

# YubiKey 5 NFC

## Technical specifications

### 5th Generation of Strong Authentication Security Keys

YubiKey 5 is a series of compact USB security keys enabling multi-factor authentication. Now comes with the FIDO2 passwordless authentication support and a USB + NFC option — YubiKey 5 NFC. Multi-factor authentication combined with hardware solutions allows improving accounts protection at all levels. It is widely known that one-time SMS passwords are vulnerable to hacks and can't offer the appropriate level of defense. Troubles caused by hacking attacks and SIM cards cloning can be avoided by using hardware keys for secure logins to applications and online services accounts. These USB keys are ready to use with Windows, Linux and macOS operating systems, as well as with popular browsers, apps and websites. The 5th generation of YubiKeys combines multiple cryptographic algorithms support with ease of use — safe login with only a touch of the button.



# Technical specifications

## Interface

<b>USB</b>	USB 2.0 type A (USB 3.0 compatible)
<b>NFC</b>	Near-field communication, range ~4 inches. MIFARE Classic 1k backward compatible.

## Applications

<b>FIDO2</b>	<p>The FIDO2 application allows for resident credentials to be stored and allows for password-less login on sites and devices that support it. The credentials can be protected with a PIN for convenient and strong two-factor authentication. The FIDO2 application is FIDO certified.</p> <p>USB Interface: FIDO</p>
<b>OTP (One-time password)</b>	<p>The OTP applet contains two programmable slots, each can hold one of the following credentials:</p> <ul style="list-style-type: none"><li>• Yubico OTP</li><li>• HMAC-SHA1 Challenge-Response</li><li>• Static Password</li><li>• OATH-HOTP</li></ul> <p>USB Interface: OTP</p>
<b>U2F (Universal 2<sup>nd</sup> factor)</b>	<p>The U2F application can hold an unlimited number of U2F credentials and is FIDO certified.</p> <p>USB Interface: FIDO</p>
<b>OATH</b>	<p>The YubiKey 5 series can hold up to 32 OATH credentials and supports both OATH-TOTP (time based) and OATH-HOTP (counter based). Accessing this applet requires Yubico Authenticator.</p>
<b>PIV (Smart Card)</b>	<p>This application provides a PIV compatible smart card. On Windows, the smart card functionality can be enhanced with the YubiKey Smart Card Minidriver.</p> <p><b>Default Values:</b></p> <ul style="list-style-type: none"><li>• PIN: 123456</li><li>• PUK: 12345678</li><li>• Management Key: 010203040506070801020304050607080102030405060708</li></ul> <p><b>Supported Algorithms:</b></p> <ul style="list-style-type: none"><li>• RSA 1024</li><li>• RSA 2048</li><li>• ECC P256</li><li>• ECC P384</li></ul> <p><b>Slot Information:</b></p> <ul style="list-style-type: none"><li>• Slot 9a: Authentication</li><li>• Slot 9b: Management Key</li><li>• Slot 9c: Digital Signature</li><li>• Slot 9d: Key Management</li><li>• Slot 9e: Card Authentication</li><li>• Slot f9: Attestation</li><li>• Slots 82-95: Retired Key Management</li></ul> <p>USB Interface: CCID</p>

## OpenPGP

This application implements version 2.0 of the [OpenPGP Smart Card specification](#) which can be used with GnuPG. For key sizes over 2048 bits, GnuPG version 2.0 or higher is required.

### Supported Algorithms:

- RSA 1024
- RSA 2048
- RSA 3072
- RSA 4096

USB Interface: CCID

## Physical Specifications

Connector	USB-A
Dimensions	18mm x 45mm x 3.3mm
Weight	3g

## Temperatures

Operational range	0 °C to 40 °C (32 °F to 104 °F)
Storage range	-20 °C to 85 °C (-4 °F to 185 °F)

## Cryptographic algorithms

RSA 1024	Max. keysize: 1024 bits
RSA 2048	Max. keysize: 2048 bits
RSA 3072	Max. keysize: 3072 bits
RSA 4096	Max. keysize: 4096 bits
ECC p256	Max. keysize: 256 bits
ECC p384	Max. keysize: 384 bits
SHA1	Max. keysize: 160 bits

## Contact us

### UAE - Headquarters

Dubai Airport Free Zone 6EA, #209. Dubai – UAE

Tel. +971 (04) 7017 260

Email: [info@thekernel.com](mailto:info@thekernel.com)