YubiHSM 2 Cryptographic Module

Yubico, Inc.
FIPS 140-2 Non-Proprietary Security Policy
Document Version: 1.3

Table Of Contents

1. Introduction

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

Hardware Version #: SLE78CLUFX3000PH, SLE78CLUFX5000PH
Firmware Version #: 2.2.0
FIPS 140-2 Security Level: 3

1.1 Purpose

This document was prepared as Federal Information Processing Standard (FIPS) 140-2 validation process. The document describes how the YubiHSM 2 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. YubiHSM 2 Cryptographic Module

The YubiHSM 2 Cryptographic Module (the module) is a single-chip module validated at FIPS 140-2 Security Level 3. 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	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-Tests	3
10	Design Assurances	3
11	Mitigation Of Other Attacks	N/A

2.1 Cryptographic Module Specification

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

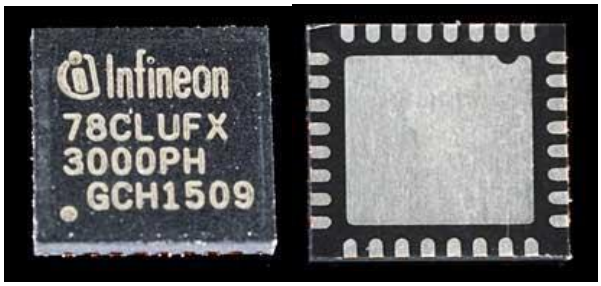

Figure 1 – YubiHSM 2 Cryptographic Module (SLE78CLUFX3000PH – **Front and Back)**

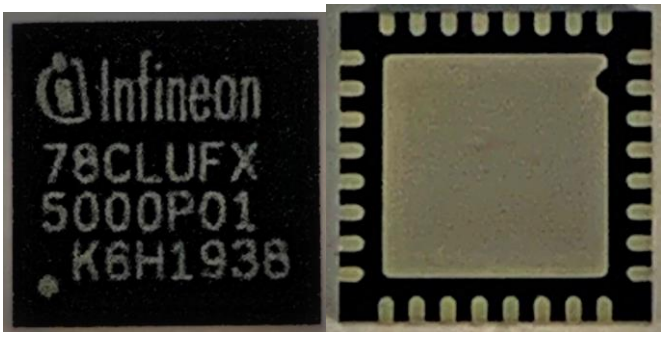

Figure 2 – YubiHSM 2 Cryptographic Module (SLE78CLUFX5000PH **– Front and Back)**

2.1.1 Cryptographic Boundary

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

2.1.2 Modes Of Operation

The module supports an Approved mode and a non-Approved mode of operation. In the Approved mode, only FIPS-Approved algorithms are supported, whereas the non-Approved mode supports additional non-Approved algorithms. Please see Section 3.2 for instructions for invoking the Approved mode of operation.

Table 2 - Supported Approved Algorithms

Cryptographic Algorithm	CAVP Cert. #	Usage
AES **Modes: CBC, CCM, CMAC, ECB** **Key Sizes: 128, 192, 256**	C1680	Encryption, Decryption, CTR_DRBG, Key Wrap
CKG (Vendor affirmed per SP800-133 and IG D.12)	Vendor Affirmed	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-224, P-256, P-384, P-521**	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

Cryptographic Algorithm	CAVP Cert. #	Usage
ECDSA **Curves: P-224, P-256, P-384, P-521** **Operations: Key Gen**	C1680	Key Generation
HMAC SHA-1, SHA2-256, SHA2-384, SHA2-512	C1680	Data Integrity
KAS-SSC **Co-Factor One-Pass DH, C(1e, 1s, ECC CDH) Scheme** **Curves: P-224, P-256, P-384, P-521, secp256k1, brainpool256r1, brainpool384r1, brainpool512r1**	Vendor Affirmed	SP800-56a-rev3 Shared Secret Calculation. Provides between 112 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.
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 CCM. Provides between 128 and 256-bits of security strength.
RSA **Key Sizes: 2048, 3072, 4096** **Operations: Key Gen, Signature Verification (PKCS#1 V1.5)**	A985, C1680	Key Generation, Signature Verification (3072 and 4096-bit key sizes not supported for Signature Verification)
SHA-1, SHA2-256, SHA2-384, SHA2-512	C1680	Hash
Triple-DES (Tested, but not used) **Mode: ECB, Keying Option 1**	C1680	Not used

Table 3 - Supported Allowed

Cryptographic Algorithm	CAVP Cert. #	Usage
EC Diffie-Hellman **Curves: secp256k1, brainpool256r1, brainpool384r1, brainpool512r1**	N/A	IG D.8 Scenario X2, IG A.2
ECDSA **Curves: secp256k1, brainpool256r1, brainpool384r1, brainpool512r1**	N/A	IG A.2. Key Generation, Signature Generation Primitive
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 supporting both OAEP and PKCS#1 V1.5 padding (key unwrapping; key establishment methodology provides between 112 and 150 bits of encryption strength) RSA (CVL Cert. #C1680, key unwrapping; key establishment methodology provides between 112 bits and 150 bits of encryption strength)

Table 4 – Non-Approved algorithms disabled in the Approved mode

Cryptographic Algorithm	Usage
RSA Signature Primitive with SHA-1	Signature Primitive
ECDSA Signature Primitive with SHA-1	Signature Primitive
EdDSA	Key Generation, Sign

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	FIPS 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
I2C I/O pins (SDA / SCL) (Qty. 2)	(Only available on the SLE78CLUFX5000PH) Secondary physical interface (I2C)	• Control in • Data in • Data out • Status out
Interface Select Pin (Qty. 1)	(Only available on the SLE78CLUFX5000PH) Select USB or I2C (Power-up only)	• Control in
Contactless interface (Qty. 2)	Not used	N/A

2.3 Roles, Services, and Authentication

The module can support a total of 256 operators, which corresponds with the total number of Authentication Keys that may be present. Up to 16 concurrent sessions are also supported.

2.3.1 Authorized Roles

The Operator implicitly assumes both the required Cryptographic Officer and User role. All services are available to the Operator with no distinction between the Cryptographic Officer and User roles.

The module also supports unauthenticated services as outlined in Table 7 below.

2.3.2 Authentication Mechanisms

The module supports identity-based authentication mechanisms as described in Table 6.

Table 6 - Authentication Mechanism Details

Role	Type Of Authentication	Authentication Strength
Operator	Unique identifier and knowledge of a 128-bit shared secret, which is the Authentication Key	The probability of successfully guessing the shared secret is 2^128, which is less than 1/1,000,000. Each session takes approximates 40 ms only perform 1500 session establishment attempts per minute (one session takes approximately 40 ms to establish), which is less than 1/100,000.

2.3.3 Services

Table 7 describes all services available and distinguishes between the various modes of operation. Note:

- Session Keys are used to secure all services with the exception of Echo, Create Session, Device Info, and Reset Device
- “Object” may refer to Authentication Keys, HMAC Keys, Wrap Keys, Asymmetric Keys, or OTP AEAD Keys.

Table 7 - Services

Service	Description	Role		Key/CSP and Type of Access
		Operator	Unauth	
Authenticate Session	Complete the mutual authentication process	X		X Authentication Key

Service	Description	Role		Key/CSP and Type of Access
		Operator	Unauth	
	started with Create Session			
Blink Device	Blink the LED of the device to identify it	X		N/A
Change Authentication Key	Change an Authentication Key	X		W Authentication Key
Close Session	Close the current Session and release it for re-use	X		Z Session Keys
Create OTP AEAD	Create a Yubico OTP AEAD	X		X OTP AEAD Key
Create Session	Begin the mutual authentication process for establishing a Session		X	X Authentication Key W Session Keys
Decrypt OAEP	Decrypt using RSA-OAEP	X		X Asymmetric Key
Decrypt OTP	Decrypt a Yubico OTP	X		X OTP AEAD Key
Decrypt PKCS1	Decrypt using RSA-PKCS#1v1.5	X		X Asymmetric Key
Delete Object	Delete an Object	X		Z Object
Derive ECDH	Perform an ECDH operation	X		X Asymmetric Key
Device Info	Gets device version, device serial, supported Algorithms a nd available log entries		X	N/A
Echo	Echo data back from the device		X	N/A
Export Wrapped	Retrieves an Object under wrap from the device. The Object is encrypted using a Wrap Key (AES-CCM)	X		R Object X Wrap Key
Generate Asymmetric Key	Generate an Asymmetric Key	X		W Asymmetric Key WX DRBG Internal State
Generate HMAC Key	Generate an HMAC Key	X		W HMAC Key WX DRBG Internal State
Generate OTP AEAD Key	Generate an OTP AEAD Key	X		W OTP AEAD Key

Service	Description	Role		Key/CSP and Type of Access
		Operator	Unauth	
				WX DRBG Internal State
Generate Wrap Key	Generate a Wrap Key (AES-CCM) that can be used for export, import, wrap data and unwrap data	X		W Wrap Key WX DRBG Internal State
Get Log Entries	Fetch device audit log	X		N/A
Get Object Info	Get Object metadata	X		N/A
Get Opaque	Retrieve an Opaque Object (user provided data) from the device	X		N/A
Get Option	Fetch a device-global option	X		N/A
Get Pseudo Random	Get pseudo-random data from device.	X		WX DRBG Internal State
Get Public Key	Fetch a public key from device	X		R Asymmetric Key
Get Storage Info	Fetch storage information.	X		N/A
Get Template	Fetch a Template Object from the device	X		N/A
Import Wrapped	Import a wrapped/encrypted object into the device	X		X Wrap Key W Object
List Objects	List Objects in device	X		N/A
Put Asymmetric Key	Import an Asymmetric Key	X		W Asymmetric Key
Put Authentication Key	Store a new Authentication Key.	X		W Authentication Key
Put HMAC Key	Import an HMAC Key.	X		W HMAC Key
Put Opaque	Stores Opaque data (user provided data) in the device	X		N/A
Put OTP AEAD Key	Import an OTP AEAD Key	X		W OTP AEAD Key
Put Template	Store a Template	X		N/A
Put Wrap Key	Import a Wrap Key	X		W Wrap Key
Randomize OTP AEAD	Create an OTP AEAD from random data	X		X OTP AEAD Key

Service	Description	Role		Key/CSP and Type of Access
		Operator	Unauth	
				WX DRBG Internal State
Reset Device	Factory reset a device (Zeroization)	X	X	Z – All CSPs
Rewrap OTP AEAD	Rewrap an OTP AEAD	X		X OTP AEAD Key
Session Message	Send a command over an established session	X		X Session Keys
Set Log Index	Set the last extracted log entry	X		N/A
Set Option	Set a device-global option	X		N/A
Generate Attestation Certificate	Generate attestation of an Asymmetric Key, output is an X.509 certificate	X		RX Asymmetric Key X Yubico Attestation Key
Signature Primitive ECDSA	Signature primitive with ECDSA	X		X Asymmetric Key WX DRBG Internal State
Sign EDDSA	Non-Approved mode only Sign with EdDSA	X		N/A
Sign HMAC	Perform an HMAC operation in device and return the result	X		X HMAC Key
Signature Primitive PKCS1	Signature primitive with RSA-PKCS#1v1.5	X		X Asymmetric Key
Signature Primitive PSS	Signature primitive using RSA-PSS	X		X Asymmetric Key
SSH Certify	Generate an SSH Certificate	X		X Asymmetric Key
Unwrap Data	Decrypt (unwrap) data using a Wrap Key	X		X Wrap Key
Verify HMAC	Verify an HMAC	X		X HMAC Key
Wrap Data	Encrypt (wrap) data using a Wrap Key	X		X Wrap Key
Self-Tests	Self-tests on demand by power cycling	X	X	N/A

R – Read, W – Write, X – Execute, Z – Zeroize

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 (Reset Device)	Seeds the DRBG
DRBG Internal State	V and Key	Internally by DRBG	N/A	N/A	Plaintext in RAM	Zeroization (Reset Device)	Random number generation
Authentication Keys	AES-128 bit keys (KENC, KMAC)	N/A. Initial value pre-loaded in manufacturing and updated via import	Encrypted over Secure Channel	Encrypted over Secure Channel	Plaintext in Flash	Zeroization (Reset Device). ID 1 will be set back to default value	Used to derive session keys
Session Keys	AES-128 CBC (SENC), AES-128 CMAC (RMAC/SMAC)	N/A. Derived from Authentication Keys via SP800-108 CMAC KDF	N/A	N/A	Plaintext in RAM	Zeroization (Reset Device)	Secures each session
Asymmetric Key	RSA 2048, 3072, 4096 bits or	Internally by DRBG	Encrypted over	Encrypted over	Plaintext in Flash	Zeroization (Reset Device)	Digital signatures (including attestations),

Key/CSP	Type	Generation	Entry	Output	Storage	Zeroization	Usage
	EC P-224/P-256/P-384/P-521 or Non-NIST curve private keys		Secure Channel	Secure Channel			key unwrap, or modular exponentiation
HMAC KEY	HMAC	Internally by DRBG	Encrypted over Secure Channel	Encrypted over Secure Channel	Plaintext in Flash	Zeroization (Reset Device)	Data integrity key
OTP AEAD Key	AES-128/192/256 CCM key	Internally by DRBG	Encrypted over Secure Channel	Encrypted over Secure Channel	Plaintext in Flash	Zeroization (Reset Device)	Secure Yubico OTP values for further verification by a validation process
Wrap Key	AES-128/192/256 CCM key	Internally by DRBG	Encrypted over Secure Channel	Encrypted over Secure Channel	Plaintext in Flash	Zeroization (Reset Device)	Secure other CSPs (“objects”)
Yubico Attestation Key	RSA 2048, 3072, 4096 bits or EC P-224/P-	N/A. Pre-loaded in manufacturing	N/A	N/A	Plaintext in Flash	N/A. This is a default value that persists across zeroization	Attests authenticity of other keys, producing a new X.509 certificate for the attested key

Key/CSP	Type	Generation	Entry	Output	Storage	Zeroization	Usage
	256/P-384/P-521 or Non-NIST curve private keys						
Asymmetric Public Keys	RSA 2048, 3072, 4096 bits or EC P-224/P-256/P-384/P-521 or Non-NIST curve public keys	Internally by DRBG	N/A	Encrypted over Secure Channel	Plaintext in Flash	N/A	Signature verification (by external entities), key wrap, or modular exponentiation
Yubico Attestation Public Key	RSA 2048, 3072, 4096 bits or EC P-224/P-256/P-	N/A. Pre-loaded in manufacturing.	N/A	Encrypted over Secure Channel	Plaintext in Flash	N/A	Signature verification (by external entities)

Key/CSP	Type	Generation	Entry	Output	Storage	Zeroization	Usage
	384/P-521 or Non-NIST curve public keys						
SSH Template Timestamp Public Key	RSA 2048 bits	N/A	Encrypted over Secure Channel	Encrypted over Secure Channel	Plaintext in Flash	N/A	SSH Public Key used for timestamp verification

2.6.1 Key Generation

The module uses an internal NDRNG to seed the SP800-90A CTR_DRBG for the generation of keys.

2.6.2 Key Entry/Output

All CSPs are always entered and output through the Secure Channel (AES-128 CBC and CMAC) and may be additionally encrypted by the Wrap Key (AES-128/192/256 CCM).

2.6.3 Zeroization Procedures

Zeroization is performed by issuing the Reset Device service, which will restore the YubiHSM 2 to factory defaults and overwrite all existing CSPs. The only exception to zeroization is the Yubico Attestation Key, which persists in order to create future public key attestations.

2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

The YubiHSM 2 conforms to 47 CFR FCC Part 15. Subpart B, Class B (Home Use) requirements.

2.8 Self-Tests

Self-tests are health check 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

All power-on self-tests may be invoked on demand by power cycling the module. 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, SHA2-256, SHA2-512) KAT
- KDF SP800-108 CMAC KAT
- CTR_DRBG KAT
- ECDSA Signature Generation Component (P-256) KAT
- ECC CDH KAT (P-256)
- RSA 2048 Signature Generation Component KAT (Implicitly tests RSA Decryption Primitive)
- RSA 2048 Signature Verification 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 both an Approved mode and non-Approved mode of operation, which can be configured per the instructions in this Security Policy.

3.1 Installation

There are no specific instructions for the installation of the YubiHSM2 Cryptographic Module. The module will come installed within a YubiHSM 2 and is ready for use once plugged-into a USB port and initialized per the instructions in Section 3.2.

3.2 Initialization

To configure the module into the Approved mode of operation, the operator shall perform the following:

1. Use the “Set Option” service as follows: 4f000405000101 or “put option 0 fips-mode 01”
2. Import new Authentication Keys to replace the default values.

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

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

To toggle the mode of operation, the module will first verify that all CSPs have been deleted, which can be performed via a “Reset Device” service.

To configure the module into the non-Approved mode of operation, the operator must issue the following service:

1. Use the “Set Option” service as follows: 4f000405000100 or “put option 0 fips-mode 00”

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
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
HMAC	Hash-based Message Authentication Code
KDF	Key Derivation Function
KTS	Key Transport Scheme
NDRNG	Non-deterministic Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm