YubiKey FIPS 4 Series Technical Manual

Yubico

May 13, 2024

CONTENTS

CHAPTER

ONE

YUBIKEY FIPS 4 SERIES

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**.

1.2 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.

1.3 Compatible Devices

Before proceeding, make sure your YubiKeys are from the (4) FIPS Series, not the 5 FIPS Series. If you're not sure how to tell, look for **v5** in the laser-markings on the keys themselves. Keys with this marking belong to the 5 FIPS Series; keys without it are from the (4) FIPS Series. See below images for clarification.

The YubiKey (4) FIPS Series, to which this article applies.

The YubiKey 5 FIPS Series.

If you determine you have YubiKey 5 FIPS Series keys, please refer to YubiKey Technical Manual instead.

CHAPTER

TWO

YUBIKEY FIPS 4 SERIES OVERVIEW

The YubiKey FIPS (4 Series) are hardware authentication devices manufactured by Yubico which support one-time passwords, public-key encryption and authentication, and the Universal 2nd Factor (U2F) protocols developed by the FIDO Alliance, with Yubico as a primary contributor and thought leader.

The cryptographic functionality of the YubiKey FIPS (4 Series) devices are powered by the FIPS 140-2 certified YubiKey 4 cryptographic module, a single-chip cryptographic processor with a non-extractable key store that handles all of the cryptographic operations. The YubiKey 4 cryptographic module is FIPS 140-2 certified (Overall Level 2, Physical Security Level 3).

2.1 YubiKey FIPS (4 Series) Devices

The YubiKey 4 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 five major functions - Yubico One Time Password (OTP), FIDO Universal 2nd Factor (U2F), PIV-compatible smart card, OpenPGP smart card and OATH OTP authentication.

2.1.1 YubiKey 4 Cryptographic Module, FIPS 140-2 Certificate #: 3517

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3517

Table 1: **YubiKey FIPS (4 Series) devices covered by this Certificate**

Product Name	Description
YubiKey FIPS (4 Series)	Keychain form factor with USB-A connector
YubiKey Nano FIPS (4 Series)	Nano form factor with USB-A connector
YubiKey C FIPS (4 Series)	Keychain form factor with USB-C connector
YubiKey C Nano FIPS (4 Series)	Nano form factor with USB-C connector

All of the models in the YubiKey FIPS (4 Series) provide a USB 2.0 interface, regardless of the form factor or the USB connector. The YubiKey presents itself as a USB composite device in addition to each individual USB interface.

The YubiKey USB PID is described in the YubiKey USB ID Values guide.

2.2 YubiKey FIPS Sub-Modules

The YubiKey FIPS Series device features are implemented in five sub-modules.

Table 2: **YubiKey FIPS 4 features by sub-module**

Sub-Module	Key Features
One Time Password (OTP)	2 Slots for OTP configurations Supported protocols - Yubico OTP - OATH-HOTP - Challenge/Response HMAC-SHA1 - Static password
OATH	32 for OATH credentials Supported protocols - OATH-TOTP - OATH-HOTP Supported Algorithms - HMAC-SHA1 - HMAC-SHA256
PIV-compatible	24 slots for private keys Support Key algorithms - RSA 2048 - ECC P256 - ECC P384
OpenPGP Card	PGP Smart Card V2.0 Supported Algorithms - RSA 2048 - RSA 3072 - RSA 4096 (imported only)
FIDO U2F	FIDO U2F

CHAPTER

THREE

FIPS (4 SERIES) DEPLOYMENT CONSIDERATIONS

3.1 Introduction

Deploying the YubiKey FIPS (Federal Information Processing Standard) Series offers organizations the option of using any of the multiple protocols on the YubiKey for strong authentication. Because not all issues can be resolved by a single authentication protocol, the YubiKey FIPS Series includes PIV, OATH, YubiOTP, and FIDO U2F protocols to address a wide range of scenarios. The FIPS guidelines and requirements are designed to ensure that in a secured environment, only devices in the FIPS-approved mode are able to authenticate. To meet FIPS requirements, corporate IT staff need to work closely with their compliance department to develop and implement strong processes. The FIPS-mandated Crypto Officer role must be incorporated into online services user registration steps that meet the needs of the organization's security and business processes.

3.1.1 Audience

This document is intended for IT administrators, Crypto Officers, and compliance officers deploying FIPS Series YubiKeys in a FIPS-compliant environment. It sets out the deployment options available to individual end users and to organization admins.

The document provides guidance on the key decisions to be made when deploying YubiKeys in a FIPS-compliant environment. This document does not list the steps for technical implementation; instead, it provides links to the appropriate deployment guides. For more detailed information pertaining to FIPS YubiKeys, please review the YubiKey FIPS Series Technical Manual.

3.2 Deployment in a FIPS-Compliant Environment

Yubico's YubiKey FIPS series presents the first multiprotocol FIPS 140-2 validated security keys. These YubiKeys meet the cryptographic requirements of the NIST (National Institute of Standards and Technology) FIPS 140-2 specifications.

These keys enable strong authentication and thus greater security across multiple sites and services. To take advantage of all the protocols on the YubiKey FIPS series, it is important to understand how they fit within a FIPS-compliant environment. To be FIPS-compliant, an organization first defines its operational processes and then applies the technology so as to align with those processes.

A FIPS compliant environment requires that the role of granting permission be distinct and separate from the role of using those permissions. In order to maintain that separation, FIPS mandates that a Crypto Officer perform all registration and enrollment activities for a user.

3.2.1 FIPS-Approved Mode Default Setting

Many organizations choose to buy YubiKey FIPS series because the hardware has been certified to enable them to achieve compliance and meet the highest levels of authentication assurance (physical level 3). Tooling and deployment approaches often differ; for example, some customers may require a default U2F sub-module Admin PIN to prevent unauthorized U2F registration, while others may not. Since each customer deployment differs, FIPS mode is not enabled by default on FIPS Series YubiKeys.

In a FIPS mode of operation, every sub-module (OTP, OATH, OpenPGP, PIV and U2F) of a FIPS YubiKey must be individually placed in FIPS mode so that the capability to load or generate authentication secrets requires a PIN. Some sub-modules, such as the U2F sub-module, do not ship with a pre-defined PIN. The organization implementing FIPS YubiKeys must therefore supply the PIN as part of their initialization process. By contrast, other submodules like the YubiKey FIPS PIV are always in a FIPS-approved mode, since the Management Key, PIN and PUK are never undefined. The YubiKey FIPS Series Technical Manual provides guidance on configuring each sub-module. Yubico can provide custom configuration to improve the process. Please work with your sales representative if your organization has custom configuration needs.

Note: Resetting the U2F sub-module of the YubiKey permanently invalidates FIPS compliance for the YubiKey overall since FIPS mode for the U2F sub-module cannot be enabled after the reset. Resetting the U2F sub-module should be limited to the decommissioning process only.

The OpenPGP and PIV sub-modules on the FIPS YubiKey come with authentication codes set by default for elevated permissions, and are considered to be in a FIPS-compatible mode out of the box. To be considered to be in the FIPS-compatible mode, the OTP, OATH and U2F sub-modules must have their elevated permissions protected with authentication codes during the initialization process. It is important to note that setting the Admin PIN on the U2F sub-module will prevent registration of new U2F sites without the PIN being provided, but it is not required for authentication. Once the OATH Admin PIN is set, the OATH sub-module will require it to be provided to display the OATH codes stored within, and/or add new ones.

The table below lists the sub-modules, their respective FIPS mode defaults, and their respective Crypto Officer roles.

Table 1: **FIPS mode crypto officer roles**

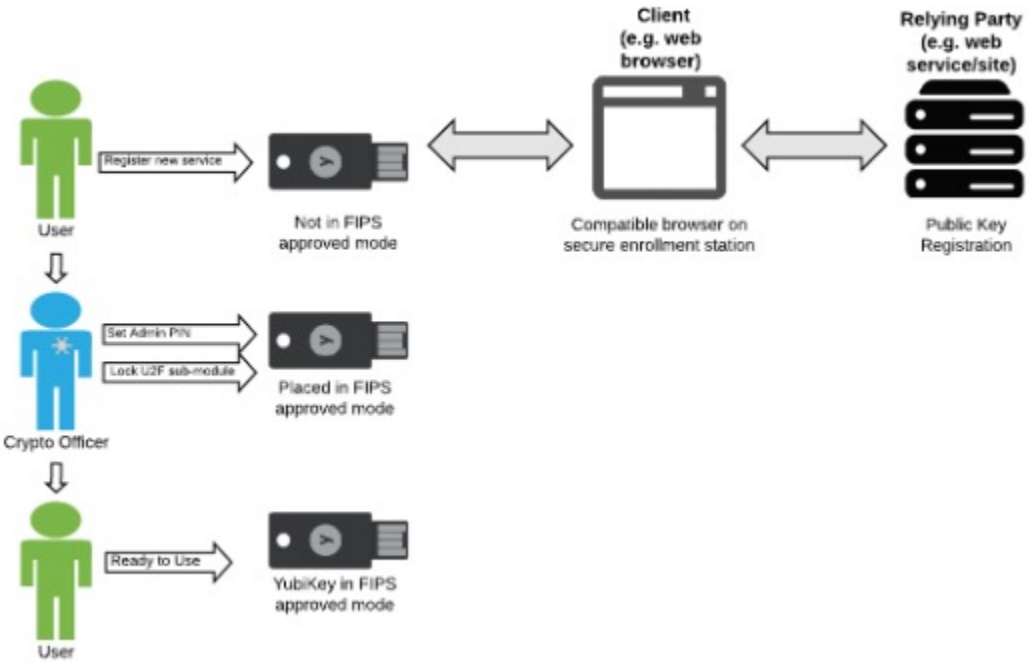
Sub-Module	Default FIPS Mode	Crypto Officer Role
PIV	Set	Manage Management key, Register new Credential(s), define PIN retries
OpenPGP	Set	Manage Admin password, Register new Credential(s), define PIN retries
OATH	Not Set	Set Authorization Password, Register new Credential(s)
OTP	Not Set	Set Admin PIN, Register new Credential(s)
U2F	Not Set	Set Admin PIN, Register new Credential(s)

3.3 Registration and Enrollment

It is important to note that once a key is in FIPS mode, the Crypto Officer must unlock the sub-module before registration can occur. For customers who are familiar with self-service registration flows, the introduction of the Crypto Officer role needs to be clearly communicated within the organization. If your organization needs to access a number of sites that do not require FIPS keys, then the case can be made for providing users with both a FIPS key and a non-FIPS key. This way end users can register themselves to sites without involving the Crypto Officer and thereby reduce operational overhead. For registration on the YubiKey FIPS series, there are a couple of approaches. The options listed below range from less restrictive to more restrictive. Work with your compliance team to determine the option that best meets your needs.

3.3.1 Option 1 - Enable FIPS-Approved Mode After Registration

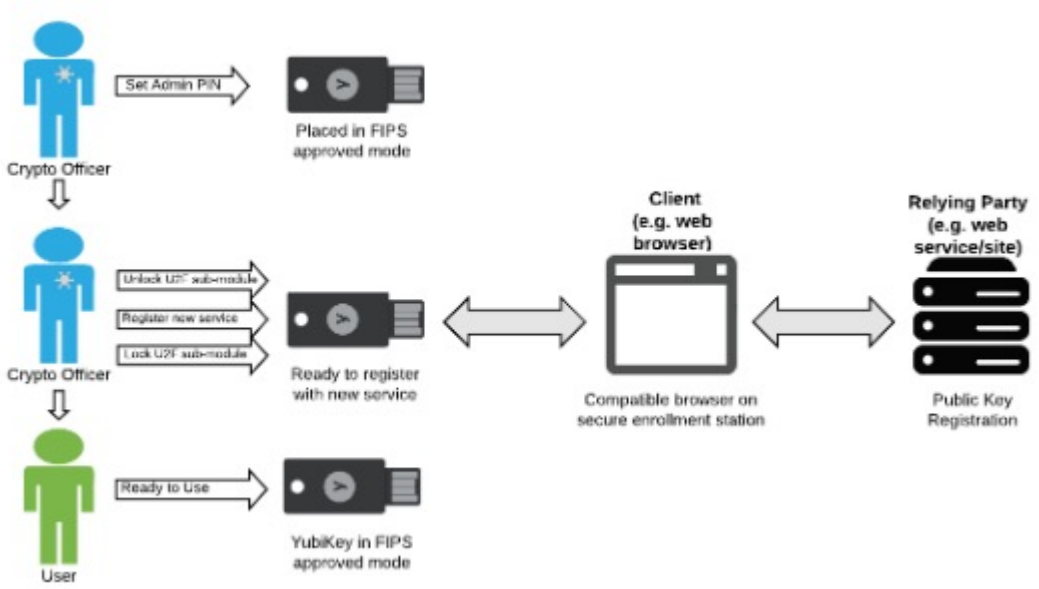
In this option, the end user is able to register the YubiKey with services. Once the end user completes their registrations, the Crypto Officer sets the sub-module's Admin PIN or passwords and locks the YubiKey. No further registrations can be performed unless the Crypto Officer unlocks the particular sub-module on the particular key.



Enable FIPS-approve mode After registration

3.3.2 Option 2 - Enable FIPS-Approved Mode Prior to Registration

In this option, the YubiKey is in FIPS-approved mode from the beginning. The Crypto Officer locks the sub-modules and registers the YubiKey with the various relying parties that the user needs to access. Once the Admin PIN and/or password is set, if registration to new sites/services is required, the Crypto Officer needs to unlock the sub-module. Depending on the service, in order to properly bind the key to the user's account, the Crypto Officer might need to have the user log into the site on a secured enrollment station prior to registering the YubiKey. Once all services are registered, the Crypto Officer will lock any unlocked sub-modules and return the key to the user who should then validate that access was set up properly.



Enable FIPS-approve mode Before registration

For both Option 1 and Option 2, after the initial registration, if the user wants to register their device to a new service, they would engage the Crypto Officer to unlock the YubiKey and register the YubiKey to the new service. Neither option is in itself preferable over the other; the preferred approach is determined by your needs. It is important to consult your compliance team before making a decision on which option is appropriate for your organization.

3.4 Authentication

Authentication for most of the protocols functions the same whether the YubiKey is in FIPS-approved mode or not. The Crypto Officer is only involved in the registration process. If the key is in FIPS-approved mode, it only needs to be unlocked for registration. It is not used for authentication.

Note: The OATH sub-module requires the Crypto Officer to be involved with the authentication process: the OATH sub-module must be unlocked by the Crypto Officer. Work with your compliance team to determine the option that best meets your needs for OATH-based authentication.

3.5 Identifying FIPS YubiKeys

The FIPS YubiKeys have "FIPS" printed on the back of the keys for easy identification. The YubiKey Manager Command Line Interface (CLI) tool can also be used to identify FIPS keys. Using the command "ykman fido info", you can identify the FIPS key and see if FIPS mode is enabled. The YubiKey manager CLI can be downloaded for Windows, Linux, and macOS at https://www.yubico.com/products/services-software/download/yubikey-manager/. Specific FIPS command instructions can be found in the YubiKey FIPS (4 Series) Technical Manual.

The FIDO U2F attestation certificate identifies the security key as an official Yubico product. Attestation is only evaluated during a registration flow and not during authentication. Furthermore, attestation can only identify YubiKey capabilities and not whether FIPS mode is enabled. The attestation certificate has limited device model information. Due to privacy concerns, the default settings for FIPS YubiKeys have no FIPS-related information. For these reasons, registering a YubiKey with a Crypto Officer becomes more important. Visit Yubico's developer U2F attestation site

for more information. Yubico can provide custom programming to meet customer attestation needs while maintaining compliance with the FIDO U2F standard. Please contact your Yubico representative for more information.

CHAPTER

FOUR

DEPLOYING YUBIKEY FIPS (4 SERIES) IN FIPS-APPROVED MODE

When using a YubiKey FIPS (4 Series) device as an authenticator in a FIPS environment, all of the sub-modules must be in a FIPS-approved mode of operation for the YubiKey FIPS (4 Series) device as a whole to be considered as operating in a FIPS-approved mode. By default, not all of the sub-modules on the YubiKey FIPS (4 Series) device are in a FIPS mode of operation. The Crypto Officer deploying the YubiKey FIPS Series (4 Series) device in a secured environment must define and supervise an initialization and delivery process which ensures that each sub-module on the YubiKey FIPS (4 Series) device is in a FIPS-approved mode of operation before being deployed to the user.

The sub-modules on the YubiKey FIPS (4 Series) device must be configured in a FIPS-approved mode; this can be done using the YubiKey Manager Command Line Interface (CLI) available in the downloads for Windows and macOS at https://www.yubico.com/products/services-software/download/yubikey-manager/.

The PIV and OpenPGP sub-modules have their respective credentials set to default values, and as such are already in a FIPS-approved mode. The OTP, OATH and U2F sub-modules must all have their respective credentials set to be in a FIPS mode. The YubiKey Manager can verify the YubiKey FIPS (4 Series) device is in a FIPS-approved mode of operation with the command:

```
ykman info
```

However, it is highly recommended that all of the credentials across all of the sub-modules are changed from the default values before the YubiKey FIPS (4 Series) device is deployed to the end user.

Table 1: **Credentials and allowed values**

Sub-module	Credential	Allowed Values	Credential owner
One Time Password (OTP)	Access Code: OTP Slot 1	6 byte access codes	Crypto Officer
	Access Code: OTP Slot 2	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 Smart Card	Admin Password (PW3)	8 to 127 byte PIN	Crypto Officer
	Reset Code (RC, Optional)	8 to 127 byte PIN	Crypto Officer
	User Password (PW1)	6 to 127 byte PIN	Authenticated User
U2F	PIN	6 to 32 byte PIN	Crypto Officer

4.1 One Time Password (OTP)

The YubiKey FIPS OTP sub-module supports 2 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 OTP slot 1's output is triggered via a short touch (1~3 seconds) on the gold contact and the OTP slot 2's is triggered via 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.

4.1.1 Placing the OTP Sub-Module in FIPS-Approved Mode

Each OTP slot must be locked down with a Access Code for the YubiKey FIPS OTP sub-module to be in a FIPS-approved mode of operation. By default, no Access Codes are set for either slot.

An Access Code must be applied to either OTP slot either when writing a new configuration or by updating the configuration in an OTP slot where one is already present. An Access Code cannot be set to an empty OTP slot. To secure an unused OTP slot, a blank OTP configuration with an Access Code must be used.

YubiKey FIPS (4 Series) devices must either be deployed with the OTP slots already set with an Access Code, or with a OTP application or service which configures the Access Code on both slots on enrollment. The OTP slot Access codes must be archived in a manner which only allows the Crypto Officer access to them, as the Access Codes are used when resetting the OTP Sub-module.

The Crypto Officer can set an Access code to the OTP slots using the YubiKey Manager Command Line Interface (CLI) available at: https://www.yubico.com/products/services-software/download/yubikey-manager/

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

```
ykman otp --access-code=<access code> [OTP configuration]
```

Where -

- `<access code>` is the Access Code to be set. The Access Code must be a hexadecimal string exactly 12 characters in length (6 bytes).
- `[OTP configuration]` is the configuration being loaded.

For full details on setting an OTP configuration using the YubiKey Manager CLI, see the YubiKey Manager documentation.

To fill a blank OTP configuration with an access code, use the command:

```
ykman otp --access-code=<access code> \

    chalresp <slot> 000000000000000000000000000000000
```

Where -

- `<access code>` is the Access Code to be set.
- `<slot>` is either `1` or `2` (without quotes) depending on if the OTP configuration is being applied to OTP slot 1 or OTP slot 2.

To apply an Access Code to an existing configuration using the YubiKey Manager CLI, use the command:

```
ykman otp --access-code=<access code> settings <slot>
```

Where -

- `<access code>` is the Access Code to be set.
- `<slot>` is the OTP slot with the existing configuration to be secured.

4.1.2 Verifying the OTP Sub-Module is in FIPS-Approved Mode

To verify the YubiKey FIPS OTP sub-module has access codes set for both OTP slots and is in a FIPS-approved mode, use the command:

```
ykman otp info
```

4.1.3 Recommended OTP Settings

YubiKey FIPS OTP sub-module will satisfy the security recommendation if the sub-module is operating in the FIPS-approved mode.

4.1.4 Resetting the OTP Sub-Module

To reset the YubiKey FIPS OTP sub-module, both OTP Slot 1 and OTP Slot 2 must be independently have their loaded configuration and encryption keys deleted. This process cannot be reversed and the OTP configurations or secrets cannot be recovered or restored. Resetting the OTP slots will remove the access code as part of the configurations for either OTP slot. To delete the configuration in an OTP slot, use the command:

```
ykman otp --access-code=<access code> delete <slot>
```

Where -

- <slot> is slot being deleted.
- <access code> is the access code for that slot. The Access Code must be provided for deleting the slots, which should be recorded and accessible by the Crypto Officer.

This command must be run for both slots to reset the YubiKey FIPS OTP sub-module.

4.1.5 User Entered Data

The YubiKey FIPS OTP sub-module will only accept user data in specific formats and lengths, dependent on the OTP configuration. The user supplied data is used to generate the OTPs supplied by the sub-module.

YubiOTP

The YubiOTP configuration will accept data in the following formats and lengths:

- **Public ID** - 1-16 byte modhex string, default 6 bytes (12 characters)
- **Private ID** - 6 byte hexadecimal string
- **AES key** - 16 byte hexadecimal string

The generated OTP codes contain the characters of the Public ID as entered, followed by a 32 character string generated as a hash of the Private ID with counter, time stamp and randomly generated data, encrypted with the provided AES key.

OATH-HOTP

The OATH-HOTP configuration will accept data in the following formats and lengths:

- **Token Identifier** - Optional 6 byte string composed of either modhex or numeric characters (12 characters).
- **Moving factor seed** - 8 byte decimal value
- **Secret key** - 20 byte hexadecimal string

The generated OTP codes contain the characters of the Token Identifier as entered if included, followed by a 6 or 8 digit numeric string generated as a truncated hash of the Secret key with the counter.

Challenge-Response

The Challenge-Response configuration will accept data in the following formats and lengths:

- **Secret key** - 20 byte hexadecimal string

The generated responses consist of a 40 character hexadecimal string generated as a HMAC-SHA1 hash of the supplied challenge and the Secret key.

Static Password

The Static Password configuration will accept data in the following formats and lengths:

- **Password** - A string of up to 38 characters as defined by the keyboard scan code ID.

The generated Static Password codes contain the characters as programed, provided that the host system is using the same keyboard layout as the system the password was programmed on.

4.1.6 OATH

The YubiKey FIPS OATH sub-module supports up to 32 OATH credentials, either OATH-HOTP or OATH-TOTP, as defined in the OATH Specification. The Yubico Authenticator is used to add or remove credentials, retrieve generated codes and optionally set an authentication key in the YubiKey FIPS OATH sub-module.

- **A 14 - 64 byte Authentication key** can be set on the OATH sub-module. Once set, the Authentication Key is required when adding, deleting and generating OATH credentials.

Placing the OATH Sub-Module in FIPS-Approved Mode

Access to the YubiKey FIPS OATH sub-module must be protected with an Authentication Key for the sub-module to be in a FIPS-approved mode of operation. By default, no Authentication Key is set.

The Crypto Officer can set Authentication Key using the YubiKey Manager Command Line Interface (CLI) available at https://www.yubico.com/products/services-software/download/yubikey-manager/.

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

```
ykman oath set-password -n <Authentication Key>
```

Where <Authentication Key> is the Authentication Key to be set. The Authentication Key must be an alphanumeric string between 14 and 64 characters in length.

Verifying the OATH Sub-Module is in FIPS-Approved Mode

Use the YubiKey Manager CLI to verify the YubiKey FIPS OATH sub-module is protected with an Authentication Key and in a FIPS-Approved mode. This can be done with the command:

```
ykman oath info
```

Recommended OATH Settings

YubiKey FIPS OATH sub-module will satisfy the security recommendation if the sub-module is operating in the FIPS-approved mode.

Resetting the OATH Sub-Module

The YubiKey FIPS OATH sub-module can be reset using the YubiKey Manager CLI. To reset the YubiKey FIPS OATH sub-module, use the command:

```
ykman oath reset
```

Resetting the YubiKey FIPS OATH sub-module will remove all loaded OATH credentials, after which they cannot be recovered or restored, as well as the Authentication Key.

User Entered Data

The YubiKey FIPS OATH sub-module will only accept user data in specific formats and lengths, dependant on the OTP configuration. The user supplied data is used to generate the OATH OTPs supplied by the sub-module, as well as identify each loaded credential.

The OATH configuration will accept data in the following formats and lengths:

- **Name** - 64 byte character string composed of alphanumeric characters.
- **Secret key** - 20 byte base32 string

The Name can be displayed, along with a 6 or 8 digit numeric string generated as a truncated hash of the Secret key with the timestamp or counter, depending on the algorithm used.

4.1.7 PIV Smart Card

The YubiKey FIPS PIV sub-module implements a PIV compatible standard as defined in the NIST SP 800-73-4 publication. Access to functions on the YubiKey FIPS PIV sub-module are 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
- Changing the PIN

The PUK is used to:

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

The YubiKey FIPS PIV sub-module has the default values:

- Management Key (010203040506070801020304050607080102030405060708)
- PIN (123456)
- PUK (12345678)

Placing the PIV Sub-Module in FIPS-Approved Mode

By default the YubiKey FIPS PIV sub-module in the FIPS-Approved mode of operation. To change the default Management Key, PIN and PUK, follow the guidance in section 2.3.4 (Recommended PIV Settings) below to secure the sub-module.

Verifying the PIV Sub-Module is in FIPS-Approved Mode

The YubiKey FIPS PIV sub-module is always in a FIPS-Approved Mode as the Management Key, PIN and PUK are never undefined.

Recommended PIV Settings

YubiKey FIPS (4 Series) devices should be deployed using a credential management tool like Microsoft ADCS with YubiKey mini-driver or 3rd party. The credential management tool will replace the default values by automatically setting a random value for the management key and PUK, and allow the end user to define the PIN.

If the YubiKey FIPS PIV sub-module 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 Command Line Interface (CLI) available at https://www.yubico.com/products/services-software/download/yubikey-manager/ can be used.

To change the Management Key, use the command:

```
ykman piv change-management-key \
      -m010203040506070801020304050607080102030405060708 \
      -n<management key>
```

Where <management key> is the new management key.

To change the PIN, use the command:

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

Where <PIN> is the new PIN.

To change the PUK, use the command:

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

Where <PUK> is the new PUK.

Resetting the PIV Sub-Module

The YubiKey FIPS PIV sub-module can only be reset if both the PIN and the PUK are blocked due to failed authentication attempts exceeding their retry counters. Once the PIN and PUK are blocked, the YubiKey FIPS PIV sub-module can be reset using the YubiKey Manager CLI with the command:

```
ykman piv reset
```

Once reset, all data within the YubiKey FIPS PIV sub-module (keys, certificates and information in other data objects) will be removed and cannot be recovered. The only exception is the attestation certificate, which will persist. Resetting the YubiKey FIPS PIV sub-module will restore the Management Key, PIN and PUK to the default values.

User Entered Data

The YubiKey FIPS PIV sub-module can be configured to hold up to 12 user uploaded x509 certificates in DER format with a maximum size of 3052 bytes each, along with associated user Data Objects. It also has 15260 bytes available for storing Certificate Chain Certificates (root and intermediate certificates).

The YubiKey FIPS PIV sub-module will accept data in the formats defined by NIST in Special Publication 800-73-4.

4.1.8 OpenPGP Smart Card

The YubiKey FIPS OpenPGP sub-module implements the OpenPGP card 2.0 specification. The functions on the OpenPGP sub-module are secured with User Password (PW1), Admin Password (PW3) and optionally the Reset Code (RC).

The Admin Password (PW3) is used for:

- Importing or generating asymmetric key pairs
- Reading from or writing to admin data objects
- Unblocking the User Password (PW1)
- Setting the Reset Code (RC)
- Setting the retry counters for PW1 and PW3

The User Password (PW1) is used for:

- Performing cryptographic operations using private keys
- Reading from or writing to user data objects

The Reset Code (RC) is used for:

- Unblocking the User Password (PW1)

The YubiKey FIPS OpenPGP sub-module has default values:

- User Password (PW1) (123456)
- Admin Password (PW3) (12345678)
- The Reset Code (RC) is optional and does not have a default value.

Placing the OpenPGP Sub-Module in FIPS-Approved Mode

By default, the YubiKey FIPS OpenPGP sub-module is in the FIPS-Approved mode of operation. To change the default User Password, Admin Password or set a Reset Code, follow the recommended OpenPGP settings to secure the sub-module.

Verifying the OpenPGP Sub-Module is in FIPS-Approved Mode

The YubiKey FIPS OpenPGP sub-module is always in a FIPS-Approved Mode as the Admin Password and User Password are never undefined.

Recommended OpenPGP Settings

YubiKey FIPS (4 Series) devices should be deployed using an OpenPGP application, such as GPG4Win, on Windows for OpenPGP card management.

The User Password (PW1) and Admin Password (PW3) must be changed from the default values. For more details on the process to change the User Password (PW1) and Admin Password (PW3) or to set a Reset Code (RC), refer to the GnuPG man pages.

Resetting the OpenPGP Sub-Module

The YubiKey FIPS OpenPGP sub-module can be reset at any time. YubiKey FIPS OpenPGP sub-module can be reset using the YubiKey Manager CLI with the command:

```
ykman openpgp reset
```

Once reset, all data within the YubiKey FIPS OpenPGP sub-module (keys and information in data objects) will be removed and cannot be recovered. Resetting the YubiKey FIPS OpenPGP sub-module will restore the Admin Password and User Password to the default values, and will remove the Reset Code if set previously.

User Entered Data

The YubiKey FIPS OpenPGP sub-module can be configured to hold a single OpenPGP RSA key with 3 subkeys, imported by the user. The user supplied data is used to provide associated information about the stored PGP key.

The OpenPGP configuration will accept data in the following formats and lengths:

- **Key** - One RSA key, up to 4096 bits (limited to 2048 on the FIPS series devices), also including the following data objects:
  - Name - 255 character UTF-8 string
  - Email - 255 character UTF-8 RFC2822 mail name-addr string
  - Comment - 255 character UTF-8 string
  - Language - 2 to 8 byte string as defined by ISO 639
  - Sex - 1 byte string as defined by ISO 5218
- **Authentication key** - One RSA sub-key, up to 4096 bits (limited to 2048 on the FIPS series devices)
- **Encryption key** - One RSA sub-key, up to 4096 bits (limited to 2048 on the FIPS series devices)
- **Signing key** - One RSA sub-key, up to 4096 bits (limited to 2048 on the FIPS series devices)

The listed data objects can be displayed when accessing the OpenPGP Applet, and are included in the OpenPGP public key when generated and exported.

4.1.9 U2F

The YubiKey FIPS U2F sub-module supports the FIDO U2F standard as defined by the FIDO Alliance U2F Specification. In addition to the functionality detailed by the FIDO U2F specification, the YubiKey FIPS U2F sub-module allows setting an Admin PIN.

Note: When set, the Admin PIN is required to register the U2F sub-module to new FIDO U2F services or accounts. Authentication to those services afterwards does not require the Admin PIN to be supplied.

Placing the U2F Sub-Module in FIPS-Approved Mode

For the YubiKey FIPS U2F sub-module to be in a FIPS-approved mode of operation, an Admin PIN must be set. By default, no Admin PIN is set. Further, if the YubiKey FIPS U2F sub-module has been reset, it cannot be set into a FIPS-approved mode of operation, even with the Admin PIN set.

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

```
ykman fido set-pin --u2f -n <Admin PIN>
```

Where <Admin PIN> is the Admin PIN to be set. The Admin PIN must be a alphanumeric string between 6 and 32 characters long.

To register a FIPS YubiKey locked with an Admin PIN, the YubiKey must first be unlocked on the host computer where the U2F registration will occur. Once unlocked, the FIPS YubiKey will allow U2F registrations until power-cycled, at which point the Admin PIN must be provided again. To unlock the U2F registration function, use the YubiKey Manager CLI with the command:

```
ykman fido unlock -P <Admin PIN>
```

Verifying the U2F Sub-Module is in FIPS-Approved Mode

Use the YubiKey Manager CLI to verify the YubiKey FIPS U2F sub-module is in a FIPS-Approved mode. This can be done with the command:

```
ykman fido info
```

If the Admin PIN is set and the YubiKey FIPS U2F sub-module has not been reset previously, then the command will indicate the U2F sub-module is in the FIPS-approved mode.

Recommended U2F Settings

YubiKey FIPS U2F sub-module will satisfy the security recommendation if the sub-module is operating in the FIPS-approved mode.

> **Warning:** The FIDO U2F Standard does not support the user entering a U2F Admin PIN at registration currently.

Resetting the U2F Sub-Module

The YubiKey FIPS U2F sub-module can be reset using the YubiKey Manager CLI. To reset the YubiKey FIPS U2F sub-module, use the command:

```
ykman fido reset
```

Resetting the YubiKey FIPS U2F sub-module will regenerate the U2F key wrapping key and thus disabling all the U2F credentials associated with the device. The device cannot be used to authenticate to previously registered U2F services or accounts. During the reset process, the U2F attestation certificate will be overwritten with a hard-coded, self-signed attestation certificate.

> **Warning:** Resetting the YubiKey FIPS U2F sub-module will prevent the sub-module to be set to the approved FIPS mode of operation afterwards. This in turn will prevent the YubiKey FIPS (4 Series) device from being set into the FIPS-approved mode overall, and it can no longer be deployed as a FIPS authenticator. Further, some U2F sites or services may not support the replacement self-signed attestation key due to requiring an attestation certificate with an verified chain to a trusted root. For U2F sites or services where this is a requirement, the reset YubiKey FIPS U2F sub-module will not be able to register or authenticate to them.

User Entered Data

The YubiKey FIPS U2F sub-module does not accept any user data which can be extracted. All keys and associated data are generated internally and only exposed to the associated service being authenticated.

U2F Attestation

The YubiKey FIPS U2F sub-module contains an attestation certificate as part of the U2F specifications. The U2F Attestation certificate for FIPS series devices with firmware 4.4.5 and above includes an Object Identifier (OID) indicating that the hardware has been FIPS 140-2 certified. The OID value for FIPS Series YubiKeys will be `1.3.6.1.4.1.41482.12`. This OID may be used during U2F registration to confirm the YubiKey being registered is a valid FIPS device by having the relying party include an attestation signature as part of the registration, then checking for this string.

CHAPTER

FIVE

COPYRIGHT

5.1 Trademarks

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

5.2 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.

5.3 Contact Information

Yubico AB
Kungsgatan 44
111 35 Stockholm
Sweden

5.4 Getting Help

Documentation is continuously updated on https://docs.yubico.com/ (this site). Additional support resources are available in the Yubico Knowledge Base.

Click the links to:

- Submit a support request
- Contact our sales team

5.5 Feedback

Yubico values and welcomes your feedback. If you think you may have discovered a flaw in our product, please submit a support request at https://support.yubico.com/hc/en-us and provide as much detail as you can.

5.6 Document Updated

2024-05-13 21:47:54 UTC