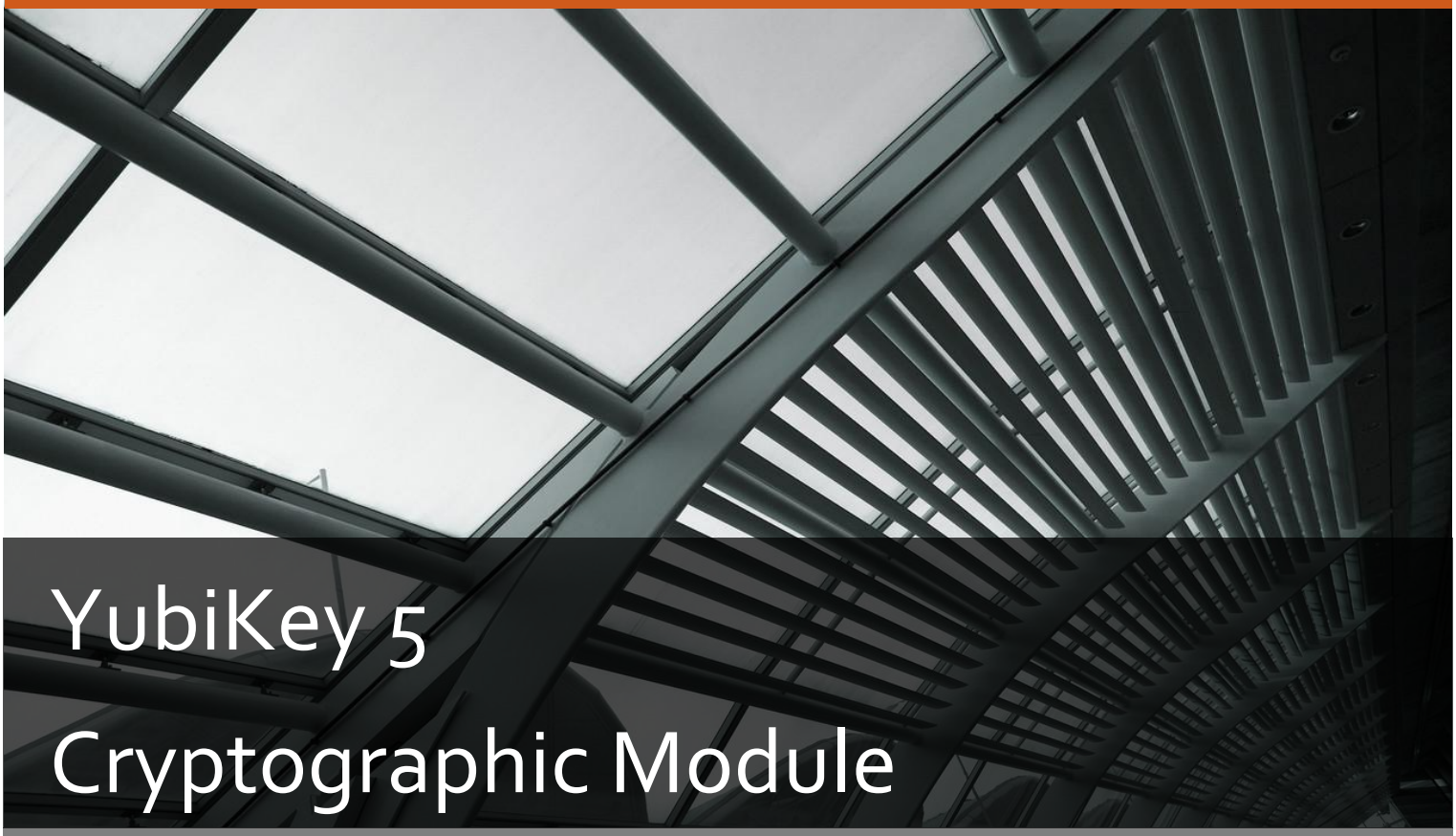

YubiKey 5 Cryptographic Module

Yubico, Inc.

FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.4

Table Of Contents

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for the Yubico, Inc. YubiKey 5 Cryptographic Module. Below are the details of the product certified:

Hardware Version #: SLE78CLUFX3000PH, SLE78CLUFX5000PH

Firmware Version #: 5.4.2 and 5.4.3

FIPS 140-2 Security Level: 2

1.1 Purpose

This document was prepared as Federal Information Processing Standard (FIPS) 140-2 validation process. The document describes how the YubiKey 5 Cryptographic Module meets the security requirements of FIPS 140-2. It also provides instructions to individuals and organizations on how to deploy the product in a secure FIPS-approved mode of operation. Target audience of this document is anyone who wishes to use or integrate this product into a solution that is meant to comply with FIPS 140-2 requirements.

1.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Yubico, Inc. and is releasable only under appropriate non-disclosure agreements.

1.3 Notices

2. YubiKey 5 Cryptographic Module

The YubiKey 5 Cryptographic Module (the module) is a single-chip module validated at FIPS 140-2 Security Level 2. Specifically, the module meets the following security levels for individual sections in FIPS 140-2 standard:

Table 1 - Security Level For Each FIPS 140-2 Section

#	Section Title	Security Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	3
9	Self-Tests	2
10	Design Assurances	3
11	Mitigation Of Other Attacks	N/A

2.1 Cryptographic Module Specification

The module is the core component for authenticators in the YubiKey 5 product family and supports several functional units: FIDO2, PIV, OTP, OpenPGP, OATH, and YubiCrypt.

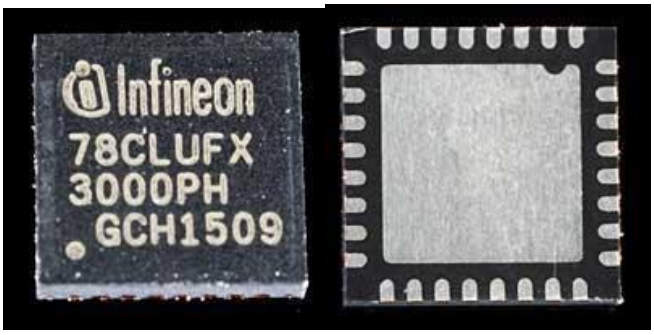

Figure 1 – YubiKey 5 Cryptographic Module (SLE78CLUFX3000PH – Front and Back)

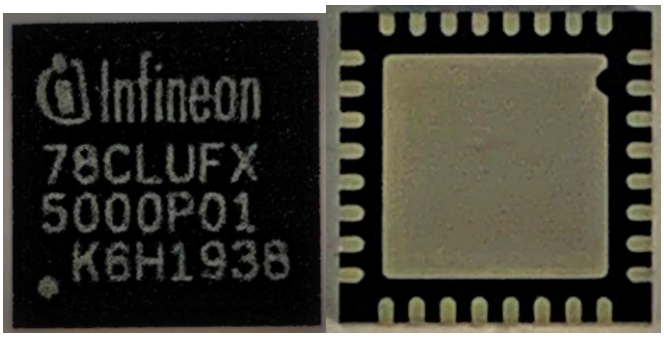

Figure 2 – YubiKey 5 Cryptographic Module (SLE78CLUFX5000PH – Front and Back)

2.1.1 Cryptographic Boundary

The cryptographic boundary is defined as the entire single-chip device itself. Please see Figures 1 and 2 above for a depiction of the module.

2.1.2 Modes Of Operation

The module supports an Approved mode of operation and a non-Approved mode of operation. The modes of operation are described below:

- Approved: Only Approved algorithms may be employed per the procedural controls set forth by this Security Policy.
- Non-Approved: Additional support for non-Approved algorithms and services, such as EdDSA, x25519, and non-Approved key sizes.

Please see Section 3 of this Security Policy for instructions on how to configure the various modes of operation.

There are algorithms, modes, and keys that have been CAVs tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

Table 2 - Supported Approved Algorithms

Cryptographic Algorithm	CAVP Cert. #	Usage
AES **Modes: CBC, CCM, CMAC, ECB** **Key Sizes: 128, 192, 256** **(CCM with 128 and 192-bit keys tested, but not used)**	C1680	Encryption, Decryption, CTR_DRBG, Key Wrap
CKG (Vendor affirmed per SP800-133 and IG D.12)		Key Generation
CVL – ECC CDH (Tested, but not used) **Curves: P-224, P-256, P-384, P-521**	C1680	Modular exponentiation
CVL - ECDSA Signature Generation Primitive **Curves: P-256, P-384, P-521 (P-224 tested, but not used)**	C1680	Signature Primitive
CVL – RSADP **Key sizes: 2048**	C1680	RSA PKCS#1 v2.1 Decryption Primitive
CVL – RSASP	C1680	Signature Primitive
DRBG: AES-256 CTR, No DF	C1680	Key Generation
ECDSA **Curves: P-256, P-384, P-521 (P-224 tested, but not used)** **Operations: Key Gen**	C1680	Key Generation
HMAC SHA-1, SHA2-256, SHA2-384, SHA2-512	C1680	Data Integrity
KAS-SSC	Vendor Affirmed	SP800-56a-rev3 Shared Secret Calculation. Provides between

Cryptographic Algorithm	CAVP Cert. #	Usage
Co-Factor One-Pass DH, C(1e, 1s, ECC CDH) Scheme **Curves: P-256, P-384, P-521, secp256k1, brainpool256r1, brainpool384r1, brainpool512r1**		128 and 256 bits of security strength) Non-NIST curves allowed by IG D.8, Scenario X.2
KBKDF: SP800-108 CMAC **MAC Mode: CMAC-AES128** **Supported Lengths: 64, 128**	C1680	Secure Channel key derivation.
KDA **Two-Step Key Derivation: HKDF**	Vendor Affirmed	SP800-56C-rev2 Key Derivation Algorithm.
KTS: AES and CMAC	C1680	SP800-38F compliant key wrap using AES-128 CBC and CMAC. Provides 128-bits of security strength.
KTS: AES CCM	C1680	SP800-38F compliant key wrap using AES-256 CCM. Provides 256-bits of security strength.
KTS: AES and HMAC	C1680	SP800-38F compliant key wrap using AES-256 CBC and HMAC SHA-256. Provides 256-bits of security strength.
RSA **Key Sizes: 2048, 3072, 4096** **Operations: Key Gen**	A985	Key Generation
SHA-1, SHA2-256, SHA2-384, SHA2-512	C1680	Hash
Triple-DES	C1680	Encryption.

Cryptographic Algorithm	CAVP Cert. #	Usage
Mode: ECB, Keying Option 1		Must not encrypt with the same 3-key Triple DES mutual challenge response key more than 2^16 times (refer to IG A.13).

Table 3 - Supported Allowed

Cryptographic Algorithm	CAVP Cert. #	Usage
DES	N/A	No security claim per IG 1.23. Used internal to the module for integrity checks (CRCs).
EC Diffie-Hellman **Curves: P256**	N/A	No security claim per IG 1.23. The module does not rely on this usage of ECDH to satisfy any FIPS 140-2 requirements; this usage of ECDH provides interoperability only.
EC Diffie-Hellman **secp256k1, brainpool256r1, brainpool384r1, brainpool512r1**	N/A.	IG A.2, D.8 Scenario X.2 secp256k1 and brainpool256r1 provide 128 bits of security strength brainpool384r1 provides 192 bits of security strength brainpool512r1 provides 256 bits of security strength
ECDSA **Curves: secp256k1, brainpool256r1,**	N/A	IG A.2. Key Generation, Signature Generation Primitive

Cryptographic Algorithm	CAVP Cert. #	Usage
brainpool384r1, brainpool512r1		secp256k1 and brainpool256r1 provide 128 bits of security strength brainpool384r1 provides 192 bits of security strength brainpool512r1 provides 256 bits of security strength
NDRNG	N/A	Hardware Non-Deterministic RNG; minimum of 16 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG. The DRBG is initialized with a 384-bit entropy input string, which contains at least 301.8 bits of entropy. The module generates cryptographic keys whose strengths are modified by available entropy
RSA (Key Unwrapping)	N/A	Non-SP800-56b RSA decryption primitive. RSA (CVL Cert. #C1680, key unwrapping; key establishment methodology provides between 112 bits and 150 bits of encryption strength)
RSA (Key Unwrapping)	N/A	Non-SP800-56b RSA decryption primitive. RSA (key unwrapping; key establishment methodology provides between 112 bits and 150 bits of encryption strength)

Table 4 – Non-Approved algorithms used in non-Approved mode only

Cryptographic Algorithm	Usage
RSA Signature Generation with 1024-bit keys	Signature Generation Component
EdDSA	Key Generation, Signature Generation Primitive
X25519	Key Generation, Key Agreement

2.2 Cryptographic Module Ports and Interfaces

The physical ports of the module are the available pins of the single-chip device. The pins are utilized as follows:

Table 5 - Module Interface Mapping

Port/Pin	Description	Logical Interface
USB pins (D+ / D-) **(Qty. 2)**	Primary physical interface (USB)	• Control in • Data in • Data out • Status out
Touch Button interface (Qty. 2)	Factory reset	• Control in
LED interface **(Qty. 1)**	Status LED	• Status Out
Power interface (Qty. 3)	Power supply (+5V, GND and supply voltage decoupling)	• Power In

Port/Pin	Description	Logical Interface
NFC Interface (Qty. 2)	Contactless interface	• Control in • Data in • Data out • Status out
I2C I/O pins (SDA / SCL) **(Qty. 2)**	(Only available on the SLE78CLUFX5000PH) Secondary physical interface (I2C)	• Control in • Status out
Interface Select Pin (Qty. 1)	(Only available on the SLE78CLUFX5000PH) Select USB or I2C (Power-up only)	• Control in

2.3 Roles, Services, and Authentication

The following sections provide details about roles supported by the module, how these roles are authenticated and the services the roles are authorized to access.

2.3.1 Authorized Roles

The module supports a Cryptographic Officer (CO), a User, and an unauthenticated role.

The CO is responsible for configuring CSPs and resetting user PINs.

The User performs cryptographic operations and utilizes the module as an authenticator.

The unauthenticated role has access to OTP output, responding to a challenge, read non-security-relevant information, self-tests, and reset services only.

2.3.2 Authentication Mechanisms

The module supports role-based authentication mechanisms for the Cryptographic Officer and User.

Table 6 - Authentication Mechanism Details

Role	Type Of Authentication	Authentication Strength
CO or User	Minimum length 4-byte PIN	A minimum 4 byte (32 bit) binary string has a probability that a random attempt will succeed or a false acceptance will occur of 1/2^32 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 1000/2^32, which is less than 1/100,000.
CO	Knowledge of a shared secret (minimum length 112 bits)	The shared secret is either a 3-key Triple DES Key, minimum 128-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 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.

2.3.3 Services

The module supports six functional units: OTP, PIV, OATH, OpenPGP, FIDO2, and YubiCrypt. The following table describes all services available:

Table 7 - Services

Service	Description	Role			CSP Access
		CO	User	Unauth	
General Services					
DEVICE CONFIGURATION	Select a functional unit and retrieve non-security relevant device information			X	N/A
SELF-TESTS	Perform all Power-On Self-Tests on demand			X	N/A
OTP Services					
WRITE CONFIG TO SLOT	Write configuration and CSP in slot Zeroization	X			WXZ – PIN WZ – OTP Key
UPDATE SLOT CONFIGURATION	Update configuration (excluding key material CSP) in slot	X			WXZ – PIN
EMIT YUBI-OTP FROM SLOT	Emit YubiOTP from slot			X	WX – DRBG State X – OTP Key
EMIT OATH-HOTP FROM SLOT	Emit OATH-HOTP from slot			X	X – OTP Key
EMIT HASH-OTP FROM SLOT	Emit HASH-OTP from slot			X	X – OTP Key
PERFORM YUBI-OTP CHALLENGE RESPONSE FROM SLOT	Perform YubiOTP challenge response with AES 128 bit key stored in slot using user supplied challenge			X	WX – DRBG State X – OTP Key

Service	Description	Role			CSP Access
		CO	User	Unauth	
PERFORM HMAC-SHA1 CHALLENGE RESPONSE FROM SLOT	Compute SHA1 HMAC using 160 bits key stored in slot using user supplied challenge			X	X – OTP Key
SLOT DEVICE SERIAL	Read serial from device			X	N/A
SLOT YK GET DEVICE INFO	Read device capabilities.			X	N/A
SLOT YK SET DEVICE INFO	Set device capabilities.			X	N/A
WRITE NDEF TO SLOT	Write the NDEF URL and choose slot	X			X – PIN
PIV Services					
SELECT APPLET	Select PIV applet			X	N/A
GET SERIAL	Get serial number			X	N/A
GET METADATA	Get metadata			X	N/A
GET VERSION	Get firmware version			X	N/A
VERIFY PIN	Verify user PIN			X	R – PIN
CHANGE MANAGEMENT KEY	Change management key	X			WX – Management Auth Key
CHANGE PUK	Change PIN unlock code	X			RW – PIN
CHANGE PIN	Change user PIN with known PIN		X		RW – PIN
UNBLOCK PIN (RESET RETRY COUNTER)	Reset retry counter and set new user PIN using known unlock code	X			RW – PIN
GENERAL AUTH	Authenticate to the applet using the Management Auth Key.			X	WX – DRBG State

Service	Description	Role			CSP Access
		CO	User	Unauth	
	This service can also perform a requested cryptographic operation with an Asymmetric Key				X – Management Auth Key X – Asymmetric Key
GENERATE KEY	Generate asymmetric key pair	X			WX – DRBG State W – Asymmetric Key
READ DATA FROM UNPROTECTED CONTAINERS	Read user data			X	N/A
READ DATA FROM PROTECTED CONTAINERS	Read protected user data		X		N/A
WRITE DATA TO CONTAINERS	Write any container	X			N/A
CHANGE RETRY COUNTERS	Set retry counter for PINs	X			W – PIN
IMPORT KEY	Import asymmetric key	X			W – Asymmetric Key W – Attestation Key
RESET	Reset PIV card state and delete all stored information Zeroization			X	Z – All, but Attestation Key
ATTEST	Generate an attestation for an internally generated key			X	X – Attestation Key
OpenPGP Services					

Service	Description	Role			CSP Access
		CO	User	Unauth	
SELECT APPLET	Select applet			X	N/A
VERIFY PW1	Verify using user PIN			X	R – PIN
VERIFY PW3	Verify using admin PIN			X	R – PIN
CHANGE PW1	Update user PIN		X		RW – PIN
CHANGE PW3	Update admin PIN	X			RW – PIN
UPDATE RESET-CODE	Set or update resetting code	X			W – PIN
UNBLOCK PW1	Reset user PW1 using resetting code or PW3	X			RW – PIN
SET PIN RETRIES	Set retry limit for PW1, PW3 and reset-code	X			N/A
GENERATE ASYMMETRIC KEY PAIR	Generate asymmetric key pair	X			WX – DRBG State W – Asymmetric Key
IMPORT ASYMMETRIC KEY	Import asymmetric key	X			W – Asymmetric Key
SET KEY ATTRIBUTE	Specify/Change a key type (RSA or EC) and length. If a key's type is changed, it will zeroize the existing key	X			Z – Asymmetric Key
READ PUBLIC KEY	Read public key			X	N/A
COMPUTE DIGITAL SIGNATURE PRIMITIVE	Perform signature primitive		X		WX – DRBG State X – Asymmetric Key
DECIPHER	RSA Unwrap operation or EC-DH shared secret calculation		X		X – Asymmetric Key

Service	Description	Role			CSP Access
		CO	User	Unauth	
INTERNAL AUTHENTICATE	Perform internal authentication (signature primitive)		X		WX – DRBG State X – Asymmetric Key
TERMINATE APPLET	Terminate OpenPGP applet and delete all stored data	X		X	N/A
ACTIVATE APPLET	Activate OpenPGP applet with factory defaults Zeroization			X	Z – All, but Attestation Key
ATTEST	Generate attestation for an internally generated key		X		X – Attestation Key
READ UNPROTECTED DATA OBJECT	Read all unprotected data			X	N/A
READ PROTECTED DATA FOR USER	Read data objects only available to user		X		N/A
READ PROTECTED DATA FOR ADMIN	Read data objects only available to admin	X			N/A
WRITE DATA	Write data objects except user writable data objects	X			N/A
WRITE USER PROTECTED DATA	Write user writable data objects		X		N/A
GET VERSION	Get firmware version			X	N/A
OATH Services					
SELECT APPLET	Select Applet			X	WX – DRBG State
RENAME	Update the Name of an OATH credential entry	X			N/A

Service	Description	Role			CSP Access
		CO	User	Unauth	
SET CODE	Set or update a Management Auth Key	X			WX – Management Auth Key
VALIDATE	Validate Management Auth Key			X	X – Management Auth Key
PUT	Add a new OATH entry	X			W – OATH Seed Key
DELETE	Remove an OATH entry	X			Z – OATH Seed Key
RESET	Delete all OATH credentials and set the applet to the factory defaults Zeroization			X	Z – All
LIST	List all the names of the OATH entries	X			N/A
CALCULATE	Calculate the code for an OATH entry	X			X – OATH Seed Key
CALCULATE ALL	Calculate code for all entries	X			X – OATH Seed Key
FIDO/FIDO2 Services					
Make Credential	Create a new FIDO credential (resident or transient)		X		WX – DRBG State X – Wrapping Key W – Asymmetric Key X – Attestation Key X – PIN token

Service	Description	Role			CSP Access
		CO	User	Unauth	
Get Assertion	Use credential		X		WX – DRBG State X – Wrapping Key X – Asymmetric Key X – Offline Key X – PIN token RWX – Asymmetric Key RWX – CTAP Session Keys
Get Information	Device information			X	N/A
PIN Service	Creating, updating, and validating PIN		X		RW – PIN RWX – PIN token RWX – Asymmetric Key RWX – CTAP Session Keys
Reset	Zeroization			X	Z – All, but Attestation Key
Credential Management	Listing credentials and deleting credentials		X		X – PIN token Z – Asymmetric Key
YubiCrypt Services					
SELECT	Select Application			X	N/A

Service	Description	Role			CSP Access
		CO	User	Unauth	
Put Keys	Load keys and associated PIN	X			W – Authentication Keys RW – PIN
Delete Keys	Delete keys	X			Z – Authentication Keys R – PIN
Reset	Zeroization			X	Z - All
List	Lists the credential names			X	N/A
Calculate	User Authenticate		X		X – Authentication Keys W – Session Keys R – PIN
Get Retry Count	Specifies the number of Login attempts remaining			X	N/A
Get Version	Get FW version			X	N/A
Change PIN	Update PIN	X			RW - PIN
Secure Channel Services					
SELECT	Select Application	X			N/A
Put Key	Load Authentication Keys	X			W - Authentication Keys WX – Sensitive Data Key X – Session Keys

Service	Description	Role			CSP Access
		CO	User	Unauth	
Delete Key	Delete key set	X			Z - Authentication Keys Z- Sensitive Data Key Z - Session Keys X – Session Keys
Get Data	Get metadata			X	N/A
Initialize Update	Create Secure Channel Session	X			X - Authentication Keys W - Session Keys
External Authenticate	Complete Session Establishment	X			X - Session Keys

2.4 Physical Security

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

2.5 Operational Environment

The module supports a non-modifiable operational environment and does not allow for the loading of firmware updates.

2.6 Cryptographic Key Management

The module supports the following Critical Security Parameters:

Table 8 - Details of Cryptographic Keys and CSPs

Key/CSP	Type	Generation	Entry	Output	Storage	Zeroization	Usage
Entropy Input	384-bits	Internally by NDRNG	N/A	N/A	Plaintext in RAM	Zeroization	Seed the DRBG
DRBG Internal State	V and Key	Internally by DRBG	N/A	N/A	Plaintext in RAM	Zeroization	Random number generation
Authentication Keys	AES-128 bit keys (KENC, KMAC)	N/A. For Secure Channel, a default set is pre-loaded.	Plaintext (direct entry - Yubicrypt only) or Encrypted by Secure Channel	N/A	Plaintext in Flash	Zeroization	Used to derive session keys for Secure Channel and YubiCrypt
Sensitive Data Key	AES-128 CBC (KDEK)	N/A, a default is pre-loaded.	Plaintext (direct entry) or Encrypted by Secure Channel	N/A	Plaintext in Flash	Zeroization	Used for Sensitive Data Decryption
Session Keys	AES-128 CBC (SENC),	N/A. Derived from	N/A	Plaintext (YubiCrypt	Plaintext in RAM	Zeroization	Secures sessions

	AES-128 CMAC (RMAC/SMAC)	Authentication Keys via SP800-108 CMAC KDF		only) or Encrypted by Secure Channel			
PINs	Minimum 4 byte values	N/A. Pre-loaded values or configured by operator.	Plaintext (direct entry) or Encrypted by Secure Channel or CTAP Session Keys	N/A	Plaintext in Flash (SHA-256 hash for FIDO2)	Zeroization	Authenticate operators
PIN token	HMAC SHA-256	Internally by DRBG	N/A	Plaintext or Encrypted by CTAP Session Keys	Plaintext in RAM	Zeroization	Used as part of FIDO2 authentication
CTAP Session Keys	AES-256 CBC and HMAC-SHA-256	N/A. Established via KAS-SSC and KDA	N/A	N/A	Plaintext in RAM	Zeroization	Used to secure FIDO/FIDO2 services in PIN Protocol 2
Management Auth Keys	3-Key TDES (PIV), AES 128/192/256-bit (PIV),or HMAC SHA1/256/512 (OATH)	N/A. PIV keys are pre-loaded. OATH Key must be configured.	Plaintext (direct entry) or Encrypted	N/A	Plaintext in Flash	Zeroization	OATH and PIV authentication secrets

			by Secure Channel				
Offline Key	HMAC SHA256	Internally, using the DRBG	N/A	N/A	Plaintext in Flash	Zeroization	To support the HMAC-Secret FIDO extension
OTP Keys	AES-128, HMAC-SHA1, or HASH-OTP Secret (byte string)	N/A. Pre-loaded values. Hash-OTP can alternatively be internally generated.	Plaintext (direct entry) or Encrypted by Secure Channel Hash-OTP cannot be imported	N/A	Plaintext in Flash	Zeroization	Used to generate OTPs
OATH Seed Key	HMAC SHA1/256/512	N/A	Plaintext (direct entry) or Encrypted by Secure Channel	N/A	Plaintext in Flash	Zeroization	Used to generate HOTPs or TOTPs
Asymmetric Keys	RSA 2048 - 4096 bits or EC P-256/P-384/P-521 or	Internally, using the DRBG	Plaintext (direct entry) or Encrypted by Secure Channel	AES CCM SP800-38F Key Wrap (FIDO2 ONLY)	Plaintext in Flash or RAM	Zeroization	Signature generation, ECDH, and RSA key unwrap

	Non-NIST curve private keys		or SP800-38F Key Wrap (AES CCM)				
Attestation Key	RSA 2048 - 4096 bits or EC P-256/P-384/P-521 or Non-NIST curve private keys	Pre-loaded values.	Plaintext (direct entry) or Encrypted by Secure Channel PIV and OpenPGP only	N/A	Plaintext in Flash	N/A.	Attest internally generated public keys
Wrapping Key	AES-256 CCM	Internally, using the DRBG	N/A	N/A	Plaintext in Flash	Zeroization	Used to wrap FIDO keys.
Asymmetric Public Keys	RSA 2048 – 4096 bits or EC P-256/P-384/P-521 or Non-NIST curve public keys.	Internally, using the DRBG	N/A	Plaintext	Plaintext in Flash	N/A	Used to verify digital signatures (external entities), ECDH, or perform RSA Key Wrap

2.6.1 Key Generation

The module uses an internal NDRNG to seed the SP800-90A CTR_DRBG for the generation of keys. DRBG is initialized with a 384-bit entropy input string, which contains at least 301.8 bits of entropy. Note that the module generates cryptographic keys whose strengths are modified by available entropy.

2.6.2 Key Entry/Output

CSPs may be entered and output in plaintext. Optionally, a Secure Channel (AES-128 CBC and CMAC) may be established within each functional unit to protect communication, inclusive of CSP entry and output. Keys may also be encrypted by the Wrapping Key (AES-256 CCM). Please see Table 8 above for complete details.

2.6.3 Zeroization Procedures

Each functional unit is zeroized using separate services that destroy the CSPs within its purview, as follows:

- PIV: “RESET” service. All CSPs zeroized with the Management Auth Key and PIN being set to their default values.
- OTP: “WRITE CONFIG TO SLOT” service. All CSPs zeroized.
- OATH: “RESET” service. All CSPs zeroized.
- OpenPGP: “TERMINATE APPLET” followed by “ACTIVATE APPLET” services. All CSPs zeroized with the PINs being set to their default value.
- FIDO/FIDO2: “RESET” service. All CSPs zeroized with the Offline Key and Wrapping Key being re-generated.
- YubiCrypt: “RESET” service. All CSPs zeroized with the ephemeral keys cleared at power cycle and PINs being set to their default values.
- Secure Channel: “DELETE KEY”. All CSPs zeroized with the ephemeral keys cleared at power cycle.

Attestation Keys will persist through a zeroization, as they are used to create public key attestations.

2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

The module conforms to 47 CFR FCC Part 15. Subpart B, Class B (Home Use) requirements.

2.8 Self-Tests

Self-tests are health checks that ensure that the cryptographic algorithms within the module are operating correctly. The self-tests identified in FIPS 140-2 broadly fall within two categories

1. Power-On Self-Tests
2. Conditional Self-Tests

2.8.1 Power-On Self-Tests

The module benefits from the allowances set forth by IG 9.11. Upon initial installation, the module performs all required power-on self-tests. Once successfully completed, a POST flag is set and is checked upon each subsequent power-on. For each subsequent power-on, if the POST flag is set, only the firmware integrity test is performed. All other self-tests may be invoked on demand. The module supports the following Power-On Self-Tests:

- Firmware Integrity Test (16-bit EDC)
- AES-128 CCM Encrypt KAT
- AES-128 ECB Decrypt KAT
- HMAC (SHA-1, SHA-256, SHA-512) KAT
-
- KDF SP800-108 CMAC KAT
- CTR_DRBG KAT
- ECDSA Signature Generation Component (P-256) KAT
- ECC CDH Primitive “Z” Computation KAT
- RSA 2048 Signature Generation Component KAT
- RSA 2048 Decryption Primitive KAT Component KAT)
- TDES 3-Key Encrypt KAT

2.8.2 Conditional Self-Tests

The module supports the following Conditional Self-Tests:

- NDRNG Continuous Test
- SP800-90A Health Tests
- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test

2.8.3 Self-Tests Error Handling

If any of the Power-On Self-Tests fail, the module enters the error state and will immediately restart.

2.9 Mitigation Of Other Attacks

The module does not assert mitigation of attacks beyond the scope of FIPS 140-2 requirements.

3. Secure Operation

The module supports an Approved mode and a non-Approved mode of operation.

3.1 Installation

There are no specific instructions for the installation of the YubiKey 5 Cryptographic Module. The module will come installed within a YubiKey 5 and is ready for use once powered-on and initialized per the instructions in Section 3.2.

3.2 Initialization

In order to operate in the Approved mode of operation, the operator must adhere to the following instructions:

- Do not use any algorithms specified in Table 4 of this Security Policy
- Select the functional units intended for use and perform the following:
    - OTP:
        - Set a PIN in OTP Slot 1 and OTP Slot 2
        - Establish a secure channel to perform the following services over NFC:
            - WRITE CONFIG TO SLOT
            - UPDATE SLOT CONFIGURATION
            - WRITE NDEF TO SLOT
    - PIV:
        - Update the default Management Auth Key and PINs
        - Establish a secure channel to perform any PIV services over NFC

  - OpenPGP:
    - Update the default User and Admin PINs
    - Establish a secure channel to perform any OpenPGP services over NFC
  - OATH:
    - Set a Management Auth Key
    - Establish a secure channel to perform the following services over NFC:
      - SET CODE
      - PUT
  - FIDO U2F:
    - FIDO U2F cannot be used in the FIPS 140-2 Level 2 configuration.
  - FIDO2:
    - Set a PIN
    - Set Credential Protection to Level 2 for all resident credentials
    - Only the following services may be performed over NFC in PIN Protocol 1:
      - GET ASSERTION
      - GET INFO
      - RESET
  - YubiCrypt:
    - Update the default Admin PIN
    - Establish a secure channel to perform any YubiCrypt services over NFC
  - Secure Channel:
    - Update the default key set

- If the instructions above are not adhered to or the operator desires to transition to the non-Approved mode, then the module must be zeroized per the instructions in Section 2.6.3.

Appendix A: Acronyms

This section describes the acronyms used throughout the document.

Table 9 - Acronyms

Acronym	Definition
AES	Advanced Encryption Algorithm
CKG	Cryptographic Key Generation
CTAP	Client to Authenticator Protocol
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FIDO	Fast Identity Online
HMAC	Hash-based Message Authentication Code
KDA	Key Derivation Algorithm
KDF	Key Derivation Function
KTS	Key Transport Scheme
LRC	Longitudinal Redundancy Check
NDRNG	Non-deterministic Random Number Generator
OATH	Open Authentication
OTP	One Time Passcode
PIN	Personal Identification Number
PIV	Personal Identification Verification
RSA	Rivest, Shamir, Adleman

SCL	Serial Clock Line
SDA	Serial Data Line
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
U2F	Universal Second Factor