

YubiKey FIPS

Технічні характеристики

Сертифіковані ключі YubiKey FIPS

Промисловий лідер серед FIPS 140-2 сертифікованих апаратних ключів безпеки — надійний і простий у застосуванні. Серія YubiKey FIPS забезпечує надійний захист від фішингу та викрадення облікових даних. Ці ключі дозволяють корпораціям та державним службам відповідати найвищому рівню вимог до безпечної автентифікації.



Технічні характеристики

Інтерфейс

USB USB 2.0 типу А (Сумісний з USB 3.0)

Режими роботи

Одноразовий пароль OTP OTP аплет містить два програмованих слоти, кожен може вміщувати один з наступних типів облікових даних:

- Одноразовий пароль Yubico
- HMAC-SHA1 Виклик-Відповідь
- Статичний пароль
- OATH-HOTP

Режим USB: OTP

Універсальна двофакторна автентифікація U2F Режим U2F дозволяє зберігати необмежену кількість облікових даних та є FIDO-сертифікованим.

Режим USB: FIDO

OATH Цей режим дозволяє зберігати до 32-х записів облікових даних OATH і підтримує як OATH-TOTP (фактор часу), так і OATH-HOTP (фактор лічильника). Для доступу до даного аплету потрібен Yubico Authenticator.

Режим USB: CCID

PIV-сумісна смарт-карта Режим смарт-карти PIV (посвідчення особистості).
Значення за замовчуванням:

- PIN: 123456
- PUK: 12345678
- Ключ керування: 10203040506070801020304050607080102030405060708

Підтримувані алгоритми:

- RSA 2048
- ECC P256
- ECC P384

Режим USB: CCID

OpenPGP Цей режим відповідає специфікаціям смарт-карт OpenPGP версії 2.0, яка може застосовуватись з GnuPG. Для ключів довжиною більш ніж 2048 біт потрібно GnuPG версії 2.0 або вище.

Підтримувані алгоритми:

- RSA 2048
- RSA 3072
- RSA 4096

Режим USB: CCID

Загальні характеристики

Інтерфейс	USB-A
Габаритні розміри (Ш*Д*В)	18мм x 45мм x 3.3мм
Вага	3 г

Температурні характеристики

Робочий режим	Від 0 °С до 40 °С
Зберігання	Від -20 °С до 85 °С

Криптографічні характеристики (протоколи та алгоритми)

RSA 2048	Макс. довжина ключа: 2048 біт
RSA 3072	Макс. довжина ключа: 3072 біт
RSA 4096	Макс. довжина ключа: 4096 біт
ECC p256	Макс. довжина ключа: 256 біт
ECC p384	Макс. довжина ключа: 384 біт
SHA1	Макс. довжина ключа: 160 біт

Виникли питання?

Об'єднані Арабські Емірати – Головний офіс

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

Tel. +971 (04) 7017 260

Email: info@thekernel.com