Рутокен ЭЦП 2.0 2100

Наименование средства криптографической защиты информации согласно формуляру производителя: СКЗИ «Рутокен ЭЦП 2.0 2100»

Наличие сертификата соответствия ФСБ России.

Криптографические возможности

- Поддержка алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (256 и 512 бит): генерация ключевых пар с проверкой качества, 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 (256 и 512 бит): вычисление значения хэш-функции данных, в том числе с возможностью последующего формирования ЭЦП.
- Поддержка алгоритма ГОСТ 28147-89: генерация 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.

Аппаратные криптографические операции

- Электронная подпись ГОСТ 34.10-2012 (256): 0,3 сек.
- Электронная подпись ГОСТ 34.10-2012 (512): 0,8 сек.
- Электронная подпись ГОСТ Р 34.10-2001: 1,6 сек.
- Скорость хеширования ГОСТ Р 34.11-2012 (256 и 512): до 0,4 КБ/сек.
- Скорость хеширования ГОСТ Р 34.11-94: до 0,8 КБ/сек.
- Скорость шифрования ГОСТ 28147-89: до 1,1 КБ/сек.

Специальные возможности

- Возможность создания специальной неудаляемой ключевой пары устройства.
- Ведение неубывающего счетчика операций электронной подписи.
- Доверенное считывание значения неубывающего счетчика, подтвержденное электронной подписью.
- Журналирование операций электронной подписи, фиксация критических параметров электронной подписи и окружения.
- Доверенное получение журнала операций, подтвержденное электронной подписью.

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 PIN кодов по-умолчанию на оригинальные.

Файловая система

- 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.
- Возможность изменения политики смены PIN-кода пользователя. Смена может быть доступна Пользователю, Администратору или обеим ролям одновременно.

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).

Встроенный контроль и индикация

- 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.

Общие характеристики

- Современный защищенный микроконтроллер.
- Идентификация с помощью 32-битного уникального серийного номера.
- Поддержка операционных систем:
    - Microsoft Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003
    - GNU/Linux
    - Apple macOS/OSX
- EEPROM память 64 КБ.
- Интерфейс USB 1.1 и выше.
- Размеры 58x16x8мм.
- Масса 6,3г.

Дополнительные возможности

- Собственный CSP со стандартным набором интерфейсов и функций API.
- Возможность интеграции в smartcard-ориентированные программные продукты.
- Библиотека minidriver для интеграции с Microsoft Base SmartCard Cryptoprovider.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-4550*** от "***01***" ***июня*** 202***3*** г.

Действителен до "***01***" ***июня*** 202***4*** 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 2100»** в комплектации согласно формуляру КБДЖ.468244.065 ФО с учётом извещения об изменениях КБДЖ.507-18

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 (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти СКЗИ, вычисление имитовставки для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти СКЗИ, 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 № 388К-001001.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру КБДЖ.468244.065 ФО с учётом извещения об изменениях КБДЖ.507-18 .

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**