

Общие характеристики

- USB-устройство с аппаратной реализацией асимметричной криптографии для выработки электронной подписи без возможности экспорта закрытый (секретный) ключа. Предназначено для использования в российских системах РКІ, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной подписи
- Интерфейс: USB 2.0 и выше
- Объем доступной пользователю EEPROM память: 64 Кбайт
- Размеры 58x16x8мм
- Масса 6,3г.
- 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
- Наличие сертификата ФСБ

Криптографические возможности

- 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
- 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
- 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)
- Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357) и VKO GOST R 34.10-2012 (RFC 7836), расшифрование по схеме EC El-Gamal
- Поддержка алгоритма RSA: поддержка ключей размером до 2048 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи
- Генерация последовательности случайных чисел требуемой длины

Возможности аутентификации владельца

- 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

Интерфейсы

- 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)



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/121-3989 от "11" декабря 2020 г.

Действителен до "11" декабря 2023 г.

Выдан _____ акционерному обществу «Актив-софт»,
_____ обществу с ограниченной ответственностью Фирма «АНКАД».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) «Рутокен ЭЦП 2.0 Исполнение А» в комплектации согласно формуляру КБДЖ.468244.094 ФО с учётом изменений согласно извещениям КБДЖ.418-17, КБДЖ.486-18, КБДЖ.615-20

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1, КС2, и может использоваться для криптографической защиты (вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти СКЗИ, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных обществом с ограниченной ответственностью Фирма «АНКАД»

сертификационных испытаний образца продукции № 388Н-001001.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру КБДЖ.468244.094 ФО с учётом изменений согласно извещениям КБДЖ.418-17, КБДЖ.486-18, КБДЖ.615-20.

Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России



О.В. Скрябин