

CSPN Security Target

YubiKey 5 Series

Document status

Current version	1.3
-----------------	-----

	Developer	Sponsor	Evaluator
Organization(s)	Yubico AB	Yubico AB	Serma Safety & Security

Distribution

Name or role	Organization
Developer	Yubico AB
Evaluator	Serma Safety & Security
Certifier	ANSSI

Revision history

Date	Version	Comment
2019-08-23	0.1	Initial version
2019-09-06	0.2	Modifications following Yubico and Serma discussions
2019-09-20	0.3	Modifications following Yubico comments
2019-09-26	0.4	Modifications following Serma internal comments
2019-10-04	0.5	Modifications following Yubico comments
2019-10-14	0.6	Modifications following Yubico comments
2019-10-15	0.7	Updated to Yubico document layout
2019-10-18	0.8	Language and editorial updates
2019-10-21	0.81	Minor edits
2019-10-23	1.0	Final version for YubiKey v5.2.4
2020-11-03	1.1	Updates for YubiKey v5.4.1
2020-11-25	1.2	Modifications following Serma's comments
2020-12-01	1.2.1	Updated to YubiKey v5.4.2
2020-12-11	1.2.2	Minor edits
2020-12-22	1.2.3	Final version for YubiKey v5.4.2
2021-01-12	1.2.4	Minor edits
2021-01-15	1.2.5	Minor edits
2021-01-21	1.2.6	Clarifications to CSPN mode, renamed YubiCrypt to YubiHSM Auth, updated references
2021-01-26	1.2.7	Minor edits
2021-02-02	1.3	Final version for the CSPN evaluation

2021-04-23	1.3.1	Minor edits
------------	-------	-------------

Contents

1. Introduction	6
1.1 References	6
1.2 Acronyms	7
2. Product description	8
2.1 YubiKey form factors	8
2.2 Supported authentication protocols	8
2.3 YubiKey architecture	9
2.4 YubiKey 5 software tools	11
2.5 YubiKey cryptographic algorithms	12
2.6 Applications	12
2.6.1 One Time Password - OTP	13
2.6.1.1 Yubico OTP	13
2.6.1.2 Yubico OTP	13
2.6.1.3 Challenge-Response	14
2.6.1.4 Static password	14
2.6.1.5 OATH-HOTP	15
2.6.2 FIDO U2F	15
2.6.3 FIDO2	15
2.6.4 Security Domain	16
2.6.5 PIV	16
2.6.6 OpenPGP	17
2.6.7 OATH	17
2.6.8 YubiHSM Auth	18
3. Target of evaluation	18
3.1 TOE configuration	18
3.2 Configuration environment	18
3.3 Operating environment	19
3.4 Product assets	19
4. Threat description	20
4.1 Attacker's profile	20
4.2 Threat 1: Bypassing the access control	20
4.3 Threat 2: Recover the PIN/password	20
4.4 Threat 3: Recover the secret keys	20
4.5 Threat 4: Perform an authentication without access to the YubiKey	20
5. Security functions	21
5.1 SF1: True Random Number Generator (TRNG)	21

5.2 SF2: User authentication mechanism	21
5.3 SF3: Data storage	22
5.4 SF4: Cryptographic operations	22
5.5 SF5: Physical access to the YubiKey 5	22
5.6 Coverage of threats	23
6. Annex: Critical security parameters	24
7. Annex: Strengths of access control mechanisms	27

1. Introduction

The aim of this document is to describe the *security target* of the YubiKey 5 Series to be used towards the assessment of obtaining a CSPN (“Certificat de Sécurité de Premier Niveau” [RD1]). It should be highlighted that the YubiKey 5 Series supports a *variety* of modes and operations, thus the device must be configured according to the guidelines as stated in this security target in order to achieve a *CSPN Approved mode* of operation valid for CSPN.

1.1 References

Code	Reference	Name
[RD1]	ANSSI-CSPN-CER-P-01/1.1	Certification de sécurité de premier niveau des technologies de l’information
[RD2]	https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/SmartCards_IC_Cryptolib/0879_0879V2_0879V3_0879V4.html	Certification Report BSI-DSZ-CC-0879-V3-2018
[RD3]	https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.html	Universal 2 nd Factor (U2F) Overview
[RD4]	https://www.w3.org/Submission/2015/SUBM-fido-key-attestation-20151120/	FIDO 2.0: Key Attestation Format
[RD5]	https://csrc.nist.gov/publications/detail/sp/800-73/4/final	NIST Special Publication 800-73
[RD6]	https://gnupg.org/ftp/spec/OpenPGP-smart-card-application-3.4.pdf	Functional Specification of the OpenPGP application
[RD7]	https://tools.ietf.org/html/rfc4226	HOTP: An HMAC-Based One-Time Password Algorithm
[RD8]	https://tools.ietf.org/html/rfc6238	TOTP: Time-Based One-Time Password Algorithm
[RD9]	https://developers.yubico.com/OTP/	Yubico OTP specifications
[RD10]	https://www.yubico.com/products/services-software/download/	Yubico software tools: downloads, release information, and open source code
[RD11]	https://globalplatform.org/specs-library/secure-channel-protocol-03-amendment-d-v1-2/	Global Platform specification for Secure Channel Protocol ‘03’ (SCP03)
[RD12]	https://arxiv.org/pdf/1708.08424.pdf	T/Key: Second-Factor Authentication From Secure Hash Chains
[RD13]	https://developers.yubico.com/YubiHSM2/	Yubico YubiHSM2 product information

Table 1 - List of references

1.2 Acronyms

Acronym	Description
2FA	Two-Factor Authentication
3DES	Triple DES
AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher Block Chaining
CC	Common Criteria
CSPN	Certificat de Sécurité de Premier Niveau
CCID	Chip Card Interface Device
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
FIDO	Fast Identity Online
GUI	Graphical User Interface
GPG	GNU Privacy Guard
HMAC	Hash-Based Message Authentication Code
HOTP	HMAC-Based One Time Password Algorithm
IC	Integrated Circuit
IETF	Internet Engineering Task Force
KSP	Key Storage Provider
MCU	Microcontroller Unit
MFA	Multi-Factor Authentication
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NVM	Non-Volatile Memory
OATH	Open AuTHentication
OTP	One Time Password
PIN	Personal Identification Number
PIV	Personal Identity Verification
PGP	Pretty Good Privacy
PTC	PIN Try Counter
SHA	Secure Hash Algorithm
TOE	Target Of Evaluation
TOTP	Time-Based One Time Password Algorithm
TRNG	True Random Number Generator
U2F	Universal Second Factor
RFC	Request For Comments
RSA	Rivest Shamir Adleman
USB	Universal Serial Bus

Table 2 - List of acronyms

2. Product description

2.1 YubiKey form factors

The YubiKey 5 Series enables encryption, supports multiple protocols and offers extensive authentication options including passwordless, strong two-factor authentication (2FA) and strong multi-factor authentication (MFA). Moreover, the YubiKey 5 Series actually details *six* different keys which, although possess the same underlying capabilities, distinguish themselves by their form factor and connectivity options, such as USB (types A and C), Lightning and/or NFC.

The available YubiKey 5 form factors and their physical attributes, are detailed in the [table](#) below.







	YubiKey 5 NFC	YubiKey 5C NFC	YubiKey 5 Nano	YubiKey 5C	YubiKey 5C Nano	YubiKey 5Ci
						
Dimensions	18mm x 45mm x 3.3mm	18mm x 45mm x 3.3mm	12mm x 13mm x 3.1mm	12.5mm x 29.5mm x 5mm	12mm x 10.1mm x 7mm	12mm x 40.3mm x 5mm.
Weight	3g	3g	1g	2g	1g	2.9g
Physical Interfaces	USB-A, NFC	USB-C, NFC	USB-A	USB-C	USB-C	USB-C, Lightning
Operating Temperatures	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)
Storage Temperatures	-20°C to 85°C (-4°F to 185°F)	-20°C to 85°C (-4°F to 185°F)	-20°C to 85°C (-4°F to 185°F)	-20°C to 85°C (-4°F to 185°F)	-20°C to 85°C (-4°F to 185°F)	-20°C to 85°C (-4°F to 185°F)

Table 3 - YubiKey 5 Series product overview

2.2 Supported authentication protocols

The YubiKey 5 Series supports the following authentication protocols:

- FIDO Universal 2nd Factor (U2F), see [\[RD3\]](#)
- FIDO2, see [\[RD4\]](#)

- Personal Identity Verification-compatible (PIV) smart card, see [\[RD5\]](#)
- OpenPGP smart card, see [\[RD6\]](#)
- OATH-HOTP (IETF RFC 4226), see [\[RD7\]](#)
- OATH-TOTP (IETF RFC 6238), see [\[RD8\]](#)
- Yubico OTP (Yubico's proprietary OTP), see [\[RD9\]](#)

The supported YubiKey 5 Series protocols are summarised in the [figure](#) below. Note that OTP (slots 1-2) actually refer to user customisable protocols which are activated by either a short touch (slot 1) or a long touch (slot 2) of the touch sensor. By default, slot 1 is configured with Yubico OTP, but slot 2 is unconfigured.

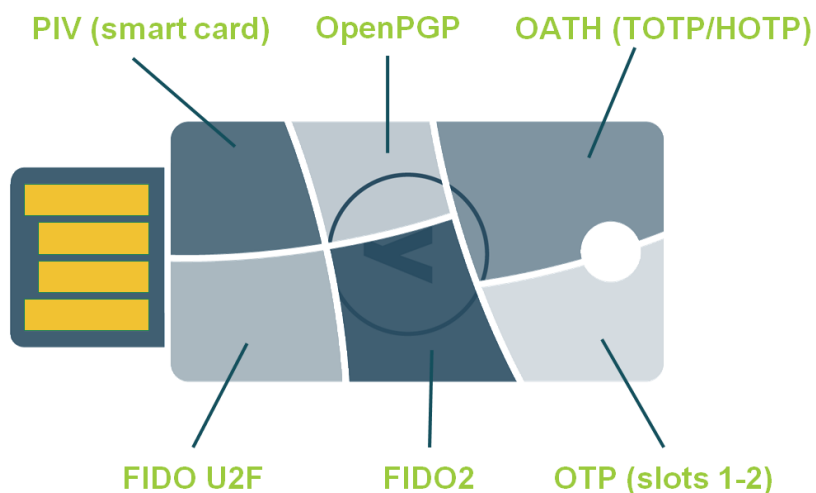


Figure 1 - YubiKey multiple applications and protocols

2.3 YubiKey architecture

All devices in the YubiKey 5 Series are composed of the following hardware components:

- Physical connector (USB-A, USB-C or Lightning as described in [table 3](#))
- Secured microcontroller (Infineon M7893 B11)
- Touch sensor (supporting the GPIO interface)
- NFC antenna based on ISO 14443 (only available on the YubiKey 5 NFC and YubiKey 5C NFC - see [table 3](#))

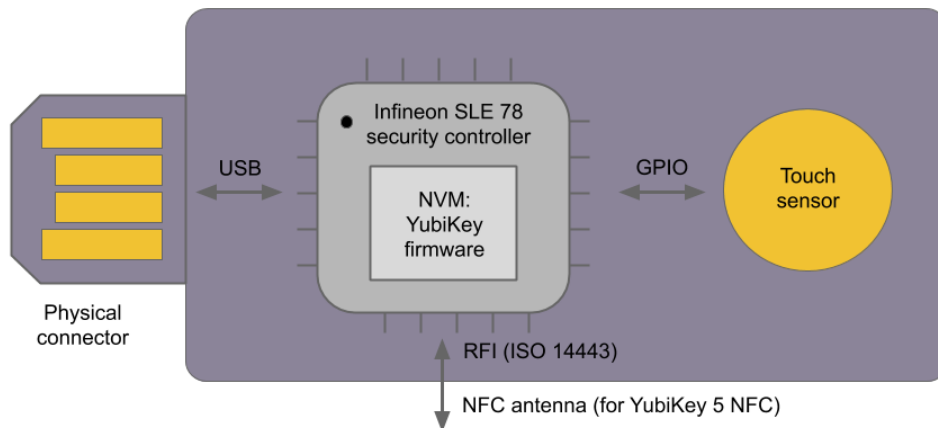


Figure 2 - YubiKey architecture overview

The secured microcontroller onboard each device in the YubiKey 5 series is the Infineon M7893 B11, which is certified according to Common Criteria EAL6+ by BSI [RD2]. There are two configurations of the microcontroller deployed, depending on the form factor of the YubiKey - the YubiKey 5Ci comes equipped with the Infineon SLE78 CLUFX5000PH whilst all other devices in the series comes with the Infineon SLE78 CLUFX3000PH. The difference between the two configurations is miniscule, that being the addition of two additional memory registers on the SLE78 CLUFX5000PH versus SLE78 CLUFX3000PH. The physical microcontroller is shown in the [figure](#) below.

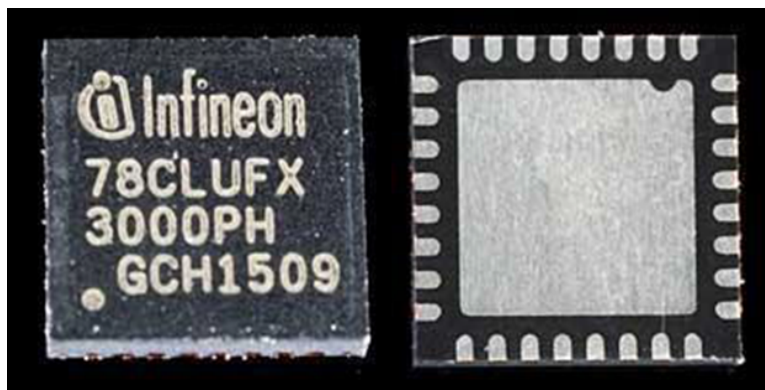


Figure 3 - Front (left) and back (right) view of the Infineon microcontroller

The YubiKey firmware is implemented within each microcontroller’s Non-Volatile Memory (NVM), and as such, *cannot* be updated. The firmware version of each YubiKey 5 can be found by using the YubiKey Manager (see [section 2.4](#)).

Furthermore, a touch sensor is also present on each YubiKey 5 and is connected to the microcontroller via the GPIO interface. The touch sensor can be thought of as a capacitor, which, before any authentication operation can be completed, must signal to the microcontroller to release the necessary credential and/or response. In other words, the YubiKey 5 touch sensor must come into physical contact with a human, before the device will provide the requested response. Therefore, a user who wants to perform an authentication operation must physically possess the

YubiKey 5 to touch the sensor (and in some cases, even to enter a PIN code, depending on the configuration and what application is being used).

The YubiKey 5 Series works across all major operating systems including Microsoft Windows, Apple MacOS, Apple iOS, Google Android, and Linux.

A block diagram of the YubiKey 5 is shown in the [figure](#) below.

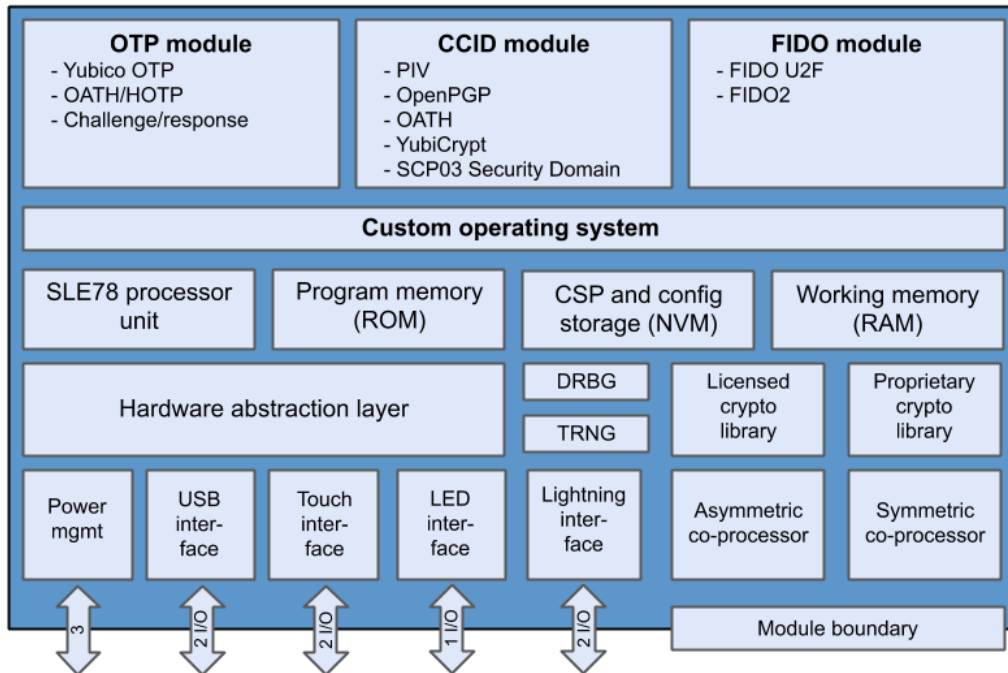


Figure 4 - YubiKey architecture diagram

* Note that the Lightning interface is only present on the YubiKey 5Ci.

2.4 YubiKey 5 software tools

The YubiKey 5 Series can be configured using the following Yubico software tools.

- YubiKey Manager, which supports:
 - GUI to configure FIDO2, OTP and PIV functionality
 - Command line tool for advanced configuration operations
- Yubico Authenticator, which can be used to:
 - Manually generate OATH credentials
 - Scan a Key Uri formatted barcode in order to generate the OATH credentials
- Yubico PIV tool, which can be used to configure the PIV application
- YubiKey Personalization Tool, which can be used to configure OTP slots 1 and 2, as previously referenced in [figure 1](#)

See reference [RD10] for more information about the Yubico software tools, downloads, release information, and open source code.

2.5 YubiKey cryptographic algorithms

The YubiKey 5 Series support the cryptographic primitives listed below:

- Symmetric cryptography: 3DES, AES
- Asymmetric cryptography: RSA (2048-4096 bits), EC (SECP, Brainpool, ed25519, x25519)
- Secure hash: HMAC, SHA-1, SHA-256, SHA-512

These cryptographic primitives are implemented in the YubiKey 5 in three different ways:

- Hardware implementation in the Infineon microcontroller (denoted as “Hardware”)
- Cryptographic Infineon Library (denoted as “Library”)
- Software implementation in the YubiKey 5 firmware (denoted as “Software”)

The implementation of each cryptographic primitive is described in the [table](#) below.

Algorithm	Implementation	Applications
AES-256-CCM	Software, Hardware	FIDO U2F, FIDO2
AES-128-ECB	Hardware	OTP, PIV, Security Domain
AES-192-ECB	Hardware	PIV
AES-256-ECB	Hardware	FIDO2, PIV
3-DES-ECB	Hardware	PIV
SHA-1	Hardware	OTP, OATH
SHA-256	Hardware	OATH, FIDO U2F, FIDO2, PIV, OpenPGP
SHA-512	Software	OATH, OpenPGP, FIDO2
EdDSA	Software, Library	OpenPGP, FIDO2
X25519	Software, Library	OpenPGP
RSA	Library	PIV, OpenPGP
ECDSA	Library	FIDO U2F, FIDO2, PIV, OpenPGP
ECDH	Library	FIDO2, PIV, OpenPGP
HMAC	Software	OATH, OTP, FIDO2
AES-CMAC	Software, Hardware	Security Domain, YubiHSM Auth
AES-CBC	Software, Hardware	Security Domain, FIDO2

Table 4 - List of cryptographic algorithms and implementations in YubiKey 5

2.6 Applications

The different applications (or security mechanisms) of the YubiKey 5 series can be enabled or disabled through configuration. These security mechanisms generally rely on a password or a PIN to restrict access to the YubiKey’s secure credentials, however, only the access control mechanisms for PIV, OpenPGP and FIDO2 (when PIN is required) allow for a limited number of attempts before access is blocked.

It is possible to both generate and import secret keys onto the YubiKey 5, but once the secret keys are loaded, it is no longer possible to subsequently recover or export them from the device.

Therefore, in case of loss or theft, it is *not* possible to perform any authentication operations if only a single YubiKey 5 has been loaded with the secret keys. It therefore becomes essential to maintain a “backup” device, but it should be noted that backup credentials can be created for OpenPGP, OTP and PIV only if the keys are not generated directly on the device.

Finally, if the secret keys (both symmetric and asymmetric) are loaded but not generated by the microcontroller on the YubiKey 5 during configuration, the keys are transferred in the clear using the applicable communication interface.

The specific security mechanisms for each application on the YubiKey, are described in the sub-sections below.

2.6.1 One Time Password - OTP

The YubiKey 5 OTP application supports five protocols:

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

2.6.1.1 Yubico OTP

The Yubico OTP scheme is a Yubico 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 it 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 YubiKey 5 touch sensor must be pressed in order to generate the Yubico OTP.

The Yubico OTP protocol is used as a second factor in the authentication process. To operate the YubiKey 5 in a CSPN Approved mode, the user must also be identified with a first factor authentication scheme (e.g. username/password) according to the description in [section 3](#).

When the Yubico OTP application is configured, an access code must be set to protect the key material and configuration.

2.6.1.2 Yubico OTP

Yubico’s Hash OTP implementation is based on the T/Key OTP scheme [T/Key]. T/Key is a time-based one-time password system that is based on hash chains, which requires no secrets on the server. Hash OTP generates a 44 character modhex string from the YubiKey, encoding 22 bytes

of data comprising 6 bytes for the prefix, the low byte of the counter and a truncated hash of 15 bytes:

$$OTP(counter) = \text{modhex}(\text{prefix} \parallel \text{low_byte}(counter) \parallel t_hash(counter))$$

Where:

$prefix = \text{identity}|6$

$t_hash(0) = \text{a random 15 byte seed}$

$t_hash(n) = \text{SHA256}(\text{domain} \parallel \text{identity} \parallel n \parallel t_hash(n-1))|15$

The YubiKey 5 touch sensor must be pressed in order to generate the Hash OTP. The protocol is used as a second factor in the authentication process. To operate the YubiKey 5 in a CSPN Approved mode, the user must also be identified with a first factor authentication scheme (e.g. username/password) according to the description in [section 3](#).

When the Hash OTP application is configured, an access code must be set to protect the key material and configuration.

Yubico's Hash OTP can be used as a replacement for current OATH-*OTP systems, and it remains secure in the event of a server-side compromise. The cost, is that the hashed one-time passwords are longer than the standard six characters used in OATH-*OTP.

2.6.1.3 Challenge-Response

The challenge-response protocol is based on the HMAC-SHA-1 algorithm. The relying party sends a challenge (with a max length of 64 bytes) to the YubiKey 5, and the device then responds with a hash of it. The secret key used in the HMAC-SHA-1 is pre-loaded by the user onto the YubiKey 5 during configuration. It is also possible to configure whether human contact of the YubiKey 5 touch sensor is required to activate the protocol, for each challenge-response request.

Depending on the use case, the HMAC-SHA-1 key can be shared between the YubiKey 5 and the relying party.

The challenge-response protocol is used as a second factor in the authentication process. To operate the YubiKey 5 in a CSPN Approved mode, the user must also be identified with a first factor authentication scheme (e.g. username/password) according to the description in [section 3](#). 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 the secret key and configuration.

2.6.1.4 Static password

This application allows the storage of a static password. The user may choose the length of the password, anywhere between 1 and 38 characters long, and the allowed characters for the password are either Modhex, or any US keyboard layout character. Additionally, the user may choose to enter the value of the password manually, or have the YubiKey 5 software tools randomly generate it.

The static password is used as a second factor in the authentication process. To operate the YubiKey 5 in a CSPN Approved mode, the user must only store one portion of the password in the YubiKey 5 and keep the other half of the password in a different, yet secure location. The user needs to construct the complete password by combining the password portion from the YubiKey with the other half stored elsewhere, and then authenticate with username/password.

The password is presented to the user in clear when the user touches the YubiKey 5 sensor. When the static password application is configured, an access code must be set in order to protect the static password and configuration.

2.6.1.5 OATH-HOTP

The OATH-HOTP protocol is the same as the OTP described in [RD7] and similar in nature to OATH-TOTP as described in [RD8]. The only algorithm that is supported by this application is HMAC-SHA-1. The user may choose the number of digits of the OTP (6 or 8) and the initial counter value. The YubiKey 5 touch sensor is pressed when generating the OATH-HOTP.

OATH-HOTP is used as a second factor in the authentication process. To operate the YubiKey 5 in a CSPN Approved mode, the user must also be identified with a first factor authentication scheme (e.g. username/password) according to the description in [section 3](#).

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.

2.6.2 FIDO U2F

The YubiKey 5 Series supports FIDO Universal 2nd Factor (U2F), which is defined in [RD3]. On a high level, the FIDO U2F protocol comprises both the registration and the authentication process.

FIDO U2F is used as a second factor in the authentication process. To operate the YubiKey 5 in a CSPN Approved mode, the user must also be identified with a first factor authentication scheme (e.g. username/password) according to the FIDO U2F standard [RD3] and the description in [section 3](#).

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

2.6.3 FIDO2

FIDO2 consists 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 defined in [RD4]. It takes into account PIN management, in addition to the new standardized protocols, WebAuthn and CTAP2. The PIN length must be greater than or equal to 4 bytes and less than or equal to 63 bytes, while the maximum number of retries is equal to 8.

WebAuthn User Verification should be set to “required” by the WebAuthn relying party when the user registers the YubiKey 5 as a FIDO2 device. The user can also use the YubiKey Manager (see [section 2.4](#)) to set a PIN code that protects the FIDO2 credentials. Hence, the YubiKey 5 requires the user to enter a PIN code when using it for FIDO2 authentication.

If WebAuthn User Verification is not enforced as recommended above, the YubiKey 5 must be used as a second factor authentication device. To operate the YubiKey 5 in a CSPN Approved mode for such a scenario, the user must also be identified with a first factor authentication scheme (e.g. username/password) according to the description in [section 3](#).

2.6.4 Security Domain

The Security Domain application is used to manage the long-lived keys used in SCP03 [RD11] that allow the generation of session-specific keys for use with the other CCID applications: OATH, PIV, OpenPGP, and YubiHSM Auth. The Security Domain allows for storing and deleting up to three (3) sets of keys. Each set consists of three (3) AES-128 keys.

After those keys are stored, the main users of the Security Domain will be other applications that can be used over the CCID interface such as PIV or OpenPGP. Those applications will request the Security Domain to establish a secure session and derive a set of session-specific keys starting from one of the initial set of long-lived keys.

In order to import new keysets, a secure channel must be established with the Security Domain application itself. This has to be done with a previously loaded keyset or the well-known, default, keyset.

2.6.5 PIV

The PIV application [[RD5](#)] can be used to authenticate, sign and decrypt. The user can, for example, use the YubiKey 5 PIV application for Windows smart card logon.

The PIV application allows for generating asymmetric key-pairs (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

The PIV application requires user verification with a PIN and a management key (Triple-DES or AES key). 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 for access to the credential in a given slot, a PIN policy should be set for that slot. This policy must be set upon key generation or importation and cannot be changed at a later time.

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

2.6.6 OpenPGP

The YubiKey 5 supports the OpenPGP application [[RD6](#)]. The private keys can be generated or loaded onto the YubiKey 5, where it has the capacity to store one key pair for each of attestation, authentication, signing, and encryption.

During configuration of the OpenPGP application, it is also possible to configure whether human contact of the YubiKey 5 touch sensor is required for each operation that uses a private key.

It is important to note that there are three PINs: an admin PIN, a user PIN and a reset code. The admin PIN is required to modify or generate keys, the user PIN is required to use a private key and finally, the reset code is a PUK that is used to reset the PIN in case it is lost.

The number of PIN retries can be modified by the administrator (via the admin PIN), and this number must be set to a value between 1 and 99 with a default value set to 3.

2.6.7 OATH

The OATH application allows for managing two types of OTP:

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

This application can use HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-512, but HOTP of the OTP application (see [section 2.6.1.5](#)) is limited to only HMAC-SHA-1.

A maximum of 32 credentials¹ can be stored within the YubiKey's OATH application. The software tools described in [section 2.4](#) may be used to configure and use this application. A password may also be set to protect the OATH credentials, and if this is configured, the password unlocks the application, which can then be used to generate any number of OTPs for the remainder of the session (until application is de-selected).

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

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 also be identified with a first factor authentication scheme (e.g. username/password) according to the description in [section 3](#).

For more cryptographic details, see [section 2.5](#).

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

2.6.8 YubiHSM Auth

The YubiHSM Auth application can off-load the storage of long-lived credentials, AES-128 keys, that are used in conjunction with a Yubico YubiHSM2² [RD13] to establish secure sessions. The YubiHSM Auth application can store up to 32 credentials. By providing an external challenge a derivation scheme is executed. This scheme yields three session-specific AES-128 keys as its output. The session-specific keys are not stored on the device but simply output as a result.

Each credential is protected by a 16-byte user access code that has to be provided contextually to each operation. Storing and deleting credentials requires a separate 16-byte admin access code.

3. Target of evaluation

The table below enumerates the specifications of the YubiKey 5 Series to be evaluated, which therefore becomes the Target of evaluation (TOE).

Product name	YubiKey 5 Series (all six form factors)
Microcontroller Unit (MCU)	M7893 B11
MCU firmware version	78.019.03.4
MCU cryptolib version	1.03.006
YubiKey 5 firmware version	5.4.2

Table 5 - TOE identification

3.1 TOE configuration

The touch sensor on the TOE must be pressed when the YubiKey 5 is used for OTP generation, FIDO U2F authentication and when FIDO2 does not require a PIN code. Moreover, the applications OTP, FIDO U2F and FIDO2 without a required PIN code are only used for second factor authentication.

The other applications must also be configured as described below:

- FIDO2: Touch sensor activated and PIN usage is required (when WebAuthn User Verification is enforced according to [section 2.6.3](#))
- PIV: The number of PIN retries is set to the default value
- OpenPGP: The number of retries of the user PIN is set to the default value
- OATH: A 20 byte sized password is set
- YubiHSM Auth: A 16 byte user access code is set per each credential

3.2 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.

² Yubico YubiHSM2 is an HSM product, for which the AES-128 keys can be used for establishing secure sessions. The YubiHSM2 is out of scope of this security target and is not required for the CSPN evaluation.

- 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.

3.3 Operating environment

For the operating environment, the TOE is considered as placed in a public area and thus may be used by the general public.

As stated in [section 3.1](#), the applications OTP, FIDO U2F and FIDO2 without PIN code must only be used as a second factor authentication. Usage of these applications must be performed with a first factor authentication correctly configured and secured. The details of the first factor authentication are out of scope of this evaluation.

3.4 Product assets

The YubiKey 5 Series is used for processing sensitive operations, therefore, the following assets must be secured with respect to confidentiality and integrity:

- Cryptographic keys
- PIN and password
- Private data

4. Threat description

4.1 Attacker's profile

The YubiKey 5 may be considered as a sensitive device, which can be used to process certain authentication operations for which it has been registered.

In the threat scenario where an attacker may be able to compromise the YubiKey 5 owner's identity, the attacker has gained physical access to the YubiKey 5. This may occur when the device has either been lost or stolen.

4.2 Threat 1: Bypassing the access control

To perform an authentication operation, access control (i.e. PIN or password) is necessary for the PIV, OpenPGP, FIDO2 (when PIN is enforced), OATH, and YubiHSM Auth applications.

In this scenario, the threat is related to a stolen YubiKey 5 whereby the attacker attempts to bypass the access control entirely, and attempt authentication operations without knowing the user PIN/password.

4.3 Threat 2: Recover the PIN/password

The PIV, OpenPGP, FIDO2 (when PIN is enforced), OATH, and YubiHSM Auth applications are configured with a PIN/password. In this scenario, the threat is an attacker who attempts to retrieve the PIN/password of these applications.

4.4 Threat 3: Recover the secret keys

The symmetric and asymmetric keys are stored in the NVM of the secured microcontroller. In this scenario, the threat is an attacker who attempts to retrieve these secret keys. Therefore, if successful, an attacker could:

- Clone the key material residing on the YubiKey 5
- Perform authentication and access restricted operations using said secret keys

4.5 Threat 4: Perform an authentication without access to the YubiKey

In this scenario, the threat is an attacker who has *no physical access* to the YubiKey 5 (i.e. not falling into the attacker profile as outlined in [section 4.1](#)) but who attempts to perform authentication or other cryptographic operations via a remote attack.

5. Security functions

5.1 SF1: True Random Number Generator (TRNG)

This security function aims at counteracting [threat 3](#).

This security function is based on the True Random Number Generator (TRNG) embedded in the secured microcontroller (M7893 B11). This TRNG, evaluated according to AIS31 methodology, has been successfully certified during the EAL6+ Common Criteria evaluation. To reinforce the entropy of the generated random number, Yubico has also implemented an additional software post-processing countermeasure.

The TRNG is used to seed a DRBG during key generation. Therefore, it is not possible to exploit a biased TRNG in order to recover the secret keys.

This security function is implemented for the following applications:

- FIDO U2F: Usage and key generation
- FIDO2: Usage and key generation
- PIV: Usage and key generation
- OpenPGP: Usage and key generation

5.2 SF2: User authentication mechanism

This security function aims at counteracting [threats 1](#) and [2](#).

To perform an authentication operation, several applications require a PIN or a password. The candidate PIN/password is compared to the reference PIN/password stored in the microcontroller (M7893 B11). A correct verification allows the authentication operation to be performed.

The PIN/passwords are either too large to perform a brute-force attack or are protected by a PIN retry counter (for FIDO2 with required PIN, PIV and OpenPGP applications). See [section 7](#) for recommended PIN/password minimal lengths.

This security function is implemented for the following applications:

- FIDO2: PIN is required according to the CSPN Approved configuration (i.e. when WebAuthn User Verification is enforced according to [section 2.6.3](#))
- PIV: PIN is required according to the CSPN Approved configuration
- OpenPGP: PIN is required according to the CSPN Approved configuration
- OATH: Password is required according to the CSPN Approved configuration
- YubiHSM Auth: Password is required to CSPN Approved configuration

If there is a default PIN set for a given application, it must be changed by the user.

5.3 SF3: Data storage

This security function aims at counteracting [threats 2](#) and [3](#).

The cryptographic keys and the PIN/passwords are stored in the microcontroller (M7893 B11). This microcontroller has been successfully certified according to the EAL6+ common criteria evaluation.

This security function is implemented for the following applications:

- FIDO U2F: Cryptographic key
- FIDO2: Cryptographic keys and PIN value
- Security Domain: Cryptographic keys
- PIV: Cryptographic keys and PIN value
- OpenPGP: Cryptographic keys and PIN value
- OATH: Cryptographic key and password value
- YubiHSM Auth: Cryptographic keys, password values
- OTP
 - Yubico OTP: Cryptographic key and Private ID value
 - Challenge-Response: Cryptographic key
 - OATH-HOTP: Cryptographic key

5.4 SF4: Cryptographic operations

This security function aims at counteracting [threat 3](#).

The cryptographic operations are performed by the certified microcontroller (M7893 B11), the microcontroller library, and the YubiKey 5 firmware code implementation. The microcontroller and its library have been successfully certified during the EAL6+ Common Criteria evaluation. The YubiKey 5 firmware implementation is resistant to both invasive and non-invasive attacks.

This security function is implemented for the following applications and algorithms:

- FIDO U2F: AES, SHA-256, ECDSA
- FIDO2: AES, SHA-256, ECDSA, ECDH, HMAC, EdDSA, SHA-512
- Security Domain: AES, AES-CMAC
- PIV: AES, 3DES, RSA, ECDSA, ECDH,, SHA-256,
- OpenPGP: EdDSA, X25519, RSA, ECDSA, ECDH, SHA-512, SHA-256
- OATH: SHA-1, SHA-256, SHA-512, HMAC
- YubiHSM Auth: AES, AES-CMAC
- OTP
 - Yubico OTP: AES
 - Challenge-response: HMAC, SHA-1, AES
 - OATH-HOTP: HMAC, SHA-1
 - Hash OTP: SHA-256

5.5 SF5: Physical access to the YubiKey 5

This security function aims at counteracting [threat 4](#).

The YubiKey 5 possesses a touch capacitive sensor, which, before performing any authentication operation, can be pressed. Therefore, any user who wishes to perform an authentication operation associated with the device, must possess the device itself.

This security function is implemented for the following applications:

- FIDO U2F
- FIDO2
- OpenPGP (when configured to be used with the touch sensor)
- OATH-HOTP/TOTP (when configured to be used with the touch sensor)
- Hash OTP
- OTP
 - Yubico OTP
 - Challenge-response
 - OATH-HOTP
 - Static password
- PIV (when configured to be used with the touch sensor)
- YubiHSM Auth (when configured to be used with the touch sensor)

5.6 Coverage of threats

A matrix of the threats and security functions on the YubiKey 5 designed to counteract them, is illustrated in the [table](#) below.

	T1	T2	T3	T4
SF1			X	
SF2	X	X		
SF3		X	X	
SF4			X	
SF5				X

Table 6 - Coverage of threats

6. Annex: Critical security parameters

Name	Description
Key	OTP CSPs
OTP Access Codes	Two 6 byte values. Used for authentication of the OTP administrator for management. When the YubiKey leaves the factory there is a default value and there is an administrator procedure for updating this value.
OTP Slot Keys	Two AES-128 bits, Hash OTP keys or HMAC-SHA-1 160 bit values, depending on the algorithms used. Used for generation of OTPs (One Time Passwords).
Key	CCID/Security Domain CSPs
CCID Security Domain CSPs	Security Domain ENC key. One to three AES-128 keys. Used for deriving keys for command and response encryption.
Security Domain MAC key	One to three AES-128 keys. Used for deriving keys for command authentication.
Security Domain R-MAC key	One to three AES-128 keys. Used for deriving keys for response authentication.
Security Domain DEK key	One to three AES-128 keys. Used for data encryption.
Key	CCID/PIV CSPs
PIV Symmetric Key for Mutual Authentication	One 3-key TDES or AES-128 or AES-192 or AES-256 key. Used for authentication of the CCID PIV administrator. There is a defined default value when it leaves the factory.
PIV Asymmetric Private Keys	0 to 24 RSA 2048 or ECDSA P-256/P-384 private keys. Used for cryptographic operations in conjunction with an external system.
PIV Attestation Private Key	One RSA 2048 or ECDSA P-256/P-384 private keys. Used to attest internally generated public keys using hash-pkcs#1v15-sign
PIV User PIN	One 6-8 byte PIN. Used for authenticating the PIV User for Asymmetric services.
PIV PUK PIN	One 6-8 byte PIN. Used for unblocking the PIV User PIN.
Key	CCID/OpenPGP CSPs

OpenPGP Admin PIN (PW3)	One 8-127 byte PIN. Used for authentication of the OpenPGP administrator. When the YubiKey leaves the factory there is a default value and there is an administrator procedure for updating this value.
OpenPGP Signature Private Key	0 or 1 RSA 2048/3072/4096, secp256r1, secp256k1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1,, or ed25519 private keys. Used for signing operations.
OpenPGP Authentication Private Key	0 or 1 RSA 2048/3072/4096, secp256r1, secp256k1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1,,or ed25519 private keys. Used for authentication as a signing operation.
OpenPGP Decryption Private Key	0 or 1 RSA 2048/3072/4096, secp256r1, secp256k1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1,, x25519, or private keys. Used for decryption.
OpenPGP User PIN (PW1)	One 6-127 byte PIN. Used for authenticating the OpenPGP User for Asymmetric services.
OpenPGP Reset Code	0 or 1 8-127 byte PIN. Used for resetting the User PIN.
Key	FIDO U2F CSPs
FIDO U2F Key Wrapping Key	One AES-256 key. Used for wrapping the FIDO U2F keys (same as the FIDO2 Key Wrapping Key).
FIDO U2F Authentication Private Keys	0 to many ECDSA P-256 private keys. Only one will exist in the YubiKey at a time. Used for subsequent signature generation.
FIDO U2F Attestation Private Key	One ECDSA P-256 private key. Used to attest internally generated public keys (same as the FIDO2 Attestation Private Key).
Key	FIDO2 CSPs
FIDO2 Key Wrapping Key	One AES-256 key. Used for wrapping the FIDO2 keys (same as the FIDO U2F Key Wrapping Key).
FIDO2 User PIN	0 or 1 4-64 byte PIN for authentication to the FIDO module.
FIDO2 Authentication Private Keys	0 to many ECDSA P-256 or ED25519 private keys. Only one will exist in the YubiKey at a time. Used for subsequent signature generation. There are also 25 resident keys.
FIDO2 Attestation Private Key	One ECDSA P-256 private key. Used to attest internally generated public keys (same as the FIDO U2F Attestation Private Key).
Offline Key	One HMAC-SHA256 key used for generating HMAC-secret for FIDO2 authentication.
Key	CCID/OATH CSPs

OATH Auth Key	0 or 1 14-64 byte HMAC SHA1/SHA256/SHA512 key. When the YubiKey leaves the factory this does not exist and there is an administrator procedure for setting this value.
OATH Seed key	0 to 32 14-64 byte HMAC SHA1/SHA256/SHA512 key.
Key	OTP CSPs
YubiHSM Auth Admin Access Code	One 16-byte access code. Used to store or delete the YubiHSM Auth credentials.
YubiHSM Auth Credential	0 to 32 sets of two AES-128 keys. Used to derive three session-specific AES-128 keys.
YubiHSM Auth User Access Code	0 to 32 16-byte access code. Used to access the YubiHSM Auth Credential to derive the session-specific AES-128 keys.

Table 7 - Critical security parameters

7. Annex: Strengths of access control mechanisms

Authentication Mechanism	Strength of Mechanism
6 byte access code (OTP)	<p>The access code is a 6 byte (48 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{48}$ which is less than $1/1,000,000$. Each authentication attempt takes approximately 60 ms which allows a maximum of 1000 attempts per minute. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is $1000/2^{48}$, which is less than $1/100,000$.</p>
3 key TDES mutual challenge response (PIV)	<p>This is a 3-key Triple DES Key which has 112 bits of security. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{112}$ which is less than $1/1,000,000$. Authentication attempts are limited to 40000 per minute. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is $40000/2^{112}$, which is less than $1/100,000$.</p>
6-8 byte digit PIN or PUK (PIV)	<p>The PIN is a 6 byte (48 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{48}$ which is less than $1/1,000,000$. The authentication is limited by the retry counter of up to 255 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is $255/2^{48}$, which is less than $1/100,000$.</p>
User PIN 6-127 byte (OpenPGP)	<p>The PIN is a 6 byte (48 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{48}$ which is less than $1/1,000,000$. The authentication is limited by the retry counter of up to 255 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is $255/2^{48}$, which is less than $1/100,000$.</p>
Admin PIN 8 -127 byte (OpenPGP)	<p>The access code is an 8 byte (64 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{64}$ which is less than $1/1,000,000$. The authentication is limited by the retry counter of up to 255 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is $255/2^{64}$, which is less than $1/100,000$.</p>

<p>Reset Code 8 - 127 byte (OpenPGP)</p>	<p>The access code is an 8 byte (64 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{64}$ which is less than $1/1,000,000$. The authentication is limited by the retry counter of up to 255 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is $255/2^{64}$, which is less than $1/100,000$.</p>
<p>FIDO2 User PIN 4-32 bytes</p>	<p>The FIDO2 user PIN is a 4-32 byte (32-256 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{32}$ in the worst case scenario, which is less than $1/1,000,000$. The authentication is limited by the retry counter of up to 8 tries. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is $8/2^{32}$, which is less than $1/100,000$.</p>
<p>Auth Key 14 to 64 byte HMAC SHA1, HMAC SHA256 key (OATH, YubiHSM Auth 16-bytes only)</p>	<p>The auth key is a 14 byte (112 bit) binary string with no restrictions on character space. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{112}$ which is less than $1/1,000,000$. Each authentication attempt takes approximately 1.5 ms which allows a maximum of 40000 attempts per minute. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is $40000/2^{112}$, which is less than $1/100,000$.</p>

Table 8 - Strengths of access control mechanisms