Спецификация СКЗИ «РУТОКЕН ЭЦП 2.0»

Криптоалгоритмы:

- Поддержка алгоритма ГОСТ Р 34.10-2001: генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи.
- Поддержка алгоритма ГОСТ Р 34.11-94: Вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП.
- Поддержка алгоритма ГОСТ Р 34.10-2012 (256 и 512 бит): генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи.
- Поддержка алгоритма ГОСТ 34.11-2012 (256 и 512 бит): Вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП.
- Поддержка алгоритма ГОСТ Р 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), расшифрование по схеме EC El-Gamal.
- Выработка сессионных ключей (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 до 2048 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи.
- Генерация последовательности случайных чисел требуемой длины.
- Ведение журнала выполненных операций электронной подписи.

Аутентификация:

- 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.

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.

Поддерживаемый функционал:

- 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).
- Контроль целостности микропрограммы (прошивки) СКЗИ «РУТОКЕН ЭЦП 2.0».

Дополнительные сервисы:

- 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.

Микроконтролер:

- Современный защищенный микроконтроллер.
- Идентификация с помощью 32-битного уникального серийного номера.
- Поддержка операционных систем: MS Windows 8/2012/7/2008/Vista/2003/XP/2000, GNU/Linux, Mac OS X.
- EEPROM память 64 КБ.
- Интерфейс USB 1.1 и выше.
- Размеры 58x16x8 мм.
- Масса 6,3г.

Гарантийный срок составляет 1 (Один) год.

С Сертификатами ФСБ на соответствие СКЗИ «РУТОКЕН ЭЦП 2.0» ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 (электронная подпись, алгоритм на основе эллиптических кривых), ГОСТ Р 34.11-2012 и ГОСТ Р 34.11-94 (хеш-функция), ГОСТ 28147-89 (симметричный криптографический алгоритм) и требованиям к СКЗИ класса КС2 можно ознакомиться на сайте www.rutoken.ru, а также в Приложении №1.

Приложение 1. Сертификат ФСБ России на СКЗИ «РУТОКЕН ЭЦП 2.0»

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-2771*** от "***25***" ***декабря*** 201***5*** г.

Действителен до "***25***" ***декабря*** 201***8*** г.

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

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **«Рутокен ЭЦП 2.0»** (исполнения 1, 2) в комплектации согласно формуляру КБДЖ.468244.065 ФО

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 1) и класса КС2 (для исполнения 2), Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения 1) и класса КС2 (для исполнения 2), 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, 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 «Центр сертификационных исследований»

сертификационных испытаний образца продукции № 388Д-000501.

Безопасность информации обеспечивается при использовании СКЗИ, изготовленного в соответствии с техническими условиями КБДЖ.468244.065 ТУ, и выполнении требований эксплуатационной документации согласно формуляру КБДЖ.468244.065 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **А.М.Ивашко**

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.Н.Ковалев