>

yubico

Price List for Standard Security Keys YubiKey 5, YubiKey FIPS and YubiHSM2 from September 2020.

	YubiKey 5 NFC	YubiKey 5C NFC	YubiKey 5 Nano	YubiKey 5C	YubiKey 5C Nano	YubiKey 5 CI	Security Key	Security Key NFC
The wholesale package (50pcs)								
Individual packing								
Price	1800,00 UAH	2100,00 UAH	1950,00 UAH	1950,00 UAH	2300,00 UAH	2700.00 UAH	1000,00 UAH	1200,00 UAH
Description	USB Authentication Key, Strong crypto, Supports FIDO2 and U2F, Passwordless Login, OTP, Static Passwords, PIV Smart Card Mode, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP. NFC support for YubiKey 5 NFC model.						USB authentication key that works instantly with any service that supports U2F or FIDO2.	USB authentication key that works instantly with any service that supports U2F or FIDO2 and over NFC with mobile devices.
Size and weight	18 x 45 x 3.3mm, 3g.	18 x 45 x 3.3mm, 3g.	12 x 13 x 3.1mm, 1g.	12.5 x 29.5 x 5mm, 2g.	12 x 10.1 x 7, 1g.	12 x 40.3 x 5mm, 2.9g.	18 x 45 x 3.3mm, 3g.	18 x 45 x 3.3mm, 3g.
Certifications								
FIDO certification™	Y	Y	Y	Y	Y	Y	Y	Y
FIPS 140 Certified								
Communications Support								
USB-A	Y		Y				Y	Y
USB-C		Y		Y	Y	Y		
Lightning (Made for iPhone)						Y		
NFC (Near Field Communcation)	Y	Y						Y
Device Type								
HID Keyboard	Y	Y	Y	Y	Y	Y		
CCID Smart Card	Y	Y	Y	Y	Y	Y		
FIDO HID Device	Y	Y	Y	Y	Y	Y	Y	Y
Cryptography specifications								
RSA 2048	Y	Y	Y	Y	Y	Y		
RSA 4096 (PGP)	Y	Y	Y	Y	Y	Y		
ECC p256	**	**	**	**	**	**	**	**
ECC p384	***	***	***	***	***	***		

** *ECC applies only to the smart card applet; does not apply to OpenPGP applet. The key type generated for the U2F key pair is ECC p256.*

*** *ECC applies only to the smart card applet; does not apply to OpenPGP applet.*

OATH-TOTP requires additional application — Yubico Authenticator; For YubiKey 5 NFC keys, FIDO certification applies to both connections — USB and NFC.

>the_kernel
We don't panic.

Ukraine, Kyiv, 02095, Darnytskyi district, Dniprovska embankment 16 D, Office 201A.
Tel. +38 (044) 22 81 888; +38 (044) 22 81 999. Mail: info@thekernel.com.ua,
www.thekernel.com.ua, yubikey.com.ua

Price list for YubiKey FIPS certified security keys from September 2020.

	YubiKey FIPS	YubiKey Nano FIPS	YubiKey C FIPS	YubiKey C Nano FIPS
Models				
Price	1900,00 UAH	2200,00 UAH	2200,00 UAH	2650,00 UAH
Description	FIPS 140-2 certified USB Authentication Key, Strong crypto, Supports FIDO2 and U2F, Passwordless Login, OTP, Static Passwords, PIV Smart Card Mode, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP.			
Size and weight	18 x 45 x 3.3мм, 3г	12 x 13 x 3.1мм, 1г	12.5 x 29.5 x 5мм, 2г	12 x 10.1 x 7, 1г
Сертификация				
FIDO certification™	Y	Y	Y	Y
FIPS 140 Certified	Y	Y	Y	Y
Поддерживаемые подключения				
USB-A	Y	Y		
USB-C			Y	Y
NFC (Near Field Communcation)				
Тип устройства				
HID Keyboard	Y	Y	Y	Y
CCID Smart Card	Y	Y	Y	Y
FIDO HID Device	Y	Y	Y	Y
Спецификации криптографии				
RSA 2048	Y	Y	Y	Y
RSA 4096 (PGP)	Y	Y	Y	Y
ECC p256	**	**	**	**
ECC p384	***	***	***	***

** *ECC applies only to the smart card applet; does not apply to OpenPGP applet. The key type generated for the U2F key pair is ECC p256.*

*** *ECC applies only to the smart card applet; does not apply to OpenPGP applet.*

NIST | *The National Institute of Standards and Technology* (USA)
YubiKey Cryptographic Module Certification

>the_kernel
We don't panic.

Ukraine, Kyiv, 02095, Darnytskyi district, Dniprovska embankment 16 D, Office 201A.
Tel. +38 (044) 22 81 888; +38 (044) 22 81 999. Mail: info@thekernel.com.ua,
www.thekernel.com.ua, yubikey.com.ua

YubiHSM 2 hardware security module for securing cryptographic keys on servers

	YubiHSM 2	
Model		
Price	25000.00 UAH	
Size and weight	12 mm x 13 mm x 3.1 mm, 1 g	
OS support		
Version	Linux	CentOS 6, CentOS 7, Debian 8, Debian 9, Fedora 25, Ubuntu 1404, Ubuntu 1604
	MS Windows	Windows 10, Windows Server 2012, Windows Server 2016
	Mac OS	10.12 Sierra, 10.13 High Sierra
Architecture	amd64	
Cryptographic capabilities		
Hashing	Applicable with HMAC and asymmetric signatures ☐ SHA-1, SHA-256, SHA-384, SHA-512	
RSA	☐ 2048, 3072, and 4096-bit keys ☐ Signature with PKCS # 1v1.5 and PSS ☐ PKCS # 1v1.5 decryption and OAEP	
Elliptic-curve cryptography (ECC)	☐ Curves: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 ☐ Signature: ECDSA (all except curve25519), EdDSA (curve25519 only) Decryption: ECDH (all except curve25519)	
Key packing	Import and export with NIST AES-CCM Wrap at 128, 196, and 256 bits	
Random numbers	On-chip real random number generator (TRNG) with the seed NIST SP 800-90 AES 256 CTR_DRBG	
Validation	Asymmetric key pairs generated on the device can be verified using a factory-certified attestation key and certificate, or with your private key imported into the security module	
Performance	Performance depends on the intended application. The example shows the metric of YubiHSM2 that is not used in other processes:	
	☐ RSA-2048-PKCS1-SHA256:	~139ms aver.
	☐ RSA-3072-PKCS1-SHA384:	~504ms aver.
	☐ RSA-4096-PKCS1-SHA512:	~852ms aver.
	☐ ECDSA-P256-SHA256:	~73ms aver.
	☐ ECDSA-P384-SHA384:	~120ms aver.
	☐ ECDSA-P521-SHA512:	~210ms aver.
	☐ EdDSA-25519-32 Byte:	~105ms aver.
	☐ EdDSA-25519-64 Byte:	~121ms aver.
	☐ EdDSA-25519-128 Byte:	~137ms aver.
	☐ EdDSA-25519-256 Byte:	~168ms aver.
	☐ EdDSA-25519-512 Byte:	~229ms aver.
	☐ EdDSA-25519-1024 Byte:	~353ms aver.
	☐ AES-(128|192|256)-CCM-Wrap:	~10ms aver.
	☐ HMAC-SHA-(1|256):	~4ms aver.
	☐ HMAC-SHA-(384|512):	~243ms aver.
Host interface	(USB) 1.x Full Speed (12Mbit/s) peripheral interface.	
Physical characteristics	☐ Form Factor: 'nano', designed for small-scale installations such as internal USB ports on servers ☐ Current consumption 20 mA average, 30 mA max. ☐ USB-A plug	
Enforcement of environmental regulations	☐ FCC ☐ CE ☐ WEEE ☐ ROHS	