>

yubico

Прайс-листная стандартные ключи безопасности YubiKey5, YubiKeyFIPS и YubiHSM2 с декабря 2021г.

	YubiKey 5 NFC	YubiKey 5C NFC	YubiKey 5 Nano	YubiKey 5C	YubiKey 5C Нано	YubiKey 5 CI	Электронный ключ	Электронный ключ NFC
Оптовой упаковке(за 50шт)								
Индивидуальнаяупаковка								
Цена	2100,00 грн	2500,00 грн.	грн2250,00	грн2250,00	2650,00 грн	2950,00 грн	1150,00 грн	1450,00 грн.
Описание	USB-ключавтентификации,криптоустойчивый,поддерживает стандарты FIDO2 и U2F, беспарольный вход, одноразовые пароли OTP, статичные пароли, режим смарт-карты PIV, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP. Поддержка NFC в модели YubiKey 5 NFC и YubiKey 5CNFC.						USB-Ключ аутентификации, работает с любой которым онлайн-сервисом с поддержкой FIDO2 или U2F.	USB/NFC-ключ аутентификации, работаетбудь-которым онлайн-сервисом с поддержкой FIDO2 абоU2F.
Размертовая	18x45x3,3 мм, 3д.	18x45x3,3 мм, 3д.	12 x 13 x 3,1 мм, 1d.	12,5x29,5x5 мм, 2 г.	12x10.1x7,1г.	12x40,3x5 мм, 2,9 г.	18x45x3,3 мм, 3д.	18x45x3,3 мм, 3д.
Сертификация								
СертификацияFIDOcertification ™	Y	Y	Y	Y	Y	Y	Y	Y
Сертификация FIPS 140								
Поддерживаемые подключения								
USB-A	Y		Y				Y	Y
USB-C		Y		Y	Y	Y		
Молния						Y		
NFC (Связная малых расстояниях)	Y	Y						Y
Типпристрою								
КлавиатураHID	Y	Y	Y	Y	Y	Y		
Смарт-картаCCID	Y	Y	Y	Y	Y	Y		
Устройство FIDO HID	Y	Y	Y	Y	Y	Y	Y	Y
Спецификации криптографии								
RSA 2048	Y	Y	Y	Y	Y	Y		
RSA 4096 (PGP)	Y	Y	Y	Y	Y	Y		
ECC p256	**	**	**	**	**	**	**	**
ECC p384	***	***	***	***	***	***		

** ECC применяется только к аплетусу карты, не применяется к апплету OpenPGP.

*** ECC применяется только к апплетусмарткарты; не применяется к апплету OpenPGP

OATH-TOTP требует дополнительное приложение- YubicoAuthenticator;

>the_kernel
We don't panic.

01001,Киев,Украина,ул. Михаила Грушевского10офис №212.

Тел.+38(044)35 81 888; +38 (044) 35 31 999. Почта: info@thekernel.com.ua ,

www.thekernel.ua, yubikey.com.ua

Прайс-лист на сертифицированные ключи безопасности YubiKey FIPS от декабря 2021г.

	YubiKey FIPS	ЮбиКей Нано FIPS	YubiKey C FIPS	YubiKey C Нано FIPS	YubiKey 5C NFC FIPS	YubiKey 5 NFC FIPS	YubiKey 5Ci FIPS
Модели							
Цена	2150,00 грн.	2550,00 грн	2550,00 грн	3500,00 грн.	3050,00 грн	2500,00 грн.	грн 3450,00
Описание	FIPS 140-2 сертифицированный USB-ключевтентификации, криптостойкий, поддерживает стандарты FIDO2 и U2F, беспарольный вход одноразовые пароли OTP, статические пароли, режим смарт-карты PIV, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP						
Размертовая	18x45x3,3 мм, 3 года	12x13x3,1 мм, 1д	12,5 x 29,5 x 5мм,2г	12x10.1x7,1г	18x45x3,3 мм, 3d	18x45x3,3 мм, 3d	12x40,3x5 мм, 2.9г.
Сертификация							
СертификацияFIDOСертификация ™	Y	Y	Y	Y	Y	Y	Y
СертификацияFIPS 140	Y	Y	Y	Y	Y	Y	Y
Поддерживаемые подключения							
USB-A	Y	Y				Y	
USB-C			Y	Y	Y		Y
NFC(Связнаямалых отст.)					Y	Y	
Молния							Y
Типпристрою							
КлавиатураHID	Y	Y	Y	Y	Y	Y	Y
Смарт-картаCCID	Y	Y	Y	Y	Y	Y	Y
УстройствоFIDO СПРЯТАННЫЙ	Y	Y	Y	Y	Y	Y	Y
Спецификации криптографии							
RSA 2048	Y	Y	Y	Y	Y	Y	Y
RSA 4096 (PGP)	Y	Y	Y	Y	Y	Y	Y
ECC p256	**	**	**	**	**	**	**
ECC p384	***	***	***	***	***	***	***

** ECC применяется только к аплетусу карты, не применяется к апплету OpenPGP.p256 ..

*** ECC применяется только к аплету смартфона; не применяется к апплету OpenPGP .

>the_kernel
We don't panic.

01001,Киев,Украина,ул. Михаила Грушевского10офис №212.
Тел.+38(044)35 81 888; +38 (044) 35 31 999. Почта: info@thekernel.com.ua ,
www.thekernel.ua, yubikey.com.ua

NIST|НациональныйИнститутСтандартовиТехнологий(США)

Сертификация криптографических модулей YubiKey

Аппаратный модуль безопасности YubiHSM 2 для защиты криптографических ключей на серверах

	ЮбиХСМ 2	YubiKey HSM 2 FIPS
Модель		
Цена	грн25800.00	34000,00 грн
Размертовая	12 мм x 13 мм x 3,1 мм, 1 г	12 мм x 13 мм x 3,1 мм, 1 г
Поддержка ОС		
Версия	Linux: CentOS 6, CentOS 7, Debian 8, Debian 9, Fedora 25, Ubuntu 1404, Ubuntu 1604	Linux: CentOS 7, Debian 8, Debian 9, Debian10, 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 Мохаве
Архитектура	amd64	amd64
Сертификация FIPS 140		Y
Криптографические возможности		
Хеширование	Применяется с HMAC и асимметричными подписями. SHA-1, SHA-256, SHA-384, SHA-512	Применяется с HMAC и асимметричными подписями. SHA-1, SHA-256, SHA-384, SHA-512
ЮАР	2048,3072,и4096-битные ключи Подпись с помощью PKCS # 1v1.5 и PSSДешифрацияPKCS#1v1.5иOAEP	2048, 3072 и 4096 битные ключи Подписание с использованием PKCS # 1v1.5 и PSS Расшифровка с использованием PKCS # 1v1.5 и OAEP
Эллиптическая криптография (ТАК ДАЛЕЕ)	Кривые:secp224r1,secp256r1,secp256k1,secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 Подпись:ECDSA(всеокремcurve25519),EdDSA(только curve25519) Расшифровка: ECDH (всеокрімcurve25519)	Кривые:secp224r1,secp256r1,secp256k1,secp384r1,secp521r, bp256r1, bp384r1, bp512r1, curve25519 Подпись:ECDSA(всеокремcurve25519),EdDSA(только curve25519) Расшифровка: ECDH (всеокрімcurve25519)
Упаковка ключей	Импорт и экспорт с помощью NISTAES-CCMWrap при 128, 196 и 256 бит	Импорт и экспорт с помощью NISTAES-CCM Wrap при 128, 196 и 256 бит
Случайные числа	Встроенный цепь генератор реальных случайных чисел (TRNG) ззерномNISTSP800-90 AES 256 CTR_DRBG	Встроенный цепь генератор реальных случайных чисел (TRNG) ззерномNISTSP800-90 AES 256 CTR_DRBG
Аттестация	Сгенерированные на устройстве ассиметричные ключевые пары могут проходить проверку с помощью заводского сертифицированного ключа аттестации и сертификата, абоза помощью Вашего личного ключа, импортированного в модульбезпеки	Сгенерированные на устройстве ассиметричные ключевые пары могут проходить проверку с помощью заводского сертифицированного ключа аттестации и сертификата, абоза помощью Вашего личного ключа, импортированного в модуль безопасности
Быстродействие	Быстрое действие зависит от целевого применения. приведенаметрикаYubiHSM2,незадіяноговіншихпроцесах: RSA-2048-PKCS1-SHA256: ~ 139 мсеред. RSA-3072-PKCS1-SHA384: ~ 504 мсеред. RSA-4096-PKCS1-SHA512: ~ 852 мсеред. ECDSA-P256-SHA256: ~ 73 мсред. ECDSA-P384-SHA384: ~ 120 мсек. ECDSA-P521-SHA512: ~ 210 мсеред. EdDSA-25519-32 Байт: ~ 105 мсред. EdDSA-25519-64Байт: ~ 121 мсред. EdDSA-25519-128Байт: ~ 137 мсред. EdDSA-25519-256Байт: ~ 168 мсред. EdDSA-25519-512Байт: ~ 229 мсред. EdDSA-25519-1024Байт: ~ 353 мсред. AES- (128 | 192 | 256) -CCM-Wrap: ~ 10 мсеред. HMAC-SHA- (1 | 256): ~ 4 мсред. HMAC-SHA- (384 | 512): ~ 243 мсред.	Быстрое действие зависит от целевого применения. приведенаметрикаYubiHSM2,незадіяноговіншихпроцесах: 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: ~ 10 мс в среднем HMAC-SHA-(1|256): ~4ms avg HMAC-SHA-(384|512): ~243ms avg
Хост-интерфейс	(USB) 1.x Full Speed (12Mbit/s) периферийный интерфейс.	(USB) 1.x Full Speed (12Mbit/s) периферийный интерфейс .
Физические характеристики	Форм-фактор: 'nano', разработанный для малогабаритных мест установки,такихяквнутрішніUSBпортисерверів С поглощением тока 20мАсред.,30мАмакс. USB-Аштекер	Форм-фактор: 'nano', разработанный для малогабаритных мест установки,такихяквнутрішніUSBпортисерверів С поглощением тока 20мАсред.,30мАмакс. USB-Аштекер
Обеспечение соблюдение экологических норм	FCC ЭТО WEEE ROHS	FCC ЭТО WEEE ROHS

>the_kernel We don't panic.

01001,Киев,Украина,ул. Михаила Грушевского10офис №212.

Тел.+38(044)35 81 888; +38 (044) 35 31 999. Почта: info@thekernel.com.ua ,

www.thekernel.ua, yubikey.com.ua

>the_kernel
We don't panic.

01001,Киев,Украина,ул. Михаила Грушевского10офис №212.
Тел.+38(044)35 81 888; +38 (044) 35 31 999. Почта: info@thekernel.com.ua ,
www.thekernel.ua, yubikey.com.ua