

YubiKey 5C

Technical specifications

ЮбиКей 5С

Технические характеристики

5-е поколение ключей безопасности для надежной аутентификации

YubiKey 5 — это серия компактных USB ключей безопасности для многофакторной аутентификации. Теперь с поддержкой FIDO2 беспарольной аутентификации и USB + NFC моделью — YubiKey 5 NFC. Многофакторная аутентификация в сочетании с аппаратными решениями, позволяет повысить защиту учетных записей до наивысшего уровня.

Широко известно, что одноразовые СМС пароли подвержены взлому и не могут обеспечить должный уровень защищенности. Избежать неприятностей, связанных с хакерскими атаками и клонированием SIM карт, можно используя аппаратный ключ безопасности для защиты доступа к учетным записям приложений и

онлайн сервисов. Данные USB ключи готовы к работе с ОС Windows, Linux и macOS, а также с популярными браузерами, приложениями и вебсайтами. Пятое поколение YubiKey сочетает в себе поддержку многих алгоритмов шифрования и простоту использования — безопасный вход в учетную запись всего лишь одним касанием к кнопке.



Технические характеристики

Интерфейс

USB USB 2.0 тип C

Режимы работы

FIDO2 Режим FIDO2 позволяет хранить учетные данные для последующего беспарольного входа в учетные записи на сайтах и устройствах.

Режим USB: FIDO

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:

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

Поддерживаемые алгоритмы:

- RSA 1024
- RSA 2048
- ECC P256
- ECC P384

Слоты информации:

- Слот 9a: Аутентификация
- Слот 9b: Ключ управления
- Слот 9c: Цифровая подпись
- Слот 9d: Управление ключами
- Слот 9e: Аутентификация карты
- Слот f9: Аттестация
- Слоты 82-95: Управление недействующими ключами

Режим USB: CCID

| | |
|----------------|---|
| 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 1024 • RSA 2048 • RSA 3072 • RSA 4096 <p>Режим USB: CCID</p> |
|----------------|---|

| Общие характеристики | |
|----------------------------|-----------------------|
| Интерфейс | USB-A |
| Габаритные размеры (Ш*Д*В) | 12.5мм x 29.5мм x 5мм |
| Вес | 2 г |

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

| Криптографические характеристики (протоколы и алгоритмы) | |
|--|-----------------------------|
| RSA 1024 | Макс. длина ключа: 1024 бит |
| 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