

CSPN Mode Configuration

YubiKey 5 Series

Document status

Current version	1.2
-----------------	-----

	Developer	Sponsor
Organization(s)	Yubico AB	Yubico AB

Revision history

Date	Version	Comment
2021-02-02	1.0	First version
2021-05-11	1.1	Added configuration environment
2021-09-23	1.2	Minor edits

Contents

1. Introduction	5
1.1 Scope	5
1.2 References	5
1.3 Acronyms	5
2. CSPN mode configuration	7
2.1. Listing the applications on the YubiKey 5	7
2.2. Password strength	8
2.3 Configuration environment	8
3. One time password - OTP	8
3.1 Yubico OTP	8
3.1.1. Feature summary	8
3.1.2. CSPN Approved mode	9
3.1.3. Technical configuration	9
3.2 Challenge-Response	10
3.2.1. Feature summary	10
3.2.2. CSPN Approved mode	10
3.2.3. Technical configuration	11
3.3. Static password	12
3.3.1. Feature summary	12
3.3.2. CSPN Approved mode	12
3.3.3. Technical configuration	12
3.4. OATH-HOTP	14
3.4.1. Feature summary	14
3.4.2. CSPN Approved mode	14
3.4.3. Technical configuration	14
4. OATH	15
4.1. Feature summary	15
4.2. CSPN Approved mode	16
4.3. Technical configuration	16
5. FIDO U2F	17
5.1. Feature summary	17
5.2. CSPN Approved mode	17
5.3. Technical configuration	17
6. FIDO2	18
6.1. Feature summary	18

6.2. CSPN Approved mode	18
6.2.1. FIDO2 with PIN code	18
6.2.2. FIDO2 without PIN code	18
6.3. Technical configuration	19
6.3.1. FIDO2 with PIN code	19
6.3.1.1. Set FIDO2 PIN code with YubiKey Manager	19
6.3.1.2. Set FIDO2 PIN code from the relying party	20
6.3.2. FIDO2 without PIN code	21
7. PIV	21
7.1. Feature summary	21
7.2. CSPN Approved mode	22
7.3. Technical configuration	22
7.3.1. YubiKey Manager for PIN configuration of PIV	22
7.3.2. Changing the PIN code	23
7.3.3. Changing the PUK code	23
7.3.4. Changing the management key	24

1. Introduction

1.1 Scope

The aim of this document is to describe how to configure and use the YubiKey 5 in a mode such that it is compliant with CSPN (“Certificat de Sécurité de Premier Niveau” [\[RD1\]](#)).

For each YubiKey application which will require specific configuration, there will be a short introduction, followed by the required settings to achieve the target, and finally, a technical description of the configuration itself.

1.2 References

Code	Document title	Reference
[RD1]	Certification de sécurité de premier niveau des technologies de l’information	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/
[RD2]	Certification Report BSI-DSZ-CC-0879-V4-2020	https://www.bsi.bund.de/SharedDocs/Zertifikate/CC/CC/SmartCards/IC/Cryptolib/0879_0879V2_0879V3_0879V4.html
[RD3]	FIDO2: WebAuthn & CTAP	https://fidoalliance.org/fido2/
[RD4]	NIST Special Publication 800-73 (PIV)	https://csrc.nist.gov/publications/detail/sp/800-73/4/final
[RD5]	RFC 4226, An HMAC-Based One-Time Password Algorithm	https://tools.ietf.org/html/rfc4226
[RD6]	T/Key: Second-Factor Authentication From Secure Hash Chains	https://arxiv.org/pdf/1708.08424.pdf
[RD7]	Universal 2 nd Factor (U2F) Overview	https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.html
[RD8]	W3C WebAuthn standard	https://www.w3.org/TR/webauthn-2/
[RD9]	YubiKey CSPN security target	To be provided when the CSPN security target is published

Table 1 - List of references

1.3 Acronyms

Acronym	Description
2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria

CCID	Chip Card Interface Device
CSPN	Certificat de Sécurité de Premier Niveau
CTAP2	Client to Authenticator Protocol v2
DES	Data Encryption Standard
FIDO	Fast Identity Online
HMAC	Hash-Based Message Authentication Code
HOTP	HMAC-Based One Time Password
NIST	National Institute of Standards and Technology
OATH	Open AuTHentication
OTP	One Time Password
PIV	Personal Identity Verification
PBKDF2	Password Based Key Derivation Function
PIN	Personal Identification Number
PIV	Personal Identity Verification
PUK	PIN Unblocking Key
SHA	Secure Hash Algorithm
TOTP	Time-Based One Time Password
U2F	Universal Second Factor
RFC	Request For Comments
W3C	World Wide Web Consortium

Table 2 - List of acronyms

2. CSPN mode configuration

The YubiKey 5 Series supports a variety of applications, modes and operations. Technical descriptions of all of these are available from the [Yubico website](#).

Additionally, as described in the YubiKey 5 CSPN security target [\[RD9\]](#), the YubiKey can also be used in a *CSPN approved mode* of operation.

The specific configurations required in order to achieve a CSPN approved mode are described in the sections below, divided by application.

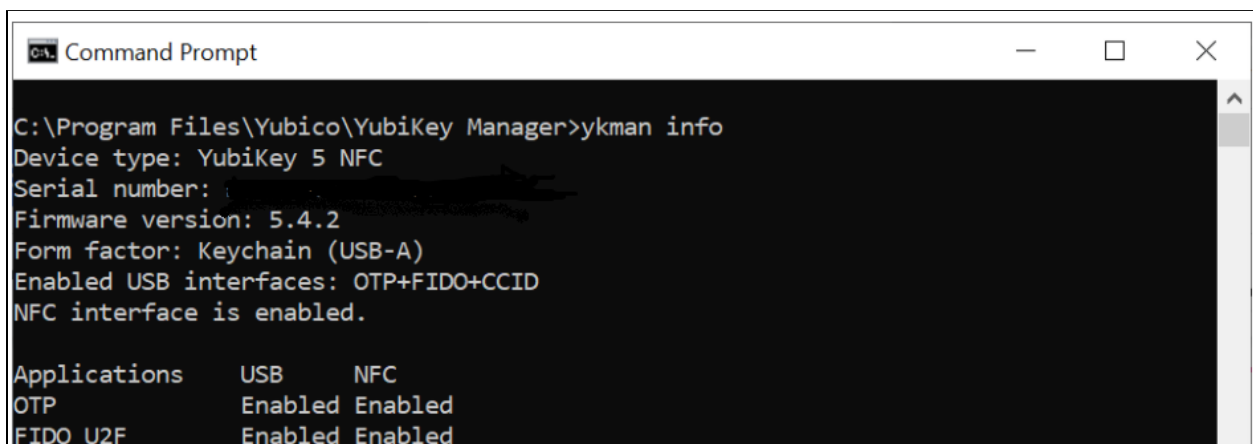
- One time password - OTP
 - [Yubico OTP](#)
 - [Challenge-Response](#)
 - [Static password](#)
 - [OATH-HOTP](#)
- [OATH](#)
- [FIDO U2F](#)
- [FIDO2](#)
- [PIV](#)

For each section there is a summary of the YubiKey application, how to operate it in a CSPN approved mode, and how the application can be technically configured.

2.1. Listing the applications on the YubiKey 5

To attain a list of all applications on the YubiKey 5, the command line [YubiKey Manager](#) (YKMan) may be used. To do so, in a command prompt, execute the command “ykman info”.

The output will contain general information about the YubiKey 5, such as the current firmware version, but also all of the available applications, both enabled and disabled. (The Security Domain application is hidden for the user and therefore not listed by YKMan.) An example of this command is shown in the screenshot below.



```
Command Prompt
C:\Program Files\Yubico\YubiKey Manager>ykman info
Device type: YubiKey 5 NFC
Serial number:
Firmware version: 5.4.2
Form factor: Keychain (USB-A)
Enabled USB interfaces: OTP+FIDO+CCID
NFC interface is enabled.

Applications      USB      NFC
OTP                Enabled Enabled
FIDO U2F           Enabled Enabled
```

Figure 1 - Example of listing the applications on a YubiKey 5

2.2. Password strength

It is highly recommended to adhere to [ANSSI's guidelines](#) on password strength whenever applicable, as it pertains to any of the YubiKey 5 applications.

2.3 Configuration environment

With regards to the configuration of the YubiKey, it can be performed in two different areas:

- If the keys of an application are generated by the secured microcontroller, the YubiKey 5 is considered as placed in a public area.
- If the keys of an application are loaded into the secured microcontroller, the YubiKey 5 is considered as placed in a secure area with restricted access.

3. One time password - OTP

The YubiKey 5 OTP application supports four protocols:

- Yubico OTP
- Challenge-Response
- Static password
- OATH-HOTP

The configuration required in order to achieve a CSPN approved mode is described in the sections below.

3.1 Yubico OTP

3.1.1. Feature summary

The Yubico OTP scheme is a proprietary algorithm based on symmetric AES encryption. To generate a Yubico OTP, the following parameters must be set:

- Public ID (1-16 bytes modhex)
- Private ID (6 bytes hexadecimal)
- Secret Key (16 bytes)

The Public ID generally represents the serial number of the YubiKey, but may be set to a different value. The Private ID is an optional secret field that may be included as an input parameter to the OTP generation algorithm. By default, when this parameter is not configured, its value is set to zero. The Secret Key is an AES-128 key which must be shared between the YubiKey 5 and the verification server by the user, during the configuration of the protocol's credentials.

The touch sensor is always used when generating a Yubico OTP, and is considered part of the standard operating procedure.

For more information about Yubico OTP, see [Yubico's website](#).

3.1.2. CSPN Approved mode

To operate the YubiKey 5 application Yubico OTP in a CSPN approved mode, the user must first be identified by a first factor authentication scheme (e.g. username/password). The details for such an authentication scheme go beyond the scope of this document however.

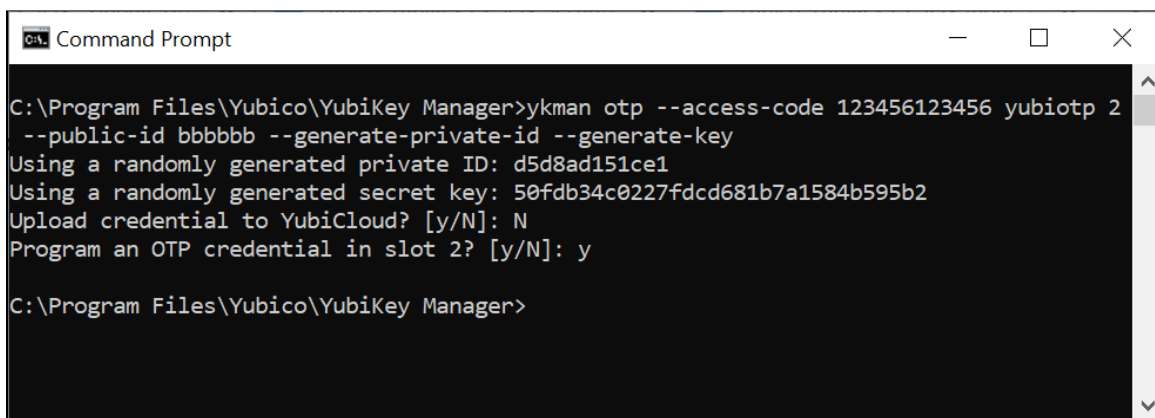
Once a Yubico OTP application has been configured, an access code must be set in order to protect the key material and configuration. More details for such a configuration are described in the section below.

3.1.3. Technical configuration

In order to protect the Yubico OTP credentials, the command line [YubiKey Manager](#) (YKMan) may be used.

The command “`ykman otp yubiotp`” should be used with the option `--access-code` for protecting the credentials. The `--access-code` parameter should be set to a six byte long hex value.

An example command line interaction for creating protected Yubico OTP credentials with YKMan is depicted in the screenshot below.



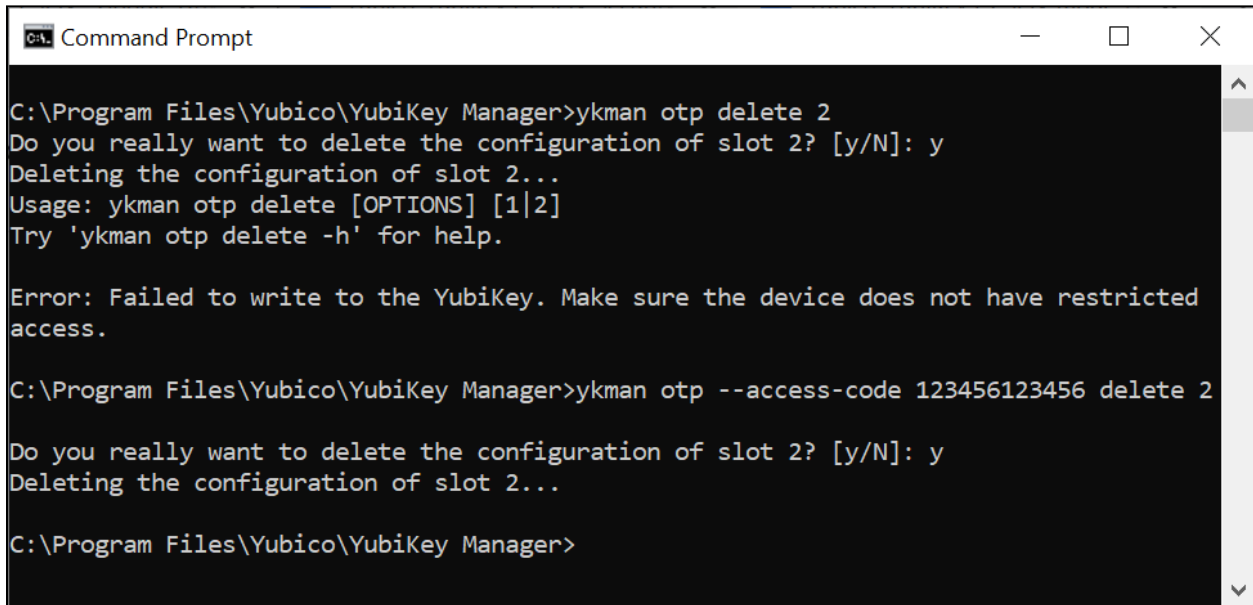
```
Command Prompt
C:\Program Files\Yubico\YubiKey Manager>ykman otp --access-code 123456123456 yubiotp 2
--public-id bbbbbb --generate-private-id --generate-key
Using a randomly generated private ID: d5d8ad151ce1
Using a randomly generated secret key: 50fdb34c0227fdcd681b7a1584b595b2
Upload credential to YubiCloud? [y/N]: N
Program an OTP credential in slot 2? [y/N]: y
C:\Program Files\Yubico\YubiKey Manager>
```

Figure 2 - Example of configuring protected Yubico OTP credentials

A code is now required for any operations that require access to the Yubico OTP credentials:

- Delete credentials: `ykman otp --access-code <value> delete [1|2]`
- Change the settings: `ykman otp --access-code <value> settings [OPTIONS] [1|2]`

For instance, it is not possible to now delete the Yubico OTP credentials without providing the correct access code. The screenshot below is another example of how to use the YkMan command line for deleting protected Yubico OTP credentials. The first attempt fails because no `--access-code` is provided, but the second attempt succeeds when the flag `--access-code` is set.



```
C:\Program Files\Yubico\YubiKey Manager>ykman otp delete 2
Do you really want to delete the configuration of slot 2? [y/N]: y
Deleting the configuration of slot 2...
Usage: ykman otp delete [OPTIONS] [1|2]
Try 'ykman otp delete -h' for help.

Error: Failed to write to the YubiKey. Make sure the device does not have restricted
access.

C:\Program Files\Yubico\YubiKey Manager>ykman otp --access-code 123456123456 delete 2
Do you really want to delete the configuration of slot 2? [y/N]: y
Deleting the configuration of slot 2...

C:\Program Files\Yubico\YubiKey Manager>
```

Figure 3 - Example of deleting protected Yubico OTP credentials

3.2 Challenge-Response

3.2.1. Feature summary

The Challenge-Response protocol is based on the HMAC-SHA-1 algorithm. The relying party sends a challenge to the YubiKey 5, and the device then responds with a hash of that challenge. The secret key used in the HMAC-SHA-1 is pre-loaded by the user onto the YubiKey 5 during configuration, and it is also possible to configure whether touching the sensor of the YubiKey 5 is required for each Challenge-Response request. The Challenge-Response protocol is used as a second factor in the authentication process.

For more information on the YubiKey application challenge-response, see [Yubico's website](#).

3.2.2. CSPN Approved mode

To operate the YubiKey 5 in a CSPN approved mode, the user must first be identified by a first factor authentication scheme (e.g. username/password). The details for such an authentication scheme go beyond the scope of this document however.

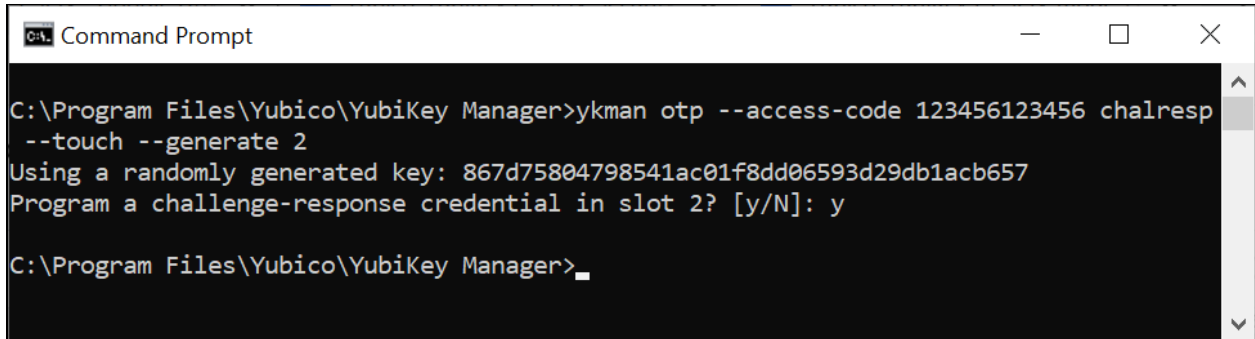
Furthermore, the usage of the YubiKey 5 touch sensor must be set to required when configuring the Challenge-Response application. Finally, when the Challenge-Response application is enabled on the YubiKey 5, an access code must be set in order to protect both the secret key and configuration. More details for such a configuration is described in the section below.

3.2.3. Technical configuration

In order to protect the Challenge-Response credentials and enforce the touch sensor, the command line [YubiKey Manager](#) (YKMan) may be used.

The command “ykman otp chalresp” should be used with the option `--access-code` for protecting the credentials and `--touch` for requesting proof of user presence. The `--access-code` parameter should be set to a six byte long hex value.

An example command line interaction for creating protected Challenge-Response credentials requiring touch with YKMan is depicted in the screenshot below.



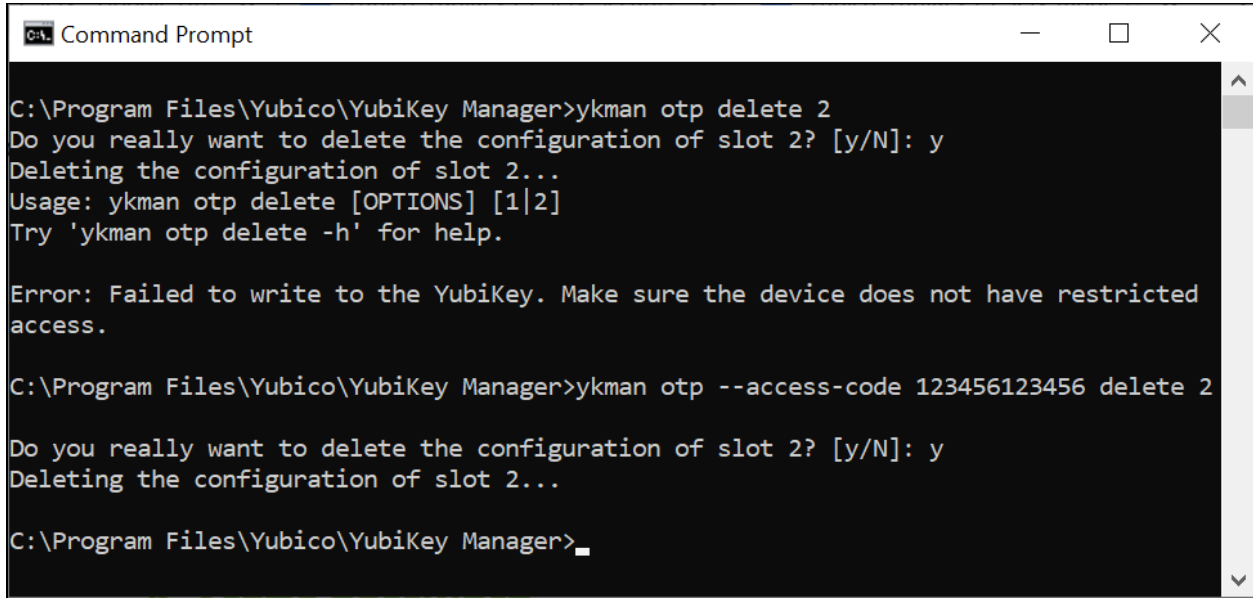
```
Command Prompt
C:\Program Files\Yubico\YubiKey Manager>ykman otp --access-code 123456123456 chalresp
--touch --generate 2
Using a randomly generated key: 867d75804798541ac01f8dd06593d29db1acb657
Program a challenge-response credential in slot 2? [y/N]: y
C:\Program Files\Yubico\YubiKey Manager>
```

Figure 4 - Example of configuring protected Challenge-Response credentials with touch sensor

A code is now required for any operations that require access to the Challenge-Response credentials:

- Delete credentials: `ykman otp --access-code <value> delete [1|2]`
- Change the settings: `ykman otp --access-code <value> settings [OPTIONS] [1|2]`

For instance, it is not possible to now delete the Challenge-Response credentials without providing the access code. The screenshot below is an example of how to use the YKMan command for deleting protected Challenge-Response credentials. The first attempt fails because no `--access-code` is provided, but the second attempt succeeds when the flag `--access-code` is set.



```
Command Prompt
C:\Program Files\Yubico\YubiKey Manager>ykman otp delete 2
Do you really want to delete the configuration of slot 2? [y/N]: y
Deleting the configuration of slot 2...
Usage: ykman otp delete [OPTIONS] [1|2]
Try 'ykman otp delete -h' for help.

Error: Failed to write to the YubiKey. Make sure the device does not have restricted
access.

C:\Program Files\Yubico\YubiKey Manager>ykman otp --access-code 123456123456 delete 2
Do you really want to delete the configuration of slot 2? [y/N]: y
Deleting the configuration of slot 2...

C:\Program Files\Yubico\YubiKey Manager>_
```

Figure 5 - Example of deleting protected Challenge-Response credentials

3.3. Static password

3.3.1. Feature summary

The static password application allows for the storage of a complete or partial static password. The password will be replayed in the clear once the user touches the YubiKey 5 sensor. The static password is used as a second factor in the authentication process.

For more information on YubiKey application for static passwords, see [Yubico's website](#).

3.3.2. CSPN Approved mode

To operate the YubiKey 5 in a CSPN approved mode, the user must only store one portion of the password within the YubiKey 5 and keep the remaining portion of the password in a different, but also secure location. The user should then reconstruct the complete password by combining the portion from the YubiKey with the other portion stored elsewhere, and then authenticate in conjunction with their username. The overall details for such a password splitting scheme go beyond the scope of this document however, as only the portion of the password to be stored within the YubiKey 5 is described.

The touch sensor is always used when displaying a portion of a static password, and is considered part of the standard operating procedure.

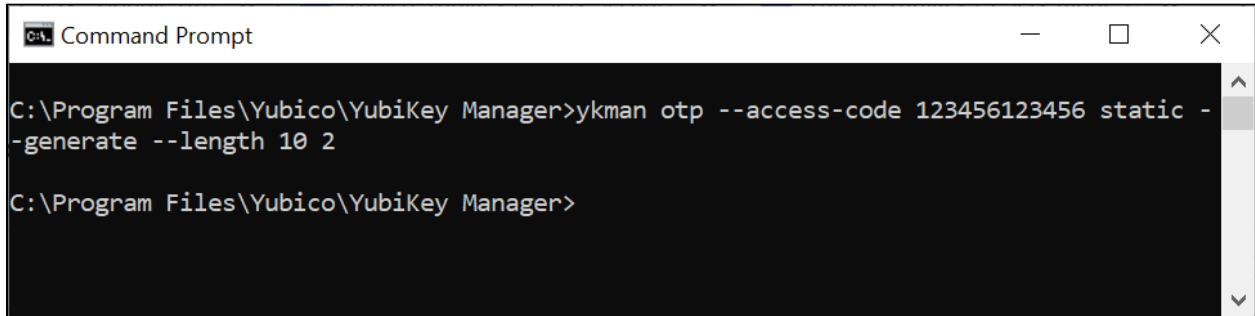
When the static password application is configured, an access code must be set in order to protect both the static password and configuration. More details for such a configuration are described in the section below.

3.3.3. Technical configuration

In order to protect the static password, the command line [YubiKey Manager](#) (YkMan) may be used.

The command “ykman otp static”, should be used with the option `--access-code` for protecting the static password. The `--access-code` parameter should be set to a six byte long hex value.

An example command line interaction for creating a protected static password with YkMan is depicted in the screenshot below.



```
Command Prompt
C:\Program Files\Yubico\YubiKey Manager>ykman otp --access-code 123456123456 static -generate --length 10 2
C:\Program Files\Yubico\YubiKey Manager>
```

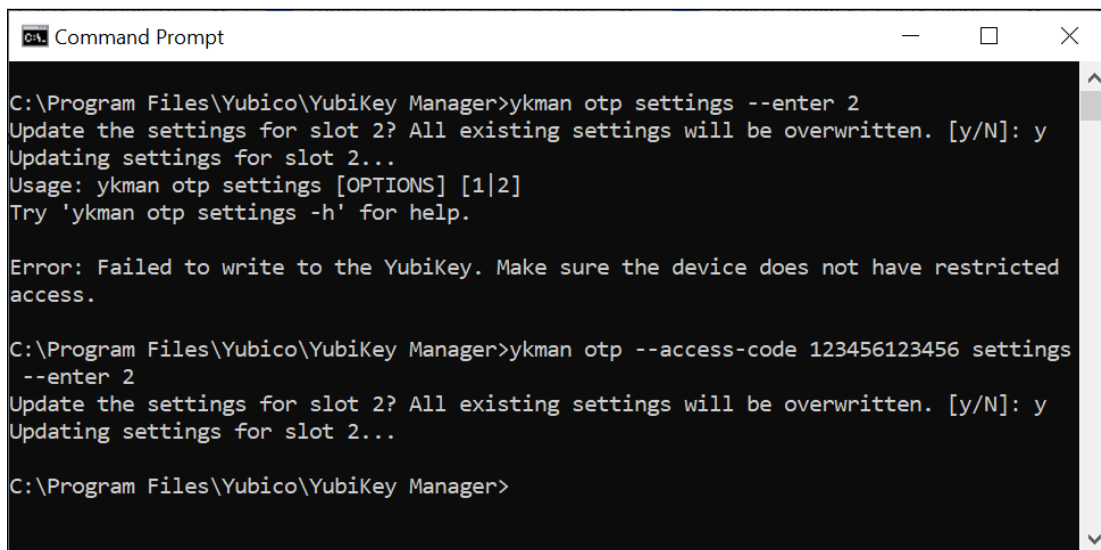
Figure 6 - Example of configuring a protected static password

A code is now required for any operations that require access to the static password:

- Delete static password: `ykman otp --access-code <value> delete [1|2]`
- Change the settings: `ykman otp --access-code <value> settings [OPTIONS] [1|2]`

For instance, it is not possible to now change the static password settings without providing the access code.

The screenshot below is an example of how to use the YkMan command line for changing the settings of a protected static password. The first attempt fails because no `--access-code` is provided, but the second attempt succeeds when the flag `--access-code` is set.



```
Command Prompt
C:\Program Files\Yubico\YubiKey Manager>ykman otp settings --enter 2
Update the settings for slot 2? All existing settings will be overwritten. [y/N]: y
Updating settings for slot 2...
Usage: ykman otp settings [OPTIONS] [1|2]
Try 'ykman otp settings -h' for help.

Error: Failed to write to the YubiKey. Make sure the device does not have restricted access.

C:\Program Files\Yubico\YubiKey Manager>ykman otp --access-code 123456123456 settings --enter 2
Update the settings for slot 2? All existing settings will be overwritten. [y/N]: y
Updating settings for slot 2...

C:\Program Files\Yubico\YubiKey Manager>
```

Figure 7 - Example of changing a protected static password

3.4. OATH-HOTP

3.4.1. Feature summary

The OATH-HOTP protocol is implemented according to RFC 4226, i.e. “An HMAC-Based One-Time Password Algorithm”, [\[RD5\]](#). The algorithm underpinning this application on the YubiKey 5 is HMAC-SHA-1. The user may choose the length of the OTP (either 6 or 8 digits) and the initial counter value. The OATH-HOTP protocol is used as a second factor in the authentication process.

The touch sensor is always used when generating the OATH-HOTP, and is considered part of the standard operating procedure.

For more information on the YubiKey application OATH-HOTP see [Yubico’s website](#).

3.4.2. CSPN Approved mode

To operate the YubiKey 5 in a CSPN approved mode, the user must first be identified by a first factor authentication scheme (e.g. username/password). The details for such a first factor authentication scheme go beyond the scope of this document however.

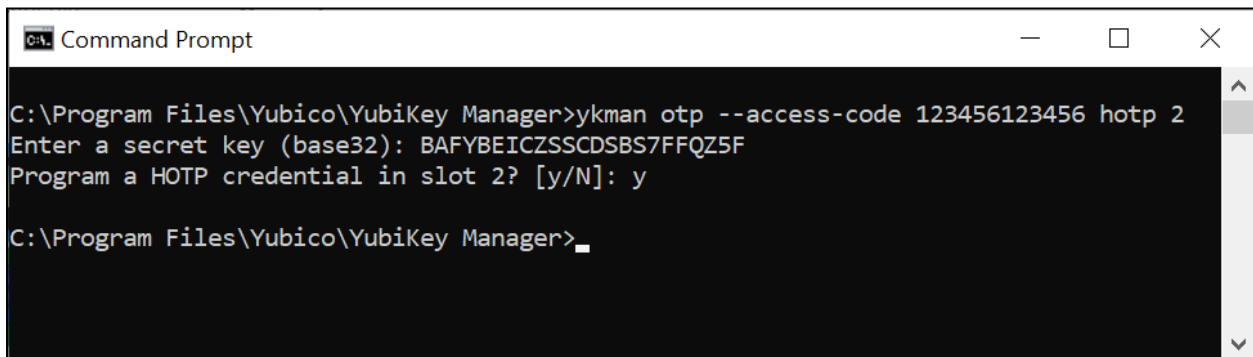
When the OATH-HOTP application is enabled on the YubiKey 5, an access code must be set to protect the initial counter value and configuration. More details for such a configuration are described in the section below.

3.4.3. Technical configuration

In order to protect the OATH-HOTP credentials, the command line [YubiKey Manager](#) (YkMan) may be used.

The command “`ykman otp hotp`” should be used with the option `--access-code` for protecting the OATH-HOTP credentials. The `--access-code` parameter should be set to a six byte long hex value.

An example command line interaction for creating a protected OATH-HOTP with YKMan is depicted in the screenshot below.



```
Command Prompt
C:\Program Files\Yubico\YubiKey Manager>ykman otp --access-code 123456123456 hotp 2
Enter a secret key (base32): BAFYBEICZSSCDSBS7FFQZ5F
Program a HOTP credential in slot 2? [y/N]: y
C:\Program Files\Yubico\YubiKey Manager>
```

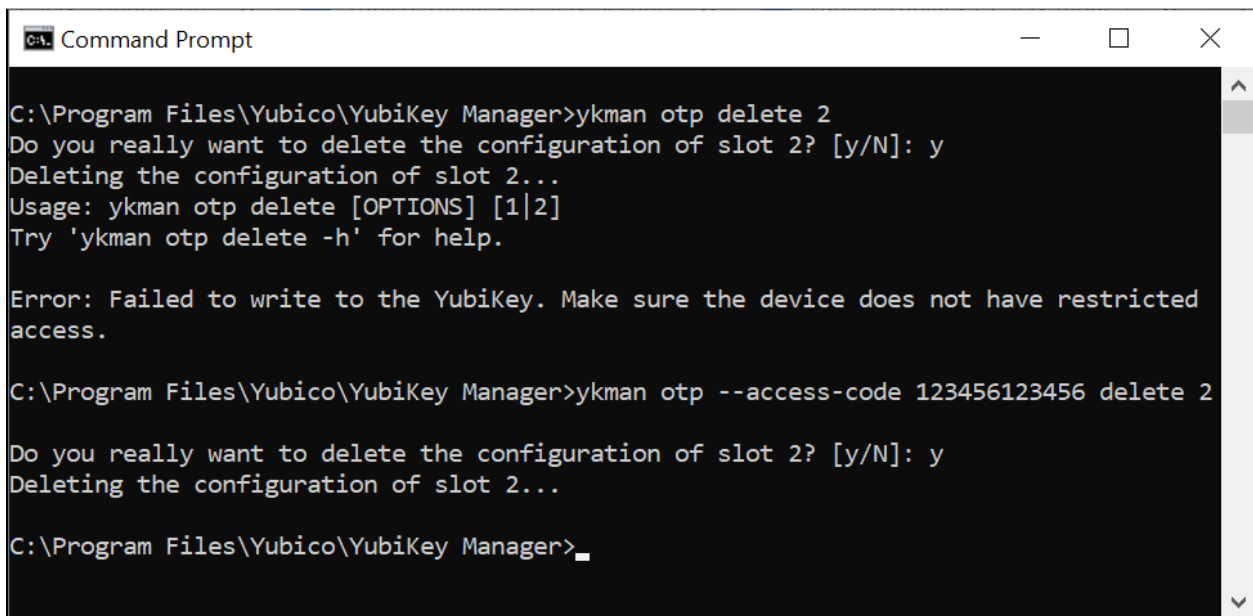
Figure 8 - Example of configuring protected OATH-HOTP credentials

A code is now required for any operations that require access to the OATH-HOTP credentials:

- Delete credentials: `ykman otp --access-code <value> delete [1|2]`
- Change the settings: `ykman otp --access-code <value> settings [OPTIONS] [1|2]`

For instance, it is not possible to now delete the OATH-HOTP credentials without providing the access code.

The screenshot below is an example of how to use the YkMan command line for deleting protected OATH-HOTP credentials. The first attempt fails because no `--access-code` is provided, but the second attempt succeeds when the flag `--access-code` is set.



```
Command Prompt
C:\Program Files\Yubico\YubiKey Manager>ykman otp delete 2
Do you really want to delete the configuration of slot 2? [y/N]: y
Deleting the configuration of slot 2...
Usage: ykman otp delete [OPTIONS] [1|2]
Try 'ykman otp delete -h' for help.

Error: Failed to write to the YubiKey. Make sure the device does not have restricted
access.

C:\Program Files\Yubico\YubiKey Manager>ykman otp --access-code 123456123456 delete 2
Do you really want to delete the configuration of slot 2? [y/N]: y
Deleting the configuration of slot 2...

C:\Program Files\Yubico\YubiKey Manager>
```

Figure 9 - Example of deleting protected OATH-HOTP credentials

4. OATH

4.1. Feature summary

The OATH application allows for managing two types of OTP over the CCID interface:

- HMAC-Based One Time Password (HOTP)
- Time-Based One Time Password (TOTP)

A maximum of 32 credentials¹ can be stored within the YubiKey's OATH application. The software tool [Yubico Authenticator](#) may be used to configure and use this application.

¹ A credential is a configuration of the OTP linked to a unique key.

A password may also be set to protect the OATH credentials, and if this is configured, the password will be required to unlock the application, which can then be used to generate any number of OTPs for the remainder of the session (i.e. until application is deselected).

During the enrollment of credentials, it is also possible to configure whether touching the sensor of the YubiKey 5 is required for each OTP generation.

4.2. CSPN Approved mode

The OATH-HOTP/TOTP protocol is used as a second factor in the authentication process. To operate the YubiKey 5 in a CSPN approved mode, the user must first be identified by a first factor authentication scheme (e.g. username/password). The details for such a first factor authentication scheme go beyond the scope of this document however.

When the OATH-HOTP/TOTP application is enabled on the YubiKey 5, a password can also be set to protect the OATH credentials. More details for such a configuration are described in the section below.

4.3. Technical configuration

In order to protect the OATH-HOTP/TOTP credentials with a password, the [Yubico Authenticator](#) should be installed and used for the configuration.

In order to set the password, launch the [Yubico Authenticator](#) application, select File from the menu and finally the option Set Password. In the dialog box that appears, enter a new password and confirm it. This configuration will protect all OATH-HOTP/TOTP credentials with the same nominated password.

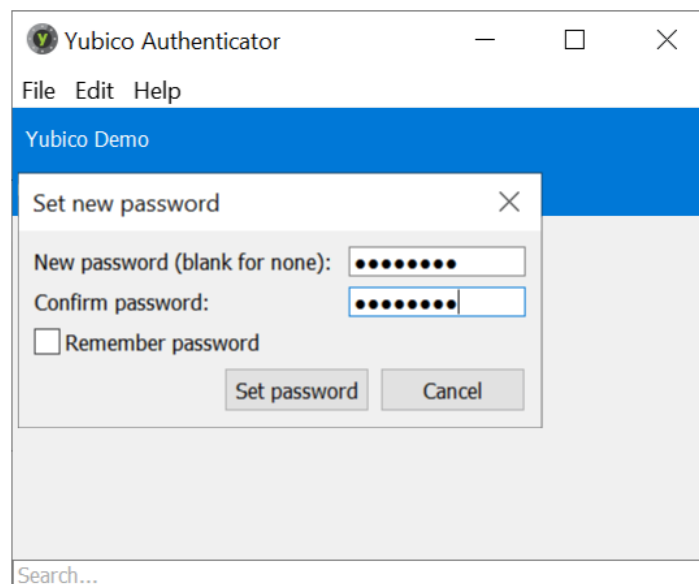


Figure 10 - Example of protecting the OATH-HOTP/TOTP credentials with a password

When [Yubico Authenticator](#) is used for generating an OATH one-time password, the user must enter the password each time in order to unlock the credentials.

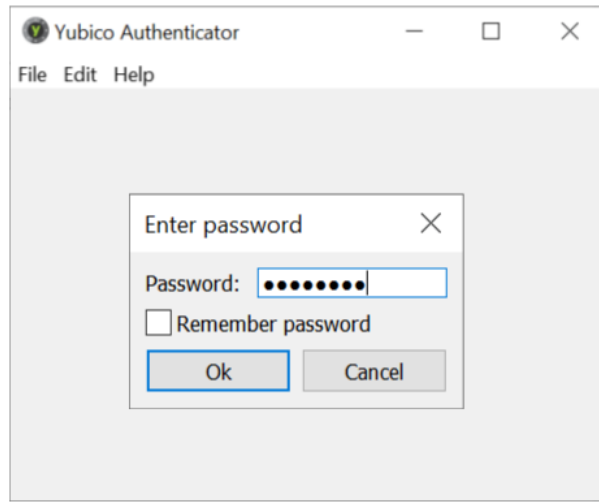


Figure 11 - Example of unlocking the OATH-HOTP/TOTP credentials

5. FIDO U2F

5.1. Feature summary

The YubiKey 5 Series supports FIDO Universal 2nd Factor (U2F), which is defined in [\[RD7\]](#). On a high level, the FIDO U2F protocol comprises both the registration and the authentication process but is only used as a second factor in the authentication process.

For more information on the YubiKey application FIDO U2F see [Yubico's website](#).

5.2. CSPN Approved mode

To operate the YubiKey 5 in a CSPN approved mode, the user must first be identified with a first factor authentication scheme (e.g. username/password) according to the FIDO U2F standard [\[RD7\]](#). The details for such a first factor authentication scheme go beyond the scope of this document however.

As part of the registration process, the user must touch the YubiKey 5 sensor when the browser or application prompts for it. Furthermore, the user must also touch the YubiKey 5 when the browser or application requests for it during the authentication process.

5.3. Technical configuration

No additional configuration is needed to achieve a CSPN approved mode, assuming the YubiKey 5 has been correctly enrolled against a U2F compatible relying party.

6. FIDO2

6.1. Feature summary

The FIDO2 protocol is an amalgamation of two standards: W3C WebAuthn (for the communication between the client and the relying party) and CTAP2 (for accessing the authenticator from the client). On a high level, the FIDO2 protocol comprises both the registration and the authentication process.

FIDO2 is an update of FIDO U2F and is defined in [\[RD3\]](#). It takes into account PIN management, in addition to the new standardized protocols, WebAuthn [\[RD8\]](#) and CTAP2.

6.2. CSPN Approved mode

The FIDO2 protocol can be used in two different CSPN modes of operation:

- FIDO2 with a PIN code set on the YubiKey 5 (see [section 6.2.1](#)), or
- FIDO2 without a PIN code set on the YubiKey 5 (see [section 6.2.2](#))

6.2.1. FIDO2 with PIN code

If WebAuthn User Verification is set to 'Required' by the WebAuthn relying party when the user registers the YubiKey 5 as a FIDO2 device, it will prompt the user's client to protect the FIDO2 credentials with a PIN code during the enrollment. Alternatively, the user may also use [YubiKey Manager](#) to set a PIN code which will protect the FIDO2 credentials. In both cases, the YubiKey 5 will require the user to enter a PIN code when using it for FIDO2 authentication.

As part of the registration process, the user must touch the YubiKey 5 sensor when the browser or application prompts for it. Furthermore the user must also touch the YubiKey 5 when the browser or application requests for it during the authentication process.

6.2.2. FIDO2 without PIN code

If WebAuthn User Verification is not enforced as recommended above, the YubiKey 5 must then be used as a second factor authentication device. To operate the YubiKey 5 in a CSPN approved mode under such a scenario, the user must first be identified with a first factor authentication scheme (e.g. username/password). The details for such a first factor authentication scheme go beyond the scope of this document however.

The YubiKey 5 will, by default, require the sensor to be touched for this configuration. As part of the registration process, the user must touch the YubiKey 5 sensor when the browser or application prompts for it. Furthermore, the user must also touch the YubiKey 5 when the browser or application requests for it during the authentication process.

6.3. Technical configuration

6.3.1. FIDO2 with PIN code

There are two ways to set the PIN code for the FIDO2 application on a YubiKey 5:

- The user can set the PIN code by using the tool [YubiKey Manager](#)
- The relying party (server application) can request the user's client to set the PIN code during the WebAuthn registration

In addition to the PIN being set on the YubiKey, the touch sensor is required by default for FIDO2.

6.3.1.1. Set FIDO2 PIN code with YubiKey Manager

The [YubiKey Manager](#) may be used to set a PIN code for the FIDO2 credentials on the YubiKey 5. When a PIN code is set, all FIDO2 credentials will be protected by the same PIN code. In order to set the PIN code with [YubiKey Manager](#), select the Applications from the menu and then the FIDO2 option. In the resulting GUI which appears, press the button "Set PIN".

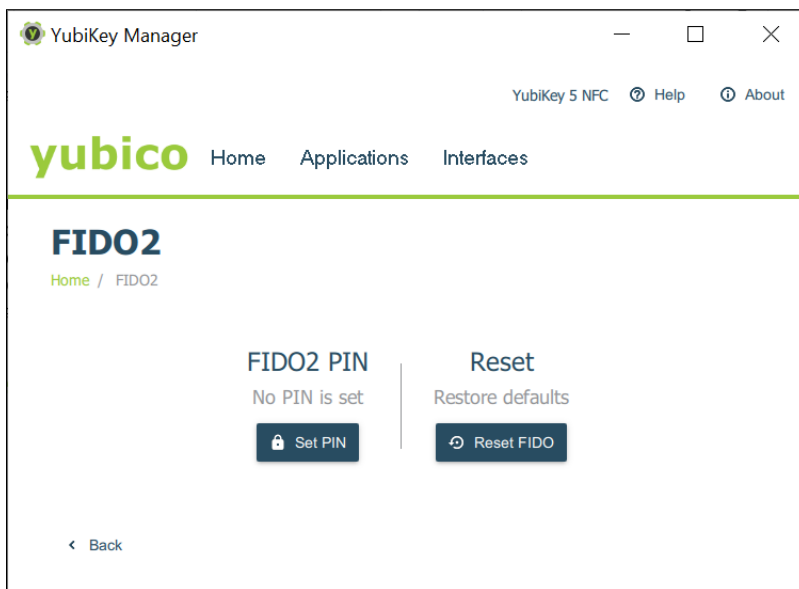


Figure 12 - Configuring the FIDO2 PIN with YubiKey Manager

In the next popup which appears, the user is prompted to set the new PIN and to confirm this PIN for the FIDO2 application.

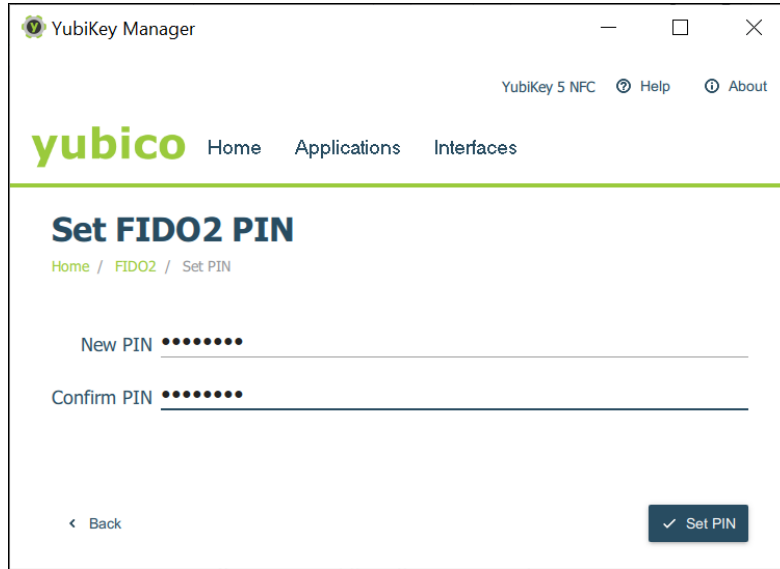


Figure 13 - Configuring the FIDO2 PIN with YubiKey Manager

6.3.1.2. Set FIDO2 PIN code from the relying party

The WebAuthn relying party (authentication server) can instruct a client to set the PIN code on an authenticator during the enrollment of the FIDO2 credentials.

A client, according to the WebAuthn/FIDO2 specifications, is any user device that supports WebAuthn/FIDO2. In practice, this is a hardware device (smartphone, tablet, laptop, etc), an operating system (Microsoft Windows, Apple MacOS, Apple iOS, Android, Linux, etc) or a web browser (Google Chrome, Apple Safari, Microsoft Edge, Mozilla Firefox, etc).

If the WebAuthn MakeCredentials parameter UserVerification is set to 'Required', this will prompt the client to set the PIN code on the YubiKey 5.

The GUI for setting the FIDO2 PIN code may differ between clients. The image below is an example of using Google Chrome with Windows 10 for setting the FIDO2 PIN on a YubiKey 5.

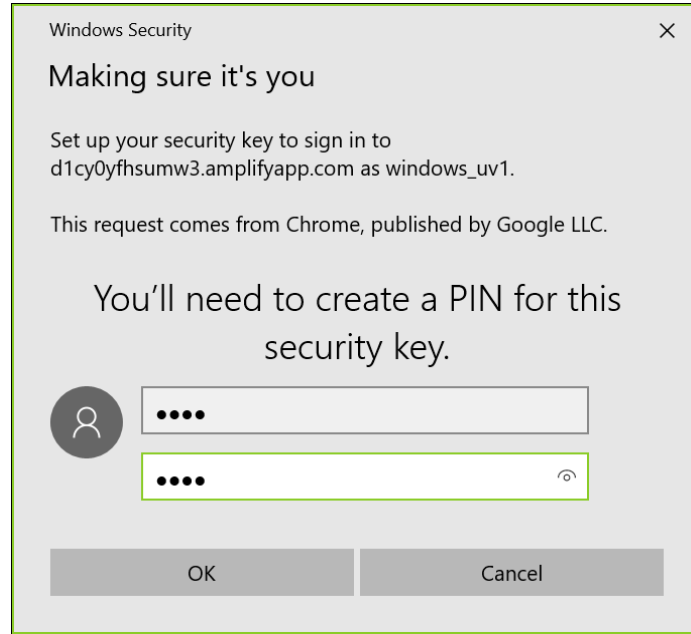


Figure 14 - Configuring the PIN code for FIDO2 with Windows 10

6.3.2. FIDO2 without PIN code

If the relying party has set the WebAuthn MakeCredentials parameter UserVerification to 'Discouraged', this will not trigger the client to set any FIDO2 PIN code on the YubiKey 5. Furthermore, if no FIDO2 PIN is set by using the [YubiKey Manager](#), then there will be no PIN set to protect the FIDO2 credentials.

However, touch will still be required, by default, for using the FIDO2 credentials during WebAuthn authentication.

When the PIN code is disabled for FIDO2 on the YubiKey 5, the CSPN approved mode is achieved by using a first factor authentication protocol in conjunction with the YubiKey 5 configured for FIDO2 and touch.

7. PIV

7.1. Feature summary

The PIV application [RD4] can be used to authenticate, sign and decrypt. The user may, for example, use the YubiKey 5 PIV application for Windows smart card logon.

The PIV application allows for generating or importing asymmetric key-pairs (both RSA or ECC) and to store multiple X.509 certificates. In total, 24 certificate slots are available:

- Slot 9a: PIV Authentication
- Slot 9c: Digital Signature
- Slot 9d: Key Management

- Slot 9e: Card Authentication
- Slots 82-95 (hexadecimal): Retired Key Management
- Slot f9: Attestation

User verification under PIV is achieved with a PIN and a management key (Triple-DES or AES key) is used for various oversight functions. The PIN must be set to a value between 6 and 8 bytes, while the maximum number of retries must be set in the range of 1 to 255 with a default value of 3.

To specify how often the PIN needs to be entered in order to access the credentials in a given slot, a PIN policy should be set for that slot. This policy must be set upon key generation or when a key is imported, and cannot be changed at a later time.

In addition to requiring the PIN, the YubiKey 5 may also be configured to require physical contact of the touch sensor. Similar to the PIN policy, the touch policy must be set upon key generation or import.

7.2. CSPN Approved mode

To operate the YubiKey's PIV application in CSPN approved mode, the PIN code, PUK code and management key must be set for the PIV application. It is imperative that the default values of these codes are also changed by the user before using the PIV application.

More details for such a configuration are described in the section below.

7.3. Technical configuration

7.3.1. YubiKey Manager for PIN configuration of PIV

The [YubiKey Manager](#) may be used for setting the PIN, PUK and management key on the YubiKey. In this scenario, a YubiKey 5 with default settings is assumed.

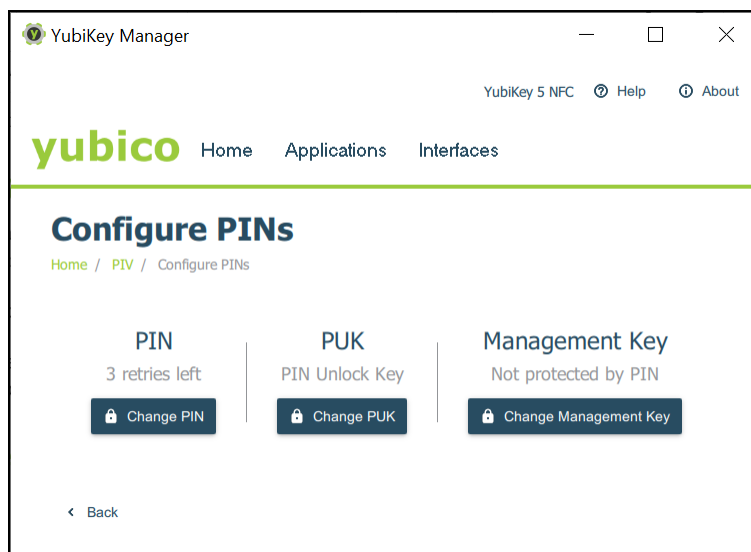


Figure 15 - Configuring the PIN, PUK and management key for PIV

7.3.2. Changing the PIN code

The PIN is used during normal operation to authorize an action such as creating a digital signature with any of the stored keys. Entering an incorrect PIN too many times, which exceeds the retry counter, will cause the PIN to become blocked, thereby rendering the PIV features unusable. The PIN must be at least 6 characters and can contain any symbol, although for cross-platform portability it is recommended to only use decimal digits. There is a limit of 8 bytes for a PIN, which allows for up to 8 ASCII characters. By default the PIN code is set to “123456”.

The PIN code is changed by pressing the “Change PIN” button in the “Configure PINs” dialog box. The resulting popup which will appear in [YubiKey Manager](#), is pictured below.

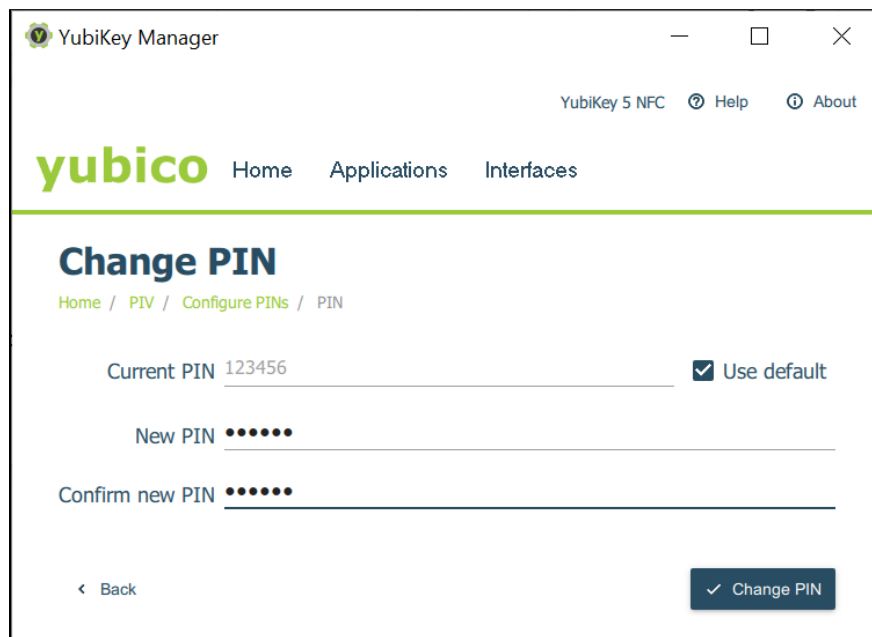


Figure 16 - Changing the PIN code for PIV

The current (default) PIN must be changed to a new PIN with a length of 6-8 digits. The user must enter the current PIN, nominate a new PIN, confirm it, and then press the “Change PIN” button.

The default PIN code mentioned above is pre-configured for slots 9a, 9c and 9d. With regards to slot 9e, the PIN policy needs to be set to enforced with the command line tool YubiKey Manager when generating or importing the key-pair on the YubiKey 5. An example of how to set the PIN policy when using the command line tool YubiKey Manager with the parameter `--pin-policy` is shown below:

```
ykman piv generate-key --pin-policy always 9e -
```

7.3.3. Changing the PUK code

The PUK can be used to reset the PIN if it is ever forgotten, lost or becomes blocked after the maximum number of incorrect attempts by the user. By default the PUK is set to “12345678”.

The PUK is changed by pressing the “Change PUK” button in the “Configure PINs” dialog box. The resulting popup which will appear in [YubiKey Manager](#), is pictured below.

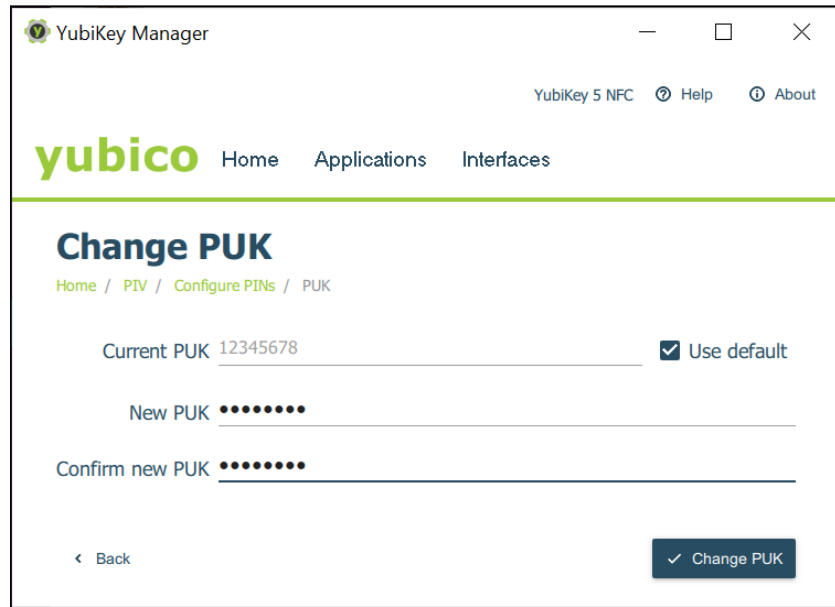


Figure 17 - Changing the PUK code for PIV

The current (default) PUK must be changed to a new PUK with a length of 6-8 digits. The user must enter the current PUK, the new PUK, confirm it, and then press the “Change PUK” button.

7.3.4. Changing the management key

All PIV management operations of the YubiKey require a 24 byte 3DES or AES key, known as the management key. By default the management key is set to “010203040506070801020304050607080102030405060708”. The user should explicitly set a 24 byte key (the YubiKey PIV Manager can also generate one).

The management key is changed by pressing the “Change Management Key” button in the “Configure PINs” dialog box. The resulting popup which will appear in [YubiKey Manager](#), is pictured below.

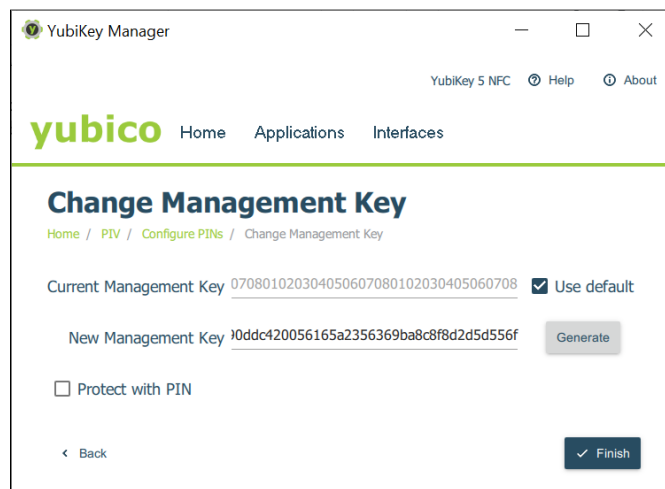


Figure 18 - Changing the management key for PIV

The current (default) management key must be changed to a new management key with a length of 48 hexadecimal digits. The user must enter the current management key, the new management key, and press the “Change management key” button.