Yubico, Inc.

YubiKey 5 Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Version 1.0

TABLE OF CONTENTS

1 General 6

1.1 Overview 6

1.2 Security Levels 6

2 Cryptographic Module Specification 7

2.1 Description 7

2.2 Tested and Vendor Affirmed Module Version and Identification 8

2.3 Excluded Components 9

2.4 Modes of Operation 9

2.5 Algorithms 10

2.6 Security Function Implementations 14

2.7 Algorithm Specific Information 19

2.8 RBG and Entropy 20

2.9 Key Generation 20

2.10 Key Establishment 20

2.11 Industry Protocols 20

3 Cryptographic Module Interfaces 21

3.1 Ports and Interfaces 21

4 Roles, Services, and Authentication 21

4.1 Authentication Methods 21

4.2 Roles 23

4.3 Approved Services 23

4.4 Non-Approved Services 50

4.5 External Software/Firmware Loaded 50

5 Software/Firmware Security 51

5.1 Integrity Techniques 51

5.2 Initiate on Demand 51

6 Operational Environment 51

6.1 Operational Environment Type and Requirements 51

7 Physical Security 51

7.1 Mechanisms and Actions Required 51

This document may be freely reproduced and distributed, but only in its entirety and without modification

7.2 EFP/EFT Information 51
7.3 Hardness Testing Temperature Ranges 52
8 Non-Invasive Security 52
8.1 Mitigation Techniques 52
9 Sensitive Security Parameters Management 52
9.1 Storage Areas 52
9.2 SSP Input-Output Methods 53
9.3 SSP Zeroization Methods 53
9.4 SSPs 55
10 Self-Tests 61
10.1 Pre-Operational Self-Tests 61
10.2 Conditional Self-Tests 61
10.3 Periodic Self-Test Information 63
10.4 Error States 64
10.5 Operator Initiation of Self-Tests 65
11 Life-Cycle Assurance 65
11.1 Installation, Initialization, and Startup Procedures 65
11.2 Administrator Guidance 66
11.3 Non-Administrator Guidance 66
11.4 Design and Rules 66
11.5 End of Life 67
12 Mitigation of Other Attacks 67
13 References 67

This document may be freely reproduced and distributed, but only in its entirety and without modification

LIST OF TABLES

Table 1: Security Levels 7

Table 2: Tested Module Identification – Hardware 8

Table 3: Modes List and Description 9

Table 4: Approved Algorithms 12

Table 5: Vendor-Affirmed Algorithms 13

Table 6: Non-Approved, Allowed Algorithms 13

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed 13

Table 8: Non-Approved, Not Allowed Algorithms 14

Table 9: Security Function Implementations 19

Table 10: Entropy Certificates 20

Table 11: Entropy Sources 20

Table 12: Ports and Interfaces 21

Table 13: Authentication Methods 22

Table 14: Roles 23

Table 15: Approved Services 49

Table 16: Non-Approved Services 50

Table 17: Mechanisms and Actions Required 51

Table 18: EFP/EFT Information 52

Table 19: Hardness Testing Temperatures 52

Table 20: Storage Areas 53

Table 21: SSP Input-Output Methods 53

Table 22: SSP Zeroization Methods 54

Table 23: SSP Table 1 57

Table 24: SSP Table 2 60

This document may be freely reproduced and distributed, but only in its entirety and without modification

Table 25: Pre-Operational Self-Tests 61

Table 26: Conditional Self-Tests 63

Table 27: Pre-Operational Periodic Information 63

Table 28: Conditional Periodic Information 64

Table 29: Error States 65

List of Figures

Figure 1: YubiKey 5 Cryptographic Module 7

Figure 2: Block Diagram 8

This document may be freely reproduced and distributed, but only in its entirety and without modification

1 GENERAL

1.1 OVERVIEW

This document defines the Security Policy for the Yubico, Inc. (Yubico) YubiKey 5 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 2.

1.2 SECURITY LEVELS

The module meets the overall requirements of FIPS 140-3 Security Level 2.

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

This document may be freely reproduced and distributed, but only in its entirety and without modification

Table 1: Security Levels

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 DESCRIPTION

The YubiKey 5 Cryptographic Module (the module) is a single-chip module validated at FIPS 140-3 Security Level 2. The module is a secure element that supports multiple protocols designed to be embedded in USB and/or NFC security tokens. The module can generate, store, and perform cryptographic operations for sensitive data and can be utilized via an external touch-button for Test of User Presence in addition to PIN for smartcard authentication. The module implements several major functions - FIDO, PIV-compatible smartcard, OpenPGP smartcard, OATH authentication, Security Domain, and YubiHSM Auth.

Figure 1: YubiKey 5 Cryptographic Module

Purpose and Use:

The YubiKey 5 Cryptographic Module is the core component for authenticators in the YubiKey 5 product family and supports several functional units: FIDO, PIV, OpenPGP, OATH, Security Domain, and YubiHSM Auth.

Module Type: Hardware

Module Embodiment: SingleChip

Module Characteristics:
The critical components within the module are encapsulated inside a single, integrated circuit. Please note that NFC is supported as a communication layer, but the antenna and wireless capability is outside of the module's boundary; as such, the wireless capability is not part of the validation.

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

This document may be freely reproduced and distributed, but only in its entirety and without modification

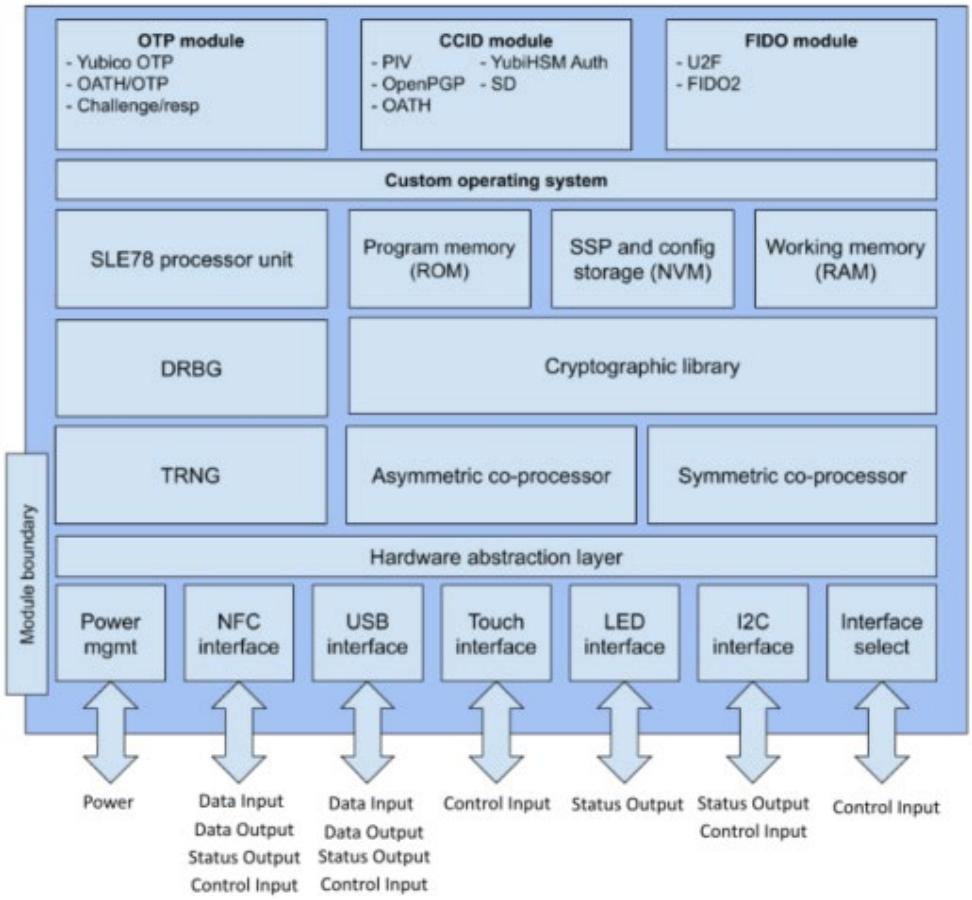

Figure 2: Block Diagram

2.2 TESTED AND VENDOR AFFIRMED MODULE VERSION AND IDENTIFICATION

The YubiKey 5 Cryptographic Module is designed to meet the requirements of FIPS 140-3 Security Level 2 (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	5.7.4	SLE78CLUFX5000P	Single-Chip

Table 2: Tested Module Identification – Hardware

This document may be freely reproduced and distributed, but only in its entirety and without modification

N.B. The module returns the hardware identifier '78CLUFX5000P' and firmware version '5.7.4' when queried.

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

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

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

N/A for this module.

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 EXCLUDED COMPONENTS

There are no components excluded from the cryptographic boundary.

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.

Mode Name	Description	Type	Status Indicator
Approved	All functional units other than OTP	Approved	The "Slot YK Get Device Info" service results in an error.
Non-Approved	OTP functional unit services	Non-Approved	The "Slot YK Get Device Info" service resolves successfully.

Table 3: Modes List and Description

The module powers up in an uninitialized state upon first use. The operator must configure the module per the instructions provided in Section 11.1. Once this process is completed, the module enters the Approved mode. The

This document may be freely reproduced and distributed, but only in its entirety and without modification

module retains its current configuration settings across power-cycling. The module is single-threaded: while one service is in process, no other service is.

Mode Change Instructions and Status:

The module enters the non-Approved mode whenever a non-Approved service is invoked and exits when the said service completes.

The only non-Approved services are contained by the OTP functional unit. In order to access the OTP functional unit, OTP must be selected (NFC) or the designated OTP endpoints must be used (USB). While OTP is selected, no other services beyond OTP services, namely those listed in Section 4.4, are available.

2.5 ALGORITHMS

The YubiKey 5 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 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 Key Length - 128, 192, 256	SP 800-38B
AES-ECB	A5891	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
Counter DRBG	A5891	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A5891	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5891	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-5)	A5891	Curve - P-224, P-256, P-384, P-521 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	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
KAS-ECC-SSC Sp800-56Ar3	A5891	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - fullUnified - KAS Role - initiator, responder onePassDh - KAS Role - initiator, responder onePassUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A5891	Derived Key Length - 256 Shared Secret Length - Shared Secret Length: 256 HMAC Algorithm - SHA2-256	SP 800-56C Rev. 2
KDF ANS 9.63 (CVL)	A5891	Hash Algorithm - SHA2-256 Key Data Length - Key Data Length: 512, 640	SP 800-135 Rev. 1

This document may be freely reproduced and distributed, but only in its entirety and without modification

Algorithm	CAVP Cert	Properties	Reference
KDF SP800-108	A5891	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-2040 Increment 8	SP 800-108 Rev. 1
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 Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - crt	FIPS 186-5
RSA SigGen (FIPS186-5)	A5891	Modulo - 2048, 3072, 4096 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 Signature Type - pkcs1v1.5	FIPS 186-5
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:

This document may be freely reproduced and distributed, but only in its entirety and without modification

The module supports the following vendor affirmed algorithms (refer to Table 5).

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:

The module supports ECDSA with non-NIST recommended curves: brainpool256r1, brainpool384r1, and brainpool512r1. These curves are allowed per IG C.A.

The module also supports KAS with non-NIST recommended curves: brainpool256r1, brainpool384r1, brainpool512r1. These curves are allowed per IG C.A.

Name	Properties	Implementation	Reference
ECDSA	Curve:brainpool256r1, brainpool384r1, brainpool512r1	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:

The module supports DES for internal integrity checks with no security claimed. In addition, the module supports ECDH with no security claimed; this ECDH is to support the legacy PIN protocol 1 over directly connected USB sessions. The ECDH implementation provides no security and all transmissions within the established session are handled as plaintext. For this reason, the module only permits PIN protocol 1 use over a directly connected USB session for which plaintext transmissions of PIN values permitted.

Name	Caveat	Use and Function
DES	No security claimed	For internal integrity checking use only
ECDH	No security claimed	For legacy use only, all information transmitted within the established sessions is treated as plaintext over a directly connected path.

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

This document may be freely reproduced and distributed, but only in its entirety and without modification

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES (non-compliant)	Supports the calculation of One-Time Passwords in the OTP functional unit.
HMAC (non-compliant)	Supports the calculation of One-Time Passwords in the OTP functional unit.

Table 8: Non-Approved, Not Allowed Algorithms

2.6 SECURITY FUNCTION IMPLEMENTATIONS

Name	Type	Description	Properties	Algorithms
AKG	AsymKeyPair-KeyGen	RSA 2048, 3072, 4096, ECDSA P-256, P-384, P-521	Standard:FIPS 186-5	CKG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A5891) RSA KeyGen (FIPS186-5): (A5891) Modulo: 2048, 3072, 4096 ECDSA KeyGen (FIPS186-5): (A5891) Curve: P-256, P-384, P-521 EDDSA KeyGen: (A5891) Curve: ed25519
DEC	BC-UnAuth	Symmetric Decryption	Standard:FIPS 197	AES-CBC: (A5891) Key Size: 128, 192, 256 AES-ECB: (A5891) Key Size: 128, 192, 256

This document may be freely reproduced and distributed, but only in its entirety and without modification

Name	Type	Description	Properties	Algorithms
ECSP	UNK	Signature Generation Primitive	Standard:FIPS 186-5	ECDSA SigGen (FIPS186-5): (A5891) Curve: P-256, P-384, P-521, brainpool256r1, brainpool384r1, brainpool512r1
ENC	BC-Auth	Symmetric Encryption	Standard:FIPS 197	AES-CBC: (A5891) Key Size: 128, 192, 256 AES-ECB: (A5891) Key Size: 128, 192, 256
ESV	ENT-ESV	SP800-90B Physical Entropy Source	Standard:SP800-90B	
KAS-KG	KAS-KeyGen	Key Generation	Standard:SP800-56Ar3	KAS-ECC-SSC Sp800-56Ar3: (A5891)
KAS-PP2	KAS-Full	NIST SP 800-56Arev3 KAS-ECC Per IG D.F Scenario 2 path (2). CTAP Session (Pin Protocol 2)	Standard:SP800-56Ar3, SP800-56Cr2 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 KDA HKDF SP800-56Cr2: (A5891)
KAS-SCP11	KAS-Full	SCP11 Security Domain implementation	Standard:SP800-56Ar3 Implementation:SCP11 Security Domain	KAS-ECC-SSC Sp800-56Ar3: (A5891)

This document may be freely reproduced and distributed, but only in its entirety and without modification

Name	Type	Description	Properties	Algorithms
		using SP800-135r1 ANSI X9.63 KDF YubiHSM-Auth	implementation using SP800-135r1 ANSI X9.63 KDF, Global Platform GPC v2.3 Amendment F v1.2.1 SCP11 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	Scheme: (2e,2s), (1e,2s) Curve: P-256 KDF ANS 9.63: (A5891)
KBKDF	KBKDF	Key-Based Key Derivation CMAC-AES128 (SCP03 and YubiHSM-Auth). Only used as part of session establishment.	Standard:SP800-108 Implementation:Global Platform GPC 2.3 Amendment D v1.2 SCP03	KDF SP800-108: (A5891)
KTS-CBC-CMAC	KTS-Wrap	Global Platform GPC 2.3 Amendment D v1.2 SCP03 Global Platform GPC v2.3 Amendment F v1.4 SCP11, SP800-56Ar3	Standard:SP800-38F IG D.G:Approved method from IG D.G Caveat:Key establishment methodology provides 128 to 256 bits of security strength	AES-CBC: (A5891) Key Size: 128, 192, 256 AES-CMAC: (A5891) Key Size: 128, 192, 256
KTS-CBC-HMAC	KTS-Wrap	FIDO Client to Authenticator Protocol (CTAP) 2.1 Pin protocol 2	Standard:SP800-38F IG D.G:Approved method from IG D.G Caveat:Key establishment methodology provides	AES-CBC: (A5891) Key Size: 128, 192, 256 HMAC-SHA2-256: (A5891)

Name	Type	Description	Properties	Algorithms
			128 to 256 bits of security strength	Key Size: 128, 192, 256
KTS-CCM	KTS-Wrap	FIDO wrapping key	Standard:SP800-108, Global Platform GPC 2.3 Amendment D v1.2 SCP03 IG D.G:Approved method from IG D.G Caveat:Key establishment methodology provides 128 to 256 bits of security strength	AES-CCM: (A5891) Key Size: 128, 192, 256
MAC	MAC	Keyed MAC	Standard:FIPS 198-2	AES-CMAC: (A5891) HMAC-SHA-1: (A5891) HMAC-SHA2-256: (A5891) HMAC-SHA2-384: (A5891) HMAC-SHA2-512: (A5891)
PKV	AsymKeyPair-PubKeyVal	Public key validation	Standard:SP800-56Ar3, FIPS186-5	ECDSA KeyGen (FIPS186-5): (A5891) KAS-ECC-SSC Sp800-56Ar3: (A5891)
RAND	DRBG	Random Number Generation	Standard:SP800-90A	Counter DRBG: (A5891)
RSADP	UNK	RSA Decryption Primitive (PKCS#1	Standard:SP800-56Br2	RSA Decryption Primitive Sp800-56Br2: (A5891)

This document may be freely reproduced and distributed, but only in its entirety and without modification

Name	Type	Description	Properties	Algorithms
		v2.1). Key size 2048 (PIV raw).		Modulo: 2048, 3072, 4096
RSASP	UNK	RSA Signature Primitive	Standard:FIPS 186-5	RSA Signature Primitive: (A5891) Modulo: 2048, 3072, 4096
SHS	SHA	Message Digest	Standard:FIPS 180	SHA-1: (A5891) SHA2-256: (A5891) SHA2-384: (A5891) SHA2-512: (A5891)
SSC	KAS-SSC	Shared Secret Calculation	Standard:SP800-56Ar3	KAS-ECC-SSC Sp800-56Ar3: (A5891) Scheme: (1e,1s, ECC CDH) Type: Co-factor One-Pass Diffie Hellman Curve: P-256, P-384, P-521, brainpool256r1, brainpool384r1, brainpool512r1
SigGen	DigSig-SigGen	Signature Generation	Standard:FIPS 186-5	RSA SigGen (FIPS186-5): (A5891) Modulo: 2048, 3072, 4096 ECDSA SigGen (FIPS186-5): (A5891) Curve: P-256, P-384, P-521, brainpool256r1, brainpool384r1,

This document may be freely reproduced and distributed, but only in its entirety and without modification

Name	Type	Description	Properties	Algorithms
				brainpool512r1 EDDSA SigGen: (A5891) Curve: ed25519
SigVer	DigSig-SigVer	Signature Verification	Standard:FIPS 186-5	RSA SigVer (FIPS186-5): (A5891) Modulo: 2048, 3072, 4096 ECDSA SigVer (FIPS186-5): (A5891) Curve: P-256, P-384, P-521, brainpool256r1, brainpool384r1, brainpool512r1 EDDSA SigVer: (A5891) Curve: ed25519
SymKG	CKG	Symmetric Key Generation	Standard:SP800-133r2	Counter DRBG: (A5891) CKG: () Key Type: Symmetric and Asymmetric

Table 9: Security Function Implementations

2.7 ALGORITHM SPECIFIC INFORMATION

The module utilizes only approved algorithms that are tested and validated under the Cryptographic Algorithm Validation Program (CAVP).

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,

This document may be freely reproduced and distributed, but only in its entirety and without modification

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.

Limited use of SHA-1:

The use of SHA-1 (Cert. #A5891) is restricted within the module to non-digital signature applications. SHA-1 is solely used within HMAC-SHA-1 (Cert. #A5891).

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 SP 800-90A.

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 supports the generation of cryptographic keys and components with a security strength of 256-bits.

2.10 KEY ESTABLISHMENT

The module supports key establishment using KAS with a supported security strength of 128 or 256-bits, depending on the selection of key sizes utilized. The module supports key transport with a supported security strength of 128 or 256-bits, depending on the selection of key sizes utilized.

2.11 INDUSTRY PROTOCOLS

The module supports the Secure Channel Protocols SCP03 & SCP11 for the establishment of ephemeral, protected communication sessions.

3 CRYPTOGRAPHIC MODULE INTERFACES

3.1 PORTS AND INTERFACES

The module incorporates physical ports and logical interfaces. The physical ports are defined within Table 12 below:

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

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. The authentication method of both Crypto Officer and User is the password-based authentication that the module performs Memorized Secret

and Single-Factor Cryptographic Device described in NIST SP 800-140E and SP 800-63B-4 (refer to Sections 3.1.1, 3.1.2, and 3.1.6). This role has separate authentication methods as indicated in Table 13. Section 11.1 describes the procedure by which an operator is to perform authentication as part of the module initialization process. The module supports three authentication methods: PIN verification, knowledge of a shared secret, and possession of a private key.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
PIN verification	PIN verification	Comparison of a 6 byte string	A minimum 6 byte (48 bit) binary string has a probability that a random attempt will succeed or a false acceptance will occur of 1/2^48 which is less than 1/1,000,000.	Each authentication attempt takes approximately 60 ms which allows a maximum of 1000 attempts per minute. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 1000/2^48, which is less than 1/100,000.
Knowledge of a shared secret	Knowledge of a shared secret	Cryptographic Software	The shared secret is either a 128, 192, or 256-bit AES key or a minimum length 112 bits HMAC key. The probability that a random attempt will succeed or a false acceptance will occur is at most 1/2^112 which is less than 1/1,000,000.	Authentication attempts are limited to 6,000 per minute due to performance constraints. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 6,000/2^112, 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.	Authentication attempts are limited to 6,000 per minute due to performance constraints. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 6,000/2^128, which is less than 1/100,000.

Table 13: Authentication Methods

4.2 ROLES

The module supports a Cryptographic Officer (CO), a User, and an unauthenticated role. The CO is responsible for configuring SSPs and resetting User credentials. The User performs cryptographic operations and utilizes the module as an authenticator. The unauthenticated role has access to respond to challenges, read non-security-relevant information, perform self-tests, and reset services only.

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	PIN verification Knowledge of a shared secret Possession of Private Key
User	Role	User	PIN verification Knowledge of a shared secret
Unauthenticated	Role	N/A	None

Table 14: Roles

4.3 APPROVED SERVICES

The module supports six functional units, each of which provides access to a unique set of services: PIV, OATH, OpenPGP, FIDO, Security Domain, and YubiHSM Auth. All Approved services and non-Approved services are accessible over both USB and NFC interfaces.

Please note that all services can be performed over a Secure Channel (SCP03 or SCP11) with the exception of:

- FIDO services conducted directly over USB
- Services that establish the Secure Channel
    - Initialize Update service and External Authenticate service that establish the SCP03 session
    - Perform Security operation service, Internal Authenticate service and Mutual Authenticate service that establish the SCP11 session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Activate Applet - OpenPGP	Activate OpenPGP applet with factory defaults. Zeroization.	return code 0x9000	none	success/error	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E - Asymmetric Public Keys: Z - Asymmetric Private Keys: Z - KAS Private Keys: Z - KAS Public Keys: Z - PINs: Z
Attest - OpenPGP	Generate attestation for an internally generated key	return code 0x9000	Key ID	success/error	RAND SigGen KTS-CBC-CMAC ENC DEC MAC	User - DRBG State: G,E - Attestation Key: E - Asymmetric Public Keys: R - KAS Public Keys: R - Secure Channel Session Keys: E
Attest - PIV	Generate an attestation for an internally generated key	return code 0x9000	Key ID	x509 attestation	SigGen RAND KTS-CBC-CMAC ENC	Unauthenticated - DRBG State: G,E - Attestation Key: E - Asymmetric

This document may be freely reproduced and distributed, but only in its entirety and without modification

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					DEC MAC	Public Keys: R - KAS Public Keys: R - Secure Channel Session Keys: E
Authenticator Config - FIDO	Set and retrieve authenticator configuration	return code 0x9000	configuration	configuration	MAC ENC DEC RAND SymKG	User - DRBG State: G,E - CTAP PIN token: G,E,Z - Secure Channel Session Keys: E
Authenticator Select - FIDO	Identify authenticator	return code 0x9000	none	success/error	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Calculate - OATH	Calculate the code for an OATH entry	return code 0x9000	OATH credential ID	HMAC response	ENC DEC MAC RAND	Crypto Officer - OATH Seed Key: E - Secure Channel Session Keys: E - DRBG State: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Calculate - YubiHSM Auth	User Authenticate	return code 0x9000	authentication challenge or public key	session keys	KAS-SCP11 KTS-CBC-CMAC KBKDF PKV RAND ENC DEC MAC	User - KAS Private Keys: E,Z - KAS Public Keys: W,E,Z - DRBG State: G,E - Secure Channel Session Keys: R,E,G - PINs: W,E - Secure Channel Authentication Keys: E
Calculate All - OATH	Calculate code for all entries	return code 0x9000	none	HMAC responses	ENC DEC MAC RAND	Crypto Officer - OATH Seed Key: E - Secure Channel Session Keys: E - DRBG State: G,E
Change Management Key - PIV	Change management key	return code 0x9000	new management key	success/error	ENC DEC MAC KTS-CBC-CMAC	Crypto Officer - PIV Management Auth Key: W - Secure Channel Session Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Change PIN - PIV	Change user PIN with known PIN	return code 0x9000	old and new PIN	success/error	ENC DEC MAC	User - PINs: W,E - Secure Channel Session Keys: E
Change PIN - YubiHSM Auth	Update PIN	return code 0x9000	old PIN and new PIN	success/error	ENC DEC MAC	Crypto Officer - PINs: E,W - Secure Channel Session Keys: E
Change PUK - PIV	Change PIN unlock code	return code 0x9000	old and new PUK	success/error	ENC DEC MAC	Crypto Officer - PINs: W,E - Secure Channel Session Keys: E
Change PW1 - OpenPGP	Update user PIN	return code 0x9000	old PW1 and new PW1	success/error	ENC DEC MAC	User - PINs: W,E - Secure Channel Session Keys: E
Change PW3 - OpenPGP	Update admin PIN	return code 0x9000	old PW3 and new PW3	success/error	ENC DEC MAC	Crypto Officer - PINs: W,E - Secure Channel Session Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Change Retry Counters - PIV	Set retry counter for PINs	return code 0x9000	new counters	success/error	ENC DEC MAC	Crypto Officer - PINs: Z - Secure Channel Session Keys: E
Close Session	Closes the secure session	None	None	None	None	Crypto Officer - Secure Channel Session Keys: Z
Compute Digital Signature Primitive - OpenPGP	Perform signature primitive	return code 0x9000	hash of message to sign	signature	RAND ECSP RSASP ENC DEC MAC	User - DRBG State: G,E - Asymmetric Private Keys: E - Secure Channel Session Keys: E
Credential Management - FIDO	Listing credentials and deleting credentials	return code 0x9000	credential ID, relying party ID	list of credentials, which include public keys, or relying parties	MAC KTS-CBC-CMAC ENC DEC RAND	User - CTAP PIN token: E - Asymmetric Private Keys: Z - Asymmetric Public Keys: R,Z - CTAP Offline Key: E - Secure Channel Session Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG State: G,E
Decipher - OpenPGP	EC-DH shared secret calculation	return code 0x9000	public key for KAS	Shared secret	RAND SSC PKV KTS-CBC-CMAC ENC DEC MAC	User - DRBG State: G,E - KAS Private Keys: E - Shared Secret: G,E,R - KAS Public Keys: W,E - Secure Channel Session Keys: E
Delete - OATH	Remove an OATH entry	return code 0x9000	OATH credential ID	success/error	ENC DEC MAC	Crypto Officer - OATH Seed Key: Z - Secure Channel Session Keys: E
Delete Key - PIV	Delete an asymmetric key	return code 0x9000	Key ID	success/error	ENC DEC MAC	Crypto Officer - Asymmetric Private Keys: Z - Attestation Key: Z - KAS Private Keys: Z - Asymmetric Public Keys: Z - KAS Public Keys: Z - Secure Channel

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Keys: E
Delete Key - SD	Delete key set	return code 0x9000	Key ID	success/error	ENC DEC MAC	Crypto Officer - Secure Channel Authentication Keys: Z - Secure Channel Sensitive Data Key: Z - KAS Private Keys: Z - KAS Public Keys: Z - Asymmetric Public Keys: Z - Secure Channel Session Keys: E
Delete Keys - YubiHSM Auth	Delete keys	return code 0x9000	Key ID	success/error	ENC DEC MAC	Crypto Officer - KAS Private Keys: Z - KAS Public Keys: Z - PINs: W,E,Z - Secure Channel Session Keys: E - Secure Channel Authentication Keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Device Configuration	Select a functional unit and retrieve or configure non-security relevant device information	return code 0x9000	request for device configuration	current device configuration	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
External Authenticate - SD	Complete Session Establishment	return code 0x9000	finishing authentication data	authentication data	MAC	Unauthenticated - Secure Channel Session Keys: E
General AUTH Decrypt - PIV	Decrypt input data. This service returns an error if the decryption key is not an RSA key.	return code 0x9000	data to be decrypted, slot number for decryption key	success/error/decrypted data	RAND RSADP ENC DEC MAC	User - DRBG State: G,E - Asymmetric Private Keys: E - Secure Channel Session Keys: E
General AUTH Key Agreement - PIV	Perform key agreement. This service returns an error if the key in the slot is not an ECC key.	return code 0x9000	partner's public key, slot number for the module's KAS private key	success/error/shared secret	RAND PKV SSC KTS-CBC-CMAC ENC DEC MAC	User - DRBG State: G,E - KAS Private Keys: E - KAS Public Keys: W,E - Shared Secret: G,E,R - Secure

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Channel Session Keys: E
General AUTH Management Authentication - PIV	Authenticate to the applet using the Management Auth Key.	return code 0x9000	applet authentication data, challenge/response	challenge/response, success/failure	RAND ENC DEC MAC	Unauthenticated - DRBG State: G,E - PIV Management Auth Key: E - Secure Channel Session Keys: E
General AUTH Sign - PIV	Sign digest data	return code 0x9000	digest to be signed, slot number for signing key	success/error/signed data	RAND RSASP ECSP ENC DEC MAC	User - DRBG State: G,E - Asymmetric Private Keys: E - Secure Channel Session Keys: E
Generate Asymmetric Key Pair - OpenPGP	Generate asymmetric key pair	return code 0x9000	Key ID	public key	RAND AKG PKV KAS-KG KTS-CBC-CMAC ENC DEC MAC	Crypto Officer - DRBG State: G,E - Asymmetric Private Keys: G,E - KAS Private Keys: G,E - Asymmetric Public Keys: G,R,E - KAS Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys: G,R,E - Secure Channel Session Keys: E
Generate Key - PIV	Generate asymmetric key pair	return code 0x9000	slot number, parameters, PIN policy	public key	RAND PKV AKG KAS-KG KTS-CBC-CMAC ENC DEC MAC	Crypto Officer - DRBG State: G,E - Asymmetric Private Keys: G,E - KAS Private Keys: G,E - Asymmetric Public Keys: G,R,E - KAS Public Keys: G,R,E - Secure Channel Session Keys: E
Generate Key Pair - SD	Generate SCP11 keypair	return code 0x9000	Key ID	public key	KAS-KG PKV KTS-CBC-CMAC ENC DEC MAC RAND	Crypto Officer - KAS Private Keys: G,Z - KAS Public Keys: G,R,Z - DRBG State: G,E
Get Assertion - FIDO	Use credential	return code 0x9000	keyhandle (potentially	signature	RAND KTS-CCM KTS-	User - DRBG State: G,E - Wrapping

This document may be freely reproduced and distributed, but only in its entirety and without modification

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			wrapped key), challenge		CBC-CMAC SigGen ENC DEC MAC	Key: E - Asymmetric Private Keys: E,W - CTAP Offline Key: E - CTAP PIN token: E - Secure Channel Session Keys: E
Get Challenge - YubiHSM Auth	Get a challenge for authentication	return code 0x9000	none	Challenge or public key	RAND KAS-KG PKV KTS-CBC-CMAC ENC DEC MAC	User - DRBG State: G,E - KAS Private Keys: G,Z - KAS Public Keys: G,R,Z - PINs: W,E - Secure Channel Session Keys: E
Get Data - SD	Get metadata	return code 0x9000	none	metadata, X.509 certificate	SigGen KTS-CBC-CMAC ENC DEC MAC RAND	Unauthenticated - Attestation Key: E - Asymmetric Public Keys: R - KAS Public Keys: R - Secure Channel Session Keys: E

This document may be freely reproduced and distributed, but only in its entirety and without modification

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG State: G,E
Get Information-FIDO	Device information	return code 0x9000	none	metadata	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Get Metadata - PIV	Get metadata	return code 0x9000	metadata of stored keys	algorithm, public keys and policies of keys	KTS-CBC-CMAC ENC DEC MAC	Unauthenticated - Asymmetric Public Keys: R - KAS Public Keys: R - Secure Channel Session Keys: E
Get Pubkey - YubiHSM Auth	Get a public key of an Authentication Key	return code 0x9000	Key ID	public key of Authentication Key	PKV KTS-CBC-CMAC ENC DEC MAC RAND	Unauthenticated - KAS Public Keys: G,R - Secure Channel Session Keys: E - DRBG State: G,E
Get Retry Count - YubiHSM Auth	Specify the number of Login attempts remaining	return code 0x9000	none	number of retries remaining	ENC DEC MAC	Unauthenticated - Secure Channel

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Keys: E
Get Serial - PIV	Get serial number	return code 0x9000	none	serial number	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Get Version - OpenPGP	Get firmware version	return code 0x9000	none	version	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Get Version - PIV	Get firmware version	return code 0x9000	none	version number	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Get Version - YubiHSM Auth	Get FW version	return code 0x9000	none	version number	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Import Asymmetric Key - OpenPGP	Import asymmetric private key	return code 0x9000	asymmetric private key	success/error	RAND PKV KTS-CBC-CMAC ENC	Crypto Officer - Asymmetric Private Keys: W,E - KAS Private Keys: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					DEC MAC	- Asymmetric Public Keys: G,E - KAS Public Keys: G,E - DRBG State: G,E - Secure Channel Session Keys: E
Import Key - PIV	Import asymmetric private key	return code 0x9000	asymmetric private key	success/error	RAND PKV KTS-CBC-CMAC ENC DEC MAC	Crypto Officer - Asymmetric Private Keys: W,E - KAS Private Keys: W,E - Asymmetric Public Keys: G,E - KAS Public Keys: G,E - Attestation Key: W,E - DRBG State: G,E - Secure Channel Session Keys: E
Initialize Update - SD	Create Secure Channel Session	return code 0x9000	initialization authentication challenge	authentication data	KBKDF RAND	Unauthenticated - Secure Channel Authentication Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Secure Channel Session Keys: G - DRBG State: G,E
Internal Authenticate - OpenPGP	Perform internal authentication (signature primitive)	return code 0x9000	hash of message to sign	signature	RAND ECSP RSASP ENC DEC MAC	User - DRBG State: G,E - Asymmetric Private Keys: E - Secure Channel Session Keys: E
Internal Authenticate - SD	Used for SCP11-b	return code 0x9000	other party ephemeral key	internal ephemeral public key	KAS-SCP11 KAS-KG PKV RAND	Unauthenticated - KAS Private Keys: G,E,Z - KAS Public Keys: G,R,E,Z - Secure Channel Session Keys: G - DRBG State: G,E
LargeBlob - FIDO	Store and retrieve data	return code 0x9000	encrypted data	encrypted data	MAC ENC DEC RAND	User - DRBG State: G,E - CTAP PIN token: E - Secure Channel

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Keys: E
List - OATH	List all the names of the OATH entries	return code 0x9000	none	list of all OATH keys	ENC DEC MAC	Crypto Officer - Secure Channel Session Keys: E
List - YubiHSM Auth	List the credential names	return code 0x9000	none	list of keys	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Make Credential - FIDO	Create a new FIDO credential (resident or transient)	return code 0x9000	credential specification	public key, attestation data and keyhandle (potentially wrapped key)	RAND KTS-CCM KTS-CBC-CMAC SigGen AKG PKV ENC DEC MAC	User - DRBG State: G,E - Wrapping Key: E - Asymmetric Private Keys: G,R - Attestation Key: E - CTAP PIN token: E - Asymmetric Public Keys: G,R - CTAP Offline Key: E - Secure Channel Session Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Move Key - PIV	Move an asymmetric key	return code 0x9000	Key ID	success/error	ENC DEC MAC	Crypto Officer - Secure Channel Session Keys: E
Mutual Authenticate - SD	Used for SCP11-a (2e,2s) & SCP11-c (1e,2s)	return code 0x9000	other party ephemeral key	internal ephemeral public key	KAS-SCP11 KAS-KG PKV RAND	Unauthenticated - KAS Private Keys: G,E,Z - KAS Public Keys: G,R,E,Z - Secure Channel Session Keys: G - DRBG State: G,E
PIN Service - FIDO	Creating, updating, and validating PIN	return code 0x9000	PIN, ephemeral KAS Public Key	encrypted PIN Token	RAND MAC KAS-PP2 KTS-CBC-HMAC KTS-CBC-CMAC SymKG SHS KAS-KG PKV ENC DEC	User - DRBG State: G,E - PINs: W,E - CTAP PIN token: G,R,Z - CTAP Session Keys: E,G - KAS Private Keys: G,R,Z - KAS Public Keys: R,W,E,G - Secure Channel Session Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform Security Operation - SD	Initial step for SCP11	return code 0x9000	static public key for SCP11	success/error	SigVer PKV RAND	Unauthenticated - KAS Public Keys: W,Z - DRBG State: G,E - Asymmetric Public Keys: W,E,Z
Power On	Power Cycling	services available	none	none	SymKG ESV	Unauthenticated - Entropy Input : G,E - DRBG Seed : G,E - CTAP Offline Key: G - Wrapping Key: G - DRBG State: G,E
Put - OATH	Add a new OATH entry	return code 0x9000	new OATH Seed key	success/error	KTS-CBC-CMAC ENC DEC MAC	Crypto Officer - OATH Seed Key: W - Secure Channel Session Keys: E
Put Key - SD	Load Authentication Keys	return code 0x9000	Secure Channel Authentication Keys, Public Key	success/error	KTS-CBC-CMAC PKV ENC DEC	Crypto Officer - Secure Channel Authentication Keys: W,Z - Secure

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					MAC RAND	Channel Sensitive Data Key: W,E,Z - KAS Private Keys: W,E,Z - KAS Public Keys: G,E,Z - Asymmetric Public Keys: W,E,Z - Secure Channel Session Keys: E - DRBG State: G,E
Put Keys - YubiHSM Auth	Load keys and associated PIN or generate keys	return code 0x9000	Authentication Key and PIN	success/error	RAND KTS-CBC-CMAC KAS-KG PKV ENC DEC MAC	Crypto Officer - KAS Private Keys: E,G - KAS Public Keys: G,E - PINs: W,E - DRBG State: G,E - Secure Channel Session Keys: E - Secure Channel Authentication Keys: W
Read Data From Protected	Read protected user data	return code 0x9000	Container ID	data	ENC DEC MAC	User - Secure Channel

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Containers - PIV						Session Keys: E
Read Data From Unprotected Containers - PIV	Read user data	return code 0x9000	Container ID	data	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Read Protected Data For Admin - OpenPGP	Read data objects only available to admin	return code 0x9000	Data Object ID	data	ENC DEC MAC	Crypto Officer - Secure Channel Session Keys: E
Read Protected Data For User - OpenPGP	Read data objects only available to user	return code 0x9000	Data Object ID	data	ENC DEC MAC	User - Secure Channel Session Keys: E
Read Public Key - OpenPGP	Read public key	return code 0x9000	Key ID	public key	KTS-CBC-CMAC ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E - Asymmetric Public Keys: R - KAS Public Keys: R
Read Unprotected Data Object - OpenPGP	Read all unprotected data	return code 0x9000	Data Object ID	data, X.509 certificate	ENC DEC MAC	Unauthenticated - Secure Channel

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Keys: E - Asymmetric Public Keys: R - KAS Public Keys: R
Rename - OATH	Update the Name of an OATH credential entry	return code 0x9000	new and old OATH Credential ID	success/error	ENC DEC MAC	Crypto Officer - Secure Channel Session Keys: E
Reset - FIDO	Zeroization	return code 0x9000	none	success/error	ENC DEC MAC	Unauthenticated - Asymmetric Private Keys: Z - Wrapping Key: G,Z - CTAP Offline Key: G,Z - PINs: Z - Secure Channel Session Keys: E
Reset - OATH	Delete all OATH credentials and set the applet to the factory defaults. Zeroization.	return code 0x9000	none	success/error	ENC DEC MAC	Unauthenticated - OATH Seed Key: Z - OATH Management Auth Key: Z - Secure Channel

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Keys: E
Reset - PIV	Reset PIV card state and delete all stored information Zeroization	return code 0x9000	none	success/error	ENC DEC MAC	Unauthenticated - Asymmetric Private Keys: Z - KAS Private Keys: Z - Asymmetric Public Keys: Z - KAS Public Keys: Z - PINs: Z - PIV Management Auth Key: Z - Secure Channel Session Keys: E
Reset - YubiHSM Auth	Zeroization	return code 0x9000	none	success/error	ENC DEC MAC	Unauthenticated - KAS Private Keys: Z - KAS Public Keys: Z - Secure Channel Session Keys: E - Secure Channel Authentication Keys: Z - PINs: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Select - SD	Select SD Application	return code 0x9000	SD AID	SD PIX	None	Unauthenticated
Select Applet - FIDO	Select FIDO applet	return code 0x9000	FIDO AID	version string	RAND KAS-KG PKV	Unauthenticated - DRBG State: G,E - KAS Private Keys: G,E - KAS Public Keys: G,E
Select Applet - OATH	Select OATH Applet	return code 0x9000	OATH AID	version, ID, authentication challenge	RAND	Unauthenticated - DRBG State: G,E
Select Applet - OpenPGP	Select OpenPGP applet	return code 0x9000	OpenPGP AID	OpenPGP PIX	None	Unauthenticated
Select Applet - PIV	Select PIV applet	return code 0x9000	PIV Applet ID (AID)	PIV Proprietary Identifier Extension (PIX)	None	Unauthenticated
Select Applet - YubiHSM Auth	Select YubiHSM Auth Application	return code 0x9000	YubiHSM Auth AID	version	None	Unauthenticated
Set Code - OATH	Set or update a Management Auth Key	return code 0x9000	new OATH Management Auth Key	authentication data for new key	KTS-CBC-CMAC ENC	Crypto Officer - OATH Management Auth Key: W,E - Secure Channel

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					DEC MAC	Session Keys: E
Set Key Attribute - OpenPGP	Specify/Change a key container type (RSA or EC) and length. If a key's type is changed, it will zeroize the existing key.	return code 0x9000	algorithm	success/error	ENC DEC MAC	Crypto Officer - Asymmetric Private Keys: Z - Asymmetric Public Keys: Z - Secure Channel Session Keys: E
Set PIN Retries - OpenPGP	Set retry limit for PW1, PW3 and reset-code	return code 0x9000	new retry limit	success/error	ENC DEC MAC	Crypto Officer - Secure Channel Session Keys: E
Terminate Applet - OpenPGP	Terminate OpenPGP applet and delete all stored data	return code 0x9000	none	success/error	ENC DEC MAC	Unauthenticated - Secure Channel Session Keys: E
Unblock PIN (reset retry counter) - PIV	Reset retry counter and set new user PIN using known unlock code	return code 0x9000	PUK and new PIN	success/error	ENC DEC MAC	Crypto Officer - PINs: W,E - Secure Channel Session Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Unblock PW1 - OpenPGP	Reset user PW1 using reset-code or PW3	return code 0x9000	Reset code and new PW1	success/error	ENC DEC MAC	Crypto Officer - PINs: W,E - Secure Channel Session Keys: E
Update Reset-Code - OpenPGP	Set or update resetting code	return code 0x9000	PW3 and reset code	success/error	ENC DEC MAC	Crypto Officer - PINs: W,E - Secure Channel Session Keys: E
Validate - OATH	Validate Management Auth Key	return code 0x9000	host challenge and response	mutual authentication response	ENC DEC MAC RAND	Unauthenticated - OATH Management Auth Key: E - Secure Channel Session Keys: E - DRBG State: G,E
Verify PIN - PIV	Verify user PIN	return code 0x9000	PIN	success/error	ENC DEC MAC	Unauthenticated - PINs: W,E - Secure Channel Session Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Verify PW1 - OpenPGP	Verify using user PIN	return code 0x9000	PW1	success/error	ENC DEC MAC	Unauthenticated - PINs: W,E - Secure Channel Session Keys: E
Verify PW3 - OpenPGP	Verify using admin PIN	return code 0x9000	PW3	success/error	ENC DEC MAC	Unauthenticated - PINs: W,E - Secure Channel Session Keys: E
Write Data - OpenPGP	Write data objects except user writable data objects	return code 0x9000	Data Object ID, data	success/error	ENC DEC MAC	Crypto Officer - Secure Channel Session Keys: E
Write Data To Containers - PIV	Write any container	return code 0x9000	Container ID, data	Success/error	ENC DEC MAC	Crypto Officer - Secure Channel Session Keys: E
Write User Protected Data - OpenPGP	Write user writable data objects	return code 0x9000	Data Object ID, data	success/error	ENC DEC MAC	User - Secure Channel Session Keys: E

Table 15: Approved Services

4.4 NON-APPROVED SERVICES

The module only supports non-Approved services within the OTP functional unit, which must be explicitly selected.

Name	Description	Algorithms	Role
Write Config to Slot	Write configuration and CSP in slot. Zeroization.	None	CO
Update Slot Configuration	Update configuration (excluding key material CSP) in slot	None	CO
Emit Yubi-OTP from Slot	Emit YubiOTP from slot	AES (non-compliant)	Unauthenticated
Emit HOTP from Slot	Emit HOTP from slot	HMAC (non-compliant)	Unauthenticated
Emit Hash-OTP from Slot	Emit HASH-OTP from slot	HMAC (non-compliant)	Unauthenticated
Perform Yubi-OTP Challenge Response from Slot	Perform YubiOTP challenge response with AES 128 bit key stored in slot using user supplied challenge	AES (non-compliant)	Unauthenticated
Perform HMAC-SHA1 Challenge Response from Slot	Compute SHA1 HMAC using 160 bits key stored in slot using user supplied challenge	HMAC (non-compliant)	Unauthenticated
Slot Device Serial	Read serial from device	None	Unauthenticated
Slot YK Get Device Info	Read device capabilities.	None	Unauthenticated
Slot YK Set Device Info	Set device capabilities.	None	Unauthenticated
Write NDEF to Slot	Write the NDEF URL and choose slot	None	CO

Table 16: Non-Approved Services

4.5 EXTERNAL SOFTWARE/FIRMWARE LOADED

The module does not support external firmware loads.

5 SOFTWARE/FIRMWARE SECURITY

The hardware module contains executable firmware components and incorporates the following self-testing.

5.1 INTEGRITY TECHNIQUES

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

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 18).

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

7.3 HARDNESS TESTING TEMPERATURE RANGES

The module has been tested at the operational, storage and distribution temperatures listed in Table 19. 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 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 including plaintext (direct entry), a secure channel, and an Approved KTS.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
EE	USB Host	NVM	Plaintext	Manual	Electronic	
EO	NVM or RAM	USB Host	Plaintext	Manual	Electronic	
SCE	USB or NFC Host	NVM	Encrypted	Automated	Electronic	KTS-CBC-CMAC
SCO	RAM	USB or NFC Host	Encrypted	Automated	Electronic	KTS-CBC-CMAC
KTSE	USB or NFC Host	NVM or RAM	Encrypted	Automated	Electronic	AES-CCM (A5891)
KTSO	NVM or RAM	USB or NFC Host	Encrypted	Automated	Electronic	AES-CCM (A5891)
PP2E	USB or NFC Host	NVM	Encrypted	Automated	Electronic	KTS-CBC-HMAC
PP2O	NVM or RAM	USB or NFC Host	Encrypted	Automated	Electronic	KTS-CBC-HMAC

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.

Zeroization Method	Description	Rationale	Operator Initiation
FIDO-Reset	All CSPs zeroized with the CTAP Offline Key and Wrapping Key being re-generated.	SSPs are immediately overwritten with 0s and the CTAP Offline Key and Wrapping Key are re-generated.	Reset - FIDO service
OATH-Reset	All CSPs zeroized	SSPs are immediately overwritten with 0s.	Reset - OATH service
OpenPGP-Terminate	"TERMINATE APPLET" followed by "ACTIVATE APPLET" services. All CSPs zeroized with the PINs being set to their default value.	CSPs are immediately overwritten with 0s and then reset to default values, as applicable	Terminate Applet - OpenPGP and Activate Applet - OpenPGP services.
PIV-Reset	All CSPs zeroized with the PIV Management Auth Key and PIN being set to their default values.	SSPs are immediately overwritten with 0s and then reset to default values, as applicable.	Reset - PIV service
SecureChannel-Delete	CSPs zeroized.	SSPs are immediately overwritten with 0s.	Delete Key - SD service
YubiHSM Auth-Reset	All CSPs zeroized with PINs being set to their default values.	SSPs are immediately overwritten with 0s and PINs being set to their default values.	Reset - YubiHSM Auth service
ZAU	Ephemeral CSPs zeroised after use.	SSPs are immediately overwritten with 0s after use.	Automatic
ZPC	Ephemeral CSPs zeroised upon power cycle.	Ephemeral SSPs are overwritten with 0s.	Power On service

Table 22: SSP Zeroization Methods

9.4 SSPS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Asymmetric Private Keys	Signature generation and RSA unencapsulate for PIV and OpenPGP	RSA 2048 - 4096; ed255199; EC P-256, P-384, P-521, or Non-NIST Curve - 112 - 256	Private - CSP	AKG		SigGen RSADP RSASP ECSP
Asymmetric Public Keys	Used to verify digital signatures (external entities) or perform RSA Key Wrap	2048 - 4096; 256 - 521 (EC); 256 (EdDSA) - 112-256	Public - PSP	AKG		SigVer
Attestation Key	Attest internally generated asymmetric keys	112-256 - 112-256	Private - Neither	Pre-loaded		SigGen
CTAP Offline Key	To support the HMAC-Secret FIDO extension	112 - 112	MAC - CSP	SymKG		MAC
CTAP PIN token	Used as part of FIDO2 authentication	112 - 112	MAC - CSP	RAND		MAC
CTAP Session Keys	Secure Session	256, 112 - 256, 112	Symmetric, MAC - CSP		KAS-PP2	ENC DEC MAC KTS-CBC-HMAC

This document may be freely reproduced and distributed, but only in its entirety and without modification

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
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	ENT - CSP	Counter DRBG (A5891)		RAND SymKG AKG
Entropy Input	Entropy for the DRBG	1216 bits - 384 (3/2 security strength)	ENT - CSP	ESV		Counter DRBG (A5891)
KAS Private Keys	Key establishment	EC P-256, P-384, P-521, or Non-NIST Curve - 128 - 256	Private - CSP	KAS-KG		KAS-PP2 KAS-SCP11 SSC
KAS Public Keys	Key establishment public keys.	128-bit minimum - 128-bit minimum	Public - PSP	KAS-KG		KAS-PP2 KAS-SCP11 SSC
OATH Management Auth Key	OATH authentication secret	112 - 112	MAC - CSP	Configured by operator		MAC
OATH Seed Key	Used to generate HOTPs or TOTPs	112 - 112	MAC - CSP			MAC
PINs	Authenticate operators	Minimum 48-bits - NA	Authentication - CSP	Pre-loaded or configured by operator		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PIV Management Auth Key	PIV authentication secret	128 - 256 - 128	Symmetric - CSP	Pre-loaded		ENC DEC
Secure Channel Authentication Keys	Used to derive session keys for Secure Channel (SCP03 or YubiHSM Auth)	128 - 128	Symmetric - CSP	Default set is pre-loaded		KBKDF
Secure Channel Sensitive Data Key	Used for Sensitive Data Decryption	128 - 128	Symmetric - CSP	Default set is pre-loaded		ENC DEC
Secure Channel Session Keys	Secure sessions (SCP03, SCP11, YubiHSM Auth)	128 - 128	Symmetric - CSP		KBKDF KAS-SCP11	ENC DEC MAC KTS-CBC-CMAC
Shared Secret	Output from ECC CDH	256-521 - 128-256	Shared Secret - CSP		SSC	SSC
Wrapping Key	Used to wrap FIDO keys	256 - 256	Symmetric - CSP	SymKG		KTS-CCM

Table 23: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Asymmetric Private Keys	EE SCE SCO	RAM:Plaintext NVM:Plaintext	Until Use	PIV-Reset OpenPGP-Terminate FIDO-Reset	DRBG State:Derived From Asymmetric Public Keys:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	KTSE KTSO			SecureChannel-Delete	
Asymmetric Public Keys	EE SCE KTSE EO SCO KTSO	NVM:Plaintext	Until Use	PIV-Reset OpenPGP-Terminate FIDO-Reset SecureChannel-Delete	DRBG State:Derived From
Attestation Key	EE SCE	NVM:Plaintext	Until Use	N/A	Secure Channel Session Keys:Used With
CTAP Offline Key		NVM:Plaintext	Until Use	FIDO-Reset	DRBG State:Derived From
CTAP PIN token	EO SCO PP2O	RAM:Plaintext	Until Use	ZPC	DRBG State:Used With CTAP Session Keys:Used With
CTAP Session Keys		RAM:Plaintext	Until Use	ZAU	PINs:Used With CTAP PIN token:Used With
DRBG Seed		RAM:Plaintext	Until use	ZAU	DRBG State:Used With Entropy Input:Used With
DRBG State		RAM:Plaintext	Until reboot	ZPC	DRBG Seed :Used With
Entropy Input		RAM:Plaintext	Until use	ZAU	DRBG Seed:Used With
KAS Private Keys	EE SCE	NVM:Plaintext RAM:Plaintext	Until Use	PIV-Reset OpenPGP-Terminate FIDO-Reset YubiHSM Auth-Reset	DRBG State:Derived From KAS Public Keys:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				SecureChannel-Delete	
KAS Public Keys	EE SCE EO SCO	RAM:Plaintext NVM:Plaintext	Until Use	PIV-Reset OpenPGP-Terminate FIDO-Reset YubiHSM Auth-Reset SecureChannel-Delete	DRBG State:Derived From Secure Channel Session Keys:Used With KAS Public Keys:Paired With
OATH Management Auth Key	EE SCE	NVM:Plaintext	Until Use	OATH-Reset	Secure Channel Session Keys:Used With
OATH Seed Key	EE SCE	NVM:Plaintext	Until Use	OATH-Reset	Secure Channel Session Keys:Used With
PINs	EE SCE PP2E	NVM:Plaintext	Until Use	PIV-Reset OpenPGP-Terminate FIDO-Reset YubiHSM Auth-Reset	Secure Channel Session Keys:Used With CTAP Session Keys:Used With
PIV Management Auth Key	EE SCE	NVM:Plaintext	Until Use	PIV-Reset	Secure Channel Session Keys:Used With
Secure Channel Authentication Keys	EE SCE	NVM:Plaintext	Until use	YubiHSM Auth-Reset SecureChannel-Delete	Secure Channel Session Keys:Used With
Secure Channel Sensitive Data Key	EE SCE	NVM:Plaintext RAM:Plaintext	Until use	SecureChannel-Delete	Secure Channel Authentication Keys:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					KAS Private Keys:Used With
Secure Channel Session Keys	EO SCO	RAM:Plaintext	Until Use	ZAU	Secure Channel Authentication Keys:Derived From Secure Channel Sensitive Data Key:Used With PINs:Used With PIV Management Auth Key:Used With OATH Management Auth Key:Used With OATH Seed Key:Used With Asymmetric Private Keys:Used With KAS Private Keys:Used With KAS Public Keys:Used With
Shared Secret	EO SCO	RAM:Plaintext	Until Use	PIV-Reset OATH-Reset OpenPGP-Terminate FIDO-Reset YubiHSM Auth-Reset SecureChannel-Delete	KAS Private Keys:Used With KAS Public Keys:Used With
Wrapping Key		NVM:Plaintext	Until Use	FIDO-Reset	DRBG State:Derived From Asymmetric Private Keys:Used With

Table 24: SSP Table 2

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 currently offers non-approved services, that is, whether OTP is selected (NFC) or the designated OTP endpoints are used. 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.

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	Power-On
AES-ECB (A5891)	128-bit	KAT	CAST	Implicit	Decrypt	Power-On
Counter DRBG (A5891)	CTR_DRBG	KAT	CAST	Implicit	SP800-90A Health Tests for Instantiate, Reseed, and Generate	Power-On
ECDSA SigGen (FIPS186-5) (A5891)	P-256, SHA2-256	KAT	CAST	Implicit	Sign	Before first use

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-5) (A5891)	P-256, SHA2-256	KAT	CAST	Implicit	Verify	Before first use
EDDSA SigGen (A5891)	Ed25519, SHA2-512	KAT	CAST	Implicit	Sign	Before first use
EDDSA SigVer (A5891)	Ed25519, SHA2-512	KAT	CAST	Implicit	Verify	Before first use
KAS-ECC-SSC Sp800-56Ar3 (A5891)	P-256	KAT	CAST	Implicit	SSC	Before first use
KDA HKDF SP800-56Cr2 (A5891)	HMAC-SHA2-256	KAT	CAST	Implicit	Key Derivation	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
PWCT	Sign/Verify	Sign/Verify	PCT	Implicit	EC, ED, RSA	Upon Key Generation
RSA SigGen (FIPS186-5) (A5891)	2048-bit PKCS#1 with SHA2-256	KAT	CAST	Implicit	Sign	Before first use
RSA SigVer (FIPS186-5) (A5891)	2048-bit PKCS#1 with SHA2-256	KAT	CAST	Implicit	Verify	Before first use
SHS (A5891)	SHA-1, SHA2-512	KAT	CAST	Implicit	Hash	Power-On

This document may be freely reproduced and distributed, but only in its entirety and without modification

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SP800-90B	APT, RCT	SP800-90B Health Tests	CAST	Implicit	APT, RCT	Upon use

Table 26: Conditional Self-Tests

10.3 PERIODIC SELF-TEST INFORMATION

The module will perform periodic self-tests every 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
EDDSA SigVer (A5891)	KAT	CAST	Power-On	Manual

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC Sp800-56Ar3 (A5891)	KAT	CAST	Power-On	Manual
KDA HKDF SP800-56Cr2 (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
PWCT	Sign/Verify	PCT	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
SP800-90B	SP800-90B Health Tests	CAST	29 hours	Automatic

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 29).

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 or invoking a soft reset through the services.

11 LIFE-CYCLE ASSURANCE

There are no specific maintenance requirements.

11.1 INSTALLATION, INITIALIZATION, AND STARTUP PROCEDURES

The module powers up in an uninitialized state. The following initialization procedures for each functional unit must be adhered to prior to first use. Only when this procedure is completed will the module operate in the Approved mode. The only non-Approved services are contained by the OTP functional unit. In order to access the OTP functional unit, OTP must be selected (NFC) or the designated OTP endpoints must be used (USB). (See Section 2.4). While OTP is selected, no other services beyond OTP services, namely those listed in Section 4.4, are available. The module enters the non-Approved mode whenever a non-Approved service is invoked and exits when the said service completes.

PIV, OpenPGP, OATH, FIDO, Security Domain (SD) and HSMAuth functional units must be initialized to be utilized in the Approved mode. The following describes the details in this regard for the individual functional units. Command-line and GUI-based instructions to be performed by the Crypto Officer or the User of the module can be found in the FIPS 140-3 Configuration section of the YubiKey Technical Manual.

- PIV:
  - Update the values for the PIV Management Auth Key, PIN and PUK the default values of which are 010203040506070801020304050607080102030405060708, 123456, and 12345678, respectively.
  - The values of the PIV Management Auth Key and the PUK are to be updated by the Crypto Officer. The value of the PIN is to be updated by the User.
- OpenPGP:
  - Update the default User PIN (PW1) and Admin PIN (PW3) the default values of which are 123456 and 12345678, respectively.
  - The value of the Admin PIN is to be updated by the Crypto Officer while the value of the User PIN is to be updated by the User.
- OATH:
  - Set an OATH Management Auth Key, which has no default value.
  - The value of the OATH Management Auth Key is to be set by the Crypto Officer.
- FIDO:
  - Set a PIN which has no default value.
  - The value of the PIN is to be set by the User.
- YubiHSM Auth:
  - Set the Admin PIN, which has no default value.
  - The value of the Admin PIN is to be set by the Crypto Officer.

- Security Domain:
    - Update the default key set the default values of which are 404142434445464748494a4b4c4d4e4f for all three keys.
    - The values of the keys in the key set are to be updated by the Crypto Officer.

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. The module inhibits data output during self-tests, firmware load, zeroization and error states.
4. The module logically separates data output from the processes performing zeroization and key generation.
5. The module enforces role-based authentication.
6. The module does not retain the authentication of an operator following power-off or reboot.
7. The module supports the following roles: Cryptographic Officer and User.
8. The module does not support a bypass mode or maintenance mode.
9. The module supports the following logically distinct interfaces:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface
10. The module protects critical security parameters from unauthorized disclosure, modification and substitution.
11. The module performs power-on, on-demand and periodic self-testing.
12. The module logs errors whenever an error state is entered.
13. The module does not perform any cryptographic functions while in an error state.
14. The module does not support multiple concurrent operators.

This document may be freely reproduced and distributed, but only in its entirety and without modification

11.5 END OF LIFE

Zeroize the module and dispose of it at a proper e-waste facility.

12 MITIGATION OF OTHER ATTACKS

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

13 REFERENCES

YubiKey Technical Manual, March 2026, https://docs.yubico.com/hardware/yubikey/yk-tech-manual/fips-140-3-nist-requirement.html