Рутокен Плагин. Описание продукта

Назначение продукта

Рутокен Плагин применяется для организации электронной подписи, шифрования и двухфакторной аутентификации в web-сервисах. Использует аппаратные реализации российских и международных криптографических алгоритмов USB-токенов и смарт-карт семейства Рутокен ЭЦП 2.0 и Рутокен ЭЦП.

Рутокен Плагин совместим с удостоверяющими центрами, в том числе российских производителей, и может применяться в информационных системах, в которых используются цифровые сертификаты и инфраструктура PKI.

Программный интерфейс плагина предназначен для вызова из java-скриптов web-страницы.

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 XP,
- Windows 7,
- Windows 8.1,
- Windows 10,
- macOS,
- Linux x86/64
- Отечественные Линуксы для x86\x64, ARM7, ARM8, Байкал-М и Эльбрус

Браузеры, в которых проводилось тестирование:

- Google Chrome
- 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- пакета 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 выбранном устройстве
- Аппаратно генерировать ключевую пару ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001 и RSA на выбранном 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 2.0 Flash Touch
- Рутокен ЭЦП Bluetooth (при подключении по USB)
- Рутокен ЭЦП 3.0
- Рутокен ЭЦП PKI (ограниченная поддержка)
- Рутокен ЭЦП (ограниченная поддержка)

Поддерживаемые стандарты

- Используются криптографические алгоритмы, соответствующие российским стандартам ГОСТ 28147-89, и ГОСТ 34.10-2012/ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2001/ГОСТ Р 34.11-94.
- Наборы параметров для этих алгоритмов соответствуют RFC 4357 и RFC
- Выработка ключа согласования по схеме VKO GOST 34.10-2001 (RFC 4357) и VKO GOST 34.10-2012 (RFC)
- Поддерживаемые форматы защищенных сообщений соответствуют RFC 3851 и 3852, использование российских алгоритмов в этих форматах соответствует RFC 4490.
- Сертификаты и списки отзывов реализованы в соответствии с RFC 3280.
- Упаковка открытых ключей алгоритмов ГОСТ реализована в соответствии с RFC 4491.
- Работа с аппаратными устройствами реализована в соответствии со стандартом PKCS#11 v. 2.20