

# ***РУТОКЕН Плагин***

## **Описание применения**



## Аннотация

Настоящий документ содержит общее описание продукта Рутокен Плагин, представляющего собой средство электронной подписи, шифрования и двухфакторной аутентификации для Web-сервисов.

Авторские права на продукт Рутокен Плагин принадлежат ЗАО «Актив-софт».

## Назначение продукта

Рутокен Плагин применяется для организации электронной подписи, шифрования и двухфакторной аутентификации в Web-сервисах с использованием аппаратной реализации российских криптографических алгоритмов в USB-токенах Рутокен ЭЦП, Рутокен Web и Рутокен PINPad.

Рутокен Плагин совместим с ПО российских производителей для Удостоверяющих центров и может применяться в информационных системах, в которых используются цифровые сертификаты и инфраструктура PKI. Программный интерфейс плагина предназначен для вызова из скриптов Web-страницы.

## Условия работы Рутокен Плагин

### ➤ Аппаратные требования

Intel-совместимые процессоры

- x86
- x86\_64

### ➤ Программные требования

Операционные системы, на которых проводилось тестирование

- Windows XP SP3 (только x86), Windows Vista, Windows 7, Windows 8
- Mac OS X 10.6, Mac OS X 10.7, Mac OS X 10.8
- Ubuntu 10.04, Ubuntu 12.04
- Alt Linux 6
- Debian 6 Squeeze
- Astra Linux
- CentOS 6.2

### ➤ Браузеры, в которых проводилось тестирование

- Chrome 19 и старше
- IE 7-10
- Firefox 3.6
- Firefox 13 и старше
- Opera 11.64
- Safari 5.1.2

## Состав Рутокен Плагин

В состав Рутокен Плагин входят:

1. Кроссплатформенная библиотека `rtPKCS11ECP`, реализующая стандарт PKCS#11 с поддержкой русского профиля;
2. Кроссплатформенная библиотека `npCryptoPlugin`, реализующая механизм Active-X для IE и NPAPI для остальных браузеров. В библиотеке реализованы высокоуровневые криптографические форматы (X.509, PKCS#10, CMS).

## Установка Рутокен Плагин

Программа установки Рутокен Плагин реализована в виде MSI-пакета для MS Windows, PKG-пакета для Mac OS X. Установка плагина не требует прав системного администратора и настроек. Для ОС Linux комплекс распространяется в виде двух библиотек (`npCryptoPlugin.so` и `librtpkcs11ecp.so`), которые требуется скопировать в `~/.mozilla/plugins/`.

## Функциональность Рутокен Плагин

Рутокен Плагин позволяет:

- Получать список всех подключенных к компьютеру USB-токенов Рутокен ЭЦП, Рутокен Web и TrustScreen-устройств Рутокен PINPad;
- Получать модель устройства;
- Получать метку устройства;
- Осуществлять логин на устройство;
- Осуществлять логат с устройства;
- Получать список всех ключевых парт ГОСТ Р 34.10-2001 на выбранном устройстве;
- Аппаратно генерировать ключевую пару ГОСТ Р 34.10-2001 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, extendedKeyUsages 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).

## Поддерживаемые устройства

В Рутокен Плагин поддерживаются устройства:

- Рутокен ЭЦП
- Рутокен Web
- Рутокен PINPad

Возможно добавление поддержки других устройств. Для этого к устройству должна прилагаться совместимая библиотека, реализующая стандарт PKCS#11 с российским профилем.

## Поддерживаемые стандарты

- Используются криптографические алгоритмы, соответствующие российским стандартам ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94.
- Наборы параметров для этих алгоритмов соответствуют RFC 4357.
- Выработка ключа согласования по схеме VKO GOST 34.10-2001 (RFC 4357).
- 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 USB-токенами реализована в соответствии со стандартом PKCS#11 v. 2.20.