Прайс-лист на стандартні ключі безпеки YubiKey 5, YubiKey FIPS, BIO та YubiHSM2 від липня 2023р.

	YubiKey 5 NFC	YubiKey 5C NFC	YubiKey 5 Nano	YubiKey 5C	YubiKey 5C Nano	YubiKey 5 CI	Security Key C NFC	Security Key NFC
В оптовій упаковці (по 50шт)								
Індивідуальна упаковка								
Ціна, грн	**3800,00**	**4000,00**	**4300,00**	**4000,00**	**4500,00**	**5100,00**	**2550,00**	**2350,00**
Опис	USB-ключ автентифікації, криптостійкий, підтримує стандарти FIDO2 та U2F, безпарольний вхід, одноразові паролі OTP, статичні паролі, режим смарт-карти PIV, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP. Підтримка NFC у моделі YubiKey 5 NFC та YubiKey 5C NFC.						USB/NFC-Ключ автентифікації, працює з будь-яким онлайн-сервісом з підтримкою FIDO2 або U2F.	USB/NFC-ключ автентифікації, працює з будь-яким онлайн-сервісом з підтримкою FIDO2 або U2F.
Розмір та вага	18 x 45 x 3.3мм, 3г.	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.	12 x 40.3 x 5мм, 2.9г.	18 x 45 x 3.3мм, 3г.	18 x 45 x 3.3мм, 3г.
Сертифікація								
Сертифікація FIDO certification™	Y	Y	Y	Y	Y	Y	Y	Y
Сертифікація FIPS 140								
Підтримувані підключення								
USB-A	Y		Y					Y
USB-C		Y		Y	Y	Y	Y	
Lightning						Y		
NFC (Зв'язок на малих відстанях)	Y	Y						Y
Тип пристрою								
Клавіатура HID	Y	Y	Y	Y	Y	Y		
Смарт-карта CCID	Y	Y	Y	Y	Y	Y		
Пристрій FIDO HID	Y	Y	Y	Y	Y	Y	Y	Y
Специфікації криптографії								
RSA 2048	Y	Y	Y	Y	Y	Y		
RSA 4096 (PGP)	Y	Y	Y	Y	Y	Y		
ECC p256	**	**	**	**	**	**	**	**
ECC p384	***	***	***	***	***	***		

** *ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP. Типом ключа, що генерується для ключової пари U2F, є ECC p256.*

*** *ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP*

OATH-TOTP вимагає додатковий додаток - Yubico Authenticator; Для ключів типу YubiKey 5 NFC, сертифікація FIDO застосовується для обох видів підключення - USB і NFC.

>the_kernel
We don't panic.

01001, Київ, Україна, вул. Михайла Грушевського 10 офіс №212.
Тел. +38 (044) 35 81 888; +38 (044) 35 31 999. Пошта: info@thekernel.com.ua,
www.thekernel.ua, yubikey.com.ua

Прайс-лист на сертифіковані ключі безпеки YubiKey FIPS від серпня 2022р.

	YubiKey 5 FIPS	YubiKey 5 Nano FIPS	YubiKey 5 C FIPS	YubiKey 5 C Nano FIPS	YubiKey 5C NFC FIPS	YubiKey 5 NFC FIPS	YubiKey 5Ci FIPS
Моделі							
Ціна, грн	**3650,00**	**6000,00**	**4550,00**	**5150,00**	**5450,00**	**5150,00**	**6600,00**
Опис	FIPS 140-2 сертифікований USB-ключ автентифікації, криптостійкий, підтримує стандарти FIDO2 та U2F, безпарольний вхід одноразові паролі OTP, статичні паролі, режим смарт-карти PIV, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP						
Розмір та вага	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	18 x 45 x 3.3мм, 3г.	18 x 45 x 3.3мм, 3г.	12 x 40.3 x 5мм, 2.9г.
Сертифікація							
Сертифікація FIDO Certification™	Y	Y	Y	Y	Y	Y	Y
Сертифікація FIPS 140	Y	Y	Y	Y	Y	Y	Y
Підтримувані підключення							
USB-A	Y	Y				Y	
USB-C			Y	Y	Y		Y
NFC (Зв'язок на малих відстнях)					Y	Y	
Lightning							Y
Тип пристрою							
Клавіатура HID	Y	Y	Y	Y	Y	Y	Y
Смарт-карта CCID	Y	Y	Y	Y	Y	Y	Y
Пристрій FIDO HID	Y	Y	Y	Y	Y	Y	Y
Специфікації криптографії							
RSA 2048	Y	Y	Y	Y	Y	Y	Y
RSA 4096 (PGP)	Y	Y	Y	Y	Y	Y	Y
ECC p256	**	**	**	**	**	**	**
ECC p384	***	***	***	***	***	***	***

*** ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP. Типом ключа, що генерується для ключової пари U2F, є ECC p256.*

**** ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP.*

>the_kernel
We don't panic.

01001, Київ, Україна, вул. Михайла Грушевського 10 офіс №212.
Тел. +38 (044) 35 81 888; +38 (044) 35 31 999. Пошта: info@thekernel.com.ua,
www.thekernel.ua, yubikey.com.ua

Прайс-лист на стандартні ключі безпеки YubiKey BIO від січня 2023р.

	YubiKey Bio – FIDO Edition	YubiKey C Bio - FIDO Edition
В оптовій упаковці (по 50шт)		
Індивідуальна упаковка		
Ціна, грн	**5900,00**	**6200,00**
Опис	Створено для бізнесу – підтримує низку бізнес-сценаріїв. Ідеально підходить для колцентрів та спільних робочих середовищ. Відповідає найсуворішим вимогам безпеки апаратного забезпечення завдяки шаблонам відбитків пальців, які зберігаються в захищеному елементі на ключі. Методи автентифікації: без пароля, надійний двофакторний, сильний багатофакторний. Працює з операційними системами та браузерами, включаючи Windows, macOS, Chrome OS, Linux, Chrome і Edge. Підтримує FIDO2/WebAuthn, FIDO U2F. Підтримує 1Password, Keeper®, Bitwarden Premium. Доступний у форм-факторах USB-A та USB-C з підтримкою біометрії.	
Розмір та вага	18 x 45 x 3,3 мм, 3 г	18 x 45 x 3,3 мм, 3 г
Біометрична автентифікація	Y	Y
Сертифікація		
FIDO certification™	Y	Y
Сертифікація FIPS 140		
Підтримувані підключення		
USB-A	Y	
USB-C		Y
Lightning		
Тип пристрою		
NFC (Зв'язок на малих відстанях)		
Клавіатура HID	Y	Y
Смарт-карта CCID		
Пристрій FIDO HID	Y	Y
Біометрична автентифікація	Y	Y
Специфікації криптографії		
RSA 2048		
RSA 4096 (PGP)		
ECC p256	**	**
ECC p384		

*** ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP. Типом ключа, що генерується для ключової пари U2F, є ECC p256.*

**** ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP*

OATH-TOTP вимагає додатковий додаток - Yubico Authenticator; Для ключів типу YubiKey 5 NFC, сертифікація FIDO застосовується для обох видів підключення – USB і NFC.

>the_kernel
We don't panic.

01001, Київ, Україна, вул. Михайла Грушевського 10 офіс №212.
Тел. +38 (044) 35 81 888; +38 (044) 35 31 999. Пошта: info@thekernel.com.ua,
www.thekernel.ua, yubikey.com.ua

Апаратний модуль безпеки YubiHSM 2 для захисту криптографічних ключів на серверах

	YubiHSM 2		YubiKey HSM 2 FIPS	
Модель				
Ціна, грн	**35 000,00**		**52 000,00**	
Розмір та вага	12 мм x 13 мм x 3.1 мм, 1 грам		12 мм x 13 мм x 3.1 мм, 1 грам	
Підтримка ОС				
Версія	Linux	CentOS 6, CentOS 7, Debian 8, Debian 9, Fedora 25, Ubuntu 1404, Ubuntu 1604	Linux	CentOS 7, Debian 8, Debian 9, Debian 10, Fedora 28, Fedora 30, Fedora 31, Ubuntu 1404, Ubuntu 1604, Ubuntu 1804, Ubuntu 1810, Ubuntu 1904, Ubuntu 1910
	MS Windows	Windows 10, Windows Server 2012, Windows Server 2016	MS Windows	Windows 10, Windows Server 2012, Windows Server 2016, Windows Server 2019
	Mac OS	10.12 Sierra, 10.13 High Sierra	Mac OS	10.12 Sierra, 10.13 High Sierra, 10.14 Mojave
Архітектура	amd64		amd64	
Сертифікація FIPS 140			Y	
Криптографічні можливості				
Хешування	Застосовується з HMAC та асиметричними підписами SHA-1, SHA-256, SHA-384, SHA-512		Застосовується з HMAC та асиметричними підписами SHA-1, SHA-256, SHA-384, SHA-512	
RSA	2048, 3072, и 4096-бітні ключі Підпис за допомогою PKCS#1v1.5 та PSS Дешифрація PKCS#1v1.5 и OAEP		2048, 3072, and 4096 bit keys Signing using PKCS#1v1.5 and PSS Decryption using PKCS#1v1.5 and OAEP	
Еліптична криптографія (ECC)	Криві: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 Підпис: ECDSA (все окрім curve25519), EdDSA (тільки curve25519) Дешифрація: ECDH (все окрім curve25519)		Криві: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 Підпис: ECDSA (все окрім curve25519), EdDSA (тільки curve25519) Дешифрація: ECDH (все окрім curve25519)	
Упаковка ключів	Імпорт та експорт за допомогою NIST AES-CCM Wrap при 128, 196, та 256 бітах		Імпорт та експорт за допомогою NIST AES-CCM Wrap при 128, 196, та 256 бітах	
Випадкові числа	Вбудований в чіп генератор реальних випадкових чисел (TRNG) з зерном NIST SP 800-90 AES 256 CTR_DRBG		Вбудований в чіп генератор реальних випадкових чисел (TRNG) з зерном NIST SP 800-90 AES 256 CTR_DRBG	
Атестація	Згенеровані на пристрої асиметричні ключові пари можуть проходити перевірку за допомогою заводського сертифікованого ключа атестації та сертифіката, або за допомогою Вашого особистого ключа, імпортованого в модуль безпеки		Згенеровані на пристрої асиметричні ключові пари можуть проходити перевірку за допомогою заводського сертифікованого ключа атестації та сертифіката, або за допомогою Вашого особистого ключа, імпортованого в модуль безпеки	
Швидкодія	Швидкодія залежить від цільового застосування. У прикладі приведена метрика YubiHSM2, незадіяного в інших процесах: RSA-2048-PKCS1-SHA256: ~139ms серед. RSA-3072-PKCS1-SHA384: ~504ms серед. RSA-4096-PKCS1-SHA512: ~852ms серед. ECDSA-P256-SHA256: ~73ms серед. ECDSA-P384-SHA384: ~120ms серед. ECDSA-P521-SHA512: ~210ms серед. EdDSA-25519-32 Байт: ~105ms серед. EdDSA-25519-64 Байт: ~121ms серед. EdDSA-25519-128 Байт: ~137ms серед. EdDSA-25519-256 Байт: ~168ms серед. EdDSA-25519-512 Байт: ~229ms серед. EdDSA-25519-1024 Байт: ~353ms сред. AES-(128|192|256)-CCM-Wrap: ~10ms серед. HMAC-SHA-(1|256): ~4ms серед. HMAC-SHA-(384|512): ~243ms серед.		Швидкодія залежить від цільового застосування. У прикладі приведена метрика YubiHSM2, незадіяного в інших процесах: RSA-2048-PKCS1-SHA256: ~139ms avg RSA-3072-PKCS1-SHA384: ~504ms avg RSA-4096-PKCS1-SHA512: ~852ms avg ECDSA-P256-SHA256: ~73ms avg ECDSA-P384-SHA384: ~120ms avg ECDSA-P521-SHA512: ~210ms avg EdDSA-25519-32Bytes: ~105ms avg EdDSA-25519-64Bytes: ~121ms avg EdDSA-25519-128Bytes: ~137ms avg EdDSA-25519-256Bytes: ~168ms avg EdDSA-25519-512Bytes: ~229ms avg EdDSA-25519-1024Bytes: ~353ms avg AES-(128|192|256)-CCM-Wrap: ~10ms avg HMAC-SHA-(1|256): ~4ms avg HMAC-SHA-(384|512): ~243ms avg	
Хост-інтерфейс	(USB) 1.x Full Speed (12Mbit/s) периферійний інтерфейс.		(USB) 1.x Full Speed (12Mbit/s) периферійний інтерфейс.	
Фізичні характеристики	Форм-фактор: 'nano', розроблений для малогабаритних місць установки, таких як внутрішні USB порти серверів З поглинанням току 20 мА серед., 30 мА макс. USB-A штекер		Форм-фактор: 'nano', розроблений для малогабаритних місць установки, таких як внутрішні USB порти серверів З поглинанням току 20 мА серед., 30 мА макс. USB-A штекер	
Забезпечення дотримання екологічних норм	FCC CE WEEE ROHS		FCC CE WEEE ROHS	

>the_kernel
We don't panic.

01001, Київ, Україна, вул. Михайла Грушевського 10 офіс №212.
Тел. +38 (044) 35 81 888; +38 (044) 35 31 999. Пошта: info@thekernel.com.ua,
www.thekernel.ua, yubikey.com.ua

NIST | Національний Інститут Стандартів та Технологій (США)
Сертифікація криптографічних модулів YubiKey