

## Устройство Рутокен ЭЦП micro серт. ФСБ

Цена: 0 р.



Рутокен ЭЦП micro серт. ФСБ - электронный идентификатор в форм-факторе микро-токена, который может использоваться для реализации функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Рутокен ЭЦП предназначен для безопасной двухфакторной аутентификации пользователей, генерации и защищенного хранения ключей шифрования и ключей электронной подписи, выполнения шифрования и самой электронной подписи «на борту» устройства, а также хранения цифровых сертификатов и иных данных.

Аппаратная реализация национальных стандартов электронной подписи, шифрования и хэширования позволяет использовать Рутокен ЭЦП в качестве интеллектуального ключевого носителя и средства электронной подписи в российских системах РКІ, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной подписи. Возможности Рутокен ЭЦП позволяют выполнять криптографические операции таким образом, что закрытая ключевая информация никогда не покидает пределы токена. Таким образом, исключается возможность компрометации ключа и увеличивается общая безопасность информационной системы.

Покупая Устройство Рутокен ЭЦП micro серт. ФСБ в нашем интернет-магазине, вы можете рассчитывать на бесплатную доставку по Москве.

### Комплектация:

- Устройство
- Сертификат



- Упаковка

## Технические данные:

Криптографические возможности	<p>Поддержка алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012: генерация ключевых пар с проверкой качества, импорт ключевых пар, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет.</p> <p>Поддержка алгоритмов ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012: Вычисление значения хэш-функции данных, в том числе с возможностью последующего формирования ЭЦП.</p> <p>Поддержка алгоритма ГОСТ 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).</p> <p>Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357) и VKO GOST R 34.10-2012 (Протокол ТК26 №13 от 24.04.2014 г.), расшифрование по схеме ЕС El-Gamal.</p> <p>Поддержка алгоритма RSA: поддержка ключей размером до 2048 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи.</p> <p>Генерация последовательности случайных чисел требуемой длины.</p>
Аппаратные криптографические операции	<p>Скорость хеширования ГОСТ Р 34.11-94: до 61 КБ/сек.</p> <p>Скорость хеширования ГОСТ Р 34.11-2012: до 61 КБ/сек.</p> <p>Скорость шифрования ГОСТ 28147-89: до 91 КБ/сек.</p>



<p>Возможности аутентификации владельца</p>	<p>Двухфакторная аутентификация: по предъявлению самого идентификатора и по предъявлению уникального PIN-кода. Поддержка 3 категорий владельцев: Администратор, Пользователь, Гость. Поддержка 2-х Глобальных PIN-кодов: Администратора и Пользователя. Поддержка Локальных PIN-кодов для защиты конкретных объектов (например, контейнеров сертификатов) в памяти устройства. Настраиваемый минимальный размер PIN-кода (для любого PIN-кода настраивается независимо). Поддержка комбинированной аутентификации: по схеме «Администратор или Пользователь» и аутентификация по Глобальным PIN-кодам в сочетании с аутентификацией по Локальным PIN-кодам. Создание локальных PIN-кодов для дополнительной защиты части ключевой информации, хранящейся на токене. Возможность одновременной работы с несколькими локальными PIN-кодами (до 7 шт.). Ограничение числа попыток ввода PIN-кода. Индикация факта смены Глобальных PIN-кодов с умалчиваемых на оригинальные.</p>
<p>Файловая система</p>	<p>Встроенная файловая структура по ISO/IEC 7816-4. Число файловых объектов внутри папки – до 255 включительно. Использование File Allocation Table (FAT) для оптимального размещения файловых объектов в памяти. Уровень вложенности папок ограничен объемом свободной памяти для файловой системы. Хранение закрытых и симметричных ключей без возможности их экспорта из устройства. Использование Security Environment для удобной настройки параметров криптографических операций. Использование файлов Rutoken Special File (RSF-файлов) для хранения ключевой информации: ключей шифрования, сертификатов и т.п. Использование предопределенных папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов.</p>
<p>Интерфейсы</p>	<p>Протокол обмена по ISO 7816-12. Поддержка USB CCID: работа без установки драйверов устройства в современных версиях ОС. Поддержка PC/SC. Microsoft Crypto API. Microsoft SmartCard API. PKCS#11 (включая российский профиль).</p>



Встроенный контроль и индикация	<p>Контроль целостности микропрограммы (прошивки) Рутокен ЭЦП. Контроль целостности системных областей памяти. Проверка целостности RSF-файлов перед любым их использованием. Счетчики изменений в файловой структуре и изменений любых PIN-кодов для контроля несанкционированных изменений. Проверка правильности функционирования криптографических алгоритмов. Светодиодный индикатор с режимами работы: готовность к работе, выполнение операции, нарушения в системной области памяти.</p>
Общие характеристики	<p>Современный защищенный микроконтроллер. Идентификация с помощью 32-битного уникального серийного номера. Поддержка операционных систем: MS Windows 10/8.1/8/2012/7/2008/Vista/2003/XP, GNU/Linux, Apple Mac OS X / OS X. EEPROM память 64 КБ. Интерфейс USB 1.1 и выше. Размеры 58x16x8мм (микро-токен 17,8x15,4x5,8мм). Масса 6,3г (микро-токен 1,6г).</p>