# YubiKey 5 FIPS Series Technical Manual

Yubico

Aug 08, 2022

# CONTENTS

CHAPTER

ONE

# INTRODUCTION

## 1.1 Why FIPS?

Federal Information Processing Standards (FIPS) are developed by the United States government for use in computer systems to establish requirements such as ensuring computer security and interoperability. The National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) run the NIST Cryptographic Module Validation Program (CMVP) as a collaborative effort.

FIPS certification demonstrates that a product has gone through a rigorous audit process and adheres to a security standard that can be measured and quantified.

Many government organizations and government contractors are required to use FIPS-approved products, as are highly-regulated industries in general. Other countries also recognize FIPS 140-2. For the US government, the default is that FIPS is **required**.

### 1.1.1 Do You Require FIPS Keys?

If you do not have a security auditor, and/or the auditor does not have a compliance requirement, you probably do not need FIPS. The standard line of YubiKeys offers the same security, algorithms and functionality. The standard line also evolves at a much more rapid pace because it does not need to go through an exhaustive validation process, which commonly takes a year or more. Yubico can release standard firmware with new features, enhancements, etc. at any time, whereas FIPS-certified products must go through the FIPS validation process every time there is a change.

## 1.2 YubiKey 5 FIPS Series

The YubiKey 5 FIPS Series is FIPS 140-2 certified. It offers strong authentication with support for multiple protocols - including FIDO2, which is the new standard that enables the replacement of password-based authentication. The YubiKey strengthens security by replacing passwords with strong hardware-based authentication using public key cryptography.

The cryptographic functionality of the YubiKey 5 FIPS Series devices is powered by the FIPS 140-2 certified YubiKey 5 cryptographic module, a single-chip cryptographic processor with a non-extractable key store that handles all of the cryptographic operations. The YubiKey 5 cryptographic module is FIPS 140-2 certified, both Level 1 and Level 2 (Physical Security Level 3).

The YubiKey 5 FIPS Series cryptographic module is a secure element that supports multiple protocols designed to be embedded in USB 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 smart card authentication. The module implements the following major functions, depending on the firmware version you have:

| Function | Firmware Versions | |
|---|---|---|
| | 5.4.2 | 5.4.3 |
| Yubico One Time Password (OTP) | yes | yes |
| OATH OTP authentication | yes | yes |
| OpenPGP version 3.4 | • | yes |
| PIV-compatible smart card | yes | yes |
| FIDO Universal 2nd Factor (U2F) | yes | yes |
| FIDO2 WebAuthn | yes | yes |
| YubiHSM Auth | • | yes |
| SCP03 | • | yes |

The YubiKey 5 FIPS Series hardware with the 5.4 firmware is certified as an authenticator under both FIPS 140-2 Level 1 and Level 2. It meets the highest authenticator assurance level 3 (AAL3) of NIST SP800-63B guidance. To use security keys from the YubiKey 5 FIPS Series as a Level 2, more stringent initialization is required than for Level 1. Guidance for Level 2 is set out in detail in the following.

## 1.3 FIPS-specific Aspects of the YubiKey 5 FIPS Series

Distinguishing the YubiKey 5 FIPS Series from the YubiKey 5 Series with the 5.4 firmware are the following configuration changes, set at programming:

| Configuration Change | Description |
|---|---|
| Functional | Enforce power-up self-test (firmware integrity and algorithm testing) |
| Minimum PIN length for FIDO2 | 6 alphanumeric characters |
| Identification (FIDO) | Unique AAGUIDs for the FIDO Attestation (see *FIDO2 AAGUIDs*) |
| Attestation (FIDO) | Attestation certificates for FIDO include a FIPS OID (1.3.6.1.4.1.41482.12) |
| FIDO `GETINFO` | Command returns a listing of FIPS, as well as the FIPS-specific OIDs in the PIV and FIDO attestation certificates.* |
| Attestation (PIV) | Attestation certificates for PIV include the FIPS Form Factor identifier** in the Form Factor OID (1.3.6.1.4.1.41482.3.9) |
| YubiKey Manager | Form factor identifies FIPS Series devices.** |

* The certifications that are supported by a FIDO authenticator can be returned in the certifications member of an authenticatorGetInfo response as set out in paragraph 7.3.1. Authenticator Actions of the Client to Authenticator Protocol (CTAP) Review Draft of March 09, 2021.

** Form factor is set during manufacturing and returned as a one-byte value. Currently defined values for this are:

Table 1: Form Factor

| Form Factor | Standard YubiKey Value | Security Key Value (FW 5.4+) | FIPS YubiKey Value (FW 5.4+) |
|---|---|---|---|
| UNDEFINED | 0x00 | N/A | N/A |
| Keychain with USB-A | 0x01 | 0x41 | 0x81 |
| Nano with USB-A | 0x02 | N/A | 0x82 |
| Keychain with USB-C | 0x03 | 0x43 | 0x83 |
| Nano with USB-C | 0x04 | N/A | 0x84 |
| Keychain with Lightning and USB-C | 0x05 | N/A | 0x85 |

## 1.4 Firmware

The YubiKey firmware is separate from the YubiKey itself in the sense that it is put onto each key in a process separate from the manufacture of the physical key. Nonetheless, it can be neither removed nor altered. Yubico periodically updates the YubiKey firmware to take advantage of features and capabilities introduced into operating systems such as Windows, MacOS, and Ubuntu, etc., as well as to enable new YubiKey features.

The firmware version on a YubiKey therefore determines whether or not a feature or a capability is available to that key. The quickest and most convenient way to determine your YubiKey's firmware version is to use the YubiKey Manager (ykman), a lightweight software package installable on any OS. The YubiKey Manager has both a graphical user interface (GUI) and a command line interface (CLI).

- Download the YubiKey Manager tool: https://www.yubico.com/products/services-software/download/yubikey-manager/
- YubiKey Manager (ykman) CLI & GUI Guide

Yubico has submitted the same firmware - releases 5.4.2 and 5.4.3 - to NIST and it has submitted release 5.4.2 to ANSSI for certification. Both organizations have approved certification.

CHAPTER

TWO

# PHYSICAL ATTRIBUTES

The serial number and its 2D barcode (QR code) is printed on the back of every key in the YubiKey 5 FIPS Series except the YubiKey 5C Nano, which is too small to accommodate the 2D barcode.

All of the keys in this series have the acronym “FIPS” underneath the QR code on the back, along with “v5” running up the left side of the QR code, except on the YubiKey 5C Nano, where it runs down the right side.

## 2.1 YubiKey 5 NFC FIPS

**Dimensions**

18mm x 45mm x 3.3mm

**Weight**
3g

**Physical Interfaces**
USB, NFC

**Operating Temperatures**
0 °C - 40 °C (32 °F - 104 °F)

**Storage Temperatures**
-20 °C - 85 °C (-4 °F - 185 °F)

## 2.2 YubiKey 5 Nano FIPS

**Dimensions**
12mm x 13mm x 3.1mm

**Weight**
1g

**Physical Interfaces**
USB

**Operating Temperatures**
0 °C - 40 °C (32 °F - 104 °F)

**Storage Temperatures**
-20 °C - 85 °C (-4 °F - 185 °F)

## 2.3 YubiKey 5C FIPS

**Dimensions**
12.5mm x 29.5mm x 5mm

**Weight**
2g

**Physical Interfaces**
USB

**Operating Temperatures**
0 °C - 40 °C (32 °F - 104 °F)

**Storage Temperatures**
-20 °C - 85 °C (-4 °F - 185 °F)

## 2.4 YubiKey 5C Nano FIPS

**Dimensions**
12mm x 10.1mm x 7mm

**Weight**
1g

**Physical Interfaces**
USB

**Operating Temperatures**
0 °C - 40 °C (32 °F - 104 °F)

**Storage Temperatures**
-20 °C - 85 °C (-4 °F - 185 °F)

## 2.5 YubiKey 5Ci FIPS

**Dimensions**
12mm x 40.3mm x 5mm

**Weight**
2.9g

**Physical Interfaces**
USB, Lightning®

**Operating Temperatures**
0 °C - 40 °C (32 °F - 104 °F)

**Storage Temperatures**
-20 °C - 85 °C (-4 °F - 185 °F)

## 2.6 YubiKey 5C NFC FIPS

**Dimensions**
18mm x 45mm x 3.7mm

**Weight**
4g

**Physical Interfaces**
USB, NFC

**Operating Temperatures**
0 °C - 40 °C (32 °F - 104 °F)

**Storage Temperatures**
-20 °C - 85 °C (-4 °F - 185 °F)

CHAPTER

THREE

# PHYSICAL INTERFACES: USB, NFC, APPLE LIGHTNING®

We refer to the ways that a computer, phone, tablet, etc. can connect with a YubiKey as the physical interfaces.

## 3.1 USB

All of the models in the YubiKey 5 FIPS Series provide a USB 2.0 interface, regardless of the form factor of the USB connector. The YubiKey will present itself as a USB composite device in addition to each individual USB interface.

USB A and USB C connectors are supported.

The USB PID and iProduct string changes depending on which of the USB interfaces are enabled. They are described in the YubiKey USB ID Values Guide.

For more information, see "Understanding the USB Interfaces" in the YubiKey 5 Series Technical Manual.

## 3.2 Apple Lightning®

The YubiKey 5Ci FIPS presents itself as an Apple iOS peripheral. It is able to interact with:

- Any iOS app utilizing the Yubico YubiKey iOS SDK
- Any app input data field via touch-triggered OTP.
- Any WebAuthn compliant appliction (starting in iOS 13). This includes the Safari browser.

All features of the YubiKey 5 FIPS are supported over Lightning®.

When connecting the YubiKey 5Ci FIPS via Lightning®, the **interfaces enabled** setting is common to both USB-C and Lightning®. Enabling or disabling an interface will apply to both connections.

The YubiKey 5Ci FIPS communication over Lightning® uses a variety of channels for communication between iOS and the YubiKey.

---

**Note:** Developers: for apps within iOS to be able to use advanced protocols that send and receive information from the YubiKey 5Ci FIPS, the Yubico iOS SDK is required and the app registered with Yubico. This can be done via the Yubico iOS SDK App Submission page.

---

For a description of the USB and iProduct string when connecting via Lightning®, see the YubiKey USB ID Values Guide.

## 3.3 NFC

In addition to USB, the YubiKey 5 NFC FIPS and YubiKey 5C NFC FIPS also provide an NFC wireless interface. The YubiKey 5 NFC FIPS and YubiKey 5C NFC FIPS include the RFID standard specific to the ISO/IEC 14443-A and ISO/IEC 14443-4 NFC format; RFID implementations not included in the listed ISO standards are not supported.

The NDEF URI has been updated to a new format; an example of the new format is provided below. The <OTP> value is replaced with the OTP generated by the YubiKey.

https://demo.yubico.com/yk/

For operations that require a touch, all touch requests within the first 20 seconds of the operation will succeed. After a period of inactivity, a YubiKey placed on a desktop NFC reader may power down to help prevent unintended access. To regain connectivity with an NFC reader, remove the YubiKey from the reader and reposition it on the reader. Some NFC readers may power-cycle and in doing so, prevent the YubiKey from powering down.

CHAPTER

FOUR

# FIDO2 AAGUIDS

The FIDO2 specification states that an Authenticator Attestation GUID (AAGUID) must be provided during attestation. An AAGUID is a 128-bit identifier indicating the type of the authenticator. Authenticators with the same capabilities and firmware - such as the YubiKey 5 series devices without NFC - can share the same AAGUID.

New AAGUIDs are issued for new YubiKey products which support FIDO2, or when existing YubiKey products have FIDO2 features added or removed.

For the current AAGUIDs for all devices in the YubiKey 5 FIPS Series, see YubiKey Hardware FIDO2 AAGUIDs.

CHAPTER

FIVE

# UNDERSTANDING THE APPLICATIONS

The YubiKey 5 FIPS Series provides applications for a wide variety of authentication options: OTP, U2F, FIDO2, Smart Card/PIV, and OATH. The applications are separate from each other, with separate storage for keys and credentials. The following sections provide detailed descriptions of each option.

## 5.1 FIPS Application Exceptions

These exceptions apply to all YubiKey 5 FIPS Series applications.

- Attestation certificates include FIPS OID.
- Pairwise consistency test verifies proper generation of all asymmetric keys (RSA & ECC). You might detect some minor performance impact on new key generation.
- When inserted in a USB port, the FIPS power-on self-test takes ~300 milliseconds before the device is usable.
- **NB: The YubiKey 5 FIPS Series supports cryptographic algorithms that are not permissible in a FIPS environment. Consult with your security auditor to ensure the YubiKey is used in a compliant manner.** For more details on this, see *Configuring the YubiKey 5 FIPS Series under FIPS 140-2 Level 1*.

## 5.2 YubiKey 5 FIPS Series Supported Functions

In addition to the applications, the **functions** listed below are also supported.

- YubiKey device configuration
- SCP03; for more information, see the chapter on Secure Channel (SCP03) in the YubiKey 5 Series Technical Manual
- YubiHSM Auth (with firmware version 5.4.3) is a YubiKey CCID application that stores the long-lived credentials used to establish secure sessions to a YubiHSM 2. The secure session protocol is based on Secure Channel Protocol 3 (SCP03). For more information, see the chapter on YubiHSM Auth in the YubiKey 5 Series Technical Manual.
- Power-on self-test
- FIPS-specific attestation certificates and FIDO2 metadata
- NFC – On NFC devices only

For information about the static password, the HMAC-SHA1, and supported extensions, see the sections of the same name in Understanding the Applications in the YubiKey 5 Series Technical Manual.

CHAPTER

SIX

# MANAGING APPLICATIONS

Use the YubiKey Manager to manage YubiKey applications.

- Download the YubiKey Manager tool: https://www.yubico.com/products/services-software/download/yubikey-manager/
- YubiKey Manager (ykman) CLI & GUI Guide: https://docs.yubico.com/ykman/

## 6.1 Enabling/Disabling

The YubiKey Manager can be used to check which applications are enabled on which interface and to enable or disable each application on each physical interface.

To find out which applications are enabled, select the **Interfaces** tab. A checkbox with a tick is shown next to each enabled applications. To change which applications are enabled, use the checkboxes to select the ones you want enabled and click Save Interfaces.

---

**Note:** For the FIPS YubiKey 5Ci, any modifications made to the applications over the USB interface will also apply to the applications over Lightning®.

---

## 6.2 Locking

Once the desired applications have been selected, a lock code can be set to prevent changes to the set of enabled applications. This is done using the YubiKey Manager command line interface command `ykman config set-lock-code`. The lock code is 16 bytes presented as 32 hex characters. For more information, see the YubiKey Manager (*ykman*) CLI & GUI Guide.

CHAPTER

SEVEN

# DEPLOYING THE YUBIKEY 5 FIPS SERIES

The YubiKey 5 FIPS Series keys are certified under FIPS 140-2 Level 1 and FIPS 140-2 Level 2. Keys in this series have two certificates, each corresponding to a different level of certification, but both certificates apply to the same keys. The YubiKey chipset is certified at FIPS 140-2 Physical Security Level 3, providing both tamper-evidence and tamper-resistance. This means the YubiKey 5 FIPS Series keys can be used in an Overall Security Level 1 or 2 environment without issue. Depending on which certification the YubiKey 5 FIPS Series is being deployed under, there are different requirements as to how the various functions are to be secured. To review the differences between the considerations and requirements for a FIPS 140-2 Level 1 authenticator and those for a FIPS 104-2 Level 2 authenticator, see *FIPS Level 1 vs FIPS Level 2*.

NIST SP 800-63-B provides guidance on the level required for your deployment.

In cases where only Level 1 is required, the end-user experience with a YubiKey 5 FIPS Series is similar to that of a user with key from the YubiKey 5 Series. The user experience with YubiKey 5 FIPS Series deployed under FIPS 140-2 Level 2 is much more onerous.

NIST classified the YubiKey 5 Series FIPS as 'composite authenticators.' As such, no device in that series can be taken out of the FIPS-approved mode after initialization without zeroizing the function. This means that once the YubiKey is correctly configured, it remains in the correct configuration. This is what renders the `--check-fips` command unnecessary. If the crypto officer ensures that the YubiKey 5 Series FIPS devices are correctly configured at initialization, they remain in FIPS-approved mode.

## 7.1 Configuring the YubiKey 5 FIPS Series under FIPS 140-2 Level 1

Without any configuration, the YubiKey 5 FIPS Series meets the requirements for the FIPS 140-2 Level 1 certification as an authenticator with FIPS-approved algorithms. Security Level 1 allows an authenticator to be used on a general purpose computing system using an unevaluated operating system. This can include computers or OSs that are configured in a FIPS-certified mode of operation, but which might not have extensive access controls or auditing features. Any function on the YubiKey may be used. The only non-approved algorithms are:

- RSA 1024-bit keys
- EdDSA keys
- X25519 keys

## 7.2 Configuring the YubiKey 5 FIPS Series under FIPS 140-2 Level 2

Security Level 2 includes all of the requirements for FIPS Level 1, but further enforces enhanced physical security mechanisms and a separation of functions with regard to role-based authentication. Security Level 2 allows an authenticator to be used on a general purpose computing system with an operating system that has been evaluated at EAL2 with role-based access control mechanisms and comprehensive auditing.

The role-based authentication minimum requirement is one in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services. A Security Officer role is required for services such as importing or generating new credentials or programming new OTP secrets on a YubiKey. The User role covers the actual usage of programmed credentials for authentication. The Crypto Officer role is that of "a cryptographic officer [who] is authorized to perform cryptographic initialization and management functions on a CKMS [Cryptographic Key Management System] and its cryptographic modules." (Quote taken from SP 800-130 (DOI).)

To act in an Overall Security Level 2 environment, a YubiKey must be configured in a FIPS-approved mode of operation OR receive an exemption from the security auditor.

---

**Note:** To load key data over NFC a secure channel must be used. For more information on Secure Channel (SCP03) in connection with YubiKeys, see the topic of that name in the YubiKey 5 Series Technical Manual. For more information on SCP03 requirements from NIST, see NIST Special Publication 800-63C and NIST Special Publication 800-63B.

---

When using a security key from the YubiKey 5 FIPS Series as a FIPS 140-2 Level 2 authenticator in a FIPS environment, in order for the device to be considered as operating in a FIPS-approved mode, all of the applications must be in a FIPS-approved mode of operation.

Not all of the applications on the YubiKey 5 FIPS Series are in a FIPS mode of operation by default. The person filling the crypto officer role in deploying the YubiKey 5 FIPS Series in a secured environment must define and supervise an initialization and delivery process that ensures that each application on the YubiKey 5 FIPS Series is in a FIPS-approved mode of operation before being deployed to end-users.

Every function of the YubiKey must require permissions defined by role; in practice, this is accomplished by setting the access codes, management keys, passwords, PINs, etc. for every function on the YubiKey.

To ensure that each application is in a FIPS-approved mode of operation, use the **YubiKey Manager (ykman)** Command Line Interface (CLI).

- Download the YubiKey Manager tool: https://www.yubico.com/products/services-software/download/yubikey-manager/
- YubiKey Manager (ykman) CLI & GUI Guide: https://docs.yubico.com/ykman/

---

**Note:** It is not permissible to use U2F when the YubiKey 5 FIPS Series is deployed as a 140-2 Level 2 authenticator.

---

---

**Note:** Even if FIPS 140-2 Level 2 does not require that all the credentials across all the applications be changed from the default values before the YubiKey 5 FIPS Series device is deployed to the end user, it is highly recommended that these default values be changed.

---

### 7.2.1 Credentials and Permitted Values

The table below lists the credentials required, allowed values, and credential owner for the supported applications.

| Application | Credential | Permitted Values | Credential Owner |
|---|---|---|---|
| One Time Password (OTP) | Access Code:<br>OTP Slot 1<br>OTP Slot 2 | 6 byte access codes<br>6 byte access codes | Crypto Officer |
| OATH | Authentication Key | 14-64 byte HMAC SHA1/SHA256 key | Crypto Officer |
| PIV Smart Card | Management Key | 3-key TDES key | Crypto Officer |
| | PUK | 6-8 byte PIN | Crypto Officer |
| | PIN | 6-8 byte PIN | Authenticated User |
| OpenPGP | User Password (PW1) | 6-127 byte PIN | Authenticated User |
| | Admin Password (PW3) | 8-127 byte PIN | Crypto Officer |
| WebAuthn | PIN | 6 to 32 byte PIN | Authenticated User |

The instructions for the individual applications are provided in the following topics:

- OTP
- OATH
- PIV
- OpenPGP
- WebAuthn

CHAPTER

EIGHT

# OTP: FIPS 140-2 WITH YUBIKEY 5 FIPS SERIES

The OTP application provides two programmable slots, each of which can hold one of the types of credentials listed below. A Yubico OTP credential is programmed to slot 1 during manufacturing.

- Trigger the YubiKey to produce the credential in the first slot by briefly touching the metal contact of the YubiKey.
- If a credential has been programmed to the second slot, trigger the YubiKey to produce it by touching the contact for 3 seconds.

Output is sent as a series of keystrokes from a virtual keyboard.

## 8.1 Yubico OTP

Yubico OTP is a strong authentication mechanism that is supported by all YubiKey 5 FIPS Series. Yubico OTP can be used as the second factor in a two-factor authentication (2FA) scheme or on its own, providing single-factor authentication.

The OTP generated by the YubiKey has two parts, with the first 12 characters being the public identity which a validation server can link to a user, while the remaining 32 characters are the unique passcode that is changed each time an OTP is generated.

The character representation of the Yubico OTP is designed to handle a variety of keyboard layouts. It is crucial that the same code is generated if a YubiKey is inserted into a German computer with a QWERTZ layout, a French one with an AZERTY layout, or a US one with a QWERTY layout. The "Modhex", or Modified Hexadecimal coding, was invented by Yubico to use only specific characters to ensure that the YubiKey works with the maximum number of keyboard layouts. (USB keyboards send their keystrokes by means of "scan codes" rather than the actual character. The translation to keystrokes is done by the device to which the YubiKey is connected).

## 8.2 OTP Deployment

The YubiKey 5 FIPS Series OTP application supports two independent OTP configurations, known as OTP slots. The OTP slots can be configured to output an OTP created with the Yubico OTP or OATH-HOTP algorithm, a HMAC-SHA1 hashed response to a provided challenge or a static password. The output of OTP slot 1 is triggered by a short touch (1~3 seconds) on the gold contact and the output of OTP slot 2 is triggered by a long touch (+3 seconds).

A 6-byte access code can be set on slot 1 and slot 2 independently. Once set, the OTP slot's access code is required when modifying, overwriting or deleting the configuration on the respective OTP slot. By default, the YubiKey is shipped without any access code.

### 8.2.1 FIPS 140-2 Level 2: Placing the OTP Application in FIPS-approved Mode

Each OTP slot must be locked down with an access code for the YubiKey 5 FIPS Series OTP application to be in a FIPS-approved mode of operation. By default, no access codes is set for either slot.

- An access code must be applied to each OTP slot, either:
  - When writing a new configuration or
  - By updating an existing configuration in an OTP slot.
- An access code cannot be applied to an empty OTP slot.
- To secure an unused OTP slot, use a blank OTP configuration with an access code.
- YubiKey 5 FIPS Series devices must either be deployed with
  - The OTP slots already set with an access code, or
  - An OTP application or service which configures the access code on both slots on enrollment.
- The OTP slot access codes must be archived so that only the crypto officer alone can access them, as the access codes are used when resetting the OTP application.

#### Using the YubiKey Manager to Set Access Codes

The crypto officer can set an access code to the OTP slots using the YubiKey Manager Command Line Interface (CLI).

- Download the YubiKey Manager tool: https://www.yubico.com/products/services-software/download/yubikey-manager/
- YubiKey Manager (ykman) CLI & GUI Guide: https://docs.yubico.com/ykman/

To **apply an access code to a configuration** using the YubiKey Manager CLI, include the flag `--new-access-code=<access code>` in the OTP configuration string. The command must be of the format:

```
ykman otp settings --new-access-code=<access code> [OTP Slot]
```

where `<access code>` is the access code to be set, and [OTP Slot] is either `1` or `2` depending on if the OTP configuration is being applied to OTP slot 1 or OTP slot 2. For the characteristics of the access code, see *Credentials and Permitted Values*. For full details on setting an OTP configuration using the YubiKey Manager CLI, see the section of that name in the YubiKey Manager CLI & GUI Guide.

To **fill a blank OTP slot** with a default configuration, use the command:

```
ykman otp chalresp --generate [OTP Slot]
```

where `[OTP Slot]` is either `1` or `2` depending on if the OTP configuration is being applied to OTP slot 1 or OTP slot 2.

CHAPTER

NINE

# OATH: FIPS 140-2 WITH YUBIKEY 5 FIPS SERIES

The YubiKey 5 FIPS OATH application can store up to 32 OATH credentials, either OATH-TOTP (time-based) or OATH-HOTP (counter-based), as defined in the OATH specification. These credentials are separate from those stored in the OTP application, and can only be accessed via the CCID channel.

When an OATH-HOTP credential is programmed, the OTP is generated using the standard RFC 4226 HOTP algorithm and the YubiKey will automatically type the OTP. Optionally, the OTP can be prefixed by a public identity, conforming to the openauthentication.org Token Identifier Specification.

To manage the OATH credentials and read the OTPs generated by the YubiKey, the Yubico Authenticator is required. The Yubico Authenticator is supported on Windows, Linux, macOS, Android and iOS.

## 9.1 FIPS 140-2 Level 2: Placing the OATH Application in FIPS-approved Mode

Access to the YubiKey 5 FIPS Series OATH application must be protected with an Authentication Key for the application to be in a FIPS-approved mode of operation. To get the permitted values for the following operation, see *Credentials and Permitted Values*.

The crypto officer can set the Authentication Key using the YubiKey Manager Command Line Interface (CLI).

- Download the YubiKey Manager tool: https://www.yubico.com/products/services-software/download/yubikey-manager/
- YubiKey Manager (ykman) CLI & GUI Guide: https://docs.yubico.com/ykman/

To set an Authentication Key using the YubiKey Manager CLI, use the command:

```
ykman oath access change -n <Authentication Key>
```

where <Authentication Key> is the Authentication Key to be set.

CHAPTER

TEN

# FIDO: FIPS 140-2 WITH YUBIKEY 5 FIPS SERIES

## 10.1 FIDO U2F

FIDO U2F is an open standard that provides strong, phishing-resistant two-factor authentication for web services using public key cryptography. U2F does not require any special drivers or configuration to use, just a compatible web browser. The U2F application on the YubiKey can be associated with an unlimited number of U2F sites.

## 10.2 FIDO2

Like FIDO U2F, the FIDO2 standard offers the same high level of security, as it is based on public key cryptography. In addition to providing phishing resistant two-factor authentication, the FIDO2 application on the YubiKey enables the storage of resident credentials. As the resident credentials can accommodate the username and other data, this enables truly passwordless authentication. Keys in the YubiKey 5 FIPS Series can hold up to 25 resident keys.

### 10.2.1 Locking FIDO2 Credentials

The resident credentials can be protected by a PIN for two-factor authentication.

- The FIDO2 PIN must be between 6 and 63 alphanumeric characters in length.
- Once a FIDO2 PIN is set, it can be changed but it cannot be removed without resetting the FIDO2 application.
- If the PIN is entered incorrectly 8 times in a row, the FIDO2 application will be locked, and FIDO2 authentication will not be possible. After 3 incorrect PIN entries, the FIDO2 application must be power cycled. In order to restore this functionality, the FIDO2 application must be reset.

---

**Note:** Resetting the FIDO2 application will also reset the U2F key. No site you have registered the YubiKey with using U2F will work until the YubiKey is re-registered with that site. However, using U2F is not compatible with FIPS 140-2 Level 2.

---

**Note:** The YubiKey 5 FIPS Series supports FIOD2 credential management, thereby enabling selective deletion of resident keys. See the Enhancements to FIDO 2 Support for details.

---

The rules governing FIPS-certified environments forbid the use of the following features of the YubiKey 5 FIPS Series:

- The P-224 curve
- Credential registration over NFC.

#### Default Values

PIN: None set.

## 10.3 Placing the WebAuthn Application in FIPS-approved Mode

For the YubiKey WebAuthn application to be in a FIPS approved mode of operation, a WebAuthn PIN must be set. By default, no WebAuthn PIN is set.

To **set or change the WebAuthn PIN**, the YubiKey Manager Command Line Interface (CLI) must be used. To set an WebAuthn PIN using the YubiKey Manager CLI, use the command:

```
ykman fido access change-pin -n<PIN>
```

where <PIN> is the WebAuthn PIN to be set. Get the PIN requirements from *Credentials and Permitted Values*.

### 10.3.1 U2F

The YubiKey 5 U2F FIPS application cannot be used in a FIPS 140-2 Level 2 mode. In place of the U2F functionality, use the FIDO WebAuthn application. FIPS-certified services should not call the U2F functionality; nonetheless, the U2F function should be disabled on the YubiKey to ensure it is not used.

To disable U2F over USB and NFC, use the commands:

```
ykman config usb -dU2F ykman config nfc -dU2F
```

To **ensure users cannot enable U2F**, access to it can be secured with a management lock code. To set this code, use the command:

```
ykman config set-lock-code -n<lock code>
```

where <lock code> is a 16 byte (32 character) hex value.

---

**Note:** The lock code prevents anyone without it from changing which functions are accessible over NFC or USB. The lock code cannot be recovered if lost, which would result in a YubiKey with features permanently inaccessible.

---

CHAPTER

ELEVEN

# PIV: FIPS 140-2 WITH YUBIKEY 5 FIPS SERIES

The YubiKey 5 FIPS Series provides a PIV-compatible smart card application. PIV, or FIPS 201, is a US government standard that enables RSA or ECC sign/encrypt operations using a private key stored on a smart card through common interfaces like PKCS#11. On Windows, the smart card functionality can be extended with the YubiKey Smart Card Minidriver. The YubiKey Smart Card Minidriver is not available for Android, Linux, macOS or iOS.

Keys in the YubiKey 5 FIPS Series support extended APDUs, extended *Answer To Reset (ATR)*, and *Answer To Select* (ATS). Using the PIV APDUs on iOS requires the Yubico iOS SDK.

For YubiKey 5 FIPS Series, some exceptions apply:

- Do not use non-NIST-approved curves
- Do not use the following keys:
  - RSA 1,024-bit
  - 3,072-bit keys.

  This applies to Attestation as well.
- PIN policy = `none` cannot be used. Select either `once` or `always`.

## 11.1 Default Values

- PIN: 123456
- PUK: 12345678
- Management Key (3DES): `010203040506070801020304050607080102030405060708`

## 11.2 Supported Algorithms

The YubiKey 5 FIPS Series supports the following algorithms on the PIV smart card application.

- RSA 1024
- RSA 2048
- ECC P-256
- ECC P-384

## 11.3 Policies

### 11.3.1 PIN Policy

To specify how often the PIN needs to be entered for access to the credential in a given slot, set a PIN policy for that slot. This policy must be set upon key generation or import; it cannot be changed later.

### 11.3.2 Touch Policy

In addition to requiring the PIN, the YubiKey can require a physical touch on the metal contact. Similar to the PIN policy, the touch policy must be set upon key generation or import.

## 11.4 Slot Information

The keys and certificates for the smart card application are stored in slots, which are described below. The PIN policies described below are the defaults, before they are overridden with a custom PIN policy. **These slots are separate from the programmable slots in the OTP application.**

### 11.4.1 Slot 9a: PIV Authentication

This certificate and its associated private key is used to authenticate the card and the cardholder. This slot is used for system login, etc. To perform any private key operations, the end user PIN is required. Once the correct PIN has been provided, multiple private key operations may be performed without additional cardholder consent.

### 11.4.2 Slot 9c: Digital Signature

This certificate and its associated private key is used for digital signatures for the purpose of document, email, file, and executable signing. To perform any private key operations, the end user PIN is required. The PIN must be submitted immediately before each sign operation to ensure cardholder participation for every digital signature generated.

### 11.4.3 Slot 9d: Key Management

This certificate and its associated private key is used for encryption to assure confidentiality. This slot is used for encrypting emails or files. The end user PIN is required to perform any private key operations. Once the correct PIN has been provided, multiple private key operations may be performed without additional cardholder consent.

### 11.4.4 Slot 9e: Card Authentication

This certificate and its associated private key is used to support additional physical access applications, such as providing physical access to buildings via PIV-enabled door locks. The end user PIN is NOT required to perform private key operations for this slot.

### 11.4.5 Slots 82-95: Retired Key Management

These slots are meant for previously used key management keys to be able to decrypt earlier encrypted documents or emails.

### 11.4.6 Slot f9: Attestation

This slot is used only for attestation of other keys generated on device with instruction f9. This slot is not cleared on reset, but can be overwritten.

## 11.5 Attestation

Attestation enables you to verify that a key on the smart card application was generated on the YubiKey rather than being imported. An X.509 certificate for the key to be attested is created if the key has been generated on the YubiKey. Included in the certificate are the following extensions that provide information about the YubiKey.

### 11.5.1 Firmware

`1.3.6.1.4.1.41482.3.3`: Firmware version, encoded as three bytes. For example, 050100 indicates firmware version 5.1.0.

### 11.5.2 Serial Number

- `1.3.6.1.4.1.41482.3.7`: Serial number of the YubiKey, encoded as an integer.
- `1.3.6.1.4.1.41482.3.8`: Two bytes, the first encoding the PIN policy and the second encoding the touch policy.

#### PIN Policy

- 01 - never require PIN
- 02 - require PIN once per session
- 03 - always require PIN.

#### Touch Policy

- 01 - never require touch
- 02 - always require touch
- 03 - cache touch for 15 seconds.

#### Form Factor

`1.3.6.1.4.1.41482.3.9`: YubiKey's form factor, encoded as a one-byte octet-string.

- USB-A Keychain: 0x01
- USB-A Nano: 0x02
- USB-C Keychain: 0x03
- USB-C Nano: 0x04
- USB-C and Lightning®: 0x05
- Undefined: 0x00

## 11.6 New in YubiKey 5 FIPS Series

### 11.6.1 ATR and ATS

The ATR has been changed from "Yubikey 4" to "YubiKey" and adds support for ATS.

### 11.6.2 PIV Attestation Root CA

There are no changes in PIV attestation between the YubiKey 5 Series and the YubiKey 5 FIPS Series. You can find the root certification authority on the PIV attestation page.

## 11.7 PIV/Smart Card Deployment

The YubiKey 5 FIPS Series PIV application implements a PIV-compatible standard as defined in the NIST SP 800-73-4 publication. Access to functions on the YubiKey 5 FIPS Series PIV application is restricted by the management key, the PIN and the PUK.

The management key is used for:

- Importing or generating asymmetric key pairs
- Importing x.509 certificates and associated information
- Setting the retry counters for PIN (also requires PIN) and PUK

The PIN is used to:

- Perform cryptographic operations using private keys
- Change the PIN

The PUK is used to:

- Unblock and set a new PIN for a blocked PIN
- Change the PUK

The YubiKey 5 FIPS Series PIV application has the default values:

- Management Key `(0102030405060708010203040506070801020304050607 08)`
- PIN `(123456)`

- PUK (12345678)

### 11.7.1 FIPS 140-2 Level 2: Placing the PIV Application in FIPS-approved Mode

To place the YubiKey 5 FIPS Series PIV application in the FIPS-approved mode of operation, change the default management key, PIN and PUK.

YubiKey 5 FIPS Series devices should be deployed using a credential management tool like Microsoft ADCS with YubiKey minidriver or a third party tool. The credential management tool will replace the default values by automatically setting a random value for the management key and PUK, allowing the end user to define the PIN.

If the YubiKey 5 FIPS Series PIV application is not being managed with a credential management tool, the management key, PIN and PUK must be changed by the crypto officer. To do so, the YubiKey Manager (ykman) can be used.

- Download the YubiKey Manager tool: https://www.yubico.com/products/services-software/download/yubikey-manager/
- YubiKey Manager (ykman) CLI & GUI Guide: https://docs.yubico.com/ykman/

To **change the management key**, use the command:

```
ykman piv access change-management-key -m010203040506070801020304050607080102030405060708
/ -a<algorithm> -n<management key>
```

where <management key> is the new management key and <algorithm> is the key type [Triple-DES, AES-128, AES-192 or AES-256].

To **change the PIN**, use the command:

```
ykman piv access change-pin -P123456 -n<PIN>
```

where <PIN> is the new PIN.

To **change the PUK**, use the command:

```
ykman piv access change-puk -p12345678 -n<PUK>
```

where <PUK> is the new PUK.

CHAPTER

TWELVE

# FIPS LEVEL 1 VS FIPS LEVEL 2

The YubiKey 5 FIPS Series is certified in two modes of operations - one configuration which meets the requirements for FIPS Level 1, and a second, more restricted configuration that meets the requirements for FIPS Level 2.

The FIPS Level 2 configuration renders keys in the YubiKey 5 FIPS Series capable of being a component in a framework meeting the highest levels of authentication assurance. However, not every deployment requires this level of security. In cases where a FIPS-certified device is required, but a lower level of assurance is acceptable, the FIPS Level 1 configuration can be used. This provides a user experience like the standard YubiKey 5 Series user experience.

## 12.1 FIPS Initialization Comparison: Level 1 vs Level 2

The FIPS Level 2 requirements include all the those for Level 1. Therefore the FIPS Level 2 column in the table below lists only the differences.

| YubiKey Function | FIPS Level 1 | FIPS Level 2 |
|---|---|---|
| Touch-Triggered OTP | If writing a configuration to a slot over NFC, use a secure channel. | Set Access code for both OTP slots. If updating a configuration of either OTP slot or the NDEF behavior, use a secure channel. |
| OATH | If writing a credential over NFC, use a secure channel. | Set the Management key. When setting the Management key over USB or NFC, use a secure channel. When writing a credential over USB or NFC, use a secure channel. |
| PIV | If importing a key or setting the management key, use a secure channel. | Change Management key, PIN and PUK from default values. For any operation with the PIV function over NFC, use a secure channel. |
| U2F | No additional requirements | Must be not be used. Recommendation Disable and use the FIDO2 function instead. |
| FIDO2 | No additional requirements | Set a PIN. Set Credential Protection to level 2 for all discoverable credentials. Credential Registration is not allowed over NFC. |
| Secure Channel | Change the default transport keys from default | No additional requirements |

For more information on secure channel requirements from NIST, see NIST SP 800-63-C and NIST SP 800-63B.

CHAPTER

# THIRTEEN

# ACRONYMS AND TERMS

**3DES**
Triple Data Encryption Algorithm

**AES**
Advanced Encryption Standard

**CCC**
Card Capability Container

**CCID**
Chip card interface device, a USB protocol for a smartcard.

**CHUID**
Card Holder Unique ID

**CMS**
Credential Management System

**CN**
Common name

**CSR**
Certificate Signing Request

**CTAP**
Client Authenticator Protocols.

**ECC**
Elliptic curve cryptography

**FIDO**
Fast Identity Online

**FIPS**
Federal Information Processing Standards (US government) covering codes and encryption standards.

**HMAC**
Hash-based message authentication code

**HOTP**
HMAC-based One-Time Password algorithm

**NFC**
Near Field Communication, a type of communication interface

**OATH**
: The Initiative for Open Authentication is an organization that specifies two open authentication standards, TOTP and HOTP

**OpenPGP**
: Open standard for Pretty Good Privacy (PGP)

**OTP**
: One-Time Password

**PIV**
: Personal Identity Verification. A National Institute of Standards and Technology (NIST) standard.

**PUK**
: PIN Unlock Key

**stdin**
: standard input - usually keyboard or CLI instructions

**stdout**
: standard output - usually print to screen

**TOTP**
: Time-based One-Time Password algorithm

**U2F**
: Universal Second Factor, a FIDO Alliance standard

**WebAuthn**
: Web Authentication API for accessing public credentials

**X.509**
: The standard defining the format of a public key certificate

CHAPTER

FOURTEEN

# COPYRIGHT



## 14.1 Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners.

### 14.1.1 Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

### 14.1.2 Contact Information

Yubico Inc.
530 Lytton Street
Suite 301
Palo Alto, CA 94301
USA

More options for getting touch with us are available on the Contact page of Yubico's website.

### 14.1.3 Document Updated

2022-08-08 16:52:19 UTC