РУТОКЕН ЭЦП

Интеллектуальный ключевой носитель

Рутокен ЭЦП — аппаратная реализация российского стандарта электронной цифровой подписи и проверенный временем конструктив идентификаторов Рутокен. Предназначен для использования в качестве интеллектуального ключевого носителя в российских системах PKI, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной цифровой подписи.

Криптографические возможности

- Алгоритм ГОСТ Р 34.10-2001:
  - Генерация ключевых пар, импорт ключевых пар;
  - Формирование и проверка электронной цифровой подписи;
- Алгоритм ГОСТ 34.11-94:
  - Вычисление значения хэш-функции данных (в т.ч. с возможностью последующего формирования ЭЦП;
- Поддержка алгоритма ГОСТ 28147-89:
  - Генерация и импортирование ключей шифрования;
  - Зашифрование и расшифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью;
  - Вычисление и проверка имитовставки;
- Выработка сессионных ключей (ключей парной связи) по схеме VKO GOST R 34.10-2001 (RFC4357);
- Генерация последовательности случайных чисел требуемой длины;
- Поддержка алгоритма RSA, с ключами до 2048 бит;
- Поддержка всех криптографических механизмов, использующихся в КриптоПро ФКН.

Возможности аутентификации владельца

- 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:
  - Администратор или Пользователь;
  - Аутентификация по Глобальным PIN-кодам в сочетании с аутентификацией по Локальным PIN-кодам;
- Индикация факта смены Глобальных PIN-кодов по умолчанию на оригинальные;
- Поддержка всех механизмов аутентификации, использующихся в КриптоПро ФКН.

Файловая система

- Стандарт ISO/IEC 7816-4;
- Использование файлов Rutoken Special File (RSF-файлов) для хранения ключевой информации: ключей шифрования, сертификатов и т.п;
- Хранение закрытых и симметричных ключей без возможности их экспорта из устройства;
- Использование предопределенных папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов;
- Использование Security Environment для удобной настройки параметров криптографических операций.

Интерфейсы

- Протокол обмена на основе ISO/IEC 7816-12;
- Поддержка PC/SC;
- Поддержка USB CCID (работа без установки драйверов в Windows Vista и Windows 7);
- Microsoft Crypto API;
- PKCS#11(включая российский профиль).

Общий объем памяти для данных и криптографических ключей — 64 Кбайт.

Рутокен ЭЦП осуществляет механизм электронной цифровой подписи таким образом, что закрытый (секретный) ключ подписи никогда не покидает пределы токена. Исключается возможность компрометации ключа и увеличивается общая безопасность информационной системы.

Аппаратная реализация функций хеширования, электронной цифровой подписи, выработки сеансовых ключей и симметричного шифрования позволяет строить на базе Рутокен ЭЦП надежные программно-аппаратные решения с богатыми возможностями.

Электронный идентификатор Рутокен ЭЦП — совместная разработка компаний «Актив» и «Анкад». Изделие находится на сертификационных испытаниях, как средство криптографической защиты информации по уровню КС2 в соответствии с требованиями ФСБ РФ.

Компания Актив

Россия, г. Москва, ул. Красина, д. 3. Тел.: +7 (495) 925-77-90
сайт: www.rutoken.ru, e-mail: info@rutoken.ru