YubiKey FIPS

Technical specifications

FIPS 140-2 validated strong security key for enterprise solutions

Industry leading FIPS 140-2 validated hardware authenticator, which is reliable and easy to deploy. The YubiKey FIPS series ensures strong security and defense against phishing and account takeovers. It enables enterprises and government agencies to meet the highest authenticator assurance level of requirements.

fido CERTIFIED U2F

FIPS 140-2
VALIDATED

yubico
Trust the Net.

Technical specifications

Interface	
USB	USB 2.0 type A (USB 3.0 compatible)

Applications	
OTP (One-time password)	The OTP applet contains two programmable slots, each can hold one of the following credentials: • Yubico OTP • HMAC-SHA1 Challenge-Response • Static Password • OATH-HOTP USB Interface: OTP
U2F (Universal 2nd factor)	The U2F application can hold an unlimited number of U2F credentials and is FIDO certified. USB Interface: FIDO
OATH	The YubiKey FIPS series can hold up to 32 OATH credentials and supports both OATH-TOTP (time based) and OATH-HOTP (counter based). Accessing this sub-module requires Yubico Authenticator.
PIV (Smart Card)	This application provides a PIV compatible smart card. On Windows, the smart card functionality can be enhanced with the YubiKey Smart Card Minidriver. **Default Values:** • PIN: 123456 • PUK: 12345678 • Management Key: 010203040506070801020304050607080102030405060708 **Supported Algorithms:** • RSA 2048 • ECC P256 • ECC P384 **Slot Information:** • Slot 9a: Authentication • Slot 9b: Management Key • Slot 9c: Digital Signature • Slot 9d: Key Management • Slot 9e: Card Authentication • Slot f9: Attestation • Slots 82-95: Retired Key Management USB Interface: CCID

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 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 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