

Обзорная информация о смарт-картах

В этом документе

- [Общая информация](#)
- [Криптографические возможности смарт-карт](#)
- [Возможности производства](#)
 - [Оснащение метками](#)
 - [Персонализация](#)
- [Считыватели смарт-карт](#)
 - [Считыватель Рутокен SCR 3001](#)

Общая информация

Смарт-карты Рутокен являются аналогами USB-токенов Рутокен. Вся информация о токенах применима к смарт-картам Рутокен.

Смарт-карты и их аналоги

| Название модели смарт-карты | Название модели аналога (USB-токена) |
|----------------------------------|--------------------------------------|
| Смарт-карта Рутокен ЭЦП 2.0 2100 | Рутокен ЭЦП 2.0 2100 |
| Смарт-карта Рутокен ЭЦП 3.0 NFC | Рутокен ЭЦП 3.0 NFC |

Криптографические возможности смарт-карт

| Критерий | Смарт-карта Рутокен ЭЦП 3.0 | Смарт-карта Рутокен ЭЦП 2.0 2100 |
|--|---|--|
| Основные характеристики | | |
| Аппаратная часть | защищенный микроконтроллер со встроенной энергонезависимой памятью | защищенный микроконтроллер со встроенной энергонезависимой памятью |
| Интерфейс | Смарт-карта ID-1 | Смарт-карта ID-1 |
| EEPROM память | 128 Кбайт | 64 Кбайта, 80 Кбайт |
| Габаритные размеры | 85,6 x 53,98 x 0,76 мм | 85,6 x 53,98 x 0,76 мм |
| Масса | 5,5 г | 5,4 г |
| Серийный номер | 32 бита, уникальный | 32 бита, уникальный |
| Поддерживаемые ОС | <ul style="list-style-type: none">• Microsoft Windows 11/10/8.1/2019/2016/2012R2/8/2012/7/2008R2/Vista/2008• GNU/Linux (в том числе отечественные)• Apple macOS 10.9 и новее• Android 5 и новее• iOS 13 и новее• Аврора 4+ | <ul style="list-style-type: none">• Microsoft Windows 10 /2019/2016/8.1/8/2012/7 /2008/Vista/2003/XP,• GNU/Linux• Apple macOS 10.9 и новее |
| Поддерживаемые интерфейсы и стандарты | | |

| | | |
|---|---|--|
| PKCS#11 версии 2.20, включая российский профиль (2.30 draft) | да | да |
| Microsoft Crypto API | да | да |
| PC/SC | да | да |
| Microsoft Smartcard API | да | да |
| USB CCID (работа без установки драйверов) | да | да |
| ISO/IEC 7816 | <ul style="list-style-type: none"> • ISO/IEC 7816-3, протокол T=0 и T=1 для контактной микросхемы, • ISO 14443 (NFC) для бесконтактной микросхемы. | ISO/IEC 7816-4, 7816-8, 7816-12 |
| Криптопровайдер | собственный Crypto Service Provider | собственный Crypto Service Provider |
| Сертификаты X.509 версии 3 на уровне программного обеспечения | да | да |
| Криптографические возможности | | |
| Поддержка алгоритма ГОСТ 28147-89 | да, аппаратная реализация | да, аппаратная реализация |
| Поддержка алгоритма ГОСТ Р 34.12-2015 (Магма) | да, аппаратная реализация | - |
| Поддержка алгоритма ГОСТ Р 34.12-2015 (Кузнечник) | да, аппаратная реализация | - |
| Режимы шифрования | <ul style="list-style-type: none"> • простая замена, • гаммирование, • гаммирование с обратной связью | <ul style="list-style-type: none"> • простая замена, • гаммирование, • гаммирование с обратной связью |
| Режим выработки имитовставки | да | да |

| | | |
|--|--|--|
| Генерация ключей шифрования | да | да |
| Импорт ключей шифрования | нет | нет |
| Запрет экспорта ключей шифрования | да | да |
| Поддержка алгоритма ГОСТ Р 34.10-2012 | да, аппаратная реализация | да, аппаратная реализация |
| Формирование и проверка электронной цифровой подписи | да | да |
| Генерация ключевых пар | да, с проверкой качества | да, с проверкой качества |
| Импорт ключевых пар | да, с помощью ключа эмитента | нет |
| Запрет экспорта ключевых пар | да | да |
| Срок действия закрытых ключей | до 3 лет | до 3 лет |
| Размер закрытого ключа | 256 и 512 бит | 256 и 512 бит |
| Поддержка алгоритма ГОСТ 34.11-2012 (256 и 512 бит) | аппаратная реализация | аппаратная реализация |
| Вычисление значения хэш-функции | да, в т.ч. с возможностью последующего формирования ЭП | да, в т.ч. с возможностью последующего формирования ЭП |

| | | |
|--|---|--|
| Формирование и проверка электронной цифровой подписи | да | да |
| Генерация ключевых пар | да, с проверкой качества | да, с проверкой качества |
| Импорт ключевых пар | нет | нет |
| Запрет экспорта ключевых пар | да | да |
| Срок действия закрытых ключей | до 3 лет | до 3 лет |
| Поддержка алгоритма ГОСТ 34.11-94 | аппаратная реализация | аппаратная реализация |
| Выработка сессионных ключей (ключей парной связи) | да <ul style="list-style-type: none"> по схеме VKO GOST R 34.10-2001 согласно RFC 4357 по схеме VKO GOST R 34.10-2012 согласно RFC 7836 по схеме KEG | да <ul style="list-style-type: none"> по схеме VKO GOST R 34.10-2001 согласно RFC 4357 по схеме VKO GOST R 34.10-2012 согласно RFC 7836 для версии 2.0 |
| Расшифрование по схеме EC El-Gamal | да | да |
| Поддержка алгоритма RSA | аппаратная реализация расшифрования и подписи (RSA-1024, RSA-2048, RSA-4096) | аппаратная реализация расшифрования и подписи |
| Формирование электронной подписи | да | да |
| Генерация ключевых пар | да, с проверкой качества | да, с проверкой качества |
| Импорт ключевых пар | да | да |
| Запрет экспорта ключевых пар | да | да |
| Размер ключей | до 4096 бит | до 2048 бит |

| | | |
|--|---|---|
| Поддержка алгоритма ECDSA | да, кривые secp256k1 и secp256r1 | нет |
| Поддержка алгоритма в DES (3DES), AES, RC2, RC4, MD4, MD5, SHA-1, SHA-256 | хранение экспортируемых ключей в EF, SHA-1, SHA-256, MD5 в PKCS#11, RC4, MD4, MD5, SHA-1, SHA-256, 3DES, AES в minidriver | хранение экспортируемых ключей в EF, SHA-1, SHA-256, MD5 в PKCS#11, RC4, MD4, MD5, SHA-1, SHA-256, 3DES, AES в minidriver |
| Формирование электронной подписи | да | - |
| Генерация ключевых пар | да, с проверкой качества | - |
| Импорт ключевых пар | да | - |
| Работа с СКЗИ «КриптоПро 5.0» по протоколу защиты канала SESPAKE (ФКН2). | да | - |
| Сведения о сертификации | | |
| Наличие сертификата ФСТЭК | в процессе | да |
| Наличие сертификата ФСБ | в процессе | да (1,2,3) |
| Файловая система | | |
| Файловая структура | встроенная, по стандарту ISO/IEC 7816-4 | встроенная, по стандарту ISO/IEC 7816-4 |
| Тип размещения файловых объектов в памяти (архитектура файловой системы) | использование File Allocation Table (FAT) | использование File Allocation Table (FAT) |
| Количество папок и уровень их вложенности | уровень ограничен объемом свободной памяти | уровень ограничен объемом свободной памяти |

| | | |
|--|---|---|
| Число файловых объектов внутри папки | до 255 включительно | до 255 включительно |
| Хранение ключевой информации | <ul style="list-style-type: none"> использование файлов Rutoken Special File (RSF-файлов) для хранения ключей шифрования, сертификатов; использование predetermined папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов | <ul style="list-style-type: none"> использование файлов Rutoken Special File (RSF-файлов) для хранения ключей шифрования, сертификатов; использование predetermined папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов |
| Запрет экспорта закрытых и симметричных ключей | да | да |
| Шифрование файловой системы | да, прозрачное, алгоритм ГОСТ 28147-89, уникальный ключ шифрования для каждого экземпляра устройства | да, прозрачное, алгоритм ГОСТ 28147-89, уникальный ключ шифрования для каждого экземпляра устройства |
| Дополнительно | использование Security Environment для удобной настройки параметров криптографических операций | использование Security Environment для удобной настройки параметров криптографических операций |
| Аутентификация и конфиденциальность | | |
| Двухфакторная аутентификация | да, предъявление токена + ввод PIN-кода | да, предъявление токена + ввод PIN-кода |
| Уровни доступа | <ul style="list-style-type: none"> Гость Пользователь Администратор | <ul style="list-style-type: none"> Гость Пользователь Администратор |
| Разграничение доступа к файловым объектам в соответствии с уровнем доступа | да | да |

| | | |
|--|---|---|
| Ограничен ие числа попыток ввода PIN- кода | да, настраиваемое | да, настраиваемое |
| Поддержка PIN-кодов | <ul style="list-style-type: none"> • глобальные PIN-коды: Администратора и Пользователя, • локальные PIN-коды (для защиты конкретных объектов в памяти устройства, например, контейнеров сертификатов) • Настраиваемые аппаратные политики качества PIN-кодов | <ul style="list-style-type: none"> • глобальные PIN-коды: Администратора и Пользователя, • локальные PIN-коды (для защиты конкретных объектов в памяти устройства, например, контейнеров сертификатов) |
| Ограничен ие минимальн ого размера PIN-кода | да, настраивается независимо для любого PIN-кода | да, настраивается независимо для любого PIN- кода |
| Дополните льно | <ul style="list-style-type: none"> • поддержка комбинированной аутентификации: <ul style="list-style-type: none"> • аутентификация по глобальным PIN-кодам • аутентификация по глобальным PIN-кодам в сочетании с аутентификацией по локальным PIN-кодам. • возможность одновременного контроля прав доступа, заданных до 7-ю локальными PIN-кодами. • индикация факта смены глобальных PIN-кодов с умалчиваемых на оригинальные. | <ul style="list-style-type: none"> • поддержка комбинированной аутентификации: <ul style="list-style-type: none"> • аутентификация по глобальным PIN-кодам • аутентификация по глобальным PIN-кодам в сочетании с аутентификацией по локальным PIN-кодам. • возможность одновременного контроля прав доступа, заданных до 7-ю локальными PIN-кодами. • индикация факта смены глобальных PIN-кодов с умалчиваемых на оригинальные. |
| Flash- память | нет | нет |
| Объем памяти, Гб | - | - |
| Средняя скорость записи, Мбайт/сек | - | - |
| Средняя скорость чтения, Мбайт/сек | - | - |

| | | |
|---|---|--|
| Возможность встраивания радиочастотной метки | да | да, модельный ряд Рутокен ЭЦП 2.0 RF, Рутокен ЭЦП 2.0 2100 RF |
| Поддерживаемые типы меток | Работа с системами контроля и управления доступом, поддерживающими протокол NFC | <ul style="list-style-type: none"> • EM-Marine, • Mifare, • ProxCard II и ISOProx II, • Indala (на заказ) |
| Встроенный контроль и индикация | | |
| Контроль целостности и прошивки | да | да |
| Контроль целостности и системных областей памяти | да | да |
| Проверка целостности и RSF-файлов перед использованием | да | да |
| Типы счетчиков | <ul style="list-style-type: none"> • счетчик изменений файловой системы • счетчик изменений PIN-кодов • счетчики последовательных неудачных попыток ввода PIN-кодов • счетчик успешных операций электронной подписи | <ul style="list-style-type: none"> • счетчик изменений файловой системы • счетчик изменений PIN-кодов • счетчики последовательных неудачных попыток ввода PIN-кодов • счетчик успешных операций электронной подписи (для версии 2.0) |
| Проверка правильности функционирования криптографических алгоритмов | да | да |
| Режимы работы светодиодного индикатора | <ul style="list-style-type: none"> • готовность к работе • выполнение операции • нарушение в системной области памяти | <ul style="list-style-type: none"> • готовность к работе • выполнение операции • нарушение в системной области памяти |

Возможности производства

Оснащение метками

Смарт-карты Рутокен ЭЦП 2.0 2100 могут быть оснащены бесконтактным интерфейсом для интеграции в СКУД и системы управления логическим доступом.

| ISO 18000-2 (125 kHz) | ISO 14443 и ISO 15693 (13,56 MHz) |
|-----------------------|-----------------------------------|
| EM 4102 | NXP Mifare Classic |
| HID ISOProx II | NXP Mifare Plus |
| HID Indala | Mifare Ultralight |
| Atmel T5577 | HID iClass |

Наше производство позволяет совмещать две RFID-метки разной частоты в одной карте: ISO 18000-2 (125 kHz) + ISO 14443/ISO 15693 (13,56 MHz). Если компания использует СКУД разных типов, то сотрудникам выдается одна карта с двумя типами RFID-меток.

Возможные варианты совместимости RFID-меток:

- HID + Mifare Classic 1K;
- Em-Marine + Mifare Classic 1K и др.

Персонализация

Для смарт-карт доступна графическая персонализация. На карту можно нанести фотографию сотрудника, его персональные данные (ФИО, должность, фотография сотрудника и пр.), логотип компании и другую необходимую информацию и изображения.

Графическое оформление смарт-карты выполняется по индивидуальному дизайн-макету.

Возможные варианты персонализации:

- полноцветная двухсторонняя печать высокого качества;
- нанесение штрих-кодов;
- нанесение QR-кода;
- печать личных данных владельца и полноцветных фотографий;
- полоса для подписи;
- кодированная магнитная полоса;
- голографическая защита.

Считыватели смарт-карт

Смарт-карта Рутокен совместима со всеми популярными на российском рынке считывателями.

Рекомендованные модели считывателей:

- **Считыватель Рутокен SCR 3001**
- ACR38U-U1
- ACR38U-I1
- ACR38U-H1
- ACR39U-U1
- ACR3901U-H3
- OMNIKEY (CardMan) 3021
- OMNIKEY (CardMan) 3121
- OMNIKEY (CardMan) 5422
- IDBridge CT30

Спецификация считывателя Рутокен SCR 3001

| Параметр | Считыватель смарт-карт |
|---------------------------------------|---------------------------------|
| Коммуникационный интерфейс | USB 2.0 (совместимый с USB 1.1) |
| Стандарты | ISO 7816 (Class A/B/C) |
| Протоколы работы считывателя с картой | T=0, T=1 |

| | |
|---|------------------------------------|
| Протоколы работы компьютера с считывателем | PC/SC, CT-API (перед PC/SC) |
| Размер карты | ID - 1 (полный размер) |
| Ресурс слота | 200.000 циклов - прижимной/Landing |
| Скорость передачи данных | 625 Кб/с |
| Скорость обмена | 480 Мбит/с (USB 2.0 High Speed) |
| Габаритные размеры | 71,4 x 70 x 59,4 мм |
| Масса | 132 г |
| Длина провода | 1,2 м |
| Диапазон рабочих температур | От 0 до +60°С |
| Подача тока на смарт-карту | 50 мА |
| Допустимая относительная влажность | IP33 |
| Время безотказной работы | До 500 000 часов |