Как установить сертификат из облачного хранилища КриптоПро DSS в КриптоАРМ

На вопрос знаете ли вы что такое облачная электронная подпись, вы скорее всего ответите, что это подпись, которая хранится в облаке, и будете правы. Облачная подпись, а точнее ключи облачной подписи, хранятся на веб-сервере организации, оказывающей услуги по предоставлению сервиса обмена электронными документами.

Плюсы такого варианта хранения в том, что такой ключ невозможно потерять или повредить, в отличии от физического носителя. Еще облачная подпись удобна тем, что она доступна всегда и с любого места. Все что нужно, это любой браузер и интернет, так что обычный смартфон автоматически превращается в готовый инструмент для электронной подписи.

Минусы у облачной подписи конечно же есть. Такая подпись не будет работать без подключенного интернета. Порой ей требуется телефон, например для подтверждения действий путем ввода коротких смс-кодов. Но основное неудобство, даже не в этом, а в том, что ключ облачной подписи может быть использован в рамках только одной определенной информационной системы или веб-сервиса.

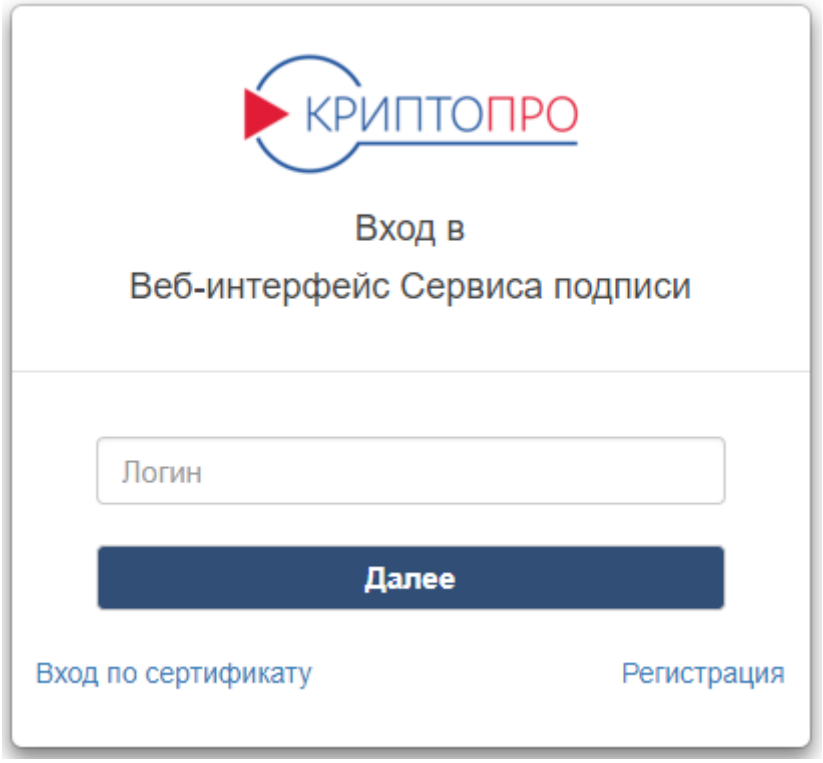
Типичный пример, это личный кабинет налогоплательщика для физических лиц. В нем есть возможность бесплатно создать ключ неквалифицированной электронной подписи. Подпись выдается облачной и хранится она на сервере налоговой. Но использовать ее можно только для подачи заявок и обращений в ФНС и никуда более.

Каким образом использовать облачную подпись для подписи любых документов и для разных систем. Решение простое, это привязать ключ облачной подписи в настольном приложении. И уже из него подписывать файлы для Росреестра, ФСРАР или др.

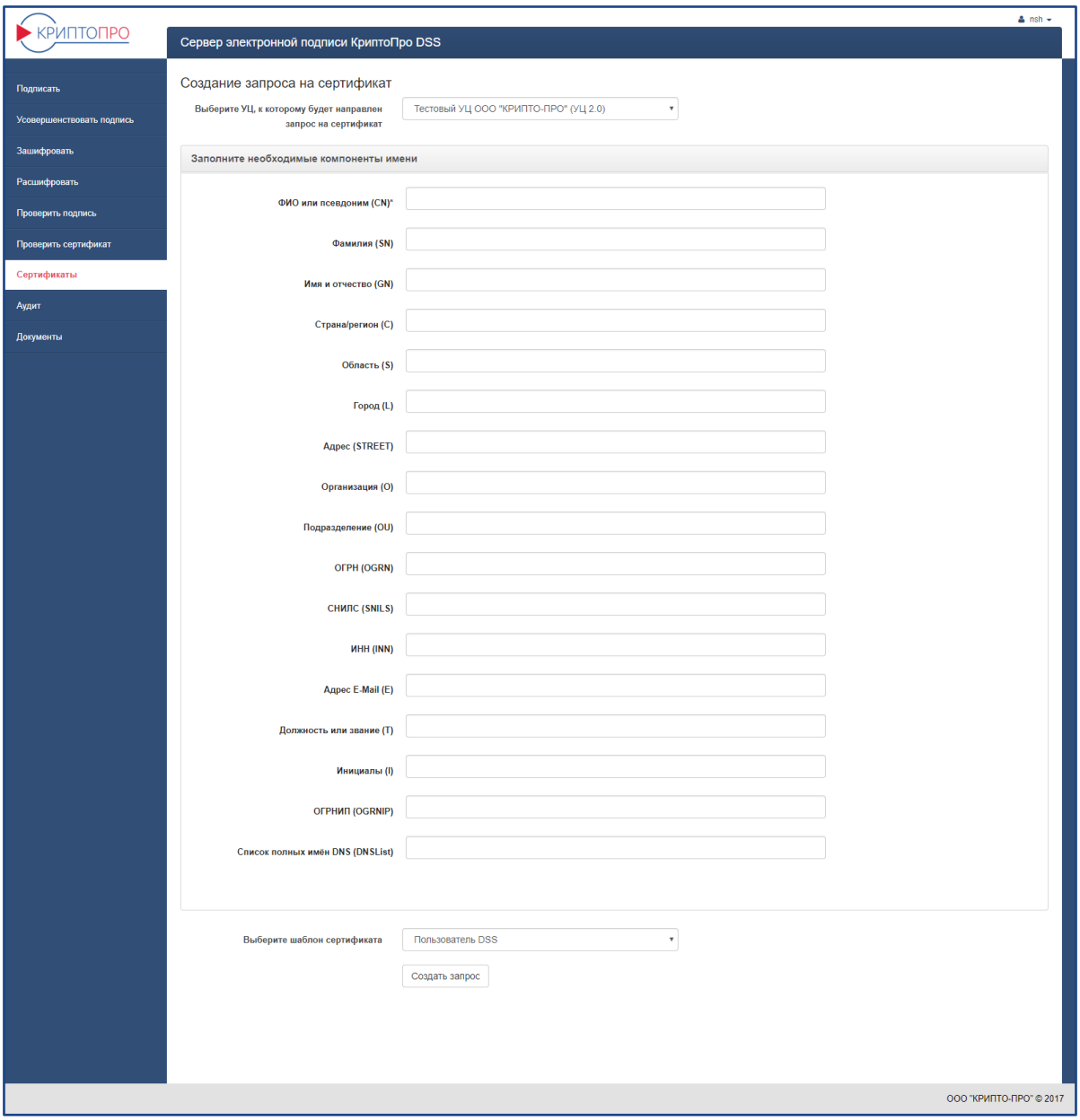
Расскажем, как это выполнить поэтапно на примере сервера электронной подписи КриптоПро DSS, первого облачного криптопровайдера КриптоПро Cloud CSP и программы КриптоАРМ. В примере разумеется показан тестовый сервис КриптоПро DSS, поэтому веб-интерфейс пользователя может отличаться.

Первый шаг. Авторизоваться в КриптоПро DSS.

Для этого нужно пройти регистрацию или войти с уже имеющимися учетными данными.



После авторизации становится доступен раздел «Сертификаты». Если нет действующих сертификатов, то можно создать запрос на новый сертификат. Для этого нужно выбрать УЦ и заполнить необходимые поля. При создании запроса в сервисе будет создан контейнер с ключами, и получен сертификат электронной подписи. В реальном обстоятельствах, ключ электронной подписи выдает Удостоверяющий центр.

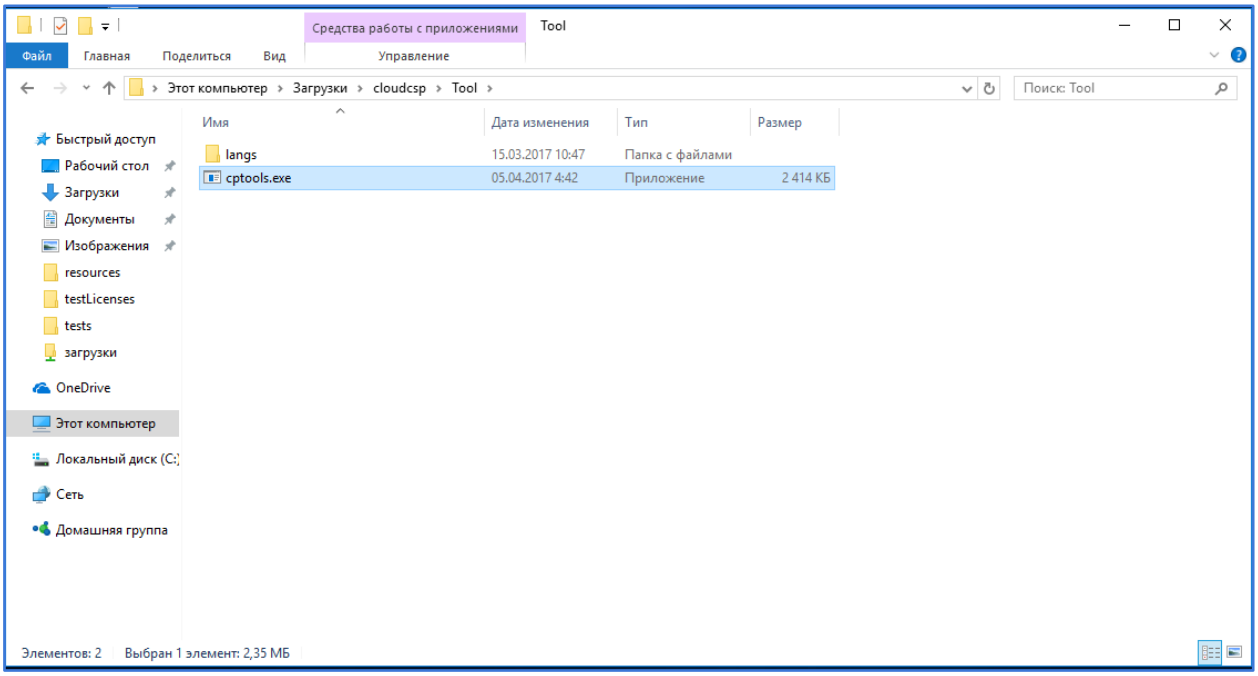


Второй шаг. Установить КриптоПро Cloud CSP.

Криптопровайдер КриптоПро Cloud CSP доступен для скачивания по ссылке. Помимо дистрибутива в архиве будет также краткая инструкция по использованию. Установка дистрибутива не вызовет сложностей. Но есть одно условие, перед установкой КриптоПро Cloud CSP нужно предварительно удалить все другие криптопровайдеры.

Третий шаг. Установить сертификат из DSS в локальное хранилище.

Найти в папке Tools утилиту cptools и запустить ее. входящую в дистрибутив КриптоПро Cloud CSP.

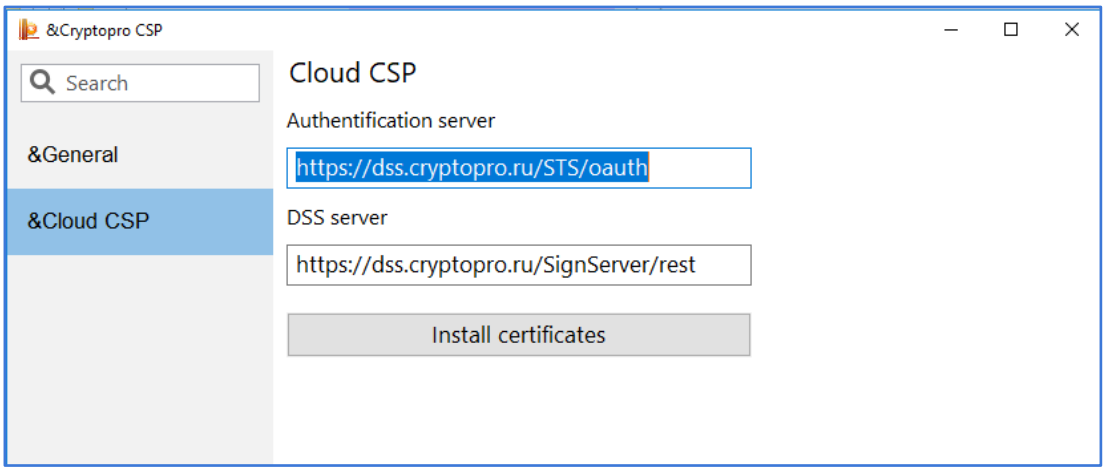


В открывшемся окне перейти на вкладку Cloud CSP и указать в настройках следующие значения для полей:

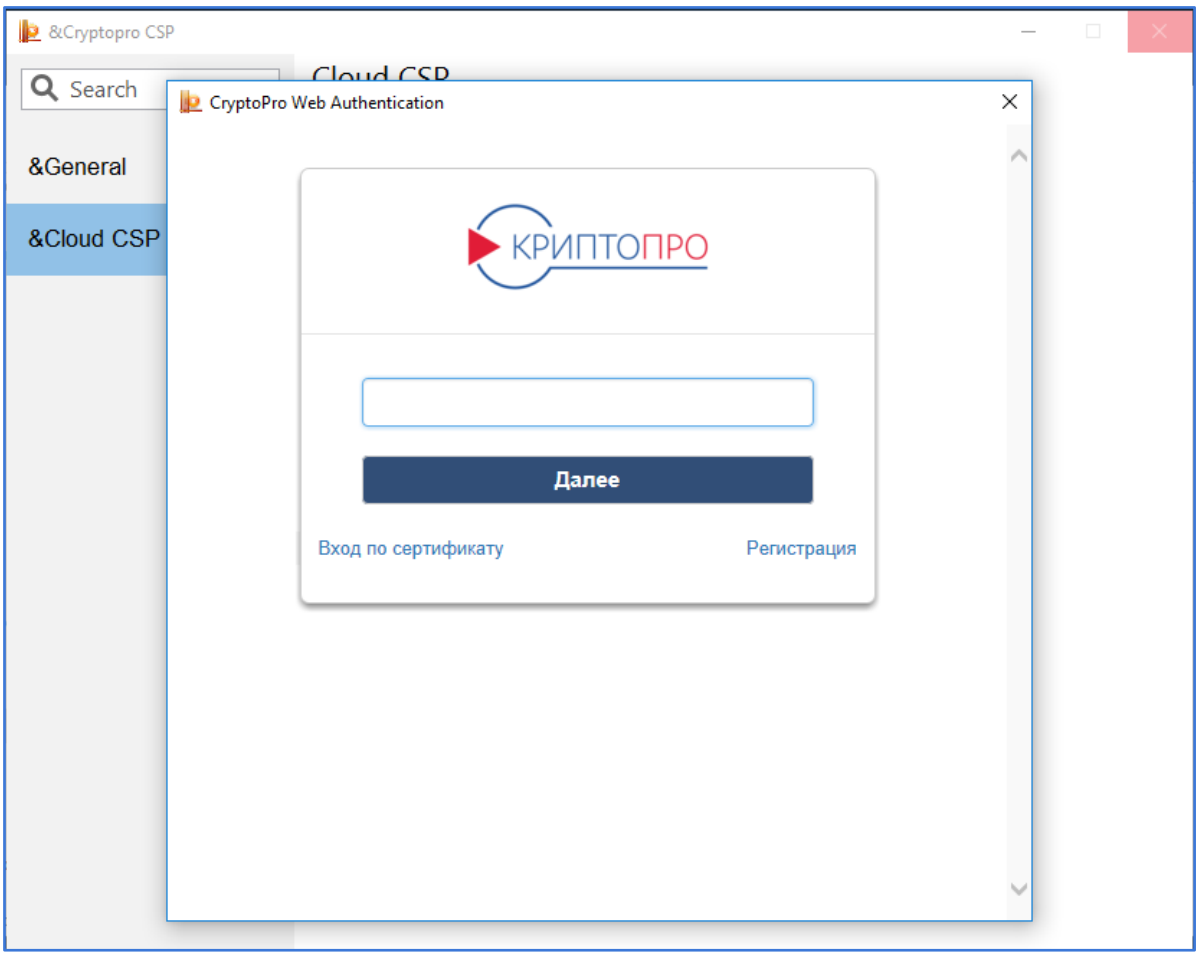
Сервер аутентификации: https://dss.cryptopro.ru/STS/oauth

DSS сервер: https://dss.cryptopro.ru/SignServer/rest

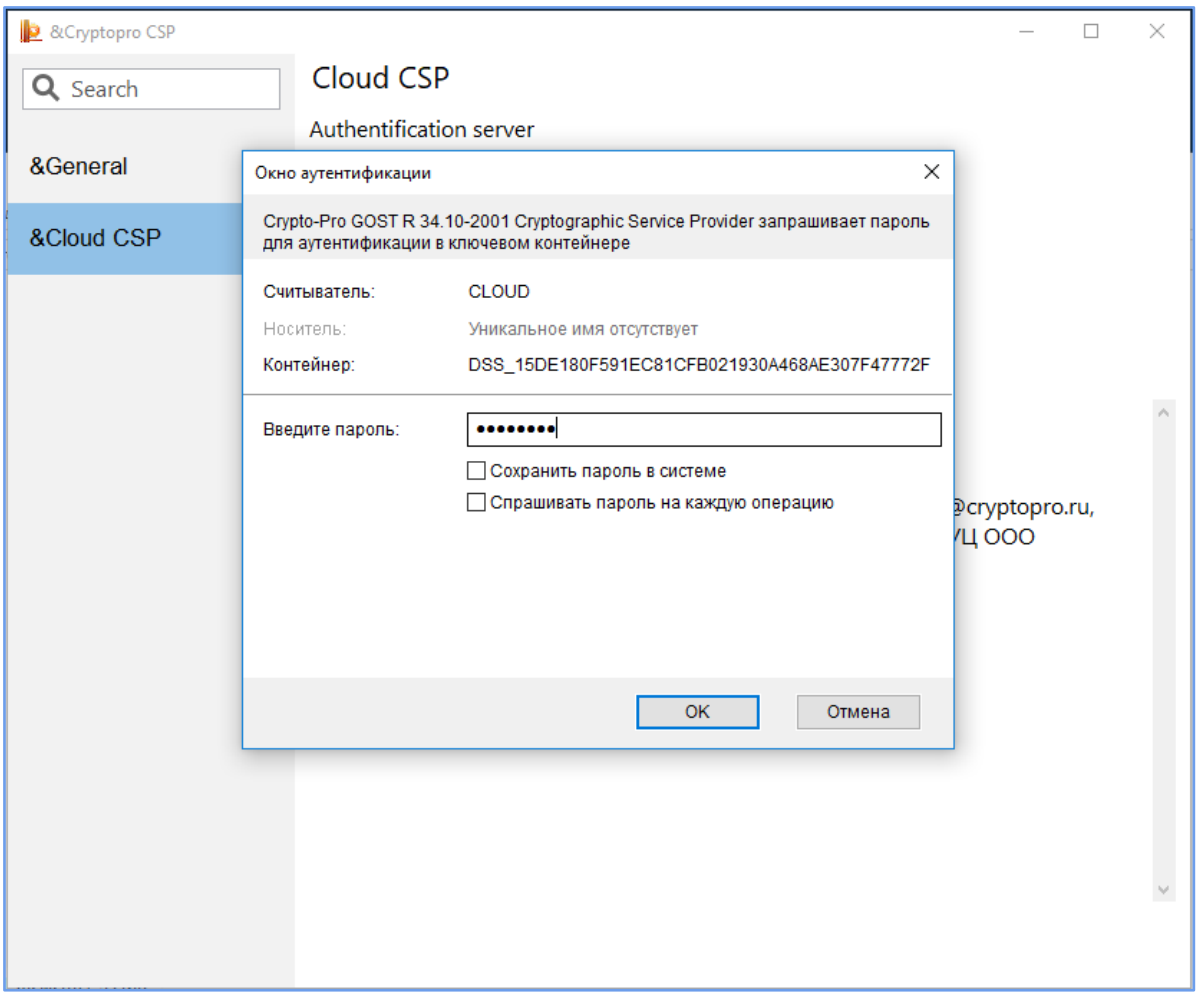
и нажать на кнопку «Установить сертификаты» («Install certificates»).



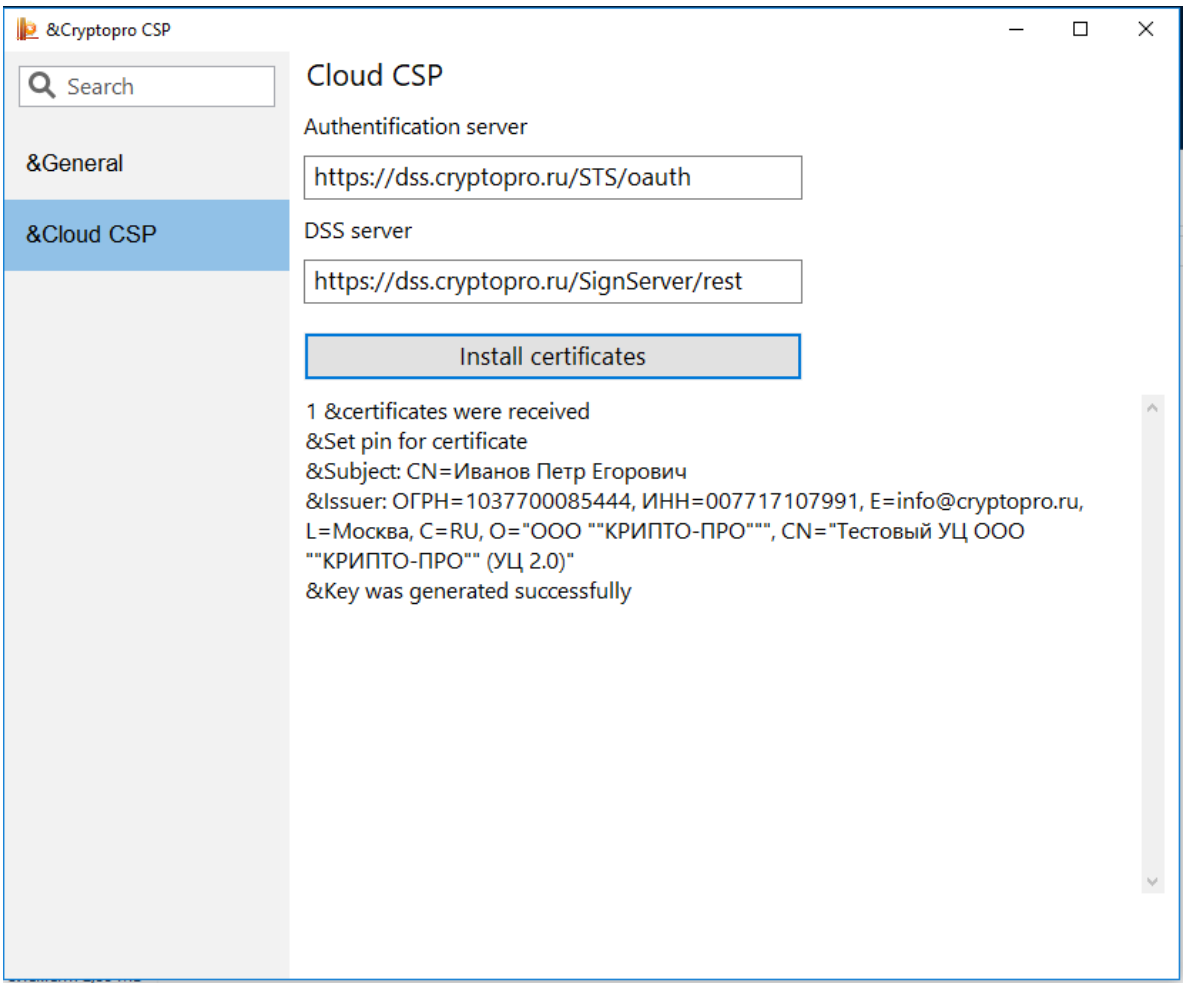
Ввести логин/пароль для входа на КриптоПро DSS.



Затем в открывшемся окне появится новый считыватель CLOUD с указанием контейнера с ключом из сервера КриптоПро DSS. Для продолжения необходимо ввести пароль (пин-код) от указанного контейнера.

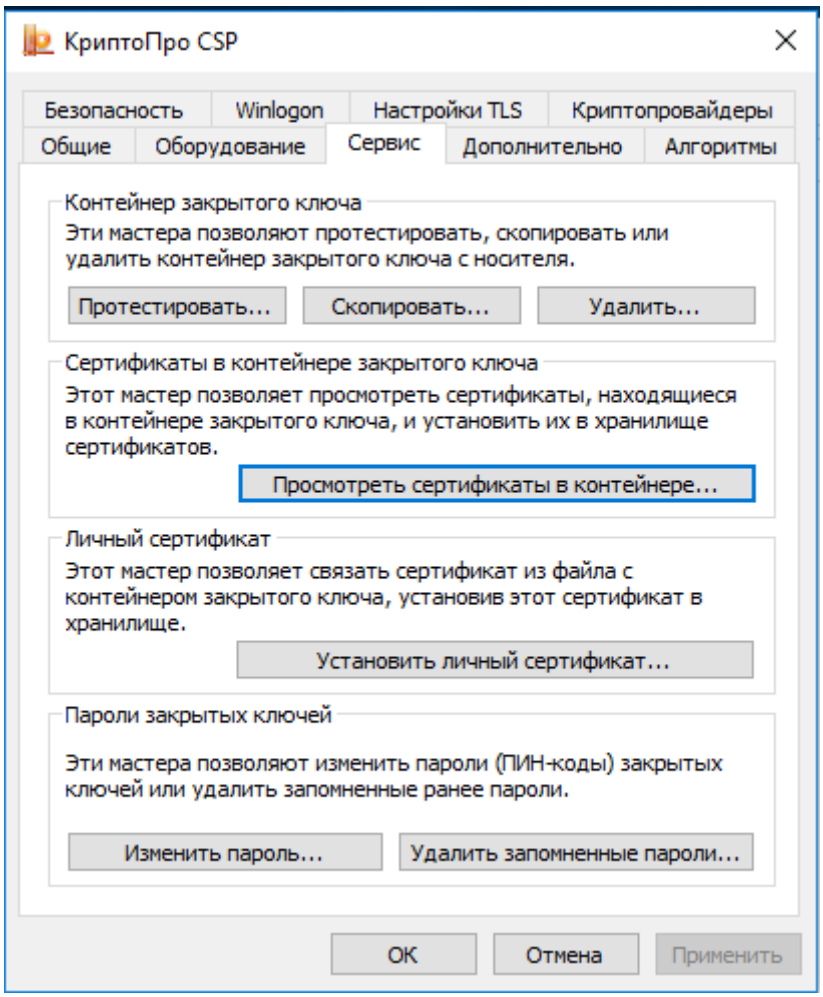


Если все введено верно, то появится следующая запись. Это означает, что сертификат из сервера КриптоПро DSS успешно установлен на локальном рабочем месте.

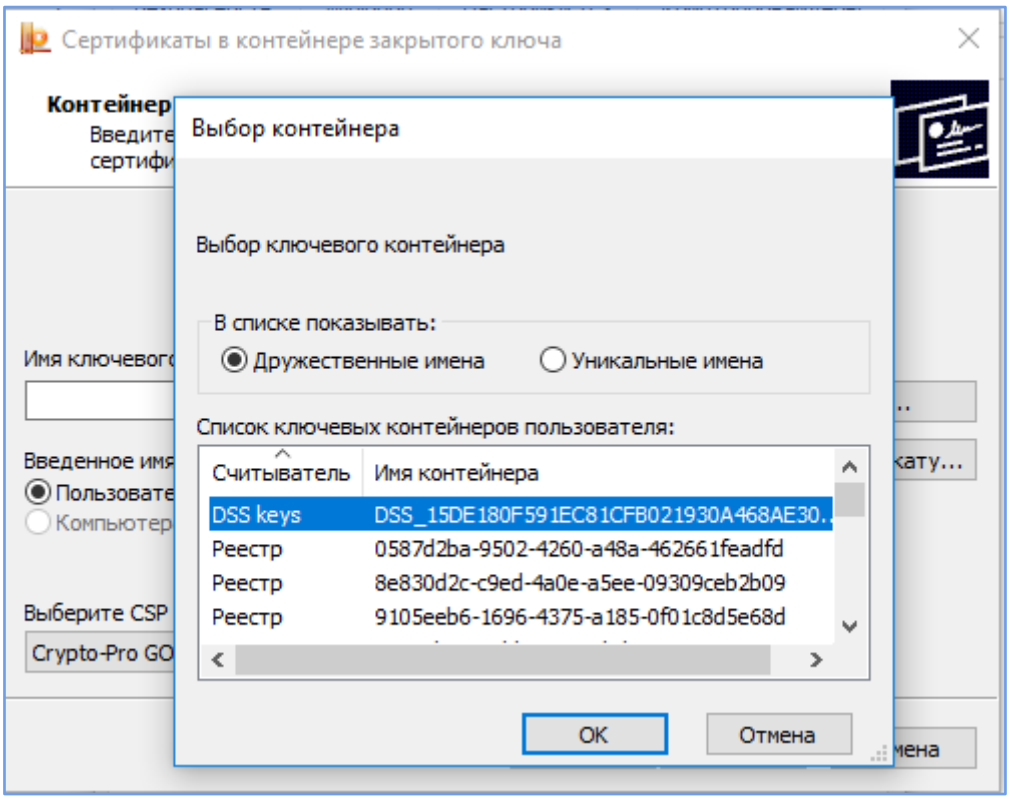


Четвертый шаг. Установить сертификат из КриптоПро DSS в КриптоАРМ.

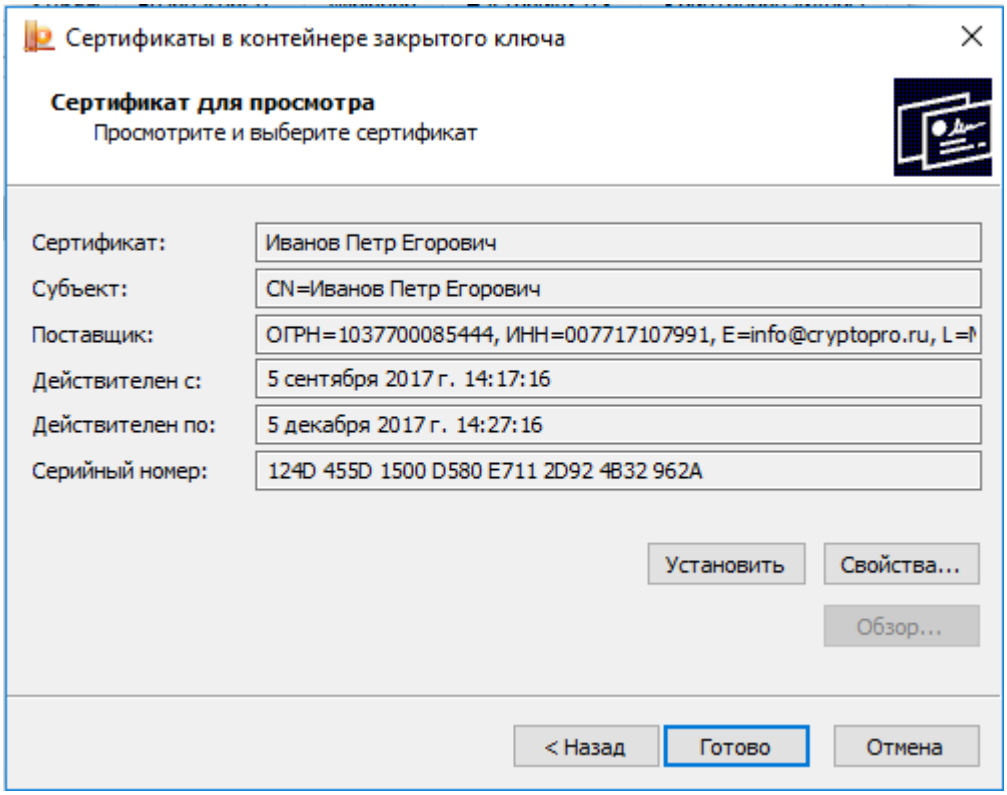
В начале открываем программу КриптоПро CSP. Выбираем вкладку «Сервис» и кнопку «Просмотреть сертификаты в контейнере...».



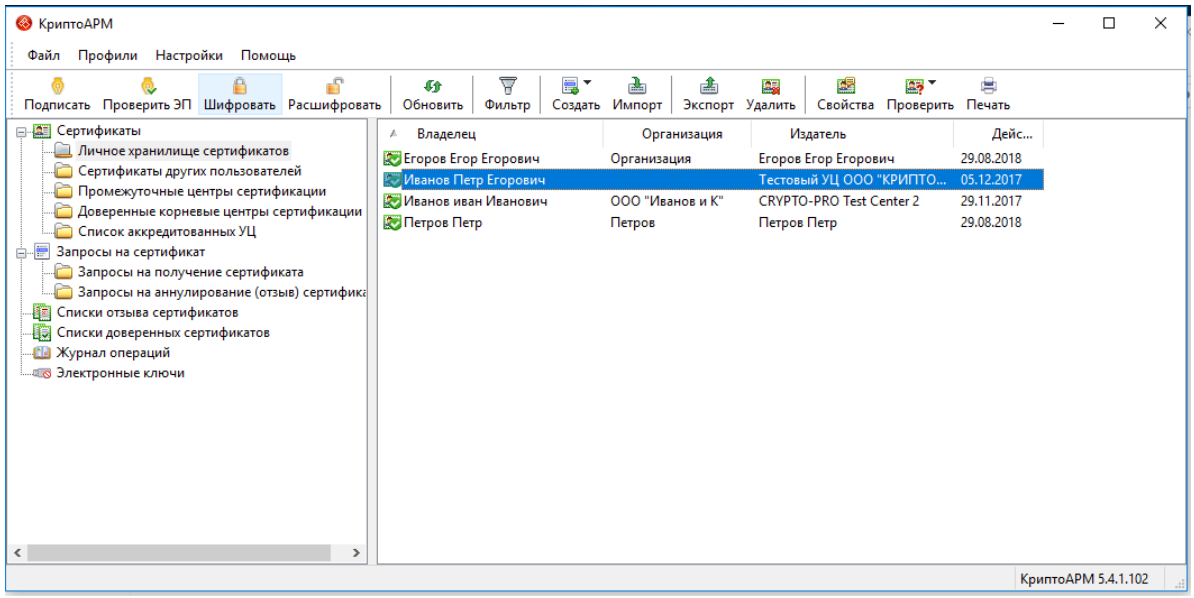
В списке ключевых контейнеров находим тот, чей тип считывателя называется DSS keys.



Выбрав нужный контейнер, нажать «ОК» и «Далее». Затем в окне «Сертификат для просмотра» нажимаем «Установить». Появится сообщение об успешной установке сертификата в хранилище «Личные». Нажимаем «Готово».



Сертификат из облачного хранилища КриптоПро DSS успешно установлен. Открываем программу КриптоАРМ находим его в «Личном хранилище сертификатов». С этого момента, данный сертификат можно использовать для подписи любых файлов, находящихся на локальном компьютера.



Ключ подписи по прежнему хранится в облаке. Интернет и телефон по прежнему необходимы для подписи. Но теперь вы можете подписывать любые файлы без ограничений. Можете подписывать их прямо с рабочего стола не

запуская браузер и не заходя на страницу веб-сервиса. Или подписывать из знакомого приложения.

Резюмируя, порталы и веб-сервисы, предлагающие облачную подпись становятся с каждым годом все более доступными и массовыми. Но в силу своей специфики у такого вида подписей есть ряд ограничений, главное из которых привязанность к определенной информационной системе. Решение КриптоПро Cloud CSP расширяет спектр применения облачной подписи, предлагая способ использовать ее в популярных приложениях, наподобие КриптоАРМ.