YubiKey FIPS

Technical specifications

ЮбиКей FIPS

Технические характеристики

Сертифицированные ключи YubiKey FIPS

Промышленный лидер среди FIPS 140-2 сертифицированных аппаратных ключей аутентификации — надежный и простой в задействовании. Серия YubiKey FIPS обеспечивает надежную безопасность и защиту от фишинга и кражи учетных данных. Данные ключи позволяют корпорациям и государственным службам соответствовать высочайшим уровням обеспечения безопасной аутентификации.

yubico
Trust the Net.

Технические характеристики

Интерфейс	
USB	USB 2.0 тип A

Режимы работы	
Одноразовый пароль OTP	OTP апплет содержит два программируемых слота, каждый может вмещать один из следующих видов учетных данных: • Одноразовый пароль Yubico • HMAC-SHA1 Вызов-Ответ • Статический пароль • OATH-HOTP Режим USB: OTP
Универсальная двухфакторная аутентификация U2F	Режим U2F позволяет хранить неограниченное количество учетных данных и является FIDO-сертифицированным. Режим USB: FIDO
OATH	Данный режим позволяет хранить до 32-х записей учетных данных OATH и поддерживает как OATH-TOTP (фактор времени), так и OATH-HOTP (фактор счетчика). Для доступа к данному апплету требуется Yubico Authenticator. Режим USB: CCID
PIV-совместимая смарт-карта	Режим смарт-карты PIV (удостоверение личности). Значения по умолчанию: Поддерживаемые алгоритмы: • RSA 2048 • ECC P256 • ECC P384 Режим USB: CCID
OpenPGP	Данный режим соответствует спецификации смарт-карт OpenPGP версии 2.0, которая может применяться с GnuPG. Для ключей длиной более 2048 бит требуется GnuPG версии 2.0 или выше. Поддерживаемые алгоритмы: • RSA 2048 • RSA 3072 • RSA 4096 Режим USB: CCID

Общие характеристики	
Интерфейс	USB-A
Габаритные размеры (Ш*Д*В)	18мм x 45мм x 3.3мм
Вес	3 г

Температурные характеристики	
Рабочий режим	От 0 °C до 40 °C
Хранение	От -20 °C до 85 °C

Криптографические характеристики (протоколы и алгоритмы)	
RSA 2048	Макс. длина ключа: 2048 бит
RSA 3072	Макс. длина ключа: 3072 бит
RSA 4096	Макс. длина ключа: 4096 бит
ECC p256	Макс. длина ключа: 256 бит
ECC p384	Макс. длина ключа: 384 бит
SHA1	Макс. длина ключа: 160 бит

Есть вопросы?

Российская Федерация:

121099, Москва, Смоленская площадь, дом 3, офис 49

Тел. +7 (495) 231 82 24

Эл. почта: info@thekernel.ru

Объединённые Арабские Эмираты - Главный офис

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

Tel. +971 (04) 7017 260

Email: info@thekernel.com