation | Standard:NIST FIPS 186-5 | RSA SigGen (FIPS186-5): (A5891)<br>Modulo: 2048, 3072, 4096<br>ECDSA SigGen (FIPS186-5): (A5891)<br>Curve: P-224, P-256, P-384, P-521, brainpool256r1, brainpool384r1, brainpool512r1<br>EDDSA SigGen: (A5891)<br>Curve: ed25519<br>SHA2-256: (A5891) |
| SigVer | DigSig-SigVer | Signature Verification | Standard:NIST FIPS 186-5 | RSA SigVer (FIPS186-5): (A5891)<br>Modulo: 2048<br>SHA2-256: (A5891)<br>ECDSA SigVer (FIPS186-5): (A5891)<br>EDDSA SigVer: (A5891) |
| KAS-SSC | KAS-SSC | Shared Secret Computation | Standard:NIST SP 800-56Ar3<br>IG :IG D.F Scenario 2, path (1) | KAS-ECC-SSC Sp800-56Ar3: (A5891)<br>Type: Co-factor One-Pass Diffie Hellman<br>Curve: P-224, P-256, P-384, P-521, brainpool256r1, |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | brainpool384r1, brainpool512r1 |
| SymKG | CKG | Symmetric Key Generation | Standard:NIST SP 800-133r2 | Counter DRBG: (A5891)<br>CKG - Sym: ()<br>Key Type: Symmetric |

Table 9: Security Function Implementations

## 2.7 ALGORITHM SPECIFIC INFORMATION

**Compliance to SP 800-56Ar3 assurances:**

For KAS-ECC, the module satisfies IG D.F Scenario 2 path (2). The key derivation functions comply with NIST SP 800-56Cr2 (i.e., KDA HKDF SP 800-56Cr2 (Cert. #A5891)) and ANS 9.63 (i.e., KDF ANS 9.63 (Cert. #A5891). Furthermore, the module obtained the appropriate assurances, as required in Sections 5.6.2 of NIST SP 800-56Ar3. Full public key validation (NIST SP 800-56Ar3 Section 5.6.2.3.3) is implemented. No key confirmation is implemented.

**Compliance to NIST SP 800-56Br2 Assurances**

For KTS RSA, the module satisfies IG D.G. The RSA keys for KTS-IFC (Cert. #A5891) have lengths of at least 2048 bits, which are acceptable per NIST SP 800-131Ar2. The modulus sizes, the method for key generation, and the roles (initiator, i.e., the module performs encapsulation, or responder, i.e., the module performs unencapsulation) are specified in Table 9. The RSA key generation algorithm is CAVP validated (Cert. #A5891). No key confirmation is implemented.

The module implements the KTS-OAEP key transport scheme and obtains the appropriate assurances as required in Sections 5 and 6 of NIST SP 800-56Br2. The module performs partial public-key validation. No key confirmation is implemented.

**ECDSA with Non NIST-Recommended Curves:** brainpool256r1, brainpool384r1, and brainpool512r1. These curves are allowed per IG C.A for ECDSA.

**KAS with NIST Allowed Curves:** brainpool256r1, brainpool384r1, brainpool512r1. These curves are allowed per IG C.A.

**DES for Integrity Checks:** The module supports DES for internal integrity checks with no security claimed.

## 2.8 RBG AND ENTROPY

The module incorporates a NIST SP 800-90A CTR-DRBG (Cert. #A5891) that is seeded from the module's NIST SP 800-90B validated entropy source. The unmodified output of the DRBG is used for generating cryptographic key material. The DRBG is instantiated anew every power-on. The threshold for reseeding is monitored to not exceed $2^{48}$ per SP800-90A.

| Cert Number | Vendor Name |
|---|---|
| E196 | Infineon Technologies AG |

Table 10: Entropy Certificates

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| Infineon 16-bit Security Controller M7893B11 Entropy Source | Physical | M7893B11 | 8 bits | 2.55928 bits | Non-Vetted Conditioning |

Table 11: Entropy Sources

### 2.9 KEY GENERATION

The module generates symmetric cryptographic keys in conformance with NIST SP 800-133r2 using a NIST SP 800-90A conforming DRBG (Cert. #A5891 ) for the encryption and protection of data and cryptographic keys. The module generates asymmetric cryptographic key pairs in conformance with FIPS 186-4 and FIPS 186-5 for the generation or verification of digital signatures, or for the facilitation of key agreement in conformance with NIST SP 800-56Ar3.

### 2.10 KEY ESTABLISHMENT

The module supports key establishment using KAS with a supported security strength of 128 bits, depending on the selection of key sizes utilized. The module supports AES-based key transport with a supported security strength between 128 and 256 bits, depending on the selection of key sizes utilized. The module supports RSA-based key transport with a supported security strength between 112 and 150 bits, depending on the selection of key sizes utilized.

The module incorporates KTS-IFC in conformance with NIST SP 800-56Br2.

### 2.11 INDUSTRY PROTOCOLS

No industry protocols are used in this module.

## 3 CRYPTOGRAPHIC MODULE INTERFACES

### 3.1 PORTS AND INTERFACES

The module incorporates physical ports and logical interfaces. The physical ports are defined within the table below:

| Physical Port | Logical Interface(s) | Data That Passes |
|---|---|---|
| USB pins (D+/D-) | Data Input<br>Data Output<br>Control Input<br>Status Output | SSPs, Operator data, Commands, Return Codes, and Error Status |
| Touch Button Interface | Control Input | Physical presence indicator |
| LED Interface | Status Output | Emits power to an LED, if attached |
| Power Interface | Power | N/A |
| I2C I/O | Data Input<br>Data Output<br>Control Input<br>Status Output | SSPs, Operator data, Commands, Return Codes, and Error Status |
| Interface Select | Control Input | Interface selection |

**Table 12: Ports and Interfaces**

# 4 ROLES, SERVICES, AND AUTHENTICATION

## 4.1 AUTHENTICATION METHODS

The module supports authentication methods for the Cryptographic Officer (CO) role. This role has separate identity -based authentication methods as indicated in Table 12. The module supports two authentication methods: Knowledge of a shared secret and possession of a private key. For each authentication attempt, the operator must present their unique identifier. The methods are in conformance with NIST SP 800-140E and SP 800-63B (refer to Section 5.1.6).

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|---|---|---|---|---|
| Knowledge of a shared secret | Knowledge of a shared secret | Cryptographic Software | The shared secret is a 128-bit AES key. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^128 which is less than 1/1,000,000. | Each session takes approximately 40 ms. The module can only perform 1500 session establishment attempts per minute (one session takes approximately 40 ms to |

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|---|---|---|---|---|
| | | | | establish), which is less than 1/100,000. |
| Possession of Private Key | Knowledge of the static private key | Cryptographic Software | The KAS-ECC private key uses curve P-256, which has a security strength of 128 bits. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^128 which is less than 1/1,000,000. | Possession of a Static Private Key (i.e., KAS-ECC, P-256) to establish a session key during session establishment. The strength of the ECC key is 128 bits. Authentication attempts take at least 150ms, which results in less than 420 attempts per minute due to performance constraints. |

**Table 13: Authentication Methods**

## 4.2 ROLES

The module supports a Cryptographic Officer (CO) role and an Unauthenticated role. The Unauthenticated role has access to non-security-relevant services only.

| Name | Type | Operator Type | Authentication Methods |
|---|---|---|---|
| Crypto Officer | Identity | CO | Knowledge of a shared secret<br>Possession of Private Key |
| Unauthenticated | Identity | N/A | None |

**Table 14: Roles**

The module supports multiple concurrent operators (up to 16) separated by unique sessions. Operator authentication does not persist beyond power-cycling the module. The selection of roles is implicit.

## 4.3 APPROVED SERVICES

This module supports the following approved services listed in Table 14. Please note that all services are protected by Session Keys except for the following services:

- Echo
- Device Info
- Get Device Public Key
- Power-On
- Reset Device (Manual Invocation)

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Authenticate Session | Complete the mutual authentication process started with Create Session | Return code: 0x84 | Challenge response Cryptogram | Success/Error | MAC | Crypto Officer<br>- Session Keys: E |
| Blink Device | Blink the LED of the device to identify it | Return code: 0xEB | None | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Change Authentication Key | Change an Authentication Key | Return code: 0xEC | New Authentication Key | Success/Error | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC<br>RAND<br>PKV | Crypto Officer<br>- Authentication Keys: W<br>- Session Keys: E<br>- DRBG State: G,E<br>- KAS Public Keys: W |
| Close Session | Close the current Session and release it for re-use | return code 0xC0 | None | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E,Z |
| Create OTP AEAD | Create a Yubico OTP AEAD | return code 0xE1 | OTP AEAD request | OTP AEAD | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-CCM<br>MAC | Crypto Officer<br>- OTP AEAD Key: E<br>- OTP ECB Key: R,W<br>- Session Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Create Session | Begin the mutual authentication process for establishing a Session | return code 0x83 | Auth ID, Host-Challenge, Public Key | Device Challenge, Cryptogram, KAS Public Key | KAS-SC<br>KAS-KG<br>KBKDF<br>MAC<br>RAND<br>PKV | Crypto Officer<br>- Authentication Keys: E<br>- Session Keys: G<br>- KAS Private Keys: E<br>- KAS Public Keys: R,W,E<br>- DRBG State: G,E |
| Decrypt CBC | Decrypt CBC with symmetric Key | Return code 0xF1 | Encrypted data | Decrypted data | ENC<br>DEC<br>MAC | Crypto Officer<br>- Encryption Keys: E<br>- Session Keys: E |
| Decrypt ECB | Decrypt ECB with symmetric Key | Return code 0xEF | Encrypted data | Decrypted data | ENC<br>DEC<br>MAC | Crypto Officer<br>- Encryption Keys: E<br>- Session Keys: E |
| Decrypt OAEP | Decrypt using RSA-OAEP | Return code 0xD9 | OAEP encrypted data | OAEP decrypted data | ENC<br>DEC<br>MAC<br>RAND<br>RSADP | Crypto Officer<br>- Asymmetric Private Keys: E<br>- DRBG State: G,E<br>- Session Keys: E |
| Decrypt OTP | Decrypt a Yubico OTP | Return code 0xE0 | OTP encrypted data, OTP AEAD, OTP ECB Key | OTP decrypted data | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-CCM<br>MAC | Crypto Officer<br>- OTP AEAD Key: E<br>- OTP ECB Key: W,E<br>- Session Keys: E |
| Delete Object | Delete an Object | Return code 0xD8 | None | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- Authentication Keys: Z<br>- HMAC Key: Z |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - AES-CCM Wrap Key: Z<br>- KAS Private Keys: Z<br>- KAS Public Keys: Z<br>- Asymmetric Private Keys: Z<br>- Asymmetric Public Keys: Z<br>- KTS-IFC Private Key: Z<br>- KTS-IFC Public Key: Z<br>- OTP AEAD Key: Z<br>- Session Keys: E |
| Derive KAS-ECC-SSC | Perform a KAS-ECC-SSC operation | Return code 0xD7 | KAS-ECC public key | Shared Secret | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC<br>RAND<br>PKV<br>KAS-SSC | Crypto Officer<br>- Asymmetric Private Keys: E<br>- Asymmetric Public Keys: W,E<br>- Shared Secret: G,R<br>- DRBG State: G,E<br>- Session Keys: E |
| Device Info | Gets device version, device serial, supported Algorithms and available log entries | Return code 0x86 | None | Device Info response message | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E<br>Unauthenticated<br>- Session Keys: E |
| Echo | Echo data back from the device | Return code 0x81 | None | Echo response | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E<br>Unauthenticate |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | d<br>- Session Keys: E |
| Encrypt CBC | Encrypt CBC with symmetric Key | Return code 0xF2 | None | Encrypted data | ENC<br>DEC<br>MAC | Crypto Officer<br>- Encryption Keys: E<br>- Session Keys: E |
| Encrypt ECB | Encrypt ECB with symmetric Key | Return code 0xF0 | None | Encrypted data | ENC<br>DEC<br>MAC | Crypto Officer<br>- Encryption Keys: E<br>- Session Keys: E |
| Export RSA Wrapped | Export KTS-IFC Data in Yubico internal format. | Return code 0xF6 | None | Exported object | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-IFC<br>KTS-KWP<br>MAC<br>RAND<br>SymKG | Crypto Officer<br>- KTS-IFC Public Key: R,E<br>- AES-KWP Wrap Key: G,R,E<br>- Authentication Keys: R<br>- HMAC Key: R<br>- AES-CCM Wrap Key: R<br>- KAS Private Keys: R<br>- KAS Public Keys: R<br>- Asymmetric Private Keys: R<br>- Asymmetric Public Keys: R<br>- KTS-IFC Private Key: R<br>- OTP AEAD Key: R<br>- DRBG State: G,E<br>- Session Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Export Wrapped | Retrieves an Object under wrap from the device. The Object is encrypted using a Wrap Key (AES-CCM) | Return code 0xCA | None | Exported object | ENC<br>DEC<br>KTS-CCM<br>MAC | Crypto Officer<br>- Authentication Keys: R<br>- HMAC Key: R<br>- AES-CCM Wrap Key: R,E<br>- KAS Private Keys: R<br>- KAS Public Keys: R<br>- Asymmetric Private Keys: R<br>- Asymmetric Public Keys: R<br>- KTS-IFC Private Key: R<br>- KTS-IFC Public Key: R<br>- OTP AEAD Key: R<br>- Session Keys: E |
| Generate Asymmetric Key | Generate an Asymmetric Key | Return code 0xC6 | None | Success/Error | AKG<br>AKV<br>ENC<br>DEC<br>KAS-KG<br>MAC<br>RAND<br>PKV | Crypto Officer<br>- Asymmetric Private Keys: G<br>- Asymmetric Public Keys: G<br>- DRBG State: G,E<br>- Session Keys: E |
| Generate Attestation Certificate | Generate attestation of an Asymmetric Key, output is an X.509 certificate | Return code 0xE4 | None | Attestation certificate | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC<br>RAND<br>SigGen | Crypto Officer<br>- Asymmetric Private Keys: E<br>- Attestation Key: E<br>- Asymmetric Public Keys: R<br>- KAS Public Keys: R |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - DRBG State: G,E<br>- Session Keys: E |
| Generate HMAC Key | Generate an HMAC Key | Return code 0xDA | None | Success/Error | ENC<br>DEC<br>MAC<br>SymKG | Crypto Officer<br>- HMAC Key: G<br>- DRBG State: G,E<br>- Session Keys: E |
| Generate OTP AEAD Key | Generate an OTP AEAD Key | Return code 0xE6 | None | Success/Error | ENC<br>DEC<br>MAC<br>SymKG | Crypto Officer<br>- DRBG State: G,E<br>- OTP AEAD Key: G<br>- Session Keys: E |
| Generate Symmetric Key | Generate a symmetric Key | Return code 0xEE | None | Success/Error | SymKG | Crypto Officer<br>- Encryption Keys: G<br>- DRBG State: G,E |
| Generate Wrap Key | Generate a Wrap Key (AES-CCM) that can be used for export, import, wrap data and unwrap data | Return code 0xDB | None | Success/Error | AKG<br>ENC<br>DEC<br>MAC<br>RAND<br>SymKG | Crypto Officer<br>- DRBG State: G,E<br>- AES-CCM Wrap Key: G<br>- KTS-IFC Private Key: G<br>- KTS-IFC Public Key: G<br>- Session Keys: E |
| Get Device Public | Get Device Public Key for KAS Authentication | Return code 0x8A | None | Device Public Key | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC | Unauthenticated<br>- KAS Public Keys: R<br>Crypto Officer<br>- KAS Public |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Keys: R<br>- Session Keys: E |
| Get Log Entries | Fetch device audit log | Return code 0xCD | None | Log entries response | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Get Object Info | Get Object metadata | Return code 0xCE | None | Object info response | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Get Opaque | Retrieve an Opaque Object (user provided data) from the device | Return code 0xC3 | None | Opaque data | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Get Option | Fetch a device-global option | Return code 0xD0 | None | Option data | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Get Pseudo Random | Get pseudo-random data from device. | Return code 0xD1 | None | Random data | ENC<br>DEC<br>MAC<br>RAND | Crypto Officer<br>- DRBG State: G,E<br>- Session Keys: E |
| Get Public Key | Fetch a public key from device | Return code 0xD4 | None | Public key | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC | Crypto Officer<br>- Asymmetric Public Keys: R<br>- KTS-IFC Public Key: R<br>- Session Keys: E |
| Get RSA Wrapped | Get KTS-IFC Data | Return code 0xF4 | None | Exported object | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-IFC<br>KTS-KWP<br>MAC | Crypto Officer<br>- KTS-IFC Public Key: R,E<br>- AES-KWP Wrap Key: G,R,E<br>- Authentication Keys: R |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | RAND<br>SymKG | - HMAC Key: R<br>- AES-CCM Wrap Key: R<br>- KAS Private Keys: R<br>- KAS Public Keys: R<br>- Asymmetric Private Keys: R<br>- Asymmetric Public Keys: R<br>- KTS-IFC Private Key: R<br>- OTP AEAD Key: R<br>- DRBG State: G,E<br>- Session Keys: E |
| Get Storage Info | Fetch storage information. | Return code 0xC1 | None | Storage information | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Get Template | Fetch a Template Object from the device | Return code 0xDF | None | Template data | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Import RSA Wrapped | Import KTS-IFC Data | Return code 0xF7 | None | Success/Error | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-IFC<br>KTS-KWP<br>MAC<br>RAND | Crypto Officer<br>- KTS-IFC Private Key: W,E<br>- AES-KWP Wrap Key: W,E<br>- Authentication Keys: W<br>- HMAC Key: W<br>- AES-CCM Wrap Key: W<br>- KAS Private Keys: W<br>- KAS Public |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Keys: W<br>- Asymmetric Private Keys: W<br>- Asymmetric Public Keys: W<br>- KTS-IFC Public Key: W<br>- OTP AEAD Key: W<br>- Session Keys: E<br>- DRBG State: G,E |
| Import Wrapped | Import a wrapped/encrypted object into the device | Return code 0xCB | Import data | Success/Error | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-CCM<br>MAC | Crypto Officer<br>- AES-CCM Wrap Key: W,E<br>- Authentication Keys: W<br>- HMAC Key: W<br>- KAS Private Keys: W<br>- KAS Public Keys: W<br>- Asymmetric Private Keys: W<br>- Asymmetric Public Keys: W<br>- KTS-IFC Private Key: W<br>- KTS-IFC Public Key: W<br>- OTP AEAD Key: W<br>- Session Keys: E |
| List Objects | List Objects in device | Return code 0xC8 | None | List of objects | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Power On | Power on the module | Services available | None | None | AKV<br>ESV<br>KAS-KG<br>RAND<br>PKV | Unauthenticated<br>- Entropy Input : G,E<br>- DRBG Seed : G,E<br>- DRBG State: G,E<br>- KAS Private Keys: G |
| Put Asymmetric Key | Import an Asymmetric Key | Return code 0xC5 | Asymmetric key | Success/Error | AKV<br>ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC<br>RAND | Crypto Officer<br>- Asymmetric Private Keys: W<br>- Asymmetric Public Keys: G<br>- DRBG State: G,E<br>- Session Keys: E |
| Put Authentication Key | Store a new Authentication Key | Return code 0xC4 | Authentication key | Success/Error | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC<br>RAND<br>PKV | Crypto Officer<br>- Authentication Keys: W<br>- DRBG State: W,E<br>- Session Keys: E<br>- KAS Public Keys: W |
| Put HMAC Key | Import an HMAC Key | Return code 0xD2 | HMAC key | Success/Error | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC | Crypto Officer<br>- HMAC Key: W<br>- Session Keys: E |
| Put Opaque | Stores Opaque data (user provided data) in the device | Return code 0xC2 | Opaque data | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Put OTP AEAD Key | Import an OTP AEAD Key | Return code 0xE5 | OTP AEAD key | Success/Error | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC | Crypto Officer<br>- OTP AEAD Key: W<br>- Session Keys: E |
| Put Public Wrap Key | Import a public KTS-IFC Key | Return code 0xF3 | Public Wrap key | Success/Error | ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC<br>RAND<br>PKV | Crypto Officer<br>- KTS-IFC Public Key: W<br>- DRBG State: W,E<br>- Session Keys: E |
| Put RSA Wrapped | Put KTS-IFC Data | Return code 0xF5 | Wrapped data | Success/Error | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-IFC<br>KTS-KWP<br>MAC<br>RAND | Crypto Officer<br>- KTS-IFC Private Key: W,E<br>- AES-KWP Wrap Key: W,E<br>- Authentication Keys: W<br>- HMAC Key: W<br>- AES-CCM Wrap Key: W<br>- KAS Private Keys: W<br>- KAS Public Keys: W<br>- Asymmetric Private Keys: W<br>- Asymmetric Public Keys: W<br>- KTS-IFC Public Key: W<br>- OTP AEAD Key: W<br>- DRBG State: G,E<br>- Session Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Put Symmetric Key | Import a symmetric Key | Return code 0xED | Symmetric key | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- Encryption Keys: W<br>- Session Keys: E |
| Put Template | Store a Template | Return code 0xDE | Template data | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Put Wrap Key | Import a Wrap Key | Return code 0xCC | Wrap key | Success/Error | AKV<br>ENC<br>DEC<br>KTS-CBC-CMAC<br>MAC<br>RAND | Crypto Officer<br>- AES-CCM Wrap Key: W<br>- KTS-IFC Private Key: W<br>- DRBG State: G,E<br>- Session Keys: E |
| Randomize OTP AEAD | Create an OTP AEAD from random data | Return code 0xE2 | None | OTP AEAD | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-CCM<br>MAC<br>RAND<br>SymKG | Crypto Officer<br>- OTP AEAD Key: E<br>- DRBG State: G,E<br>- OTP ECB Key: G,R<br>- Session Keys: E |
| Reset Device | Factory reset a device (Zeroization) | Return code 0x88 | None | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- DRBG State: Z<br>- Authentication Keys: Z<br>- Session Keys: E,Z<br>- Encryption Keys: Z<br>- Asymmetric Private Keys: Z<br>- KAS Private Keys: Z<br>- KTS-IFC Private |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Key: Z<br>- Asymmetric Public Keys: Z<br>- KAS Public Keys: Z<br>- KTS-IFC Public Key: Z<br>- Attestation Key: Z<br>- AES-KWP Wrap Key: Z<br>- AES-CCM Wrap Key: Z<br>- OTP AEAD Key: Z<br>- HMAC Key: Z<br>Unauthenticated<br>- DRBG State: Z<br>- Authentication Keys: Z<br>- Session Keys: E,Z<br>- Encryption Keys: Z<br>- Asymmetric Private Keys: Z<br>- KAS Private Keys: Z<br>- KTS-IFC Private Key: Z<br>- Asymmetric Public Keys: Z<br>- KAS Public Keys: Z<br>- KTS-IFC Public Key: Z<br>- Attestation Key: Z<br>- AES-KWP Wrap Key: Z |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - AES-CCM Wrap Key: Z<br>- OTP AEAD Key: Z<br>- HMAC Key: Z |
| Rewrap OTP AEAD | Rewrap an OTP AEAD | Return code 0xE3 | OTP AEAD | OTP AEAD | ENC<br>DEC<br>KTS-CBC-CMAC<br>KTS-CCM<br>MAC | Crypto Officer<br>- OTP AEAD Key: E<br>- OTP ECB Key: R,W<br>- Session Keys: E |
| Session Message | Send a command over an established session | Return code 0x85 | Encrypted message | Encrypted response | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Set Log Index | Set the last extracted log entry | Return code 0xE7 | None | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Set Option | Set a device-global option | Return code 0xCF | None | Success/Error | ENC<br>DEC<br>MAC | Crypto Officer<br>- Session Keys: E |
| Signature Primitive ECDSA | Signature primitive with ECDSA | Return code 0xD6 | None | ECDSA signature | ECSP<br>ENC<br>DEC<br>MAC<br>RAND | Crypto Officer<br>- Asymmetric Private Keys: E<br>- DRBG State: G,E<br>- Session Keys: E |
| Sign EdDSA | Sign with EdDSA | Return code 0xEA | Message | EdDSA digital signature | ENC<br>DEC<br>MAC<br>RAND<br>SigGen | Crypto Officer<br>- Asymmetric Private Keys: E<br>- DRBG State: G,E<br>- Session Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Sign HMAC | Perform an HMAC operation in device and return the result | Return code 0xD3 | Message | HMAC signature | ENC<br>DEC<br>MAC<br>RAND | Crypto Officer<br>- HMAC Key: E<br>- DRBG State: G,E<br>- Session Keys: E |
| Signature Primitive PKCS1 | Signature primitive with RSA-PKCS#1v1.5 | Return code 0xC7 | Message | PKCS1 signature | ENC<br>DEC<br>MAC<br>RSASP | Crypto Officer<br>- Asymmetric Private Keys: E<br>- Asymmetric Public Keys: E<br>- Session Keys: E |
| Signature Primitive PSS | Signature primitive using RSA-PSS | Return code 0xD5 | Message | PSS signature | ENC<br>DEC<br>MAC<br>RAND<br>RSASP | Crypto Officer<br>- Asymmetric Private Keys: E<br>- DRBG State: G,E<br>- Session Keys: E |
| SSH Certify | Generate an SSH Certificate | Return code 0xDD | None | SSH cert | ENC<br>DEC<br>MAC<br>RAND<br>SigGen<br>SigVer | Crypto Officer<br>- Asymmetric Private Keys: E<br>- Asymmetric Public Keys: E<br>- DRBG State: G,E<br>- Session Keys: E |
| Unwrap Data | Decrypt (unwrap) data using a Wrap Key | Return code 0xE9 | None | None | ENC<br>DEC<br>DEC-A<br>MAC | Crypto Officer<br>- AES-CCM Wrap Key: E<br>- Session Keys: E |
| Verify HMAC | Verify an HMAC | Return code 0xDC | None | Success/Error | ENC<br>DEC<br>MAC<br>RAND | Crypto Officer<br>- HMAC Key: E<br>- DRBG State: G,E<br>- Session Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Wrap Data | Encrypt (wrap) data using a Wrap Key | Return code 0xE8 | None | Wrapped data | ENC<br>ENC-A<br>DEC<br>MAC<br>RAND | Crypto Officer<br>- AES-CCM Wrap Key: E<br>- DRBG State: G,E<br>- Session Keys: E |

Table 15: Approved Services

## 4.4 NON-APPROVED SERVICES

In the non-Approved mode, the module supports all services from the Approved mode with the following additional services and modifications:

- Decrypt PKCS#1
- ECDSA service with SHA-1
- RSA PKCS#1 Signature Generation with SHA-1
- RSA PSS Signature Generation with SHA-1
- ECDSA service with secp256k1
- Decrypt ECDH service with secp256k1The module only supports non-Approved services within the OTP functional unit, which must be explicitly selected.

| Name | Description | Algorithms | Role |
|---|---|---|---|
| Decrypt PKCS1 | RSA Decryption primitive with PKCS#1 v1.5 | Decrypt PKCS#1 | CO |
| Derive ECDH with secp256k1 | Derive ECDH with secp256k1 | secp256k1 (ECDSA and KAS) - Currently not included as part of IG C.A for key agreement | CO |
| Signature Primitive ECDSA with secp256k1 or SHA1 | Signature Primitive ECDSA with secp256k1 or SHA1 | ECDSA Signature Primitive with SHA-1 | CO |
| Signature Primitive PKCS1 with SHA1 | Signature Primitive PKCS1 with SHA1 | RSA PKCS#1 v1.5 Signature Primitive with SHA-1 | CO |
| Signature Primitive PSS with SHA1 | Signature Primitive PSS with SHA1 | RSA PSS Signature Primitive with SHA-1 | CO |

Table 16: Non-Approved Services

### 4.5 EXTERNAL SOFTWARE/FIRMWARE LOADED

The module does not support external firmware loads.

## 5 SOFTWARE/FIRMWARE SECURITY

### 5.1 INTEGRITY TECHNIQUES

The module performs a 16-bit Error Detection Code (EDC) for the Firmware Integrity Test, covering all executable code.

### 5.2 INITIATE ON DEMAND

All self-tests may be invoked on demand by power cycling the module.

## 6 OPERATIONAL ENVIRONMENT

### 6.1 OPERATIONAL ENVIRONMENT TYPE AND REQUIREMENTS

**Type of Operational Environment**: Non-Modifiable

**How Requirements are Satisfied**:

The module is defined as a single-chip embodiment whose operational environment is classified as non-modifiable. The firmware is loaded within manufacturing and then locked from being modified.

## 7 PHYSICAL SECURITY

### 7.1 MECHANISMS AND ACTIONS REQUIRED

The module is a single-chip embodiment with a hard, opaque enclosure. The IC packaging is tamper-evident and removal-resistant.

| Mechanism | Inspection Frequency | Inspection Guidance |
|---|---|---|
| IC packaging | Monthly | Inspect for physical evidence of tamper |

Table 17: Mechanisms and Actions Required

### 7.2 EFP/EFT INFORMATION

The module does not support Environmental Failure Protection (EFP) mechanisms for high/low voltage and temperature extremes. The module underwent Environmental Failure Testing (EFT) instead (refer to Table 17).

| Temp/Voltage Type | Temperature or Voltage | EFP or EFT | Result |
|---|---|---|---|
| LowTemperature | -42C | EFT | Undefined Failure. |
| HighTemperature | 128C | EFT | Undefined Failure. |
| LowVoltage | 1.85v | EFT | The module shuts down. |
| HighVoltage | 10.6v | EFT | Undefined Failure. |

Table 18: EFP/EFT Information

*N.B. There are two sets of possibilities for the last column. For EFP, states can be Shutdown or Zeroise. For EFT, states can be Shutdown, Zeroization, Undefined Failure, Known Error State, or Continues to Operate Normally.*

### 7.3 HARDNESS TESTING TEMPERATURE RANGES

The module has been tested at the operational, storage and distribution temperatures listed in Table 18. The module's hardness is assured within these ranges.

| Temperature Type | Temperature |
|---|---|
| LowTemperature | -25C |
| HighTemperature | 85C |

Table 19: Hardness Testing Temperatures

## 8 NON-INVASIVE SECURITY

### 8.1 MITIGATION TECHNIQUES

The module does not provide protections against non-invasive security methods.

## 9 SENSITIVE SECURITY PARAMETERS MANAGEMENT

### 9.1 STORAGE AREAS

All SSPs are stored in plaintext form within the volatile RAM or non-volatile flash memory.

| Storage Area Name | Description | Persistence Type |
|---|---|---|
| RAM | Plaintext in volatile RAM | Dynamic |
| NVM | Plaintext in persistent NVM | Static |

Table 20: Storage Areas

## 9.2 SSP INPUT-OUTPUT METHODS

Specific SSPs may be entered and output from the module via various methods, which include plaintext (direct entry) or protected by either a secure channel or an Approved KTS.

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|---|---|---|---|
| PubKey-Entry | USB Host | NVM or RAM | Plaintext | Automated | Electronic | |
| PubKey-Output | NVM or RAM | USB Host | Plaintext | Automated | Electronic | |
| Secure-Channel-Entry | USB Host | NVM | Encrypted | Automated | Electronic | KTS-CBC-CMAC |
| Secure-Channel-Output | RAM | USB Host | Encrypted | Automated | Electronic | KTS-CBC-CMAC |

Table 21: SSP Input-Output Methods

## 9.3 SSP ZEROIZATION METHODS

Each of the six functional units includes separate instructions for zeroization. In all cases, zeroization is the active overwriting of SSP values with 0s (zeros).

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Zeroisation | All CSPs zeroized | SSPs are immediately overwritten with 0s | Reset Device service |
| Delete Object | Specified object is zeroized | Specified CSP is immediately overwritten with 0s | Delete Object service |

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Close Session | Secure Channel CSPs are zeroized | CSPs are immediately overwritten with 0s | Close Session service |
| Zeroisation-PowerCycle | Ephemeral CSPs zeroised upon power cycle | Ephemeral SSPs are overwritten with 0s | Power Cycle |
| Zeroisation-AfterUse | Ephemeral CSPs zeroised after use | SSPs are immediately overwritten with 0s after use | Automatic |

**Table 22: SSP Zeroization Methods**

## 9.4 SSPS

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| AES-CCM Wrap Key | Secures other CSPs ("objects"). | 128, 192, 256 - 128 - 256 | Symmetric - CSP | SymKG | | KTS-CCM |
| AES-KWP Wrap Key | Secures other CSPs ("objects"). | 128, 192, 256 - 128 - 256 | Symmetric - CSP | SymKG | | KTS-KWP |
| Asymmetric Private Keys | Signature generation, ECC CDH Component Primitive, or modular exponentiation | RSA 2048 - 4096; ed25519; EC P-224, P-256, P-384, P-521, or Non-NIST Curve - 112 - 256 | Private - CSP | AKG | | ECSP RSADP RSASP SigGen KAS-SSC |
| Asymmetric Public Keys | Signature verification (by external entities), ECC CDH Component Primitive | RSA 2048 - 4096 bits or EC P-224, P-256, P-384, P-521 or Non-NIST curves - 112 - 256 | Public - PSP | AKG | | SigVer KAS-SSC |
| Attestation Key | Attests authenticity of other keys, | RSA 2048 - 4096 bits or EC | Private - Neither | | | SigGen |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | producing a new X.509 certificate for the attested key | P-224, P-256, P-384, P-521 or Non-NIST curves - 112 - 256 | | | | |
| Authentication Keys | Used to derive session keys for Secure Channel and authenticates the operator | 128 - 128 | Symmetric - CSP | | | KBKDF |
| DRBG Seed | Seeds the DRBG. Personalization string is 384 bits. | 1600 bits - 384 | ENT - CSP | ESV | | Counter DRBG (A5891) |
| DRBG State | Random number generation. V and Key | V = 128, Key = 256 - 256 bit | DRBG - CSP | Counter DRBG (A5891) | | Counter DRBG (A5891) |
| Encryption Keys | Used for data encryption | 128 - 256 - 128 - 256 | Symmetric - CSP | SymKG | | ENC DEC |
| Entropy Input | Entropy for the DRBG | 1216 bits - 384 (3/2 security strength) | ENT - CSP | ESV | | ESV |
| HMAC Key | Data integrity key | >= 128 bits - >= 128 bits | Symmetric - CSP | SymKG | | MAC |
| KAS Private Keys | Key establishment private keys for secure channel | EC P-256 - 128 bits | Private - CSP | KAS-KG | | KAS-SC |
| KAS Public Keys | Key establishment public keys. | EC P-256 - 128 bits | Public - PSP | KAS-KG | | KAS-SC |
| KTS-IFC Private Key | KTS-IFC Unwrap | RSA 2048, 3072, 4096 - 112 - 150 bits | Private - CSP | AKG | | KTS-IFC |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| KTS-IFC Public Key | KTS-IFC Wrap | RSA 2048, 3072, 4096 - 112 - 150 bits | Public - PSP | AKG | | KTS-IFC |
| OTP AEAD Key | Secure Yubico OTP values for further verification by a validation process | 128, 192, 256 - 128 - 256 | Symmetric - CSP | SymKG | | KTS-CCM |
| OTP ECB Key | Decrypts OTPs generated by a YubiKey | 128 - 128 | Symmetric - CSP | SymKG | | DEC |
| Session Keys | Session keys for Secure Channel | 128 - 128 | Symmetric - CSP | | KAS-SC KBKDF | ENC DEC MAC |
| Shared Secret | Shared secret calculated from a key agreement handshake | 256 - 521 - 128 | Shared Secret - CSP | | KAS-SSC | KAS-SSC |

**Table 23: SSP Table 1**

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| AES-CCM Wrap Key | Secure-Channel-Entry Secure-Channel-Output | NVM:Plaintext RAM:Plaintext | Until Use | Zeroisation Delete Object | DRBG State:Generates Authentication Keys:Protected By HMAC Key:Protected By Asymmetric Private Keys:Protected By OTP AEAD Key:Protected By Session Keys:Encrypts AES-KWP Wrap Key:Encrypts |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| AES-KWP Wrap Key | Secure-Channel-Entry<br>Secure-Channel-Output | RAM:Plaintext | Until Use | Zeroisation-AfterUse | DRBG State:Generates<br>KTS-IFC Public Key:Encrypts<br>KTS-IFC Private Key:Encrypts<br>Session Keys:Encrypts |
| Asymmetric Private Keys | Secure-Channel-Entry<br>Secure-Channel-Output | RAM:Plaintext<br>NVM:Plaintext | Until Use | Zeroisation<br>Delete Object | DRBG State:Generates<br>Asymmetric Public Keys:Paired With<br>Shared Secret:Derives<br>Session Keys:Encrypts<br>AES-CCM Wrap Key:Encrypts<br>AES-KWP Wrap Key:Protected by |
| Asymmetric Public Keys | Secure-Channel-Entry<br>Secure-Channel-Output | NVM:Plaintext<br>RAM:Plaintext | Until Use | Zeroisation<br>Delete Object | DRBG State:Generates<br>Asymmetric Private Keys:Paired With<br>Session Keys:Encrypts<br>AES-CCM Wrap Key:Encrypts<br>AES-KWP Wrap Key:Encrypts<br>Shared Secret:Derived From |
| Attestation Key | | NVM:Plaintext<br>RAM:Plaintext | Until Use | N/A | Asymmetric Public Keys:Paired With<br>Asymmetric Public Keys:Signs |
| Authentication Keys | Secure-Channel-Entry<br>Secure-Channel-Output | NVM:Plaintext<br>RAM:Plaintext | Until use | Zeroisation<br>Delete Object | Session Keys:Encrypts<br>AES-KWP Wrap Key:Encrypts<br>AES-CCM Wrap Key:Encrypts |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| DRBG Seed | | RAM:Plaintext | Until use | Zeroisation-AfterUse | DRBG State:Derived From |
| DRBG State | | RAM:Plaintext | Until reboot | Zeroisation-PowerCycle | DRBG Seed :Derives Asymmetric Private Keys:Generated From Asymmetric Public Keys:Generated From HMAC Key:Generated From AES-KWP Wrap Key:Generated From KAS Private Keys:Generated From KAS Public Keys:Generated From KTS-IFC Private Key:Generated From KTS-IFC Public Key:Generated From Encryption Keys:Generated From OTP AEAD Key:Generated From OTP ECB Key:Generated From |
| Encryption Keys | Secure-Channel-Entry Secure-Channel-Output | NVM:Plaintext | Until Use | Zeroisation Delete Object | DRBG State:Generates Session Keys:Encrypts |
| Entropy Input | | RAM:Plaintext | Until use | Zeroisation-AfterUse | DRBG Seed :Derived From |
| HMAC Key | Secure-Channel-Entry Secure- | NVM:Plaintext RAM:Plaintext | Until Use | Zeroisation Delete Object | DRBG State:Generates Session Keys:Encrypts AES-CCM Wrap Key:Encrypts |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | Channel-Output | | | | AES-KWP Wrap Key:Encrypts |
| KAS Private Keys | Secure-Channel-Entry | NVM:Plaintext RAM:Plaintext | Until Use | Zeroisation Delete Object Zeroisation-AfterUse | DRBG State:Generated KAS Public Keys:Paired With Session Keys:Derived From |
| KAS Public Keys | Secure-Channel-Entry Secure-Channel-Output PubKey-Entry PubKey-Output | RAM:Plaintext NVM:Plaintext | Until Use | Zeroisation Delete Object Zeroisation-AfterUse | DRBG State:Generates KAS Private Keys:Paired With Session Keys:Derived From |
| KTS-IFC Private Key | Secure-Channel-Output | NVM:Plaintext RAM:Plaintext | Until Use | Zeroisation Delete Object | DRBG State:Generated KTS-IFC Public Key:Paired With |
| KTS-IFC Public Key | Secure-Channel-Entry Secure-Channel-Output | NVM:Plaintext RAM:Plaintext | Until Use | Zeroisation Delete Object | KTS-IFC Private Key:Paired With Session Keys:Encrypts DRBG State:Generates AES-CCM Wrap Key:Encrypts AES-KWP Wrap Key:Protected by |
| OTP AEAD Key | Secure-Channel-Entry Secure-Channel-Output | NVM:Plaintext RAM:Plaintext | Until Use | Zeroisation Delete Object | DRBG State:Generates Session Keys:Encrypts OTP ECB Key:Protected By AES-CCM Wrap Key:Encrypts AES-KWP Wrap Key:Encrypts |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| OTP ECB Key | Secure-Channel-Entry<br>Secure-Channel-Output | RAM:Plaintext | Until Use | Zeroisation-AfterUse | DRBG State:Generates<br>OTP AEAD Key:Encrypts<br>Session Keys:Encrypts |
| Session Keys | | RAM:Plaintext | Until Use | Zeroisation<br>Close Session | Authentication Keys:Protected By or Derives<br>KAS Private Keys:Derives<br>KAS Public Keys:Protected By or Derives<br>Encryption Keys:Protected By<br>Asymmetric Private Keys:Protected By<br>Asymmetric Public Keys:Protected By<br>KTS-IFC Private Key:Protected By<br>KTS-IFC Public Key:Protected By<br>Shared Secret:Protected By<br>HMAC Key:Protected By<br>OTP AEAD Key:Protected By<br>OTP ECB Key:Protected By<br>AES-CCM Wrap Key:Protected By<br>AES-KWP Wrap Key:Protected By |
| Shared Secret | | RAM:Plaintext | Until Use | Zeroisation-AfterUse | Asymmetric Private Keys:Derives<br>Asymmetric Public Keys:Derives<br>Session Keys:Encrypts |

Table 24: SSP Table 2

### 9.5 TRANSITIONS

**SHA-1:** The module uses SHA-1 for HMAC. Per CMVP Programmatic Transitions and NIST SP 800-131Ar2, usage of SHA-1 for non-digital-signature applications is deprecated through Dec 31, 2030.

**Minimum key size transition:** In accordance with NIST SP 800-131Ar2, the module meets the minimum key size requirement of 112. NIST SP 800-57, Part 1 includes a transition to a security strength of 128 bits from 2031 and beyond.

## 10 SELF-TESTS

The following pre-operational and conditional self-tests are performed by the module. All self-tests are performed regardless of whether the module is in the approved or non-approved mode. The data output interface is inhibited whenever the cryptographic module is in a self-test condition.

### 10.1 PRE-OPERATIONAL SELF-TESTS

The following pre-operational test is performed upon power-up and on-demand, the latter by power-cycling the module. The module transitions to its error state if the test fails.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| LRC | 16-bit Error Detection Code | KAT | SW/FW Integrity | Implicit | N/A |

Table 25: Pre-Operational Self-Tests

### 10.2 CONDITIONAL SELF-TESTS

The following conditional tests are performed upon power-up, on-demand and periodically.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CCM (A5891) | 128-bit | KAT | CAST | Implicit | Encrypt KAT | Power-On |
| AES-ECB (A5891) | 128-bit | KAT | CAST | Implicit | Decrypt KAT | Power-On |
| Counter DRBG (A5891) | CTR_DRBG | KAT | CAST | Implicit | SP800-90A Health Tests for Instantiate, Reseed, and Generate | Power-On |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| ECDSA SigGen (FIPS186-5) (A5891) | P-256, SHA2-256 | KAT | CAST | Implicit | Digital Signature Generation KAT | Power-On |
| ECDSA SigVer (FIPS186-5) (A5891) | P-256, SHA2-256 | KAT | CAST | Implicit | Digital Signature Verification KAT | Power-On |
| EDDSA SigGen (A5891) | Ed25519, SHA2-512 | KAT | CAST | Implicit | Digital Signature Generation KAT | Power-On |
| EDDSA SigVer (A5891) | Ed25519, SHA2-512 | KAT | CAST | Implicit | Digital Signature Verification KAT | Power-On |
| HMAC-SHA2-256 (A5891) | SHA2-256 | KAT | CAST | Implicit | MAC | Power-On |
| KAS-ECC-SSC Sp800-56Ar3 (A5891) | P-256 | KAT | CAST | Implicit | Shared Secret Computation KAT | Power-On |
| KDF ANS 9.63 (A5891) | X9.63 | KAT | CAST | Implicit | Key Derivation | Power-On |
| KDF SP800-108 (A5891) | AES CMAC | KAT | CAST | Implicit | Key Derivation | Power-On |
| RSA SigGen (FIPS186-5) (A5891) | 2048-bit PKCS#1 with SHA2-256 | KAT | CAST | Implicit | Digital signature generation KAT. Satisfies KTS-IFC un-encapsulation self-test requirements per IG D.G | Power-On |
| RSA SigVer (FIPS186-5) (A5891) | 2048-bit PKCS#1 with SHA2-256 | KAT | CAST | Implicit | Digital signature verification KAT. Satisfies KTS-IFC encapsulation self-test requirements per IG D.G | Power-On |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| SHS (A5891) | SHA-1, SHA2-512 | KAT | CAST | Implicit | Hash KAT | Power-On |
| NIST SP 800-90B Entropy | APT, RCT | SP800-90B Health Tests | CAST | Implicit | APT, RCT | Upon use |
| PWCT | Sign/Verify | Sign/Verify | PCT | Implicit | EC, ED, RSA | Upon Key Generation |

Table 26: Conditional Self-Tests

## 10.3 PERIODIC SELF-TEST INFORMATION

The module regularly performs its periodic self-tests at an interval of 29 hours.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| LRC | KAT | SW/FW Integrity | 29 hours | Automatic |

Table 27: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-CCM (A5891) | KAT | CAST | Power-On | Manual |
| AES-ECB (A5891) | KAT | CAST | Power-On | Manual |
| Counter DRBG (A5891) | KAT | CAST | Power-On | Manual |
| ECDSA SigGen (FIPS186-5) (A5891) | KAT | CAST | Power-On | Manual |
| ECDSA SigVer (FIPS186-5) (A5891) | KAT | CAST | Power-On | Manual |
| EDDSA SigGen (A5891) | KAT | CAST | Power-On | Manual |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| EDDSA SigVer (A5891) | KAT | CAST | Power-On | Manual |
| HMAC-SHA2-256 (A5891) | KAT | CAST | Power-On | Manual |
| KAS-ECC-SSC Sp800-56Ar3 (A5891) | KAT | CAST | Power-On | Manual |
| KDF ANS 9.63 (A5891) | KAT | CAST | Power-On | Manual |
| KDF SP800-108 (A5891) | KAT | CAST | Power-On | Manual |
| RSA SigGen (FIPS186-5) (A5891) | KAT | CAST | Power-On | Manual |
| RSA SigVer (FIPS186-5) (A5891) | KAT | CAST | Power-On | Manual |
| SHS (A5891) | KAT | CAST | Power-On | Manual |
| NIST SP 800-90B Entropy | SP800-90B Health Tests | CAST | 29 hours | Automatic |
| PWCT | Sign/Verify | PCT | Power-On | Manual |

**Table 28: Conditional Periodic Information**

## 10.4 ERROR STATES

The module transitions into the error state when an error condition is encountered and provides an error status indicator (i.e., blinking an attached LED before rebooting). All data output and cryptographic functions are inhibited while the module is in the error state (refer to Table 28).

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| Error State | Upon detection of any failures in a pre-operational or conditional self-test | Self-test failure | Power Cycle | Attached LED blinks special sequence, then reboots. |

Table 29: Error States

### 10.5 OPERATOR INITIATION OF SELF-TESTS

Self-tests may be invoked on demand by power cycling the module.

## 11 LIFE-CYCLE ASSURANCE

There are no specific maintenance requirements.

### 11.1 INSTALLATION, INITIALIZATION, AND STARTUP PROCEDURES

The following initialization procedures must be adhered to prior to first use. Only when this procedure is completed will the module operate in the approved mode.
The module operates in the non-Approved mode by default. To configure the module into the Approved mode of operation, the operator shall perform the following:

1. Use the “Reset Device” service as follows: “reset 0”. This step may be omitted if the module has never been used
2. Use the “Set Option” service as follows: “put option 0 fips-mode 01”
3. Import new Authentication Keys to replace the default values. (Enforced in Approved mode)

To configure the module into the non-Approved mode of operation from the Approved mode, the operator need only invoke the “Reset Device” service. After a “Reset Device” service, the module will verify that all CSPs have been zeroized and then assume the non-Approved mode.

To check the mode of operation, the operator may perform the following:

- Use the “Get Option” service as follows: “get option 0 fips-mode”
  - “01” return code indicates the Approved mode
  - “00” return code indicates the non-Approved mode

### 11.2 ADMINISTRATOR GUIDANCE

There are no further instructions for administrators beyond those outlined in the Installation, Initialization, and Startup Procedures.

### 11.3 NON-ADMINISTRATOR GUIDANCE

There are no further instructions for non-administrators beyond those outlined in the Installation, Initialization, and Startup Procedures.

### 11.4 DESIGN AND RULES

The following security rules are enforced by the cryptographic module to ensure the FIPS 140-3 security requirements are met.

1. The module supports an Approved and non-Approved mode of operation. The Approved mode indicator must be returned to the end user.
2. The module does not allow unauthenticated operators to have any access to the module's cryptographic services.
3. Concurrent operators are separated by unique sessions. No services from a given session can modify the services/data of another separate session.
4. The module inhibits data output during self-tests, firmware load, zeroization and error states.
5. The module logically disconnects data output from the processes performing zeroization and key generation.
6. The module enforces identity-based authentication.
7. The module does not retain the authentication of an operator following power-off or reboot.
8. The module supports the following role: Cryptographic Officer (CO).
9. The module does not support a bypass mode or maintenance mode.
10. The module does not support the following logically distinct interfaces:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface
11. The module protects critical security parameters from unauthorized disclosure, modification and substitution.
12. The module performs power-on, on-demand and periodic self-testing.
13. The module logs errors whenever an error state is entered.
14. The module does not perform any cryptographic functions while in an error state.

### 11.5 END OF LIFE

To prepare the module for disposal, zeroize the module using the "Reset Device" service and dispose of it at an electronic recycling facility.

## 12 MITIGATION OF OTHER ATTACKS

The module is not purposefully designed to mitigate any attacks beyond the scope of FIPS 140-3 requirements.