Использование сертификата ключа электронной подписи

Руководство пользователя

Версия документа 1.1.2

27.03.2017

История изменений

Версия 1.1.0, 20 ноября 2015 года
Обновлена информация для настройки КриптоПро ЭЦП Browser plug-in.

Содержание

1. Требования к сертификату ключа электронной подписи

Для подписания электронных документов клиент — резидент РФ должен получить квалифицированный сертификат ключа электронной подписи, изготовленный в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи». Структура сертификата ключа электронной подписи должна соответствовать международному стандарту ISO/IEC 9594-8:2008 “Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks”. Профиль сертификата ключа электронной подписи должен соответствовать рекомендациям IETF RFC 5280 (2008) “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

Клиент — нерезидент РФ может осуществлять подписание электронных документов с использованием неквалифицированной электронной подписи, соответствующей следующим требованиям:

- ключ проверки электронной подписи должен быть создан с использованием алгоритма RSA;
- структура сертификата ключа электронной подписи должна соответствовать международному стандарту ISO/IEC 9594-8:2008 “Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks”; профиль сертификата должен соответствовать рекомендациям IETF RFC 5280 (2008) “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”;
- сертификат ключа электронной подписи должен быть выпущен удостоверяющим центром, включенным в хранилище доверенных корневых сертификатов операционных систем семейства MS Windows, либо удостоверяющим центром Некоммерческое партнерство развития финансового рынка РТС.

Для регистрации сертификата ключа электронной подписи клиенту следует предоставить его в НП РТС.

2. Использование КриптоПро

2.1. Перечень необходимого программного обеспечения

Для корректного использования КриптоПро требуется следующее программное обеспечение:

- КриптоПро CSP версии 3.6 и выше в зависимости от операционной системы. Дистрибутив для тестовых целей с периодом бесплатного функционирования в 90 дней доступен для скачивания после регистрации по следующему адресу: http://www.cryptopro.ru/downloads;
- КриптоПро ЭЦП Browser plug-in версия 2.0 и выше, поставляется бесплатно и работает на любом компьютере с установленным пакетом КриптоПро CSP. Подробнее прочитать об этом плагине и скачать его можно на сайте: http://www.cryptopro.ru/products/cades/plugin. Для браузеров Google Chrome и Mozilla Firefox с версией 52 необходимо произвести дополнительную настройку в браузере для включения плагина, подробнее см. раздел 2.3.

Не рекомендуется совместное использование КриптоПро CSP и других программ для работы с ЭЦП, таких как VipNet CSP или Validata CSP. При необходимости одновременного использования КриптоПро CSP и VipNet CSP/Validata CSP, то для корректной работы КриптоПро CSP ознакомьтесь с этой инструкцией по установке данных продуктов.

2.2. Установка программного обеспечения

Установку всех компонентов должен осуществить пользователь с правами администратора операционной системы.

Первым на рабочее место устанавливается КриптоПро CSP. В его установке нет особенностей. По завершении установки может потребоваться перезагрузка, о которой уведомит мастер установки; необходимо произвести перезагрузку до установки второго пакета.

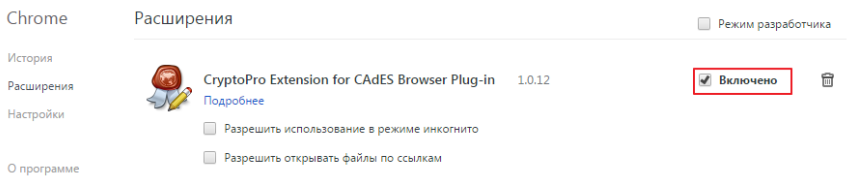
Далее следует устанавить приложение КриптоПро ЭЦП Browser plug-in. При установке данного плагина возникали единичные сложности, когда мастер установки демонстрировал код ошибки и не мог продолжить установку. В этом случае необходимо очистить хранилище временных файлов операционной системы. Также мастер установки может потребовать перезагрузить систему, ее следует произвести перед началом настройки.

2.3. Настройка программного обеспечения

Компонент КриптоПро CSP не требует дополнительной настройки.

Для браузера Google Chrome, перед настройкой КриптоПро ЭЦП Browser plug-in, необходимо сначала убедиться, что плагин включен в Расширениях. Для этого в браузере выполните Настройки >> Дополнительные инструменты >> Расширения и, при необходимости, включите плагин.

Рисунок 2.1. Включение КриптоПро ЭЦП Browser plug-in для браузера Google Chrome

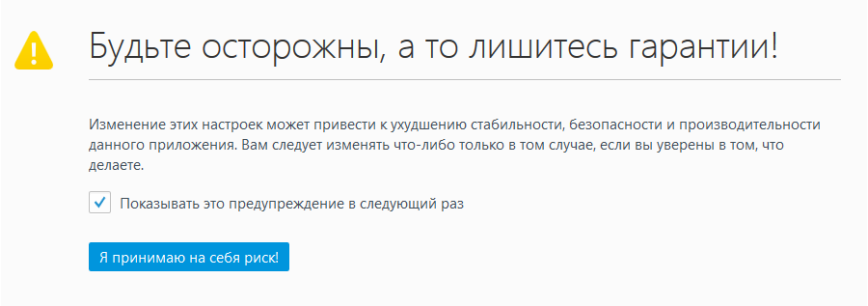


Для браузера Mozilla Firefox 52 версии, перед настройкой КриптоПро ЭЦП Browser plug-in, необходимо включить поддержку плагинов следующим образом:

Операция включения плагинов работает только для браузера Mozilla Firefox 52 версии.

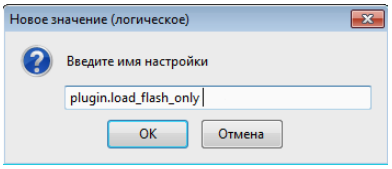
- В браузере открыть новое окно и в адресной строке вставьте текст - **about:config** и нажмите на клавишу **Enter**.
- После появления предупреждения следует нажать на кнопку **Я принимаю на себя риск!**

Рисунок 2.2. Окно предупреждения для браузера Mozilla Firefox



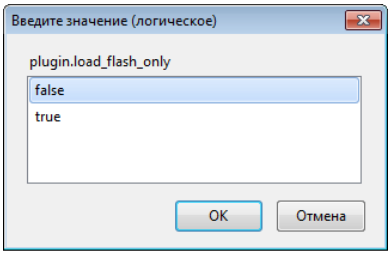
- Необходимо создать новую логическую настройку, выполнив ПКМ >> Создать >> Логичесское, и дать настройке имя - **plugin.load_flash_only**

Рисунок 2.3. Окно создания логической настройки



- Для логической настройки следует выбрать значение **false**.

Рисунок 2.4. Окно выбора значений

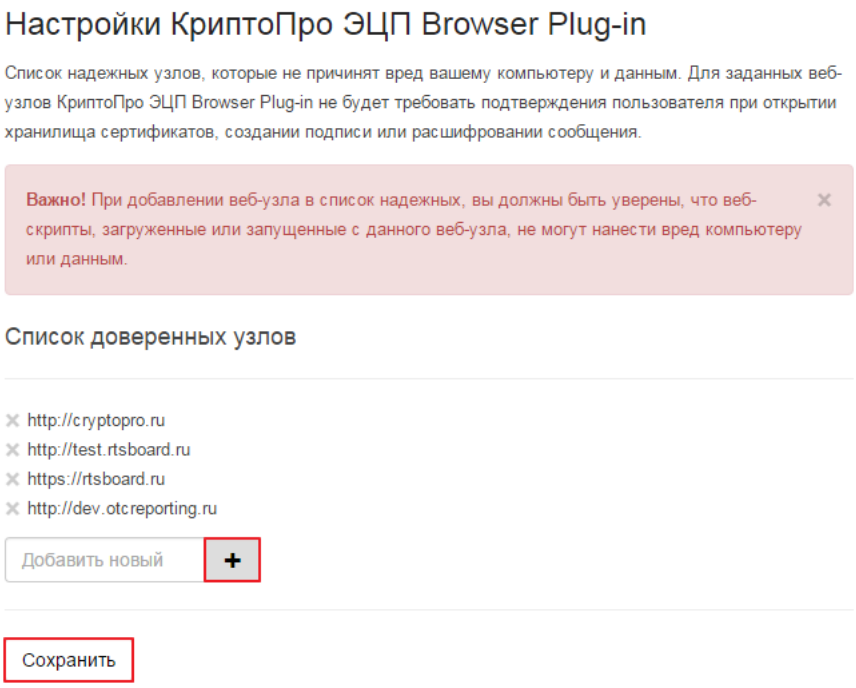


- Для завершения операции следует перезагрузить браузер.

Для настройки КриптоПро ЭЦП Browser plug-in под управлением ОС Windows необходимо запустить мастер настройки, выполнив Пуск >> Все программы >> КРИПТО-ПРО >> Настройки ЭЦП Browser plug-in.

Далее следует добавить адреса, которым нужен сертификат ключа электронной подписи, в список разрешенных адресов путем внесения их в поле ввода и нажатия кнопки **+**. После добавления необходимо выбрать действие **Сохранить** для применения внесенных изменений.

Рисунок 2.5. Добавление узлов в список разрешений подключаемого модуля



2.4. Установка сертификата пользователя с использованием КриптоПро CSP

Для установки личного сертификата с проставленной ссылкой на закрытый ключ используется приложение КриптоПро CSP. Запустить его в ОС Windows можно выполнив Пуск >> Все программы >> КРИПТО-ПРО >> КриптоПро CSP. В появившемся окне приложения нужно выбрать вкладку **Сервис** и в ней нажать на кнопку **Установить личный сертификат**. Далее следует указать расположение файла сертификата (файл с расширением .cer) и нажать кнопку **Далее**. Окно просмотра свойств сертификата позволяет убедиться, что выбран правильный сертификат; после проверки снова нажмите на кнопку **Далее**.

В следующем окне необходимо задать ключевой контейнер, содержащий в себе закрытые ключи пользователя.

ВАЖНО! В этом шаге используются только съемные USB-носители или смарт-карты, а также реестр операционной системы.

Приложение КриптоПРО CSP версии 3.9 позволяет найти контейнер автоматически путем проставления соответствующего флажка; более ранние версии после нажатия кнопки **Обзор** предоставляют список имеющихся носителей, из которых требуется выбрать нужный. После выбора контейнера нажмите **Далее**. Следующее окно позволяет задать параметры установки сертификата в хранилище. Выбрав необходимое хранилище, нажмите на кнопку **Далее**.

Сертификаты ключей электронной подписи, которые созданы с использованием алгоритма RSA, необходимо устанавливать в личное хранилище для ключевого контейнера — .**Компьютер**.

Следующий шаг финальный и не требует каких-либо действий, кроме нажатия кнопки **Готово**.

Для начала установки сертификата, который заключен в контейнер **pfx** (файл с расширением .pfx), дважды нажмите на него левой кнопкой мыши. В окне **Пароль** необходимо указать пароль для закрытого ключа и нажать на кнопку **Далее**. Дальнейшая установка аналогична установке сертификата без контейнера **pfx**.

2.5. Начало работы с системой

После открытия в браузере контура системы, при необходимости, нужно разрешить исполнение подключаемого модуля КриптоПро ЭЦП Browser plug-in.