Рутокен Плагин. Описание продукта

Назначение продукта

Рутокен Плагин — это программа, которая в сочетании с токенами и смарт-картами Рутокен ЭЦП 2.0/3.0/PKI является комплексным решением для электронной подписи и двухфакторной аутентификации в браузере.

Рутокен Плагин помогает:

- Сохранить удобство использования сайта для клиентов;
- Снизить затраты на внедрение и использование электронной подписи;
- Исключить риск подбора логина-пароля в личном кабинете.

Взаимодействие в браузере происходит через JavaScript API. Есть инструменты для:

- Создания запросов и записи сертификатов;
- Вычисления электронной подписи разными алгоритмами;
- Шифрования;
- Управления PIN-кодами, ключами и сертификатами RSA- и ГОСТ-2012 на устройствах;
- Работы со средствами визуализации и контроля подписываемых данных;
- Добавления в подпись информации о времени и месте подписания для антифрод анализа.

При установке Рутокен Плагин не требует полномочий администратора системы и использует только встроенные в браузер возможности и API. Подойдет любой компьютер под управлением ОС Windows, macOS или Linux с любым популярным браузером.

Взаимодействие с USB-устройствами

Рутокен Плагин работает с токенами и смарт-картами семейства Рутокен ЭЦП. Эти устройства не требуют установки драйверов и готовы к работе сразу после подключения к компьютеру.

blocked URL

При вычислении электронной подписи Рутокен Плагин напрямую обращается к криптоядру в устройствах Рутокен. Криптографические операции происходят внутри токена или смарт-карты, без возможности выдачи наружу закрытого ключа. Это исключает риск копирования ключей.

Условия работы

Аппаратные требования

Intel-совместимые процессоры x86/x86_64

Российские процессоры Эльбрус, Байкал

ARM7, ARM64

Программные требования

Операционные системы, на которых проводилось тестирование:

- Windows 7 и новее
- macOS,
- Linux
- Отечественные Линуксы для x86\x64, ARM7, ARM8, Байкал-М и Эльбрус

Браузеры, в которых проводилось тестирование:

- Google Chrome / Chromium
- Internet Explorer
- Mozilla Firefox
- Opera
- Edge
- Яндекс.Браузер
- Спутник

Состав

В состав Рутокен Плагин входят:

1. Библиотека rtPKCS11ECP, реализующая стандарт PKCS#11 с поддержкой российского профиля.
2. Библиотека npCryptoPlugin, реализующая механизм Active-X для IE.
3. Библиотека npRutokenPlugin и файлы, требуемые для использования Native Messaging в браузерах Google Chrome, Mozilla Firefox, Opera и других chromium-based.
4. Расширения для Google Chrome, Opera и Mozilla Firefox.

Установка

Программа установки Рутокен Плагин реализована в виде

- MSI-пакета для ОС Windows.
- pkg-пакета для macOS,
- deb/rpm- пакетов для Линукс.

Функциональность

Плагин позволяет:

- Получать список всех подключенных к компьютеру поддерживаемых устройств
- Получать модель поддерживаемого устройства
- Получать метку поддерживаемого устройства
- Осуществлять логин на устройство
- Осуществлять логаут с устройства
- Получать список всех ключевых пар ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001 и RSA на устройстве
- Аппаратно генерировать ключевую пару ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001 и RSA на устройстве
- Получать метку ключевой пары
- Устанавливать метку для ключевой пары
- Формировать запрос на сертификат в формате PKCS#10 для выбранной ключевой пары (поддерживаются расширения, необходимые для получения квалифицированного сертификата)
- Импортировать на устройство сертификат формата X.509, переданный в виде base64-строки
- Удалять выбранный сертификат с устройства
- Получать информацию, содержащуюся в сертификате X.509 (DN, keyUsages, extendedKeysUsages и т.п.), с поддержкой расширений квалифицированного сертификата.
- Выдавать информацию о сертификате в виде текста для печати
- Получать список сертификатов, хранящихся на устройстве. Опционально можно задать поиск только тех сертификатов, которые связаны с закрытым ключом
- Осуществлять подпись строки в формате CMS. Опционально строка может быть перекодирована из base64 и подписан бинарный массив.
- Шифровать данные в формате CMS
- Проводить процедуру аутентификации по сертификату (подпись случайных данных)
- Производить вычисление хеш-функции от данных по алгоритму ГОСТ Р 34.11-2012 и ГОСТ Р 34.11-94

Поддерживаемые устройства

В Рутокен Плагин поддерживаются устройства:

- Рутокен ЭЦП 2.0
- Рутокен ЭЦП 2.0 2100
- Рутокен ЭЦП 2.0 3000
- Рутокен ЭЦП 2.0 Flash
- Рутокен ЭЦП 2.0 Touch
- Рутокен ЭЦП Bluetooth (при подключении по USB)
- Рутокен ЭЦП 3.0
- Рутокен ЭЦП PKI (ограниченная поддержка)

Поддерживаемые стандарты

- Электронная подпись по ГОСТ Р 34.10-2012 (256 и 512 бит), ГОСТ Р 34.10-2001 и RSA.
- Вычисление хеш-функции по ГОСТ Р 34.11-2012 (256 и 512 бит) и ГОСТ Р 34.11-94.
- Вычисление ключа согласования по схеме VKO GOST 34.10-2012 (256 и 512 бит) и VKO GOST 34.10-2001.

- Шифрование по ГОСТ 28147-89.
- Формат цифрового сертификата X.509.
- Формат запроса на сертификат PKCS#10 и Certificate Management over CMS (CMC).
- Формат подписанных и зашифрованных сообщений CMS (PKCS#7), в том числе для нескольких адресатов.
- Формирование запроса на штамп времени.
- Добавление в CMS (PKCS#7) подпись ответа сервера штампов времени.