Рутокен ЭЦП 3.0

Наименование средства криптографической защиты информации согласно формуляру производителя: СКЗИ «Рутокен ЭЦП 3.0»

Вариант исполнения: 5

Серия: 3220

Наличие сертификата соответствия ФСБ России

Криптографические возможности

− USB-устройство с аппаратной реализацией: ГОСТ Р 34.10-2012 с длиной ключа 256/512 бит и ГОСТ Р 34.11-2012, а также новых симметричные шифров Магма и Кузнечик и международных алгоритмов электронной подписи RSA и ECDSA. Криптографические операции выполняются без копирования ключа в память компьютера.

− Интерфейс: USB 1.1 и выше.

− Объем EEPROM память (не менее): 128 Кбайт.

− Поддержка алгоритмов ГОСТ Р 34.10-2012/ГОСТ 34.10-2018 (256 и 512 бит): генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет.

− Поддержка алгоритма ГОСТ Р 34.11-2012/ГОСТ 34.11-2018 (256 и 512 бит): вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП.

− ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 (Кузнечик): 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).

− ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 (Магма): 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 парной связи):

− по схеме VKO GOST R 34.10-2012 (RFC 7836);

− расшифрование по схеме EC El-Gamal.

− Поддержка алгоритма RSA: поддержка ключей размером 1024, 2048, 4096 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи.

− ECDSA с кривыми secp256k1 и secp256r1: 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.

− Настраиваемые аппаратные политики качества PIN-кодов, обрабатываются микропрограммой при соответствующих операциях. Устанавливаются при форматировании, опционально могут изменяться позднее по PIN-коду Администратора;

− Варианты политик:

-Ограничение минимальной длина PIN-кода;

-Ограничение использования PIN-кода по умолчанию;

-Запрет PIN-кода, состоящего из одного повторяющегося символа;

-Независимые требования по наличию в PIN-коде: прописных, строчных букв латинского и русского алфавитов; цифр; специальных символов;

-Запоминание до 10 устанавливаемых значений PIN-кода, и возможность запрета установки ранее использованного PIN-кода.

− 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 USB-токене. Возможность одновременной работы с несколькими локальными PIN-кодами (до 7 шт.).

− Ограничение числа попыток ввода PIN-кода.

− Индикация факта смены Глобальных PIN-кодов по умолчанию на оригинальные.

Интерфейсы

− Протокол обмена по ISO/IEC 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).

− Современный защищенный микроконтроллер.

− Идентификация с помощью 32-битного уникального серийного номера.

− Поддержка операционных систем: MS Windows11/10/8.1/8/2012/7/2008/Vista, GNU/Linux (в том числе отечественные), Apple macOS 10.9 и новее.

− Работа с СКЗИ «КриптоПро CSP 5.0 R2» и новее по протоколу защиты канала SESPAKE (ФКН2) для контактного и беспроводного подключения по NFC.

− Собственный CSP со стандартным набором интерфейсов и функций API.

− Minidriver для интеграции с Microsoft Base Smart Card Cryptographic Service Provider.

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.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-4398*** от "***01***" ***декабря*** 2022 г.

Действителен до "***01***" ***декабря*** 2025 г.

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

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **«Рутокен ЭЦП 3.0»** (вариант исполнения 5) в комплектации согласно формуляру КБДЖ.468244.119-01 ФО

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 № 1064-080476.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру КБДЖ.468244.119-01 ФО.

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