

Настройка криптопровайдера КриптоПро

Для работы с функциональностью подписания с помощью ЭП-СП файлов-результатов (решений) в АРМ ПГС 2.0 необходимо установить и настроить криптопровайдер КриптоПро, Cades плагин для web-браузера и сертификат ЭП.

Установка криптопровайдера КриптоПро CSP версии 4.0 и выше должна производиться в соответствии с инструкцией, расположенной на общедоступном ресурсе в сети Интернет по ссылке: https://www.cryptopro.ru/sites/default/files/docs/instruction_manual_csp_r3.pdf.

После установки КриптоПро CSP необходимо установить Cades-плагин для web-браузера с ресурса: <https://www.cryptopro.ru/products/cades/plugin>, в соответствии с инструкцией по установке <http://docs.cryptopro.ru/plugin/plugin-installation-windows>, см. рисунок 1.

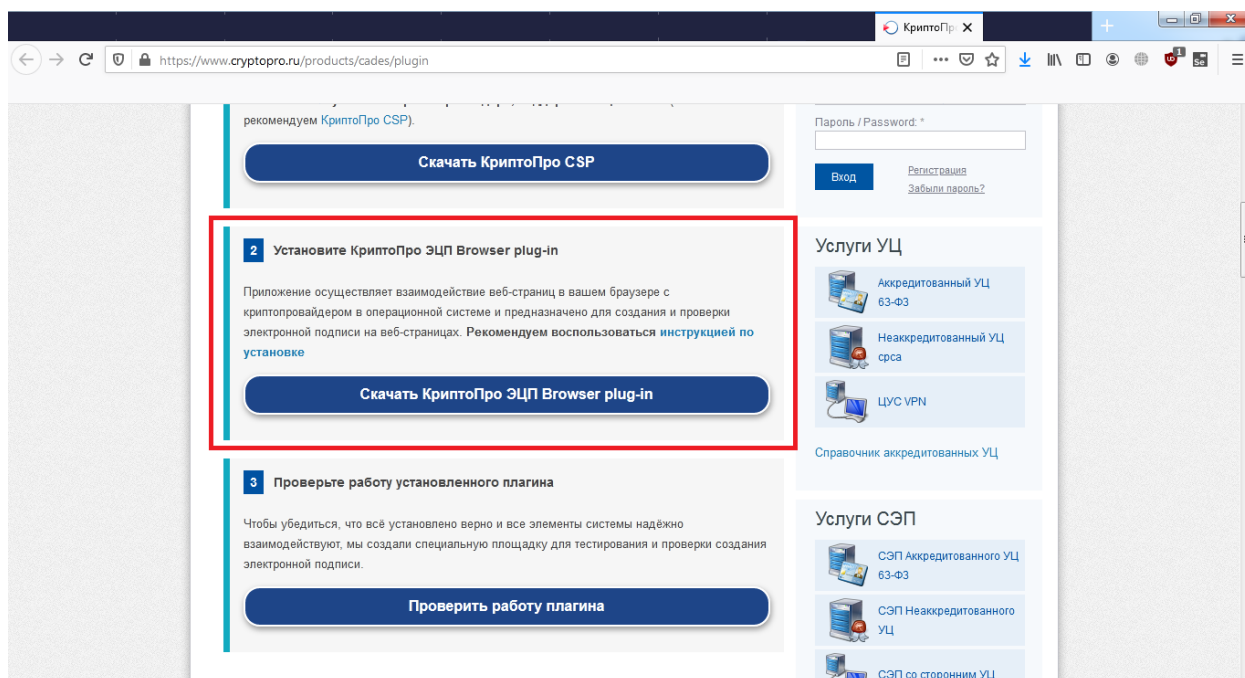


Рисунок 1. Установка Cades-плагин для web-браузера

Для выпуска тестового сертификата необходимо перейти на сайт тестового удостоверяющего центра КриптоПро <https://www.cryptopro.ru/certsrv/>. Далее перейти по ссылке «Сформировать ключи и отправить запрос на сертификат», см. рисунок 2.

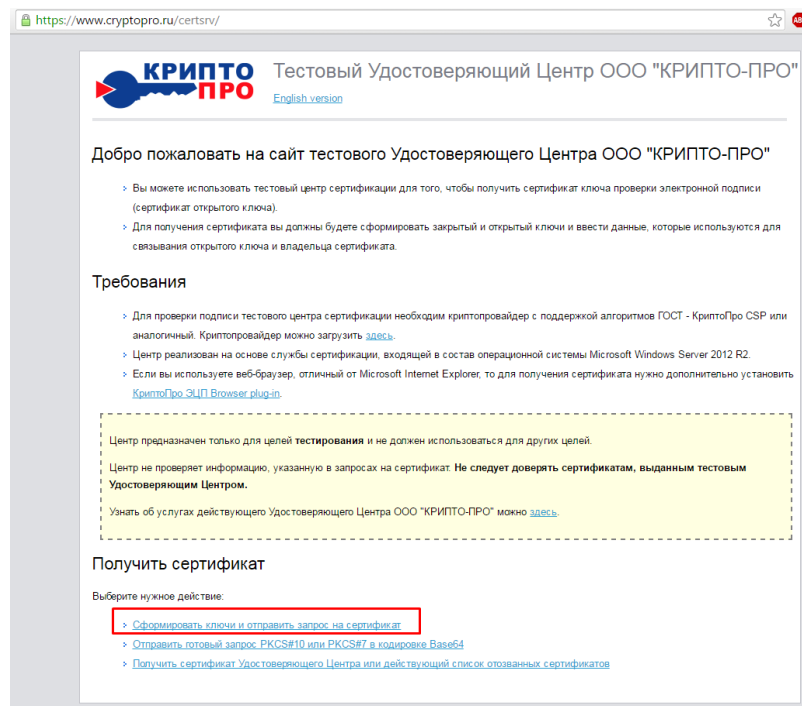


Рисунок 2. Выпуск тестового сертификата

Заполнить форму запроса сертификата тестовыми данными (можно выбрать опцию «Пометить ключ как экспортируемый») и нажать кнопку «**Выдать**» (рисунок 3).

← → C <https://www.cryptopro.ru/certsrv/certqma.asp>

Службы сертификации Active Directory (Microsoft) – CRYPTO-PRO Test Center 2

Расширенный запрос сертификата

Идентифицирующие сведения:

Имя:

Электронная почта:

Организация:

Подразделение:

Город:

Область, штат:

Страна, регион:

Тип требуемого сертификата:

Параметры ключа:

Создать новый набор ключей Использовать существующий набор ключей

CSP:

Использование ключей: Exchange Подпись Оба

Размер ключа: Минимальный: 512 Максимальный: 512 (стандартные размеры ключей: [512](#))

Автоматическое имя контейнера ключа Заданное пользователем имя контейнера ключа

Пометить ключ как экспортируемый

Использовать локальное хранилище компьютера для сертификата
 Сохраняет сертификат в локальном хранилище вместо пользовательского хранилища сертификатов.
 Не устанавливает корневой сертификат ЦС.
 Необходимо быть администратором, чтобы создать локальное хранилище.

Дополнительные параметры:

Формат запроса: CMC PKCS10

Алгоритм хеширования: Используется только для подписания запроса.

Сохранить запрос

Атрибуты:

Понятное имя:

Рисунок 3. Формирование сертификата

Далее на форме в списке устройств выбрать «Реестр» как носитель для хранения контейнера закрытого ключа (рисунок 4).

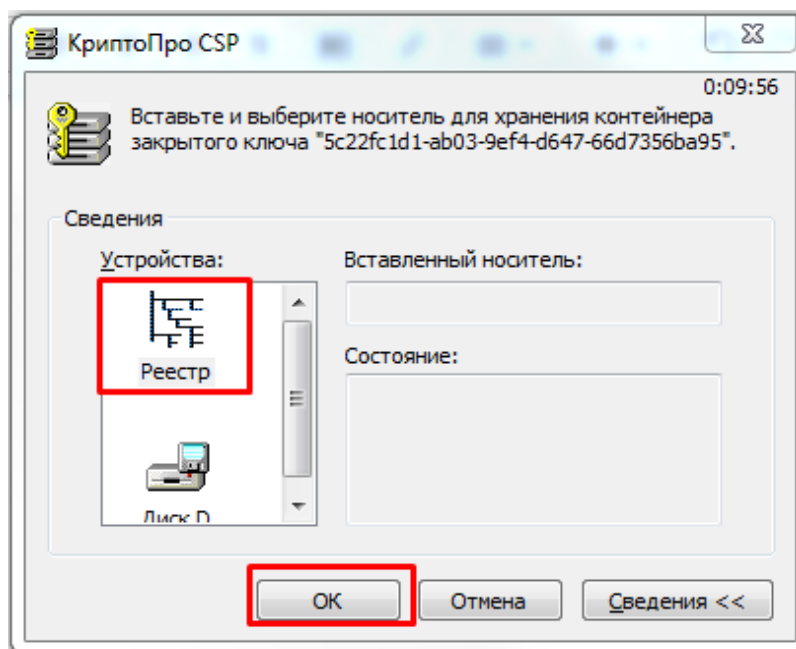


Рисунок 4. Установка сертификата

Для генерации случайной последовательности необходимо перемещать курсор мыши по экрану и нажимать на различные кнопки до тех пор, пока процесс не завершится (рисунок 5).

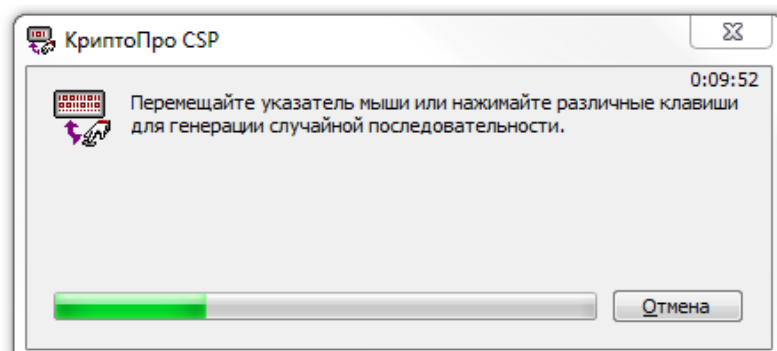


Рисунок 5. Генерация случайной последовательности

Определить пароль для закрытого ключа сертификата ЭП (рисунок 6).

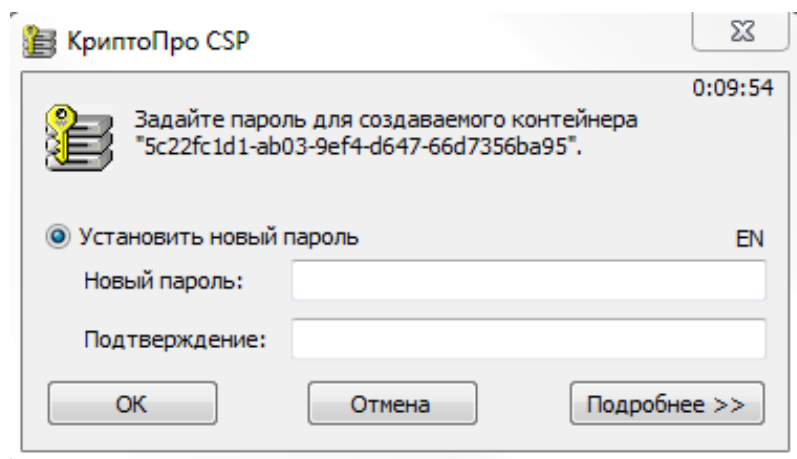


Рисунок 6. Ввод пароля

После ввода пароля пользователя сервис перенаправит Вас на страницу выдачи сертификата, где необходимо нажать на ссылку «Установить этот сертификат», см. рисунок 7.

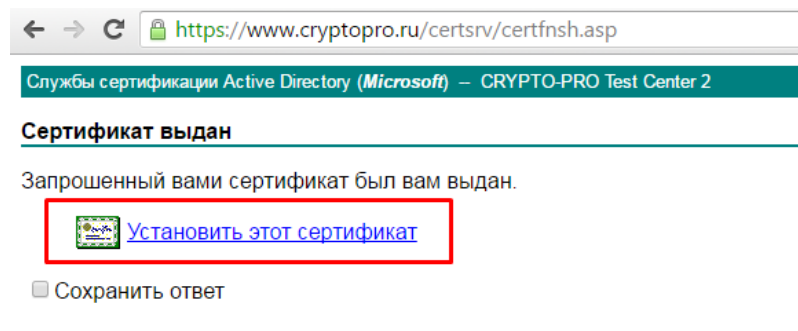


Рисунок 7. Установка сертификата

В открытой форме ввести, определенный ранее на предыдущем этапе, пароль для закрытого ключа сертификата ЭП, см. рисунок 8.

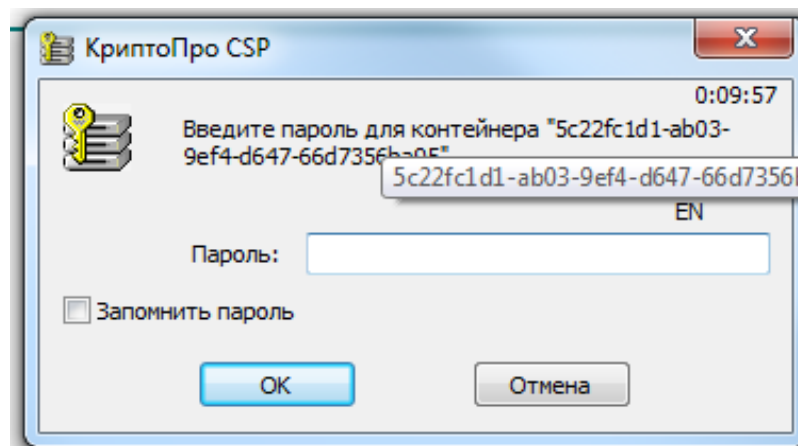


Рисунок 8. Ввод пароля

В случае успешного завершения процесса должно быть отображено соответствующее сообщение, см. рисунок 9.

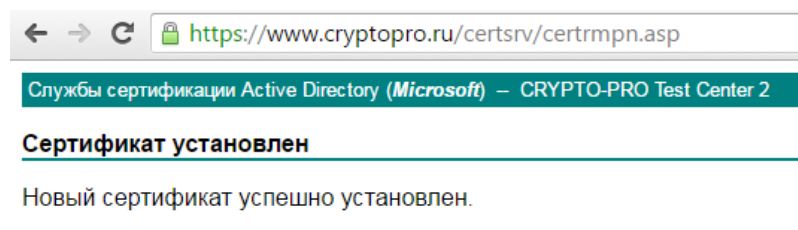


Рисунок 9

Для проверки корректности установленного сертификата необходимо перейти на портал https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html, где убедиться, что плагин корректно установлен в браузере. Об этом можно узнать по сообщению, выведенному на экран, см. рисунок 10.

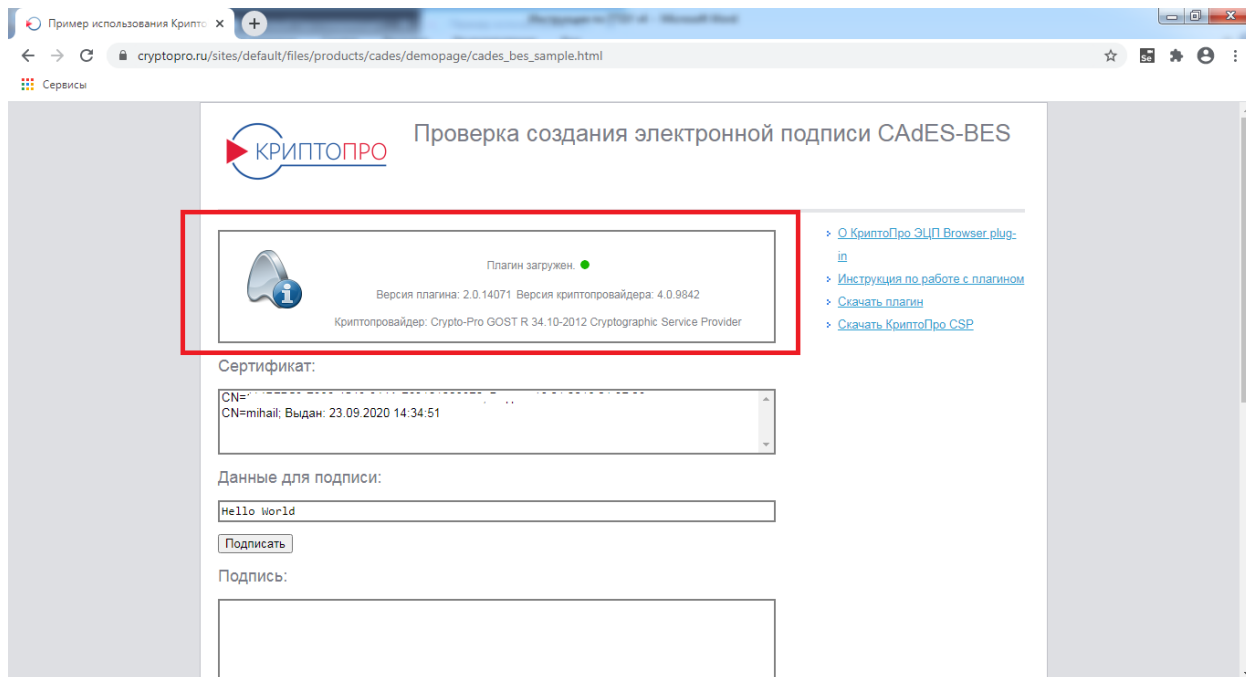


Рисунок 10. Проверка плагина

Далее необходимо выбрать ранее установленный сертификат в поле «Сертификат», после чего откроется форма с подробной информацией о сертификате, см. рисунок 11.

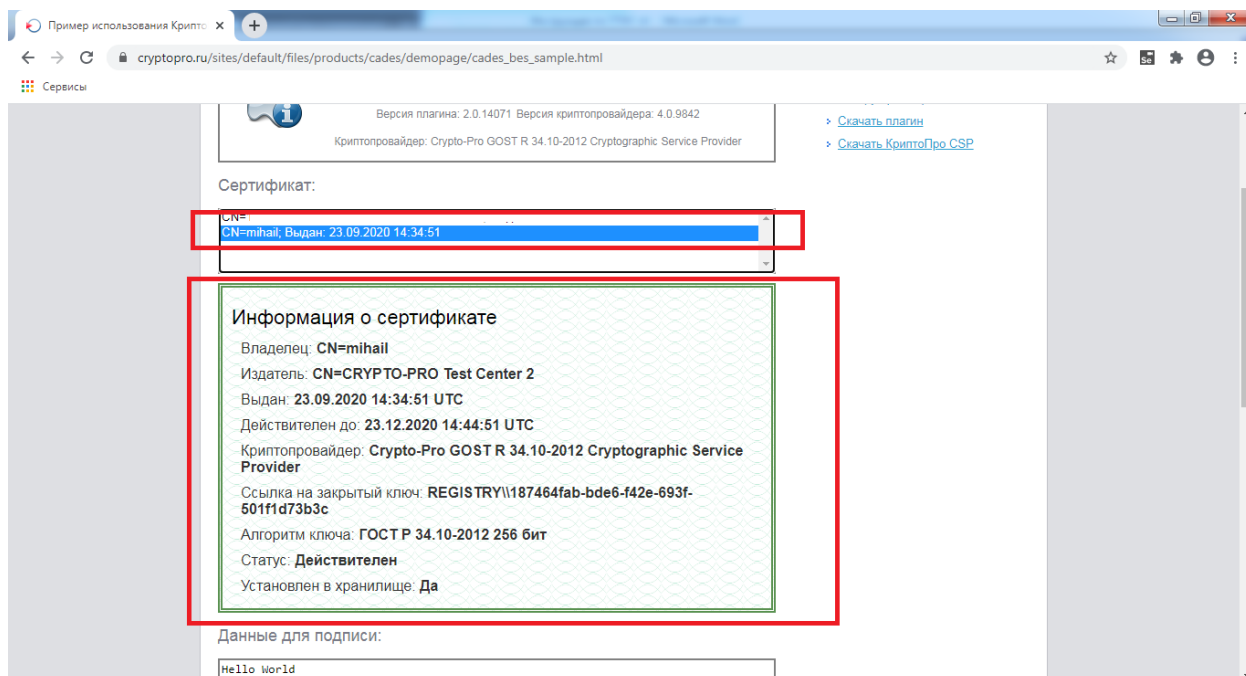


Рисунок 11. Выбор сертификата

После выбора сертификата необходимо нажать на кнопку «Подписать». В появившейся форме ввести пароль. В случае успешной установки сертификата будет сформирована ЭП (рисунок 12).

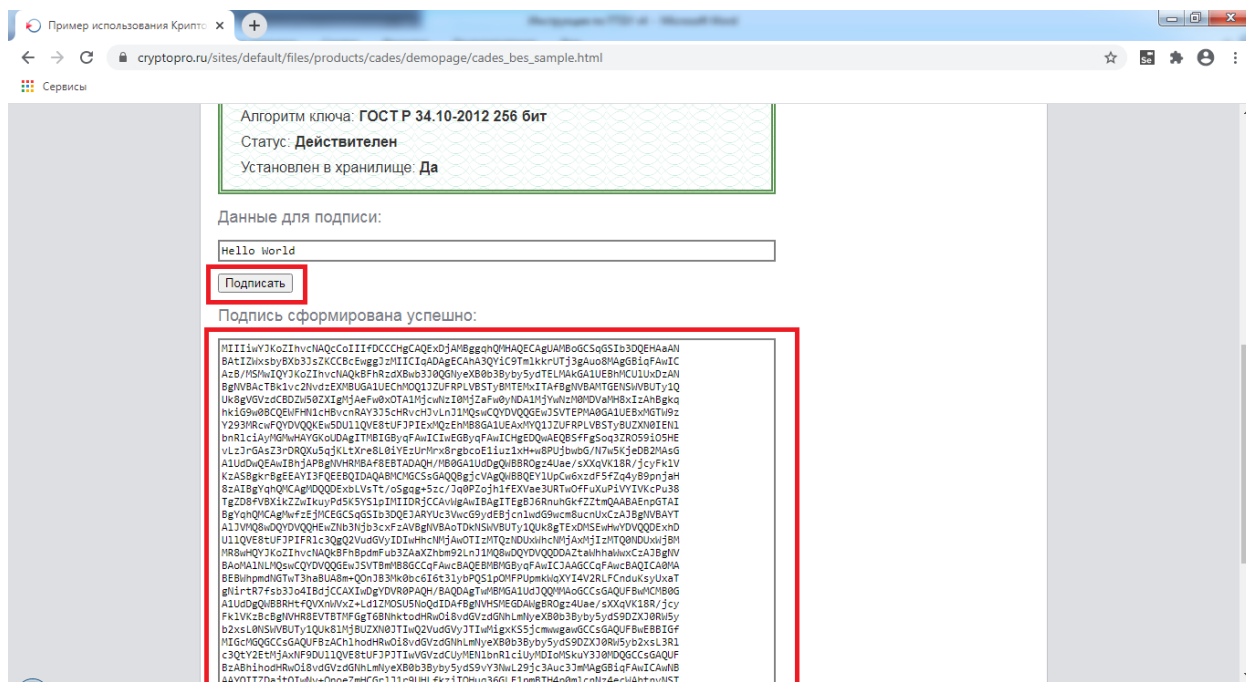


Рисунок 12. Сформированная ЭП

На этом процедура установки и настройки криптопровайдера КриптоПро, Cades-плагина для web-браузера и сертификата ЭП считается выполненной.