

YubiKey C FIPS

Technical specifications

ЮбиКей С 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.



Технические характеристики

Интерфейс

USB	USB 2.0 тип C
-----	---------------

Режимы работы

Одноразовый пароль OTP	<p>OTP апплет содержит два программируемых слота, каждый может вмещать один из следующих видов учетных данных:</p> <ul style="list-style-type: none">• Одноразовый пароль Yubico• HMAC-SHA1 Вызов-Ответ• Статический пароль• OATH-HOTP <p>Режим USB: OTP</p>
Универсальная двухфакторная аутентификация U2F	<p>Режим U2F позволяет хранить неограниченное количество учетных данных и является FIDO-сертифицированным.</p> <p>Режим USB: FIDO</p>
OATH	<p>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.</p> <p>Режим USB: CCID</p>
PIV-совместимая смарт-карта	<p>Режим смарт-карты PIV (удостоверение личности).</p> <p>Поддерживаемые алгоритмы:</p> <ul style="list-style-type: none">• RSA 2048• ECC P256• ECC P384 <p>Режим USB: CCID</p>
OpenPGP	<p>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.</p> <p>Поддерживаемые алгоритмы:</p> <ul style="list-style-type: none">• RSA 2048• RSA 3072• RSA 4096 <p>Режим USB: CCID</p>

Общие характеристики

Интерфейс	USB-C
Габаритные размеры (Ш*Д*В)	12.5мм x 29.5мм x 5мм
Вес	2 г

Температурные характеристики

Рабочий режим	От 0 °С до 40 °С
Хранение	От -20 °С до 85 °С

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