Yubico, Inc.

YubiKey 4 Cryptographic Module

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.0

Date: May 18, 2018

yubico

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Yubico YubiKey 4 Cryptographic Module, hereafter denoted the Module. The Module is the core component for authenticators in the YubiKey 4 product family. The Module meets FIPS 140-2 overall Level 2 requirements.

Table 1.1 – Cryptographic Module Configurations

Module	HW P/N and Version	FW Version
YubiKey 4 Cryptographic Module	SLE78CLUFX3000PH	4.4.2

The Module is intended to be embedded into a hardware authenticator for use by US Federal agencies and other markets that require FIPS 140-2 validated hardware authenticator. The Module is a single-chip embodiment.

The FIPS 140-2 security levels for the Module are as follows:

Table 1.2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figures 1.1 and 1.2. The boundary is defined as the entire device.

Figure 1.1 – YubiKey 4 Cryptographic Module (Front)

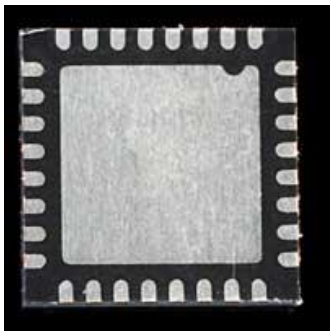

Figure 1.2 – YubiKey 4 Cryptographic Module (Back)

1.2 Firmware and Logical Cryptographic Boundary

Figure 1.3 depicts the Module's logical boundary.

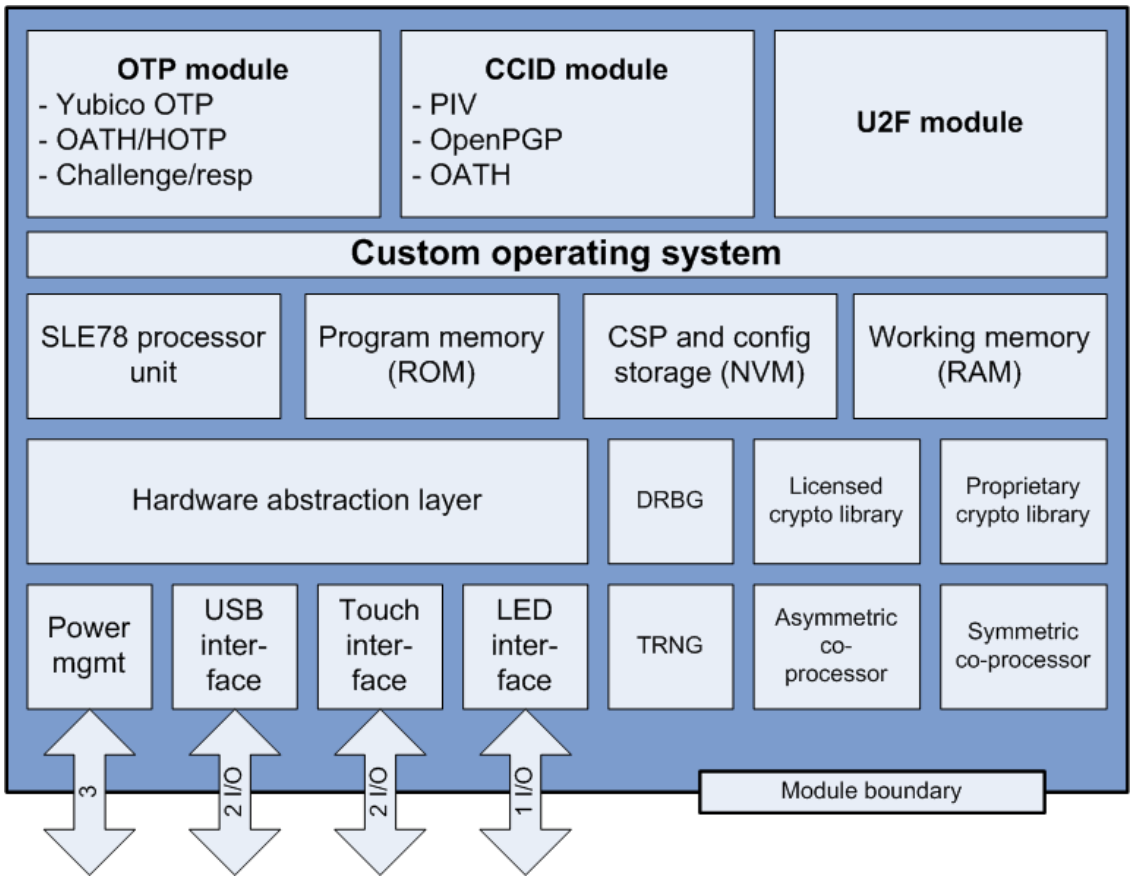

Figure 1.3 – YubiKey 4 Logical Block Diagram with Physical Connections

Table 1.3 – Ports and Interfaces

Port / pins	Description	Logical Interface Type	FIPS Interfaces
USB pins (D+ / D-) (# Pins: 2)	Primary physical interface (USB)	HID-Keyboard: OTP Smart Card Reader/Smartcard: CCID (PIV, OpenPGP) HID: U2F	• Control in • Data in • Data out • Status out
Touch Button interface (# Pins: 2)	Authorize operation	Manual Control	• Control in
LED interface (# Pins: 1)	Status LED	LED	• Status Out
Power interface (# Pins: 3)	Power supply (+5V, GND and supply voltage decoupling)		• Power In

1.3 Mode of Operation

The Module supports an Approved and a non-Approved mode of operation. The Module supports a non-Approved mode of operation in the following functional units: OTP, CCID OATH, and U2F.

To place the Module into the Approved mode of operation, configure the module according to the YubiKey Delivery and Initialization document.

To assure that a Module is running the FIPS certified firmware version, check the firmware version in Table 1.1, as provided in the USB device descriptor returned by the Get Descriptor service. See [USB 2.0].

The YubiKey FIPS Mode Verification Tool can be used to verify if the device is operating in FIPS mode.

1.3.1 OTP functional unit non-Approved mode

The OTP slots can be configured without an access code. Without the access code configured, the OTP Crypto Officer role is eliminated for the functional unit and will remain in a non-Approved FIPS mode. All OTP services will be available to the OTP Unauthenticated User in the non-Approved mode.

To verify if the OTP functional unit is operating in the Approved FIPS mode, perform “VERIFY FIPS MODE” service.

The following services are only available in non-Approved mode

- SWAP CONFIG FROM SLOT 1 TO 2
- DEVICE CONFIG
- SCAN MAP

1.3.2 CCID OATH functional unit non-Approved mode

The OATH functional unit can be configured without the OATH Auth Key. Without the OATH Auth Key configured, the OTP Crypto Officer role is eliminated for the functional unit. All CCID OATH services will be available to the OTP Unauthenticated User in the non-Approved mode except “VALIDATE”.

To verify if the OATH functional unit is operating in the Approved FIPS mode, verify the output of the SELECT APPLET to contain a challenge for HMAC-SHA{1, 256} set by the OATH Auth Key.

1.3.3 U2F functional unit non-Approved mode

The U2F functional unit can be configured without the U2F Admin PIN. Without the U2F Admin PIN configured, the U2F Crypto Officer role is eliminated for the functional unit and will remain in a non-Approved FIPS mode. All the crypto officer services, except “SET PIN” and “VERIFY PIN” can be performed by the U2F Unauthenticated User. The “SET PIN” and “VERIFY PIN” services are not applicable in non-Approved mode.

After the U2F Reset command is executed, the U2F functional unit cannot be place into the Approved mode of operation anymore as the factory loaded U2F Attestation Private Key will be overwritten by a reset U2F Attestation Private Key.

To verify if the U2F functional unit is operating in the Approved FIPS mode, perform “VERIFY FIPS MODE” service.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 2.1 –Approved and CAVP Validated Cryptographic Functions

Algorithm	Functional Unit	Description	Cert #
AES [FIPS 197, SP 800-38A, SP 800-38B, SP 800-38C, SP 800-38F]	OTP - Yubikey	Functions: Encryption Modes: CBC Key sizes: 128, 256 bits (Note: CBC 192 bits also CAVP tested but not used in this module. CMAC also CAVP tested but not used in this module.)	AES #4712
	DRBG CCID (indirectly) U2F (indirectly) OTP (indirectly)	Functions: Encryption Modes: ECB Key sizes: 256 bits	AES #4713
	OTP - Yubikey	Functions: Encryption Modes: ECB Key sizes: 128 and 256 bits (Note: ECB 192 bits also CAVP tested but not used in this module. ECB decryption also CAVP tested but not used in this module.)	AES #4714
	U2F key wrap	Functions: Key Wrap via AES-CCM Modes: CCM Key sizes: 256 bits (Note: CCM 128 and 192 bits also CAVP tested but not used in this module. Only a 256-bit key is used to wrap ECC-P256 private keys.)	AES #4714
CKG [IG D.12]	CCID – PIV OpenPGP	Functions: Key Generation SP800-133 Section 6.1	Vendor Affirmed

	U2F	Asymmetric signature key generation using unmodified DRBG output SP800-133 Section 7.1 Direct symmetric key generation using unmodified DRBG output	
CVL - ECC CDH	CCID – PIV	[SP800-56A] Section 5.7.1.2 Functions: Key agreement Curves/Key sizes: P-256, P-384 (Note: P-521 also CAVP tested but not used in this module)	CVL #1356 - ECC CDH Primitive
DRBG [SP 800-90A]	CCID – PIV CCID - OpenPGP U2F OTP	Functions: CTR DRBG, with no DF and Reseed Security Strengths: 256 bits	DRBG #1604
ECDSA [FIPS 186-4]	CCID – PIV	Functions: Key Pair Generation, Signature Generation Component Curves/Key sizes: P-256, P-384 (Note: P-521 also CAVP tested but not used in this module)	ECDSA #1165 CVL #1360 - ECDSA SigGen Component
	U2F	Functions: Key Pair Generation, Signature Generation Component Curves/Key sizes: P-256 (Note: P-521 also CAVP tested but not used in this module)	
HMAC [FIPS 198-1]	OTP – OATH HOTP OTP - CR CCID - OATH	Functions: Message Authentication, One Time Password (OTP) Generation SHA sizes: SHA-1, SHA-256 Key size: Restricted to >= 14 bytes (Note: HMAC-SHA-384 and HMAC-SHA-512 are CAVP tested but not used in this module)	HMAC #3133 HMAC #3134

KTS [SP 800-38F]	U2F Key Wrap	Function: Key Wrap via AES-CCM Mode: CCM Key size: 256 bits (Note: This is the same AES-CCM algorithm with the same AES certificate #4714 as the AES CCM entry above.)	AES #4714
RSA [FIPS 186-4 and PKCS #1 v2.1]	CCID - PIV	Functions: Key pair Generation, Signature Generation Component Key sizes: 2048 bits	RSA #2569 CVL #1358 - RSASP1
	CCID - OpenPGP	Functions: Key Pair Generation, Signature Generation Component Key sizes: 2048, 3072, 4096 bits (Note: 4096 bits also used but not CAVS testable. 4096-bit key generation not supported.)	
RSA Decryption [SP800-56B]	CCID OpenPGP	Functions: Decryption (Key Unwrap) Key sizes: 2048 bits (Note: 3072 and 4096 bits also used but not CAVS testable)	CVL #1395 - RSADP
SHA [FIPS 180-4]	OTP – OATH OTP - CR CCID - OATH CCID – PIV U2F	Functions: Digital Signature Generation and HMAC SHA sizes: SHA-1, SHA-256	SHA #3861
	CCID – OATH	Functions: HMAC (Note: SHA-384 and SHA-512 are CAVP tested but not used in this module)	SHA #3862

Triple-DES (TDES) [SP 800-67 Rev2] [SP 800-20]	CCID - PIV	Functions: Encryption Modes: TECB Key sizes: 3-key (Note: Decryption also CAVP tested but not used in this module. The number of encryptions with the same Triple-DES key is not limited in this module. See security rule #16 in Section 7.)	TDES #2498

Table 2.2 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
DES	No security claim per IG 1.23. Used internal to the module for CRCs. Modes: CBC and CRC
EC Diffie-Hellman	Legacy use allowed by IG D.8 for key agreement. Key establishment methodology provides 128 or 192 bits of encryption strength.
NDRNG	Hardware Non-Deterministic RNG; minimum of 16 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG. Given the min-entropy of the entropy source, which is 7.54409 bits out of an 8-bit block, and given the 256-bit key size with the AES-256 CTR_DRBG, there will be (7.54409 / 8) * 256 = ~241 bits of security strength. The module generates cryptographic keys whose strengths are modified by available entropy.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 2.3 – Critical Security Parameters (CSPs)

Name	Description
Key	**General Use CSPs**
Entropy Input and Nonce	Entropy Input and Nonce generated by the NDRNG. The size of the Entropy Input is 384 bits. The Nonce size is N/A
DRBG Internal State	DRBG Internal State (v and key).

Key	OTP CSPs
OTP Access Codes	Two 6 byte values. Used for authentication of the OTP CO (Crypto Officer) for management. When the module leaves the factory there is a default value and there is a CO procedure for updating this value.
OTP Slot Keys	Two AES-128 bits or HMAC-SHA-1 160 bit values, depending on the algorithms used. Used for generation of OTPs (One Time Passwords).
Key	**CCID/PIV CSPs**
PIV Symmetric Key for Mutual Authentication	One 3-key TDES key. Used for authentication of the CCID PIV CO. There is a defined default value when it leaves the factory.
PIV Asymmetric Private Keys	0 to 24 RSA 2048 or ECDSA P-256/P-384 private keys. Used for cryptographic operations in conjunction with an external system.
PIV Attestation Private Key	One RSA 2048 or ECDSA P-256/P-384 private keys. Used to attest internally generated public keys using hash-pkcs#1v15-sign
PIV User PIN	One 6-8 byte PIN. Used for authenticating the PIV User for Asymmetric services.
PIV PUK PIN	One 6-8 byte PIN. Used for unblocking the PIV User PIN.
Key	**CCID/OpenPGP CSPs**
OpenPGP Admin PIN (PW3)	One 8-127 bytes. Used for authentication of the OpenPGP CO. When the module leaves the factory there is a default value and there is a CO procedure for updating this value.
OpenPGP Signature Private Key	0 or 1 RSA 2048/3072/4096 private keys. Used for PKCS#1 v1.5 signing operation.
OpenPGP Authentication Private Key	0 or 1 RSA 2048/3072/4096 private keys. Used for authentication as PKCS#1 v1.5 signing operation.
OpenPGP Decryption Private Key	0 or 1 RSA 2048/3072/4096 private keys. Used for decryption with PKCS#1 v1.5.
OpenPGP User PIN (PW1)	One 6-127 bytes. Used for authenticating the OpenPGP User for Asymmetric services.
OpenPGP Reset Code	0 or 1 8-127 bytes. Optional. Used for resetting the User PIN.
Key	**U2F CSPs**
U2F Key Wrapping Key	One AES-256 key. Used for wrapping the U2F keys.
U2F Admin PIN	0 or 1 6-32 byte PIN. When the module leaves the factory this does not exist and there is a CO procedure for setting this value.
U2F User PIN	0 to many 64 byte PIN (U2F key handle). When the module leaves the factory this does not exist and is set during the registration.
U2F Authentication Private Keys	0 to many ECDSA P-256 private keys. Only one will exist in the module at a time. Used for subsequent signature generation.
U2F Attestation Private Key	One ECDSA P-256 private key. Used to attest internally generated public keys.
Key	**CCID/OATH CSPs**
OATH Auth Key	0 or 1 14-64 byte HMAC SHA1/SHA256 key. When the module leaves the factory this does not exist and there is a CO procedure for setting this value.
OATH Seed key	0 to 32 14-64 byte HMAC SHA1/SHA256 key

2.2 Public Keys

Table 2.4 – Public Keys

Name	Description
Key	**OTP Public Keys**
None	
Key	**CCID/PIV Public Keys**
PIV Asymmetric Public Keys	1 to 25 RSA 2048 or ECDSA P-256/P-384 public keys. Used for cryptographic operations in conjunction with an external system.
Key	**CCID/OpenPGP Public Keys**
OpenPGP Signature Public Key	0 or 1 RSA 2048/3072/4096 public keys. Used for PKCS#1 v1.5 signing operation.
OpenPGP Authentication Public Key	0 or 1 RSA 2048/3072/4096 public keys. Used for authentication as PKCS#1 v1.5 signing operation.
OpenPGP Decryption Public Key	0 or 1 RSA 2048/3072/4096 public keys. Used for decryption with PKCS#1 v1.5.
Key	**U2F Public Keys**
U2F Public Keys	0 to many ECDSA P-256 public keys. Only one will exist in the module at a time. Used for subsequent signature verification outside of the module.
Key	**CCID/OATH Public Keys**
None	

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module contains five (5) functional units, each with its own distinct roles and services. The listed functional units are OTP, PIV, OpenPGP, OATH and U2F. Each functional unit operates independently of the others. They do not share roles, services, or CSPs.

Tables 3.1 and 3.2 list all operator roles supported by the Module along with their description and authentication data. Table 3.3 outlines each authentication mechanism and the associated strengths. The Module does not support a maintenance role or bypass capability. The Module supports concurrent operators, but each functional unit does not support concurrent operators.

For all functional units, authentication is cleared when the device is power cycled or if wrong credentials are used to authenticate to the device.

As the functional units accept role credentials via its low level interfaces, authentication data is not visible in plaintext form when it is sent to the functional unit. Since the authentication data is handled by the host application, care should be taken by the application implementers to mask or hide the authentication data while being entered by the user.

Table 3.1 – Authenticated Roles Description

Role ID	Role Description	Authentication Data
OTP Crypto Officer	This is a Cryptographic Officer role. This role is responsible for configuring the OTP CSPs.	6 byte access code
CCID PIV Crypto Officer	This is a Cryptographic Officer role. This role is responsible for configuring the PIV CSPs and resetting the user PIN using PUK.	3 key TDES mutual challenge-response or 6-8 bytes PUK
CCID PIV User	This is a User role. This role is allowed to perform cryptographic operations using PIV keys, update user PIN, and can read from the four PIV read protected objects.	At least 6 bytes and up to 8 bytes PIN or PUK
CCID OpenPGP Crypto Officer	This is a Cryptographic Officer role. This role is responsible for configuring CSPs and unblocking / resetting PW1 (User PIN) using the resetting code or PW3.	Admin PIN 8 -127 byte
CCID OpenPGP User	This is a User role. This role is allowed to perform cryptographic operations with the encryption, signature and authentication keys, update PW1 (user PIN) and read 2 objects and write 1 object.	PIN 6 -127 bytes

U2F Crypto Officer	This is a Cryptographic Officer role. This role is responsible for creating U2F key handles and changing the PIN	At least 6 bytes and up to 32 bytes PIN
U2F User	This is a User role. This role is allowed to perform cryptographic authentication operation with the PIN (U2F key handles).	A 64 bytes PIN
CCID OATH Crypto Officer	This is a Cryptographic Officer role. This role is responsible for creating and using CSPs.	14 - 64 bytes HMAC-SHA1 or HMAC-SHA256 authentication key

Table 3.2 – Unauthenticated Roles Description

Role ID	Role Description	Authentication Data
OTP Unauthenticated User	This is a User role for OTP output or responding to the challenge.	Unauthenticated - N/A
CCID PIV Unauthenticated User	This is a User role. This role can reset the PIV applet to factory defaults, and can read all non-read-protected objects.	Unauthenticated - N/A
CCID OpenPGP Unauthenticated User	This is a User role. This role can reset the OpenPGP applet to factory defaults, and can read all non-read-protected objects.	Unauthenticated - N/A
U2F Unauthenticated User	This is a User role for U2F authentication. This role can also optionally reset the U2F functional unit to factory defaults.	Unauthenticated - N/A
OATH Unauthenticated User	This role can reset the OATH applet.	Unauthenticated - N/A
USB Unauthenticated User	This role has access to services required for USB 2.0 compliance	Unauthenticated - N/A

Table 3.3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
6 byte access code (OTP)	The access code is a 6 byte (48 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is 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.
3 key TDES mutual challenge response (CCID PIV)	This is a 3-key Triple DES Key which has 112 bits of security. 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 40000 per minute. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 40000/2^112, which is less than 1/100,000.
6-8 byte digit PIN or PUK (CCID PIV)	The PIN is a 6 byte (48 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^48 which is less than 1/1,000,000. The authentication is limited by the retry counter of up to 255 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 255/2^48, which is less than 1/100,000.
User PIN 6-127 byte (CCID OpenPGP)	The PIN is a 6 byte (48 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^48 which is less than 1/1,000,000. The authentication is limited by the retry counter of up to 255 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 255/2^48, which is less than 1/100,000.
Admin PIN 8 -127 byte (CCID OpenPGP)	The access code is an 8 byte (64 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^64 which is less than 1/1,000,000. The authentication is limited by the retry counter of up to 255 tries. Therefore, the probability of successfully authenticating to the module

	within one minute through random attempts is 255/2^64, which is less than 1/100,000.
Reset Code 8 - 127 byte (CCID OpenPGP)	The access code is an 8 byte (64 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^64 which is less than 1/1,000,000. The authentication is limited by the retry counter of up to 255 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 255/2^64, which is less than 1/100,000.
U2F User PIN 64 bytes	The PIN is a 64 byte (512 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^512 which is less than 1/1,000,000. Authentication attempts are limited to 40000 per minute. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 40000/2^512, which is less than 1/100,000.
U2F Admin PIN (for key handle generation) 6-32 bytes (U2F)	The PIN is a 6 byte (48 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^48 which is less than 1/1,000,000. The authentication is limited by the retry counter of 3 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 3/2^48, which is less than 1/100,000.
Auth Key 14 to 64 byte HMAC SHA1, HMAC SHA256 key (CCID OATH)	The auth key is a 14 byte (112 bit) binary string with no restrictions on character space. 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. Each authentication attempt takes approximately 1.5 ms which allows a maximum of 40000 attempts per minute. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 40000/2^112, which is less than 1/100,000.

3.2 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Table 3.4 – OTP Services

Service	Description	OTP Crypto Officer	OTP Unauthenticated User
WRITE CONFIG TO SLOT	Write configuration and CSP in slot. Note: The Zeroization service includes this service. See the YubiKey 4: FIPS Technical Manual for zeroization procedures.	X	
UPDATE SLOT CONFIGURATION	Update configuration (excluding key material CSP) in slot	X	
EMIT YUBI-OTP FROM SLOT	Emit YubiOTP from slot		X
EMIT OATH-HOTP FROM SLOT	Emit OATH-HOTP from slot		X
PERFORM YUBI-OTP CHALLENGE RESPONSE FROM SLOT	Perform YubiOTP challenge response with AES 128 bit key stored in slot using user supplied challenge		X
PERFORM HMAC-SHA1 CHALLENGE RESPONSE FROM SLOT	Compute SHA1 HMAC using 160 bits key stored in slot using user supplied challenge		X
VERIFY FIPS MODE	Verifies if the device is operating in FIPS mode		X
SLOT DEVICE SERIAL	Read serial from device		X
SLOT YK4 CAPABILITIES	Read device capabilities.		X

Table 3.5 – CCID PIV Services

Service	Description	CCID PIV Crypto Officer	CCID PIV User	CCID PIV Unauthenticated User
SELECT APPLET	Select PIV applet			X
GET VERSION	Get firmware version			X
VERIFY PIN	Verify user PIN			X

CHANGE MANAGEMENT KEY	Change management key	X		
CHANGE PUK	Change PIN unlock code using known PUK	X		
CHANGE PIN	Change user PIN with known PIN		X	
UNBLOCK PIN (RESET RETRY COUNTER)	Reset retry counter and set new user PIN using known PUK	X		
GENERAL AUTH (Management auth)	Authenticate to the applet using the 3DES management key			X
GENERAL AUTH (RSA/ECDSA)	Transform data using a private key stored in a slot		X	
GENERAL AUTH (ECDH)	Perform ECDH using a EC private key stored in a slot		X	
GENERATE KEY	Generate asymmetric key pair Note: The Zeroization service includes this service. See the YubiKey 4: FIPS Technical Manual for zeroization procedures.	X		
READ DATA FROM UNPROTECTED CONTAINERS	Read certificates, CCC, CHUID, Security Object, Discovery object, key history object Biometric information templates group template, Secure Messaging Certificate Signer			X
READ DATA FROM PROTECTED CONTAINERS	Cardholder Fingerprints, Read Cardholder Facial Image, Printed Information, Cardholder Iris Images, Pairing Code Reference Data Container		X	
WRITE DATA TO CONTAINERS	Write any container	X		
CHANGE RETRY COUNTERS	Set retry counter for PIN and PUK	X (+ User PIN)		
IMPORT KEY	Import asymmetric key	X		
RESET	Reset PIV card state and delete all stored information. Note: The Zeroization service includes this service. See the YubiKey 4: FIPS Technical Manual for zeroization procedures.			X
ATTEST	Attest and sign a generated key			X

Table 3.6 – CCID OpenPGP Services

Service	Description	OpenPGP Crypto Officer (PW3, RC)	OpenPGP User (PW1)	OpenPGP Unauthenticated User
SELECT APPLET	Select applet			X
VERIFY PW1	Verify using user PW1			X
VERIFY PW3	Verify using admin PW3			X
CHANGE PW1	Update user PW1		X	
CHANGE PW3	Update admin PW3	X		
UPDATE RESET-CODE	Set or update resetting code	X		
UNBLOCK PW1	Reset user PW1 using resetting code or PW3	X		
SET PIN RETRIES	Set retry limit for PW1, PW3 and reset-code	X		
GENERATE ASYMMETRIC KEY PAIR	Generate asymmetric key pair	X		
IMPORT ASYMMETRIC KEY	Import asymmetric key	X		
READ PUBLIC KEY	Read public key			X
COMPUTE DIGITAL SIGNATURE	Perform compute digital signature		X	
DECIPHER	Decipher encrypted data		X	
INTERNAL AUTHENTICATE	Perform internal authentication		X	
TERMINATE APPLET	Terminate OpenPGP applet and delete all stored data Note: The Zeroization service includes this service. See the YubiKey 4: FIPS Technical Manual for zeroization procedures.	X		X

ACTIVATE APPLET	Activate OpenPGP applet with factory defaults Note: The Zeroization service includes this service. See the YubiKey 4: FIPS Technical Manual for zeroization procedures.			X
READ UNPROTECTED DATA OBJECT	Read all unprotected data			X
READ PROTECTED DATA FOR USER	Read data objects only available to user		X	
READ PROTECTED DATA FOR ADMIN	Read data objects only available to admin	X		
WRITE DATA	Write data objects except user writable DOs	X		
WRITE USER PROTECTED DATA	Write user writable data objects		X	
GET VERSION	Get firmware version			X

Table 3.7 – CCID OATH Services

Service	Description	OATH Crypto Officer	OATH Unauthenticated User
SELECT APPLET	Select Applet and verify if the OATH module is in FIPS mode		X
SET CODE	Set or update an auth key	X	
VALIDATE	Validate auth key		X
PUT	Add a new OATH entry	X	
DELETE	Remove an OATH entry	X	
RESET	Delete all OATH credentials and set the applet to the factory defaults Note: The Zeroization service includes this service. See the YubiKey 4: FIPS Technical Manual for zeroization procedures.		X

LIST	List all the names of the OATH entries	X	
CALCULATE	Calculate the code for an OATH entry	X	
CALCULATE ALL	Calculate code for all entries	X	

Table 3.8 – U2F Services

Service	Description	U2F Crypto Officer	U2F Authenticated user	U2F Unauthenticated user
Registration	Create a U2F key handle	X		
Authentication	Generate an assertion using a U2F key handle		X	
Version	Read the U2F version string			X
Set PIN	Set or change the U2F CO PIN	X		
Verify PIN	Verify the U2F CO PIN	X		
Reset	Delete and generate U2F key wrapping key Note: The Zeroization service includes this service. See the YubiKey 4: FIPS Technical Manual for zeroization procedures.			X
Verify FIPS mode	Verifies if the device is operating in FIPS mode			X
Echo	Echo data over the U2F protocol			X

USB Services

Refer to the USB 2.0 specification [USB 2.0] for details about USB services.

Power On / Reset Power Service

The power on / reset power service is how self-tests can be invoked by any authorized role.

Tables 3.9 to 3.13 define the relationship between access to CSPs/Public Keys and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The Module internally generates or derives the CSP.
- W = Write: The key is written to (stored) by the Module.
- O = Output: The Module outputs the CSP. The read access is typically performed before the Module uses the CSP.
- U = Use: The Module uses the CSP.
- I = Input: The Module receives the CSP.
- Z = Zeroize: The Module zeroizes the CSP.

Note: if a table does not include a particular set of CSPs, then those CSPs are not accessed by the set of services listed in that table.

Table 3.9 – OTP CSP and Public Key Access Rights within Services

Service	CSP			
	Entropy Input and Nonce	DRBG Internal State	OTP Access Codes	OTP Slot Keys
WRITE CONFIG TO SLOT			I,U,W, Z	I,W, Z
UPDATE SLOT CONFIGURATION			I,U,W	
EMIT YUBI-OTP FROM SLOT		U,G		U
EMIT OATH-HOTP FROM SLOT				U
PERFORM YUBI-OTP CHALLENGE RESPONSE FROM SLOT		U,G		U
PERFORM HMAC-SHA1 CHALLENGE RESPONSE FROM SLOT				U
VERIFY FIPS MODE			U	
SLOT DEVICE SERIAL				
SLOT YK4 CAPABILITIES				

Table 3.10 – CCID PIV CSP and Public Key Access Rights within Services

Service	CSP							
	Entropy Input and Nonce	DRBG Internal State	PIV Symmetric Key for Mutual Authentication	PIV Asymmetric Private Keys	PIV Attestation Private Key	PIV User PIN	PIV PUK PIN	PIV Asymmetric Public Keys
SELECT APPLET								
GET VERSION								
VERIFY PIN						I,U		
CHANGE MANAGEMENT KEY			I,U,W					
CHANGE PUK							I,U,W	
CHANGE PIN						I,U,W		
UNBLOCK PIN (RESET RETRY COUNTER)						W	I,U	
GENERAL AUTH (Management auth)		U,G	U					
GENERAL AUTH (RSA/ECDSA)		U,G		U				
GENERAL AUTH (ECDH)				U				
GENERATE KEY		U,G		G,W				G,O
READ DATA FROM UNPROTECTED CONTAINERS								O
READ DATA FROM PROTECTED CONTAINERS								
WRITE DATA TO CONTAINERS								

CHANGE RETRY COUNTERS						W	W	
IMPORT KEY				I,W	I,W,Z			
RESET			Z	Z		Z	Z	Z
ATTEST					U			G,O

Table 3.11 – CCID OpenPGP CSP and Public Key Access Rights within Services

Service	CSP										
	Entropy Input and Nonce	DRBG Internal State	OpenPGP Admin PIN (PW3)	OpenPGP Signature Private Key	OpenPGP Authentication Private Key	OpenPGP Decryption Private Key	OpenPGP User PIN (PW1)	Open PGP Reset Code	OpenPGP Signature Public Key	OpenPGP Authentication Public Key	OpenPGP Decryption Public Key
SELECT											
VERIFY PW1							I,U				
VERIFY PW3			I,U								
CHANGE PW1							I,U,W				
CHANGE PW3			I,U,W								
UPDATE RESET-CODE								I,W			
UNBLOCK PW1							W	I,U			
SET PIN RETRIES											
GENERATE ASYMMETRIC KEY PAIR		U,G		G,W	G,W	G,W			G,O	G,O	G,O
IMPORT ASYMMETRIC KEY				I,W	I,W	I,W					
READ PUBLIC KEY									O	O	O
COMPUTE DIGITAL SIGNATURE				U							
DECIPHER						U					

INTERNAL AUTHENTICATE					U						
TERMINATE APPLET											
ACTIVATE APPLET			Z	Z	Z	Z	Z	Z	Z	Z	Z
READ UNPROTECTED DATA OBJECT											
READ PROTECTED DATA FOR USER											
READ PROTECTED DATA FOR ADMIN											
WRITE DATA											
WRITE USER PROTECTED DATA											
GET VERSION											

Table 3.12 – CCID OATH CSP and Public Key Access Rights within Services

Service	CSP			
	Entropy Input and Nonce	DRBG Internal State	OATH Auth key	OATH Seed key
SELECT APPLET		U,G	U	
SET CODE			I,U,W	
VALIDATE			U	
PUT				I,W
DELETE				Z
RESET			Z	Z
LIST				
CALCULATE				U
CALCULATE ALL				U

Table 3.13 – U2F CSP and Public Key Access Rights within Services

Service	CSP								
	Entropy Input and Nonce	DRBG Internal State	U2F Key Wrapping Key	U2F Admin PIN	U2F User PIN	U2F Authentication Private Keys	U2F Attestation Private Key	U2F Public Keys	U2F Attestation Public Key
Registration		U,G	U		G,O	G,O	U	G,O	U,O
Authentication		U,G	U		I,U	I,U			
Version									
Set PIN				I,U,W					
Verify PIN				I,U					
Reset		U,G	Z,G	Z			Z		
Verify FIPS mode				U					
Echo									

USB CSP and Public Key Access Rights within Services
USB services in this module do not have access rights to any CSPs or public keys.

Power On / Reset Power Service

Power On / Reset Power services in this module do not have access rights to any CSPs or public keys but they will trigger zeroization of volatile CSPs.

4 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly. Power up self–tests are available on demand by power cycling the Module.

On power up or reset, the Module performs the self-tests described in Table 4.1 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the critical error state and immediately restarts.

The status indicator is a signal output physically via a physical port used to turn on an external LED. Until all power-up self-tests have completed successfully, the primary interface (USB) is not enabled and the status indicator signal is not turned on.

Conditional tests are performed by the Module as described in Table 4.2 below. The status indicator for pairwise consistency tests for ECDSA and RSA is an error code that is returned. The status indicator for a failed NDRNG continuous test is the Module becomes non-functional until it is power cycled.

Table 4.1 – Power Up Self-tests

Test Target	Description
Firmware Integrity	16-bit LRC performed over all code in NVM.
AES Secure	KATs: Encryption, Decryption Modes: CCM (implicitly covers ECB Encryption), ECB Decryption Key Size: 128 bits
AES DRBG	Implicitly tested by AES-ECB encryption KAT.
HMAC	KATs: Generation SHA sizes: SHA-1, SHA-256
SHA	SHA-1 and SHA-256 are implicitly tested by HMAC KATs.
DRBG	KATs: CTR DRBG SP800-90A Section 11.3 Health Tests (covers AES Encrypt KAT) Security Strengths: 256 bits
ECDSA	KAT: Signature Generation Component Curves/Key sizes: P-256 (Note: Key Pair Generation tested during ECDSA Pairwise Consistency Test)
ECC CDH	KATs: Primitive "Z" Computation KAT per IG 9.6 Curves/Key sizes: P-256
RSA	KAT: Signature Generation Component Key sizes: 2048 bits (Note: Key Pair Generation tested during RSA Pairwise Consistency Test)
RSA Decryption	KATs: SP 800-56B Decryption Primitive Key sizes: 2048 bits (Implicitly tested by RSA Signature Generation Component)
TDES	KATs: Encryption Modes: TECB Key sizes: 3-key

Table 4.2 – Conditional Self-tests

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
DRBG	N/A. DRBG Continuous Test is no longer required by IG 9.8.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation using sign/verify.
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation using sign/verify.

5 Physical Security

The Module is opaque and meets Level 3 for tamper resistance and evidence. The Module is encased in a removal-resistant IC packaging material. The physical security mechanism is a hard, opaque tamper-evident coating. The Module should be inspected for tamper before each use. Tamper will be indicated by scratches or other damage to the coating, as seen in Figures 5.1 and 5.2 below.

The module hardness testing was only performed at a single ambient temperature (≈23°C). No assurance is provided for Level 3 hardness conformance at any other temperatures.

Figure 5.1 - Tamper Evidence on Packaging

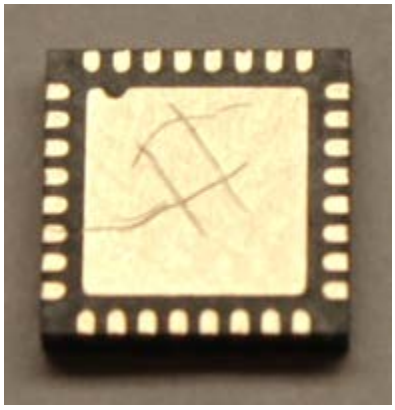

Figure 5.2 - Tamper Evidence on Ground Pad

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module does not support firmware updates.

7 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The Module clears previous authentications on power cycle. All authenticated states are stored in volatile memory.
2. The operator is capable of commanding the Module to perform the power up self-tests by cycling power or resetting the Module.
3. Power up self-tests do not require any operator action.
4. Data output is inhibited during self-tests and error states.
5. Data output is logically disconnected during key generation and zeroization.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
7. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
8. The Module does support concurrent operators.
9. The Module does not support a maintenance interface or role.
10. The Module does not support manual key entry.
11. The Module does not have any external input/output devices used for entry/output of data.
12. The Module does not output plaintext CSPs.
13. The Module does not output intermediate key values.
14. Any CSPs that are programmed into the module must be done so in a secured environment in the presence of the Crypto Officers (OTP Crypto Officer, CCID PIV Crypto Officer, CCID OpenPGP Crypto Officer, U2F Crypto Officer, and CCID OATH Crypto Officer). For plaintext CSPs, please see IG 7.7 for the manual distribution requirement.
15. The OTP Crypto Officer must be present with the module during the Zeroization service. There are multiple commands that need to run in succession. See the YubiKey 4: FIPS Technical Manual for zeroization procedures.
16. The CCID PIV Crypto Officer must not authenticate/encrypt with the same 3-key Triple DES mutual challenge response key more than 2^28 times (refer to IG A.13).
17. The allowable environmental conditions for the entropy source require operation of the module within the temperature range of -40°C to +85°C.

8 Mitigation of Other Attacks

Area 11 – Mitigation of Other Attacks – of the FIPS 140-2 requirements do not apply to this module as it has not been designed to mitigate any specific attacks outside the scope of the FIPS 140-2 requirements.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 9.1 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[CCID Rev 1.1]	CCID 1.1 Specification - http://www.usb.org/developers/docs/devclass_docs/DWG_Smart-Card_CCID_Rev110.pdf
[HID 1.1]	HID 1.1 Specification - http://www.usb.org/developers/hidpage/HID1_11.pdf
[FIDO U2F]	FIDO U2F specification - https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.pdf
[ISO 7816-4:2013]	ISO 7816-4:2013 Specification - http://www.iso.org
[OpenPGP Card 2.1]	OpenPGP Card 2.1 Specification - https://gnupg.org/ftp/specs/OpenPGP-smart-card-application-2.1.pdf
[FIPS 201]	FIPS 201 Specification - http://csrc.nist.gov/groups/SNS/piv/index.html
[USB 2.0]	USB 2.0 Specification- http://www.usb.org/developers/docs/usb20_docs
[OATH 2.0]	OATH 2.0 Specification - https://openauthentication.org/specifications-technical-resources/

Table 9.2 – Acronyms and Definitions

Acronym	Definition
FIDO	Fast Identity Online
LRC	Longitudinal Redundancy Check
U2F	Universal Second Factor