

# 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
<b>Основные характеристики</b>		
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"><li>• Microsoft Windows 11/10/8.1/2019/2016/2012R2/8/2012/7/2008R2/Vista/2008</li><li>• GNU/Linux (в том числе отечественные)</li><li>• Apple macOS 10.9 и новее</li><li>• Android 5 и новее</li><li>• iOS 13 и новее</li><li>• Аврора 4+</li></ul>	<ul style="list-style-type: none"><li>• Microsoft Windows 10 /2019/2016/8.1/8/2012/7 /2008/Vista/2003/XP,</li><li>• GNU/Linux</li><li>• Apple macOS 10.9 и новее</li></ul>
<b>Поддерживаемые интерфейсы и стандарты</b>		

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"> <li>• ISO/IEC 7816-3, протокол T=0 и T=1 для контактной микросхемы,</li> <li>• <b>ISO 14443 (NFC) для бесконтактной микросхемы.</b></li> </ul>	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
<b>Криптографические возможности</b>		
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"> <li>• простая замена,</li> <li>• гаммирование,</li> <li>• гаммирование с обратной связью</li> </ul>	<ul style="list-style-type: none"> <li>• простая замена,</li> <li>• гаммирование,</li> <li>• гаммирование с обратной связью</li> </ul>
Режим выработки имитовставки	да	да

Генерация ключей шифрования	да	да
Импорт ключей шифрования	нет	нет
Запрет экспорта ключей шифрования	да	да
<b>Поддержка алгоритма ГОСТ Р 34.10-2012</b>	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
<b>Поддержка алгоритма ГОСТ 34.11-2012 (256 и 512 бит)</b>	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
<b>Поддержка алгоритма ГОСТ 34.11-94</b>	аппаратная реализация	аппаратная реализация
<b>Выработка сессионных ключей (ключей парной связи)</b>	да <ul style="list-style-type: none"> <li>по схеме VKO GOST R 34.10-2001 согласно RFC 4357</li> <li>по схеме VKO GOST R 34.10-2012 согласно RFC 7836</li> <li>по схеме KEG</li> </ul>	да <ul style="list-style-type: none"> <li>по схеме VKO GOST R 34.10-2001 согласно RFC 4357</li> <li>по схеме VKO GOST R 34.10-2012 согласно RFC 7836 для версии 2.0</li> </ul>
<b>Расшифрование по схеме EC El-Gamal</b>	да	да
<b>Поддержка алгоритма RSA</b>	аппаратная реализация расшифрования и подписи (RSA-1024, RSA-2048, <b>RSA-4096</b> )	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	<b>до 4096 бит</b>	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	-
<b>Сведения о сертификации</b>		
Наличие сертификата ФСТЭК	в процессе	да
Наличие сертификата ФСБ	в процессе	да (1,2,3)
<b>Файловая система</b>		
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"> <li>использование файлов Rutoken Special File (RSF-файлов) для хранения ключей шифрования, сертификатов;</li> <li>использование предопределенных папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов</li> </ul>	<ul style="list-style-type: none"> <li>использование файлов Rutoken Special File (RSF-файлов) для хранения ключей шифрования, сертификатов;</li> <li>использование предопределенных папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов</li> </ul>
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
<b>Аутентификация и конфиденциальность</b>		
Двухфакторная аутентификация	да, предъявление токена + ввод PIN-кода	да, предъявление токена + ввод PIN-кода
Уровни доступа	<ul style="list-style-type: none"> <li>Гость</li> <li>Пользователь</li> <li>Администратор</li> </ul>	<ul style="list-style-type: none"> <li>Гость</li> <li>Пользователь</li> <li>Администратор</li> </ul>
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"> <li>• глобальные PIN-коды: Администратора и Пользователя,</li> <li>• локальные PIN-коды (для защиты конкретных объектов в памяти устройства, например, контейнеров сертификатов)</li> <li>• <b>Настраиваемые аппаратные политики качества PIN-кодов</b></li> </ul>	<ul style="list-style-type: none"> <li>• глобальные PIN-коды: Администратора и Пользователя,</li> <li>• локальные PIN-коды (для защиты конкретных объектов в памяти устройства, например, контейнеров сертификатов)</li> </ul>
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"> <li>• поддержка комбинированной аутентификации: <ul style="list-style-type: none"> <li>• аутентификация по глобальным PIN-кодам</li> <li>• аутентификация по глобальным PIN-кодам в сочетании с аутентификацией по локальным PIN-кодам.</li> </ul> </li> <li>• возможность одновременного контроля прав доступа, заданных до 7-ю локальными PIN-кодами.</li> <li>• индикация факта смены глобальных PIN-кодов с умалчиваемых на оригинальные.</li> </ul>	<ul style="list-style-type: none"> <li>• поддержка комбинированной аутентификации: <ul style="list-style-type: none"> <li>• аутентификация по глобальным PIN-кодам</li> <li>• аутентификация по глобальным PIN-кодам в сочетании с аутентификацией по локальным PIN-кодам.</li> </ul> </li> <li>• возможность одновременного контроля прав доступа, заданных до 7-ю локальными PIN-кодами.</li> <li>• индикация факта смены глобальных PIN-кодов с умалчиваемых на оригинальные.</li> </ul>
<b>Flash- память</b>	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"> <li>• EM-Marine,</li> <li>• Mifare,</li> <li>• ProxCard II и ISOProx II,</li> <li>• Indala (на заказ)</li> </ul>
<b>Встроенный контроль и индикация</b>		
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"> <li>• счетчик изменений файловой системы</li> <li>• счетчик изменений PIN-кодов</li> <li>• счетчики последовательных неудачных попыток ввода PIN-кодов</li> <li>• счетчик успешных операций электронной подписи</li> </ul>	<ul style="list-style-type: none"> <li>• счетчик изменений файловой системы</li> <li>• счетчик изменений PIN-кодов</li> <li>• счетчики последовательных неудачных попыток ввода PIN-кодов</li> <li>• счетчик успешных операций электронной подписи (для версии 2.0)</li> </ul>
Проверка правильности функционирования криптографических алгоритмов	да	да
Режимы работы светодиода индикатора	<ul style="list-style-type: none"> <li>• готовность к работе</li> <li>• выполнение операции</li> <li>• нарушение в системной области памяти</li> </ul>	<ul style="list-style-type: none"> <li>• готовность к работе</li> <li>• выполнение операции</li> <li>• нарушение в системной области памяти</li> </ul>

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

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