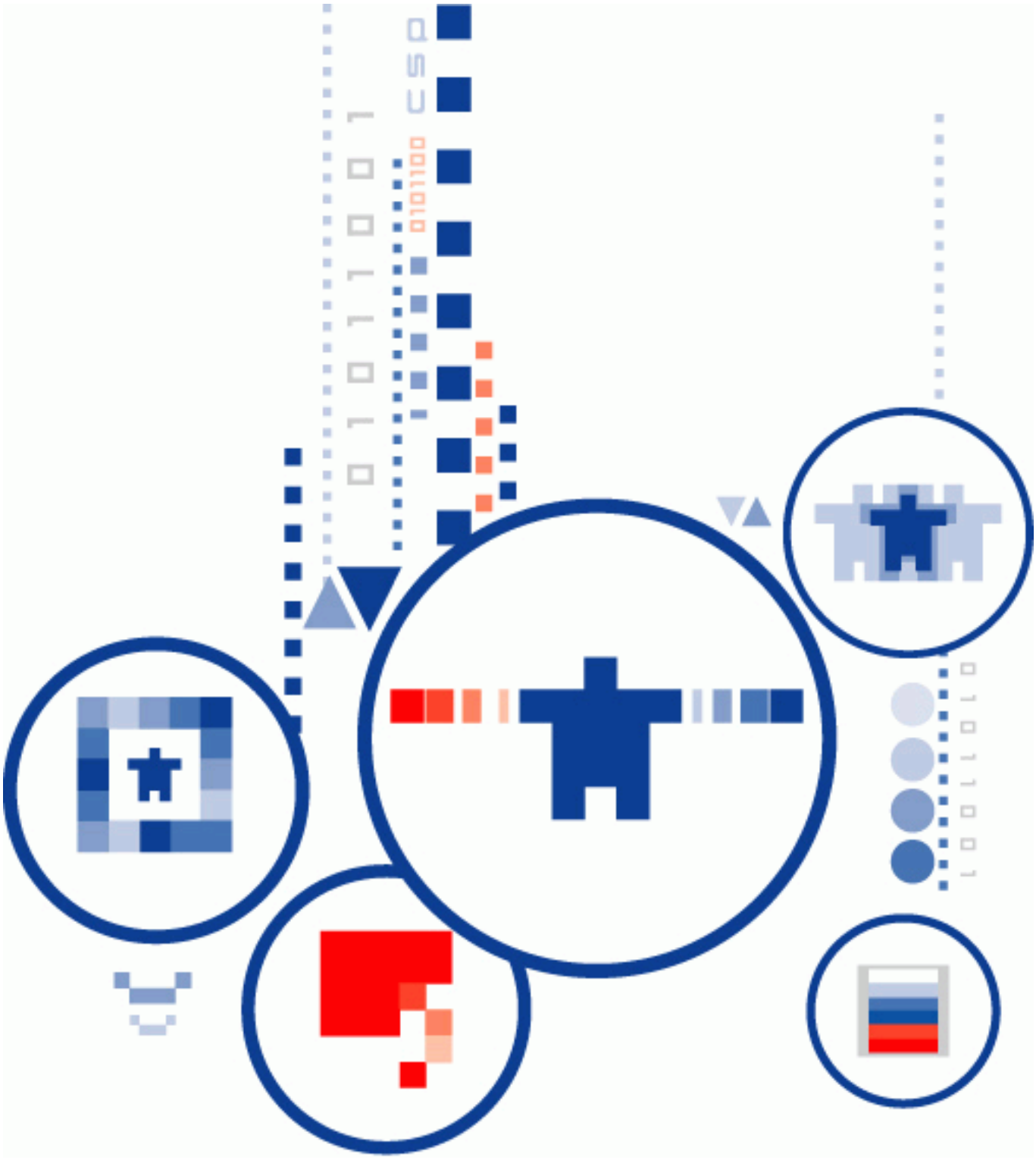
УТВЕРЖДЁН
ЖТЯИ.00082-01 90 04 06-ЛУ

ЖТЯИ.00082-01 90 04 06



ПАК «КриптоПро DSS»

Тестовый сервис электронной подписи

Инструкция Пользователя СЭП

ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Пользователей тестового сервиса электронной подписи ООО «КРИПТО-ПРО» базе ПАК «КриптоПро DSS» (далее – СЭП) и определяет порядок использования Веб-интерфейса СЭП для осуществления операций по доступу и управлению сертификатами ключей проверки электронной подписи, созданию и проверке электронной подписи, шифрованию и расшифрованию электронных документов.

Информация о разработчике ПАК «КриптоПро DSS»:

ООО «КРИПТО-ПРО»

127 018, Москва, Улица Сущевский Вал, д.18, эт.17

Телефон: (495) 995 4820

http://www.CryptoPro.ru

https://www.cryptopro.ru/service/sign

E-mail: info@CryptoPro.ru

Содержание

1. Общие положения

Тестовый сервис электронной подписи ООО «КРИПТО-ПРО» на базе ПАК «КриптоПро DSS» (далее – СЭП) предназначен для демонстрации и тестирования операций создания и хранения ключей электронной подписи, формирования запросов на создание и управление тестовыми сертификатами ключей проверки электронной подписи (далее – сертификаты), выполнения операций по созданию и проверке электронной подписи различного формата криптографических сообщений, шифрования и расшифрования электронных документов.

Настоящая инструкция определяет порядок действия Пользователя СЭП (далее – Пользователь) при выполнении операций формирования, усовершенствования и проверки электронной подписи, шифрования и расшифрования электронных документов, а также создания запросов на сертификаты ключей проверки электронных подписей и проверки электронных подписей и сертификатов ключей проверки электронных подписей.

1.1. Требования и подготовка рабочего места Пользователя

В случае если первичная аутентификация Пользователя в СЭП производится *без использования сертификата аутентификации Пользователя*, на рабочем месте Пользователя под управлением операционной системы (далее – ОС) Microsoft Windows 7 или выше должен быть установлен и использоваться Интернет-обозреватель Internet Explorer версии 10 или выше.

В случае если первичная аутентификация Пользователя в СЭП производится *по сертификату аутентификации Пользователя*, на рабочем месте Пользователя под управлением ОС Microsoft Windows 7 или выше должно быть установлено СКЗИ «КриптоПро CSP» версии 4.0 (СКЗИ «КриптоПро CSP» версии 5.0 для использования «облачного» токена – см. **Использование «облачного» токена в СКЗИ «КриптоПро CSP 5.0»**).

или выше в соответствии с эксплуатационной документацией на СКЗИ. Для подключения к СЭП обязательно использование Интернет-обозревателя Internet Explorer версии 10 (далее – браузер) или выше.

Для аутентификации Пользователя в СЭП *по сертификату* необходимо установить предоставленные Оператором СЭП сертификаты в следующие хранилища сертификатов ОС Windows:

- **Сертификат Тестового УЦ ООО «КРИПТО-ПРО» (УЦ 2.0)** – в хранилище «Доверенные корневые центры сертификации».
- **Сертификат Sub-TESTCA20-CA** – в хранилище «Промежуточные центры сертификации».
- **Сертификат первичной аутентификации Пользователя** – в хранилище «Личное».

Для корректной работы с СЭП в свойствах браузера нужно выбрать вкладку «*Безопасность*», в список надежных сайтов добавить узел https://stenddss.cryptopro.ru/ и сохранить изменения свойств (см. **Рисунок 1. Добавление в надёжные сайты**):

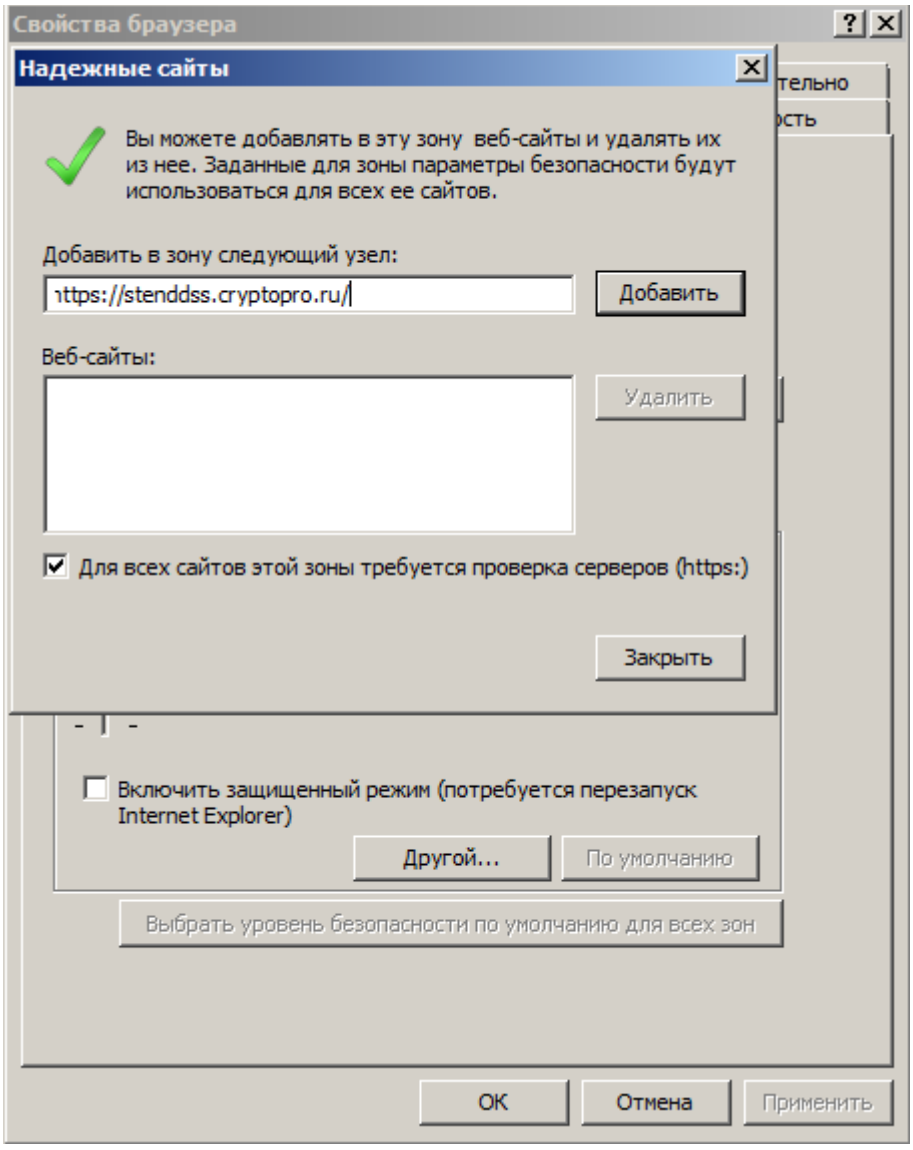


Рисунок 1. Добавление в надёжные сайты

2. Вход в веб-интерфейс СЭП

Аутентификация входа Пользователя в СЭП происходит с использованием методов первичной и вторичной аутентификации в СЭП. Каждому Пользователю Оператором СЭП назначается как минимум один метод первичной аутентификации и как минимум один метод вторичной аутентификации. Заданные методы первичной и вторичной аутентификации, а также перечень операций, подтверждаемых Пользователем с их помощью, сообщаются Пользователю Оператором СЭП, выполняющим регистрацию Пользователя в СЭП.

Возможные методы первичной аутентификации Пользователя:

- «*Только идентификация*» – первичная аутентификация Пользователя происходит посредством ввода наименования учётной записи Пользователя в СЭП (логин).
- «*Аутентификация по сертификату*» – первичная аутентификация Пользователя происходит по сертификату, выданному Пользователю Оператором СЭП.
- «*Аутентификация по паролю*» – первичная аутентификация Пользователя происходит по паролю, выданному Пользователю Оператором СЭП.

Возможные методы вторичной аутентификации Пользователя:

- «*Аутентификация по SMS*» – вторичная аутентификация Пользователя происходит по коду в SMS, отправляемых СЭП на мобильный телефон Пользователя.
- «*Аутентификация по протоколу OATH*» – вторичная аутентификация Пользователя происходит по одноразовому паролю OTP-токена.
- «*Аутентификация по электронной почте*» – вторичная аутентификация Пользователя происходит по коду, отправляемому СЭП на электронную почту Пользователя.
- «*Аутентификация с помощью мобильного приложения*» – вторичная аутентификация Пользователя происходит в мобильном приложении «*КриптоПро myDSS*».

Для работы в СЭП Пользователю нужно осуществить вход в веб-интерфейс Пользователя по адресу https://stenddss.cryptopro.ru/FrontEnd.

2.1. Вход в веб-интерфейс СЭП (только идентификация)

В случае если Оператором СЭП выбран метод первичной аутентификации «*Только идентификация*» Пользователю необходимо ввести имя учётной записи (логин) в поле ввода и нажать кнопку «*Далее*» (см. **Рисунок 2. Вход в СЭП. Окно ввода учётной записи**).

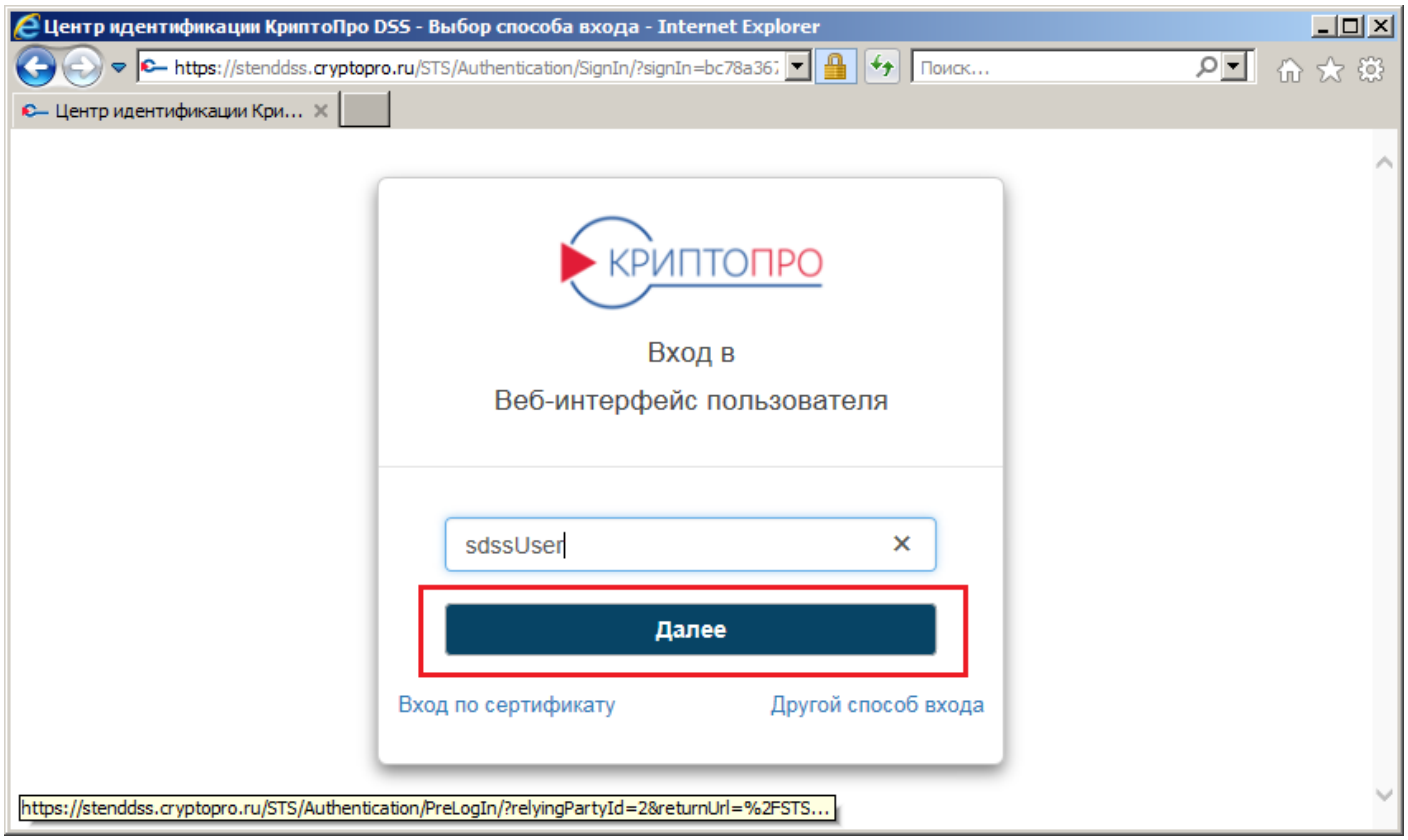


Рисунок 2. Вход в СЭП. Окно ввода учётной записи

Если Оператором СЭП задано подтверждение Пользователем операции входа в веб-интерфейс СЭП при помощи метода вторичной аутентификации, Пользователь должен подтвердить операцию входа соответствующим методом вторичной аутентификации (см. ***Методы вторичной аутентификации***).

Если все процедуры аутентификации Пользователя пройдены успешно, будет отображен интерфейс Пользователя СЭП (см. **Рисунок 3. Интерфейс Пользователя СЭП**).

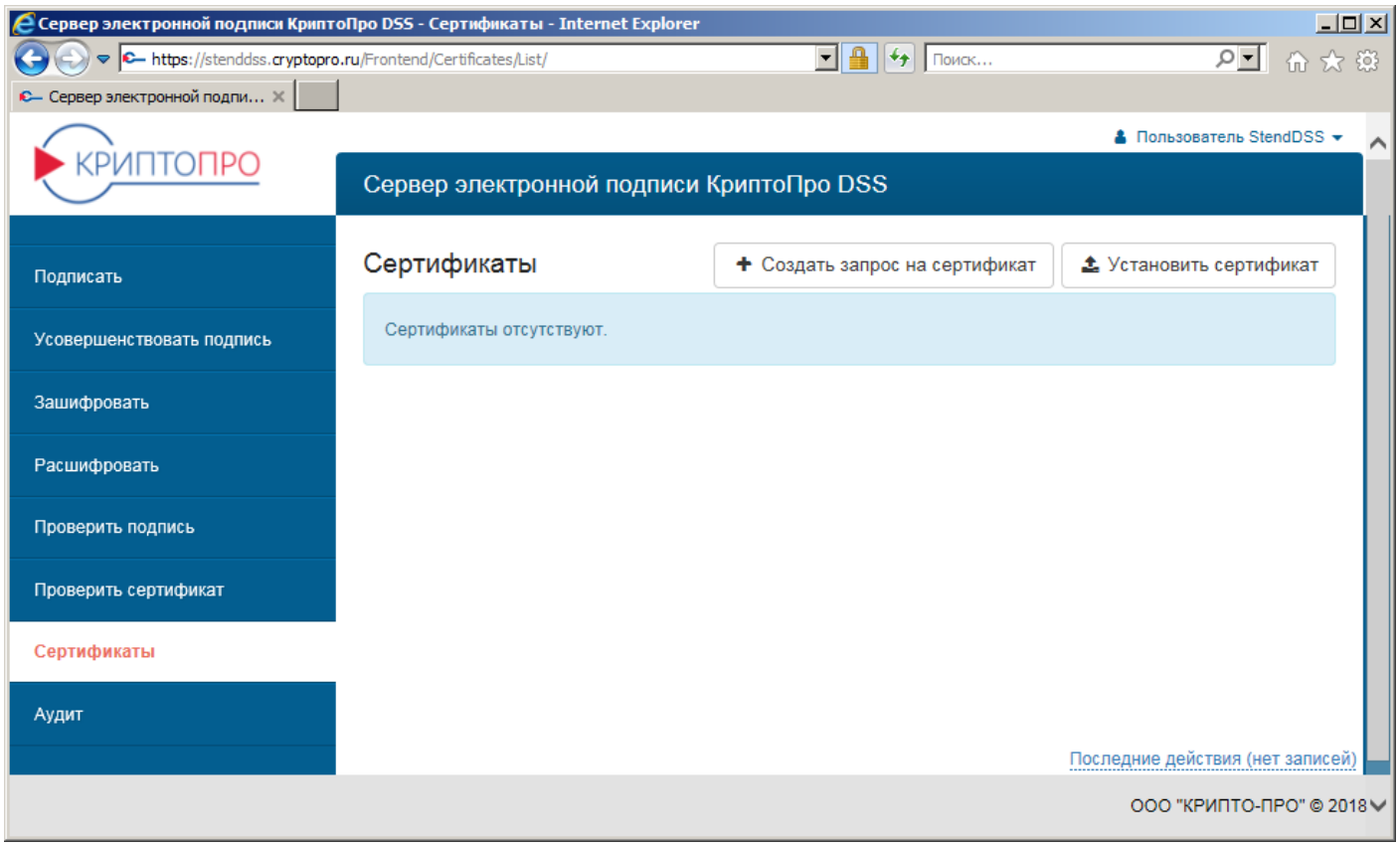


Рисунок 3. Интерфейс Пользователя СЭП

2.2. Вход в веб-интерфейс СЭП (аутентификация по сертификату)

В случае если Оператором СЭП выбран метод первичной аутентификации «*Аутентификация по сертификату*» Пользователю нужно нажать кнопку «*Вход по сертификату*», после чего в появившемся окне подтверждения сертификата выбрать сертификат Пользователя и нажать кнопку «*ОК*» (см. **Рисунок 4. Вход в СЭП (аутентификация по сертификату)**). Далее нужно ввести ПИН-код доступа к ключевому контейнеру и нажать кнопку «*ОК*» (см. **Рисунок 5. Ввод ПИН-кода**).

Если Оператором СЭП задано подтверждение Пользователем операции входа в веб-интерфейс СЭП при помощи метода вторичной аутентификации, Пользователь должен подтвердить операцию входа соответствующим методом вторичной аутентификации (см. ***Методы вторичной аутентификации***).

Если все процедуры аутентификации Пользователя пройдены успешно, будет отображен интерфейс Пользователя СЭП (см. **Рисунок 3. Интерфейс Пользователя СЭП**).

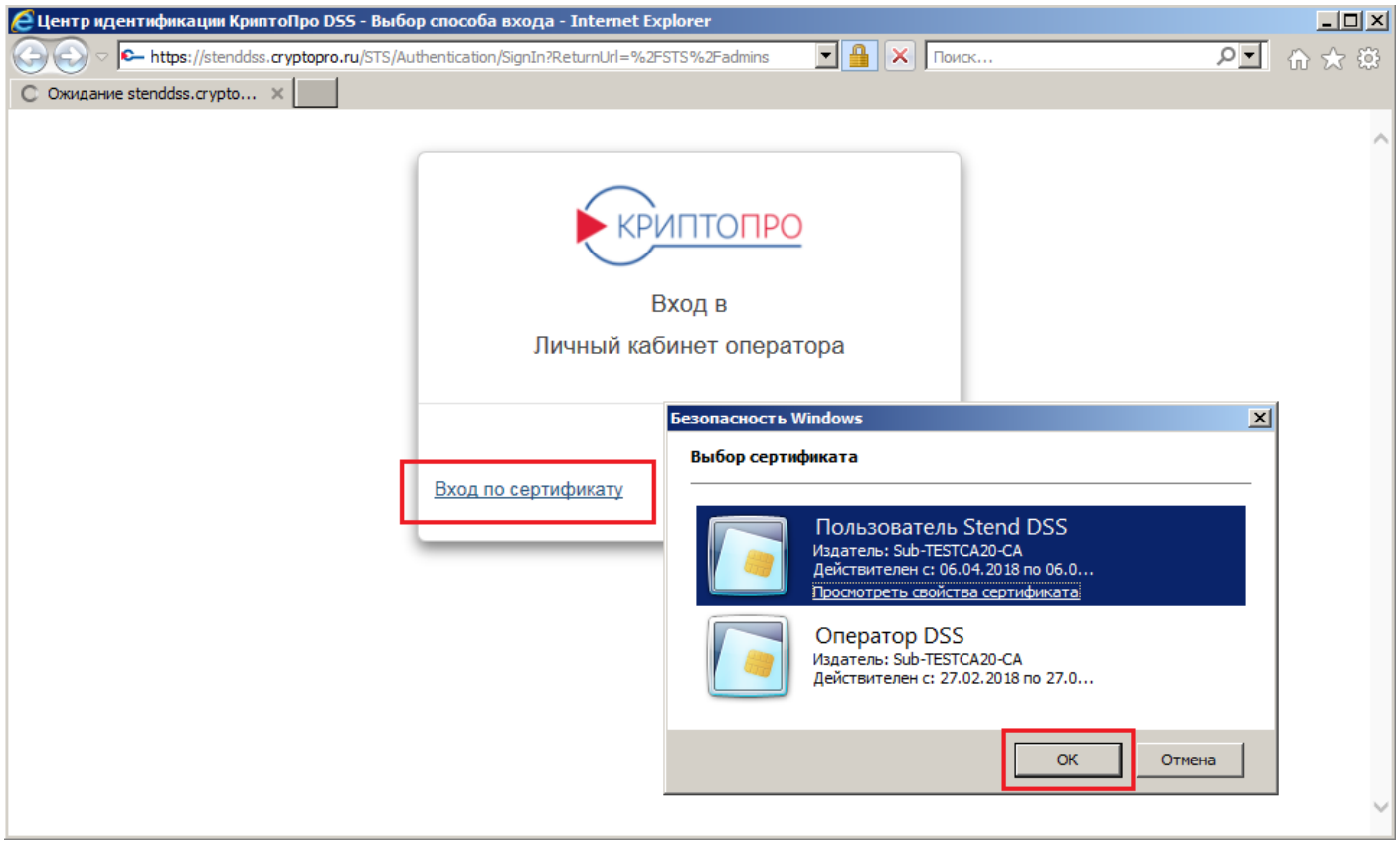


Рисунок 4. Вход в СЭП (аутентификация по сертификату)

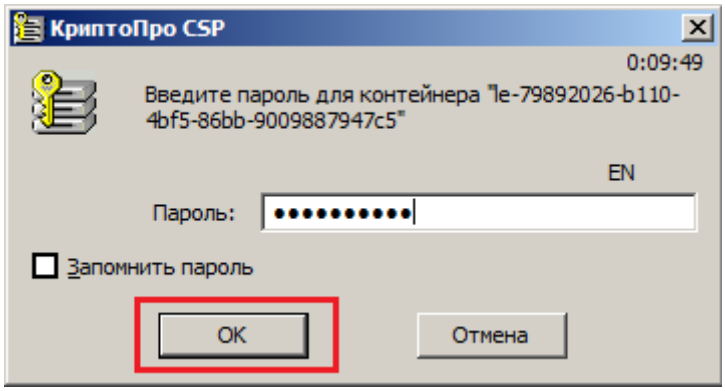


Рисунок 5. Ввод ПИН-кода

2.3. Вход в веб-интерфейс СЭП (аутентификация по паролю)

В случае если Оператором СЭП выбран метод первичной аутентификации «*Аутентификация по паролю*» Пользователю необходимо ввести имя учётной записи (логин) в поле ввода и нажать кнопку «*Далее*» (см. **Рисунок 2. Вход в СЭП. Окно ввода учётной записи**).

Если имя учётной записи введено верно, появится форма для ввода пароля, выданного Пользователю Оператором СЭП при регистрации (см. **Рисунок 6. Вход в СЭП (аутентификация по паролю)**). Если Оператором СЭП задано подтверждение Пользователем операции входа в веб-интерфейс СЭП при помощи метода вторичной

аутентификации, Пользователь должен подтвердить операцию входа соответствующим методом вторичной аутентификации (см. ***Методы вторичной аутентификации***).

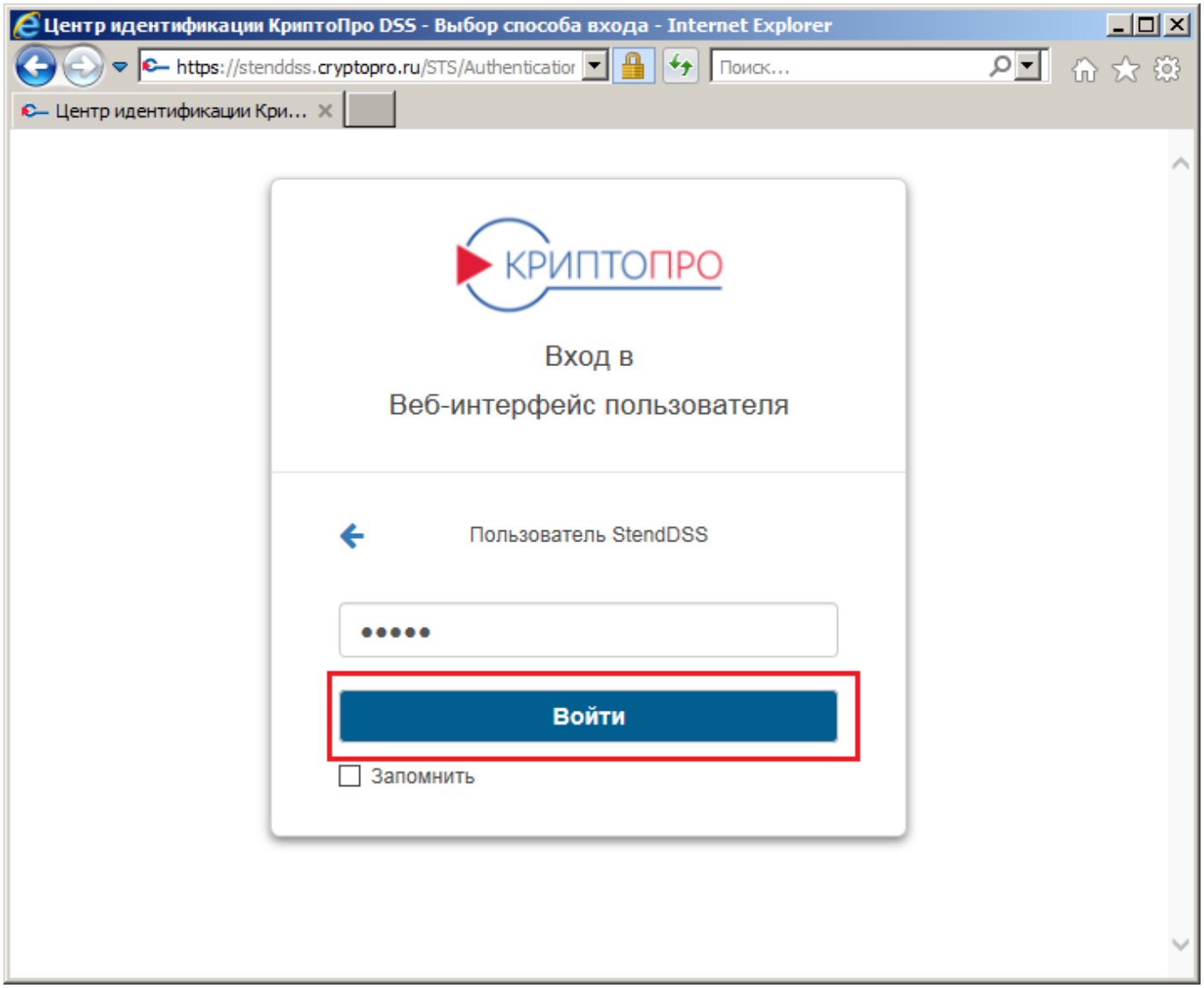


Рисунок 6. Вход в СЭП (аутентификация по паролю)

Если все процедуры аутентификации Пользователя пройдены успешно, будет отображен интерфейс Пользователя СЭП (см. **Рисунок 3. Интерфейс Пользователя СЭП**).

2.4. Методы вторичной аутентификации

Заданные Оператором методы вторичной аутентификации применяются при подтверждении операций Пользователя в СЭП. В случае если какая-либо операция требует подтверждения методом вторичной аутентификации, СЭП сообщит Пользователю об этом с указанием операции, требующей подтверждения (см. например **Рисунок 7. Запрос вторичной аутентификации пользователя в СЭП**).

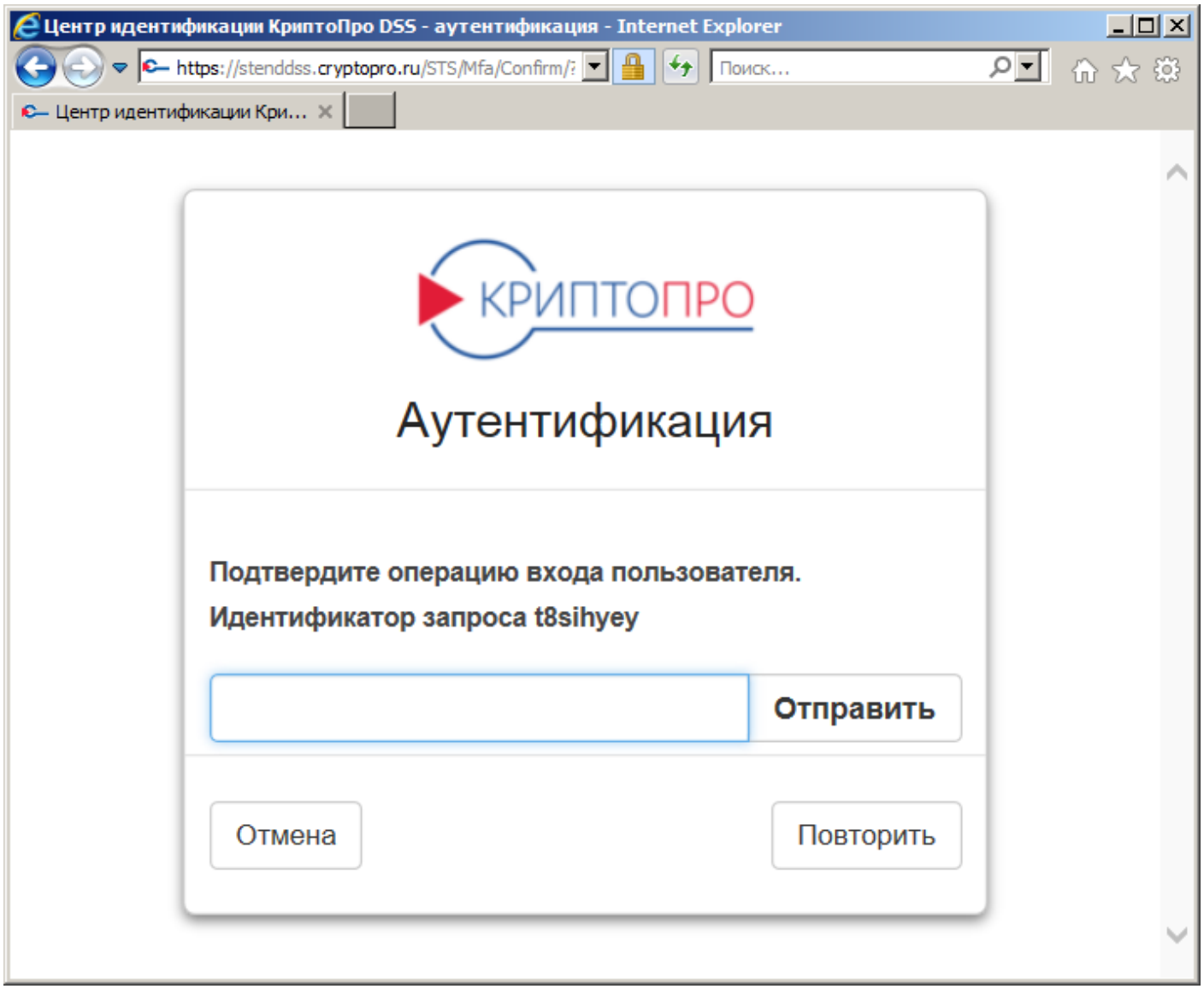


Рисунок 7. Запрос вторичной аутентификации пользователя в СЭП

2.4.1. Вторичная аутентификация по SMS/ OATH/электронной почте

В случае запроса вторичной аутентификации по SMS/протоколу OATH/электронной почте Пользователь должен ввести в поле ввода запроса подтверждения операции *код подтверждения*, полученный в сообщении SMS/одноразовый пароль, сгенерированный токеном OTP/код подтверждения, полученный в сообщении электронной почты.

2.4.2. Вторичная аутентификация с помощью мобильного приложения

Для обеспечения работоспособности вторичной аутентификации с помощью мобильного приложения Пользователю нужно установить мобильное приложение «*КриптоПро myDSS*» из магазина Google Play или Apple App Store.

После установки мобильного приложения «*КриптоПро myDSS*» (далее – *myDSS*) нужно создать локальную ключевую информацию на устройстве Пользователя. Для создания локальной ключевой информации на устройстве Пользователя нужно запустить приложение *myDSS* и отсканировать QR-код, переданный Пользователю Оператором СЭП при регистрации.

Как только QR-код будет успешно отсканирован, Пользователь должен ввести полученный им ранее при регистрации секретный ключ. Далее предложение *myDSS* предложит создать ключ на устройстве пользователя, для чего нужно будет задать имя и пароль доступа к ключу. После выполнения всех описанных выше действий Пользователь сможет подтверждать операции методом вторичной аутентификации с помощью мобильного приложения *myDSS* (см. **Рисунок 8. Создание ключей в мобильном приложении myDSS**).

При необходимости подтверждения операции с помощью мобильного приложения *myDSS* СЭП выдаст соответствующий запрос (см. **Рисунок 9. Запрос аутентификации с помощью мобильного приложения myDSS**).

После получения PUSH-уведомления о подтверждении операции в мобильном приложении *myDSS* нужно ввести пароль к ключу, если он задан, и нажать кнопку «*Подтвердить*», после чего операция будет успешно подтверждена (см. **Рисунок 10. Подтверждение операции с помощью мобильного приложения myDSS**).

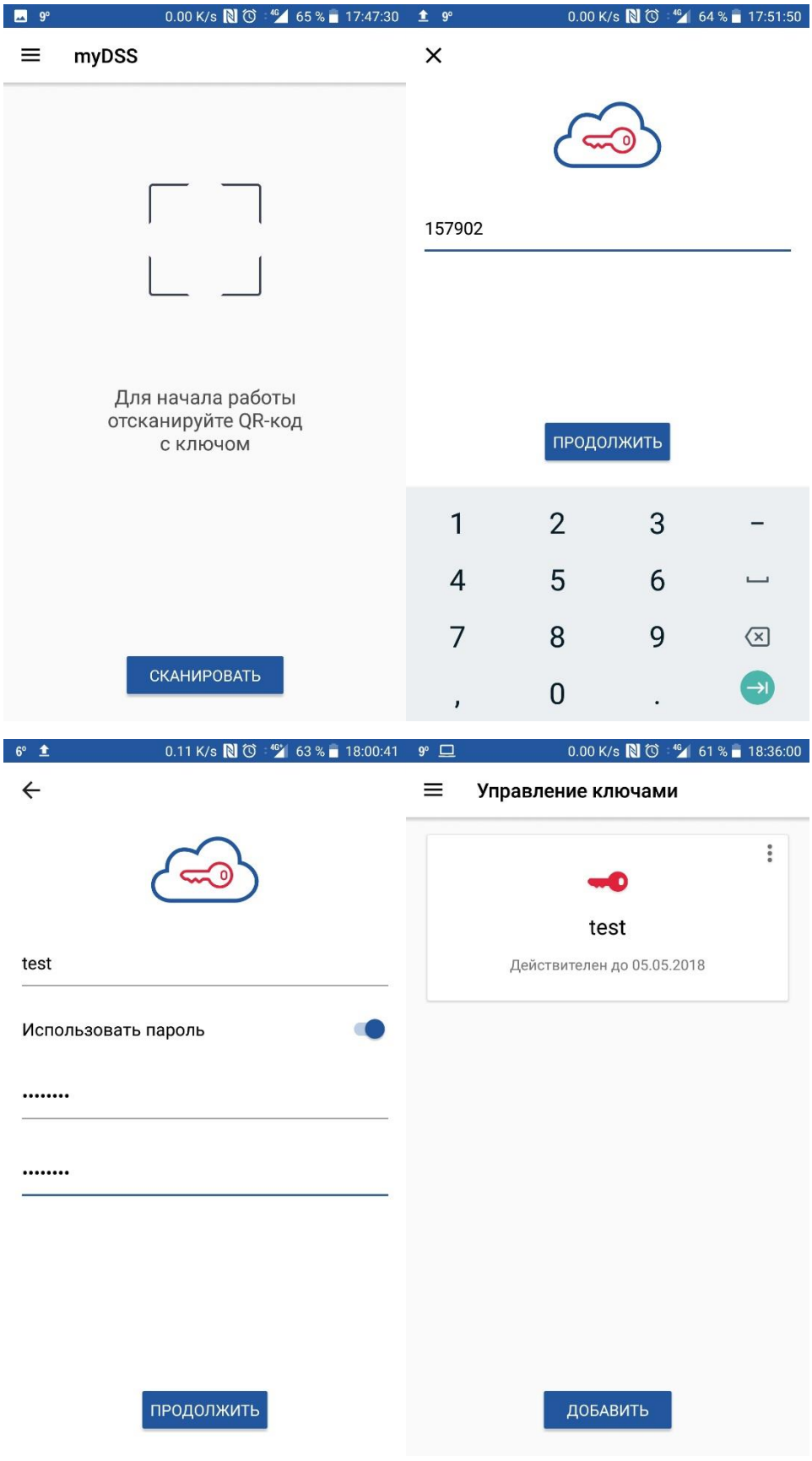


Рисунок 8. Создание ключей в мобильном приложении myDSS

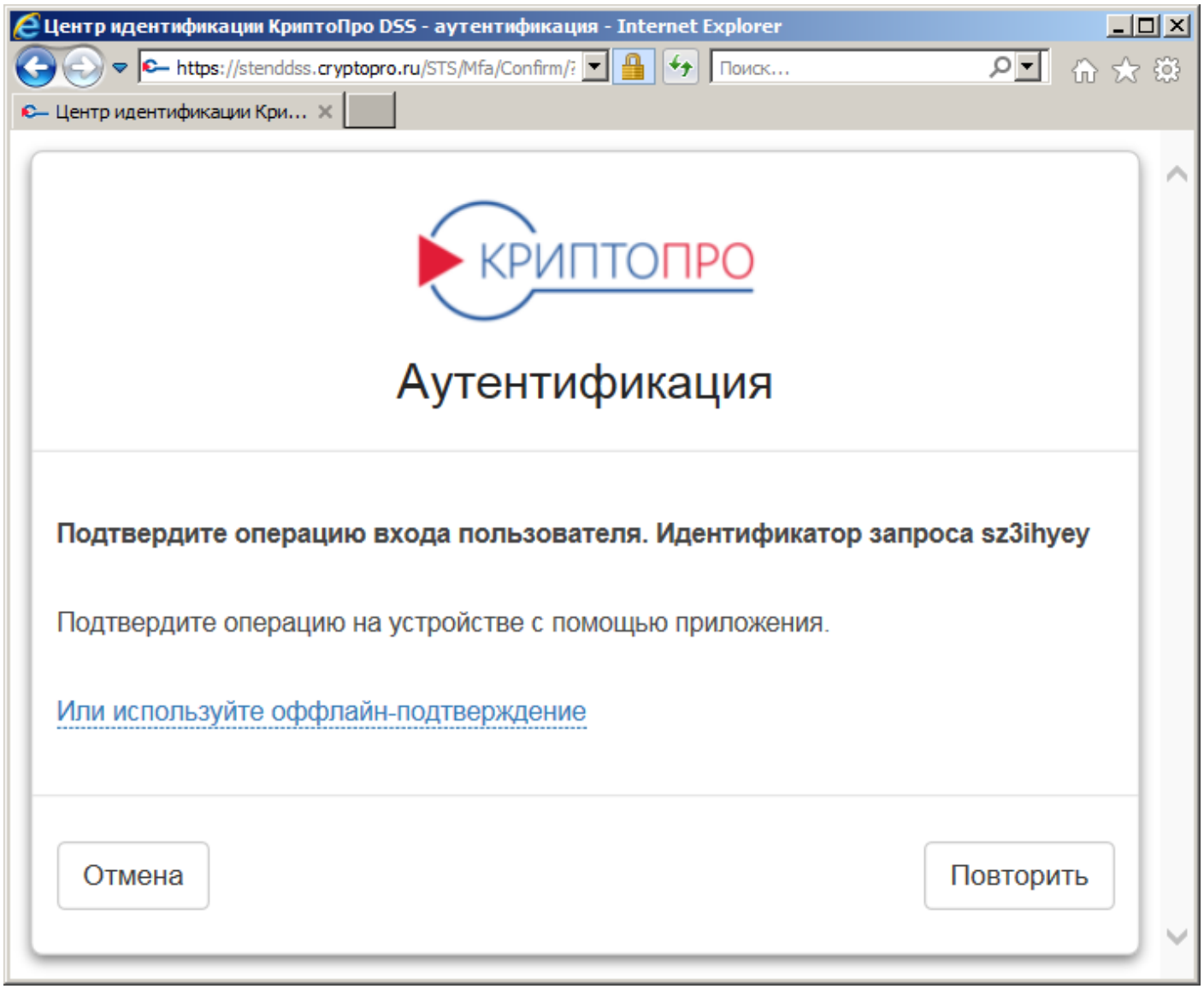


Рисунок 9. Запрос аутентификации с помощью мобильного приложения myDSS

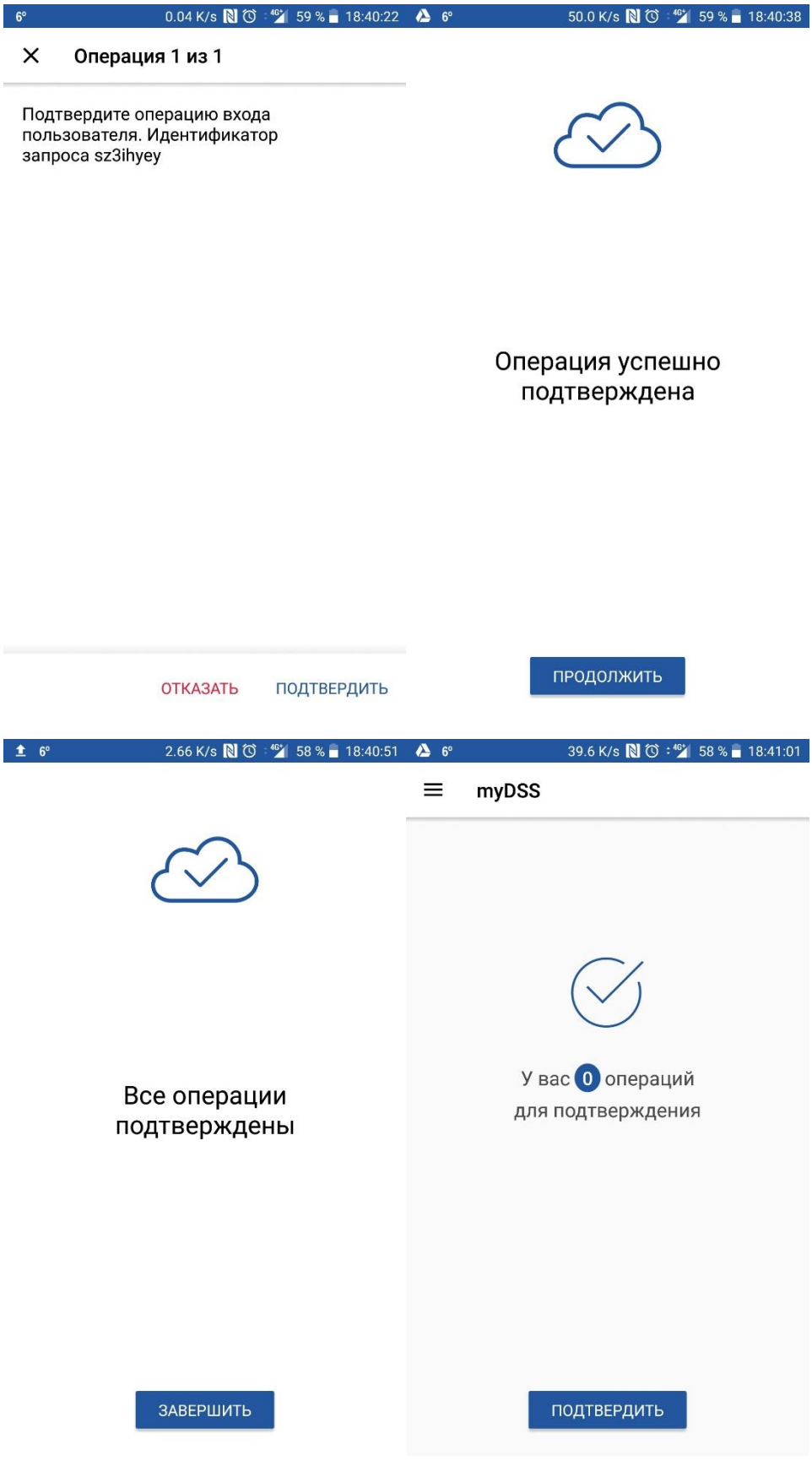


Рисунок 10. Подтверждение операции с помощью мобильного приложения myDSS

3. Меню интерфейса Пользователя СЭП

В меню начальной страницы Оператора доступны 8 разделов:

- «*Подписать*»
- «*Усовершенствовать подпись*»
- «*Зашифровать*»
- «*Расшифровать*»
- «*Проверить подпись*»
- «*Проверить сертификат*»
- «*Сертификаты*»
- «*Аудит*»

3.1. Раздел «Подписать»

Раздел предназначен для формирования электронной подписи электронных документов Пользователя. Для того, чтобы Пользователь мог подписывать электронные документы, ему необходимо иметь хотя бы один действующий сертификат в СЭП (см. ***Раздел «Сертификаты»***).

Для формирования электронной подписи электронного документа нужно перейти в раздел «*Подписать*» и выполнить следующие действия:

1) Загрузить электронный документ, который нужно подписать, в СЭП, нажав кнопку «*Обзор*» в секции «*Документ*».
2) Выбрать нужный формат электронной подписи в секции «*Формат подписи*».
3) Выбрать параметры электронной подписи в секции «*Параметры подписи*».
4) Выбрать нужный сертификат Пользователя в секции «*Сертификат*».
5) Нажать кнопку «*Подписать*» и ввести ПИН-код к ключу в СЭП (см. **Рисунок 11. Формирование подписи документа**).
6) Загрузить полученную электронную подпись (см. **Рисунок 12. Загрузка файла подписи документа**).

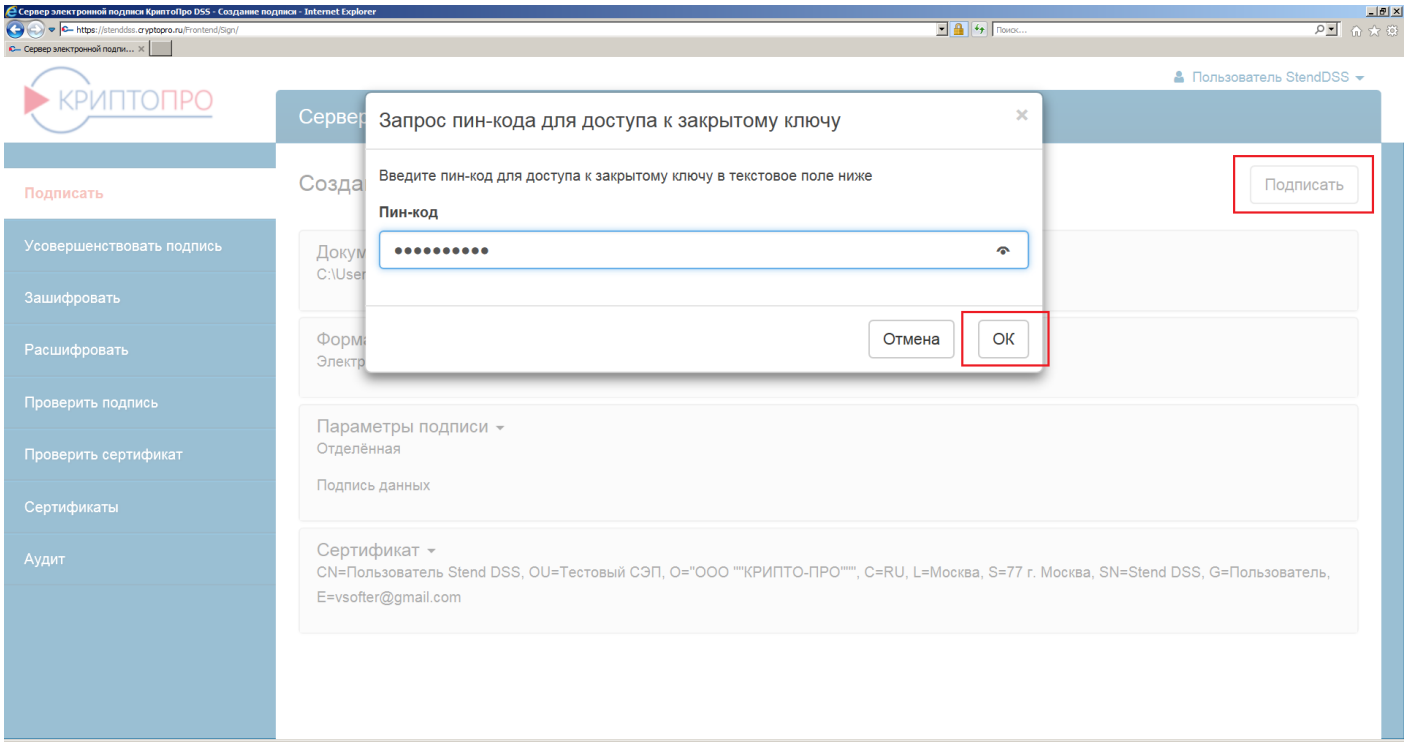


Рисунок 11. Формирование подписи документа

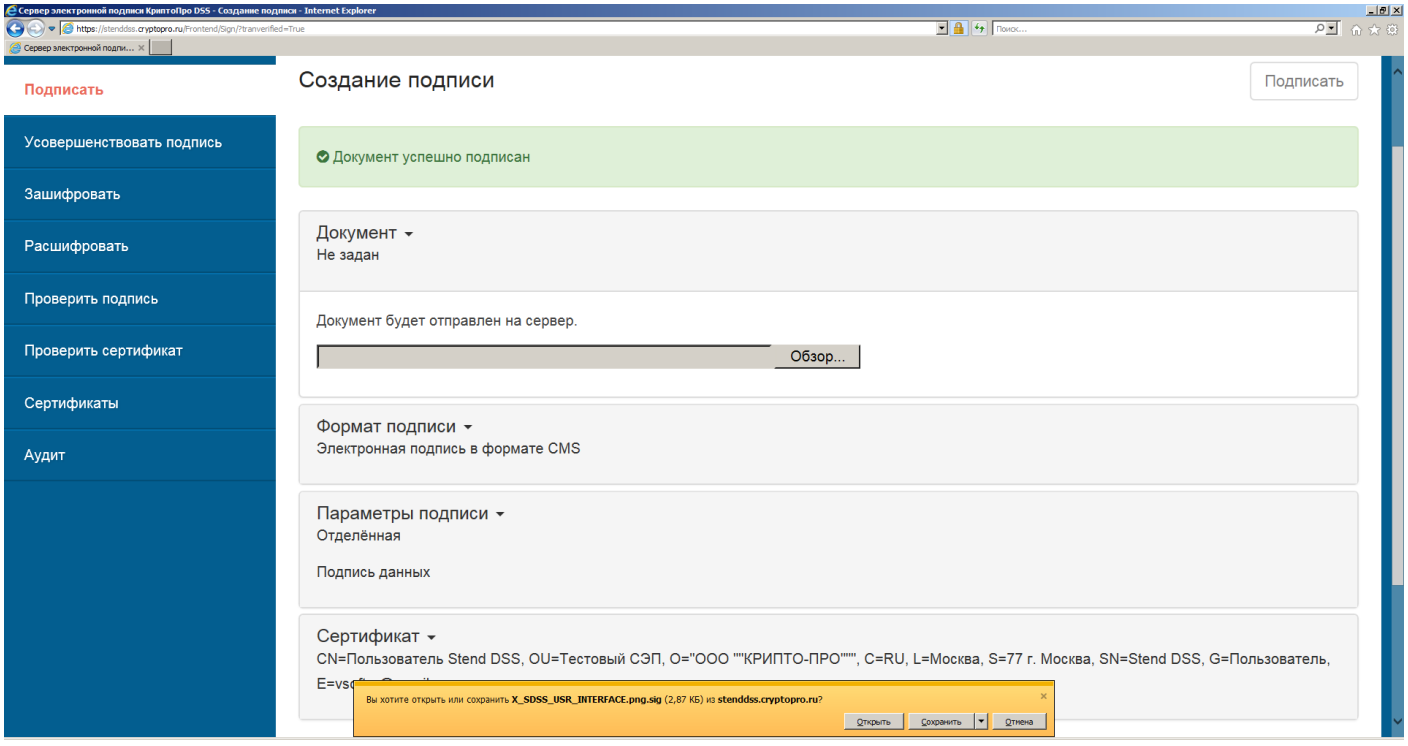


Рисунок 12. Загрузка файла подписи документа

3.2. Раздел «Усовершенствовать подпись»

Раздел предназначен для усовершенствования (дополнения) электронной подписи документа до формата усовершенствованной электронной подписи: CAdES-T (добавление штампа времени к электронной подписи), CAdES-XLT1 (добавление статуса сертификата на момент подписания и штампа времени).

Для усовершенствования электронной подписи электронного документа необходимо перейти в раздел «*Усовершенствовать*» и выполнить следующие действия:

1) Загрузить файл подписи, которую нужно усовершенствовать, в СЭП, нажав кнопку «*Обзор*» в секции «*Документ*».
2) Выбрать параметры электронной подписи в секции «*Параметры подписи*», экземпляр службы штампов времени (TSP).
3) Установить флажок «*Удалить имеющиеся доказательства подлинности*» в случае если нужно удалить из подписи существующие штампы времени/статусы сертификатов.
4) Нажать кнопку «*Усовершенствовать*» (см. **Рисунок 13. Формирование усовершенствованной подписи документа**).
5) Загрузить полученную усовершенствованную электронную подпись (см. **Рисунок 14. Загрузка файла усовершенствованной подписи документа**).

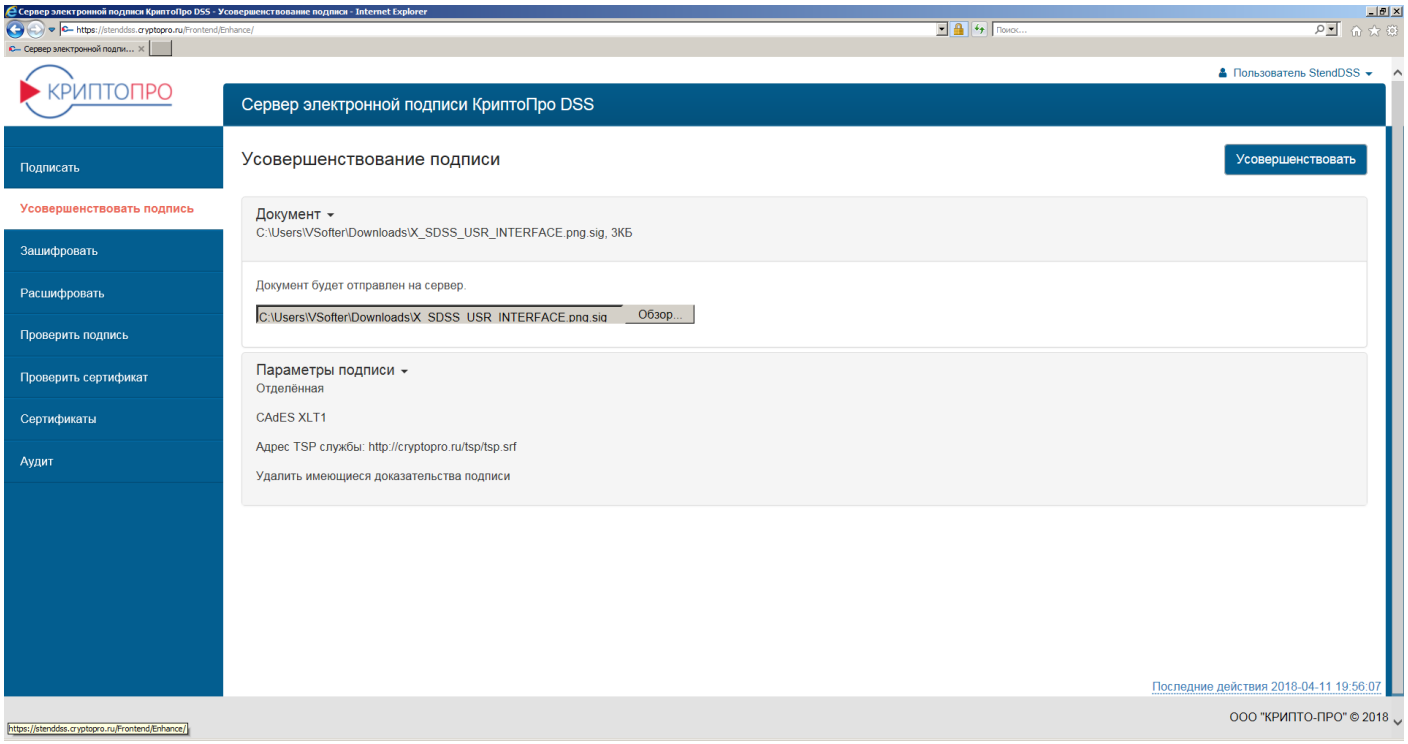


Рисунок 13. Формирование усовершенствованной подписи документа

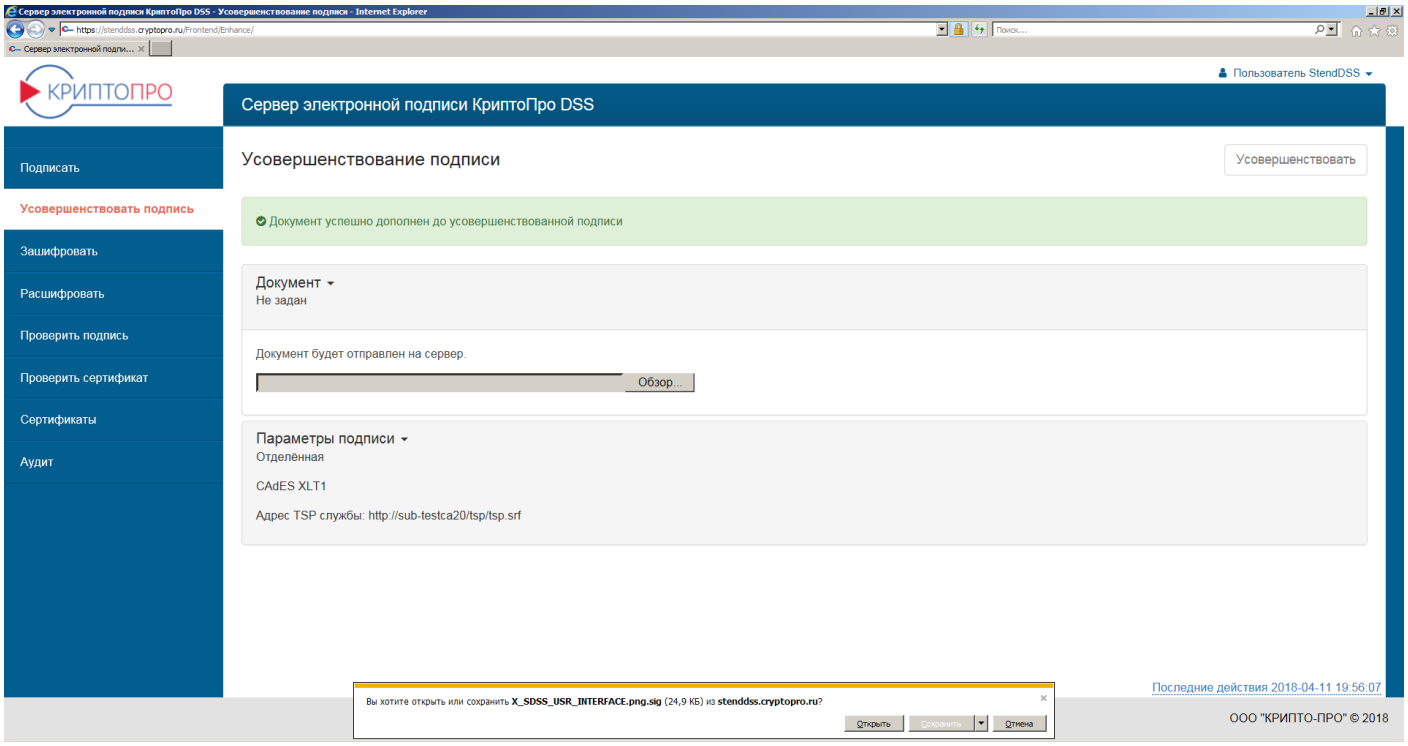


Рисунок 14. Загрузка файла усовершенствованной подписи документа

3.3. Раздел «Зашифровать»

Раздел предназначен для адресного шифрования электронных документов. Для адресного шифрования электронного документа нужен файл электронного документа и сертификат/сертификаты адресата/адресатов.

Для адресного шифрования электронного документа необходимо перейти в раздел «*Зашифровать*» и выполнить следующие действия:

1) Загрузить файл электронного документа, который нужно зашифровать, в СЭП, нажав кнопку «*Обзор*» в секции «*Документ*».
2) Загрузить сертификат/сертификаты адресата/адресатов, для которого/которых будет шифроваться электронный документ, в СЭП, нажав кнопку «*Обзор*» в секции «*Сертификаты получателей*».
3) Нажать кнопку «*Зашифровать*» (см. **Рисунок 15. Адресное шифрование электронного документа**).
4) Загрузить полученный зашифрованный электронный документ (см. **Рисунок 16. Загрузка зашифрованного электронного документа**).

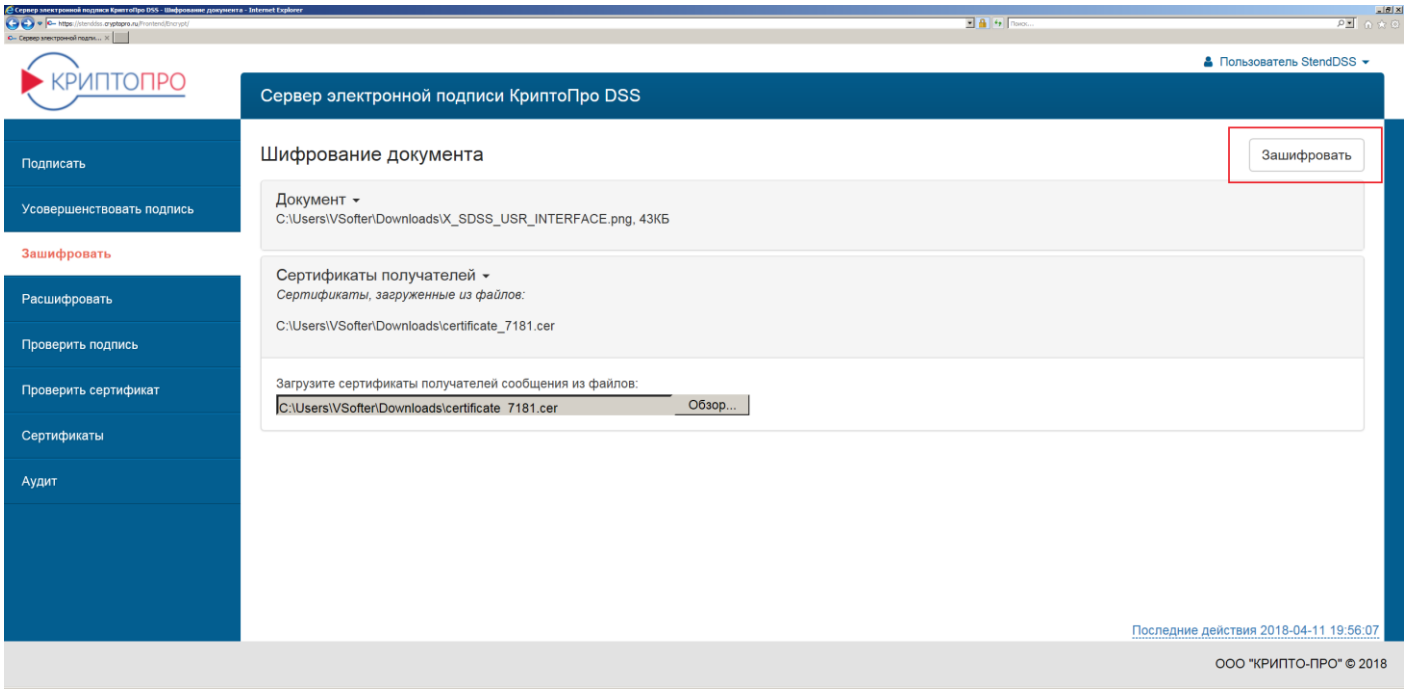


Рисунок 15. Адресное шифрование электронного документа

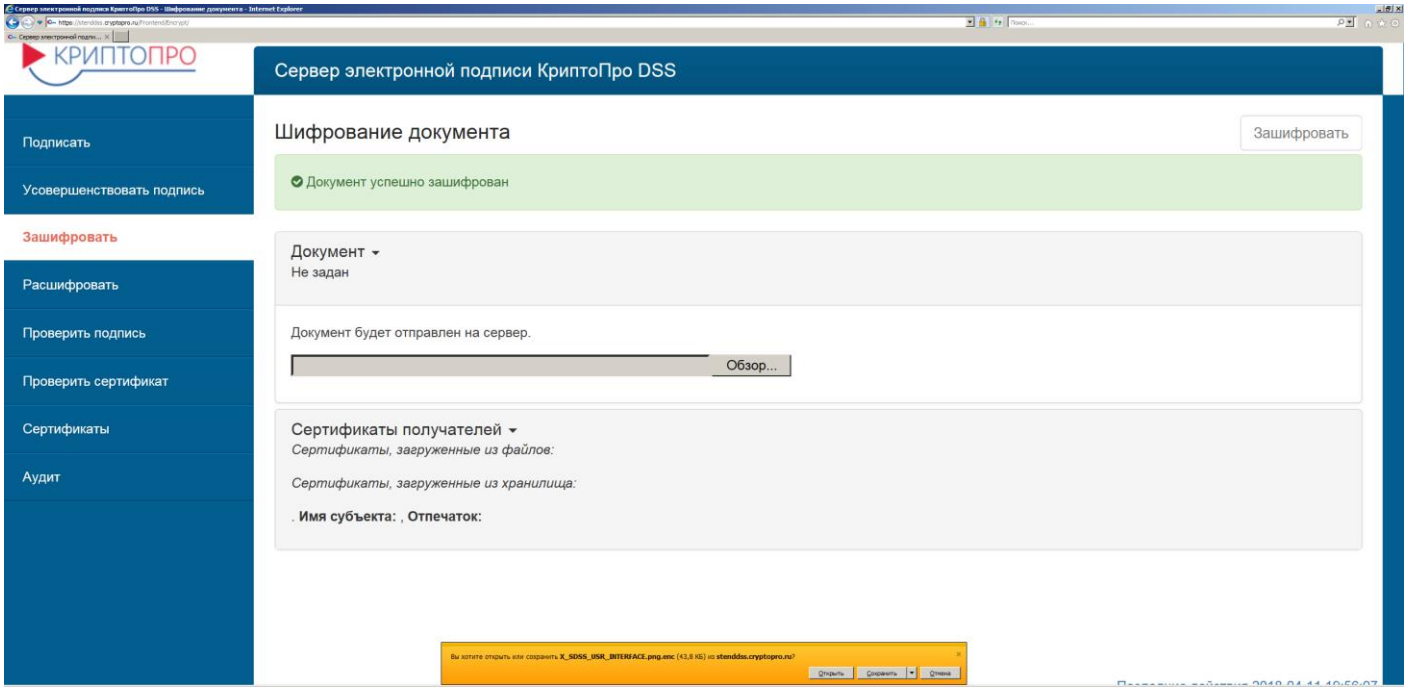


Рисунок 16. Загрузка зашифрованного электронного документа

3.4. Раздел «Расшифровать»

Раздел предназначен для расшифрования электронных документов, зашифрованных для Пользователя. Для расшифрования электронного документа нужен зашифрованный файл электронного документа. Для того, чтобы Пользователь мог подписывать электронные документы, ему необходимо иметь хотя бы один действующий сертификат в СЭП (см. ***Раздел «Сертификаты»***).

Для расшифрования электронного документа необходимо перейти в раздел «*Расшифровать*» и выполнить следующие действия:

1) Загрузить зашифрованный для Пользователя файл электронного документа, который нужно расшифровать, в СЭП, нажав кнопку «*Обзор*» в секции «*Документ*».
2) В поле сертификат автоматически будет отображён сертификат Пользователя, для которого зашифрован электронный документ.
3) Нажать кнопку «*Расшифровать*».
4) Ввести ПИН-код доступа к ключу Пользователя в СЭП.
5) Загрузить расшифрованный электронный документ.

3.5. Раздел «Проверить подпись»

Раздел предназначен для проверки подписи электронных документов. Для проверки подписи электронного документа нужен файл подписи электронного документа и файл электронного документа (для отсоединённой подписи).

Для проверки подписи электронного документа необходимо перейти в раздел «*Проверить подпись*» и выполнить следующие действия:

1) Загрузить файл подписи электронного документа в СЭП, нажав кнопку «*Обзор*» в секции «*Документ для проверки*».
2) Формат подписи будет определён автоматически.
3) В секции «*Параметры*» указать параметры подписи (присоединённая/отсоединённая, подпись данных/подпись хэш-функции).
4) Для отсоединённой подписи загрузить файл электронного документа в СЭП, нажав кнопку «*Обзор*» в секции «*Исходный документ*».
5) Нажать кнопку «*Проверить*» (см. **Рисунок 17. Проверка подписи электронного документа**).
6) Получить результат проверки подписи (см. **Рисунок 18. Результат проверки подписи электронного документа**).

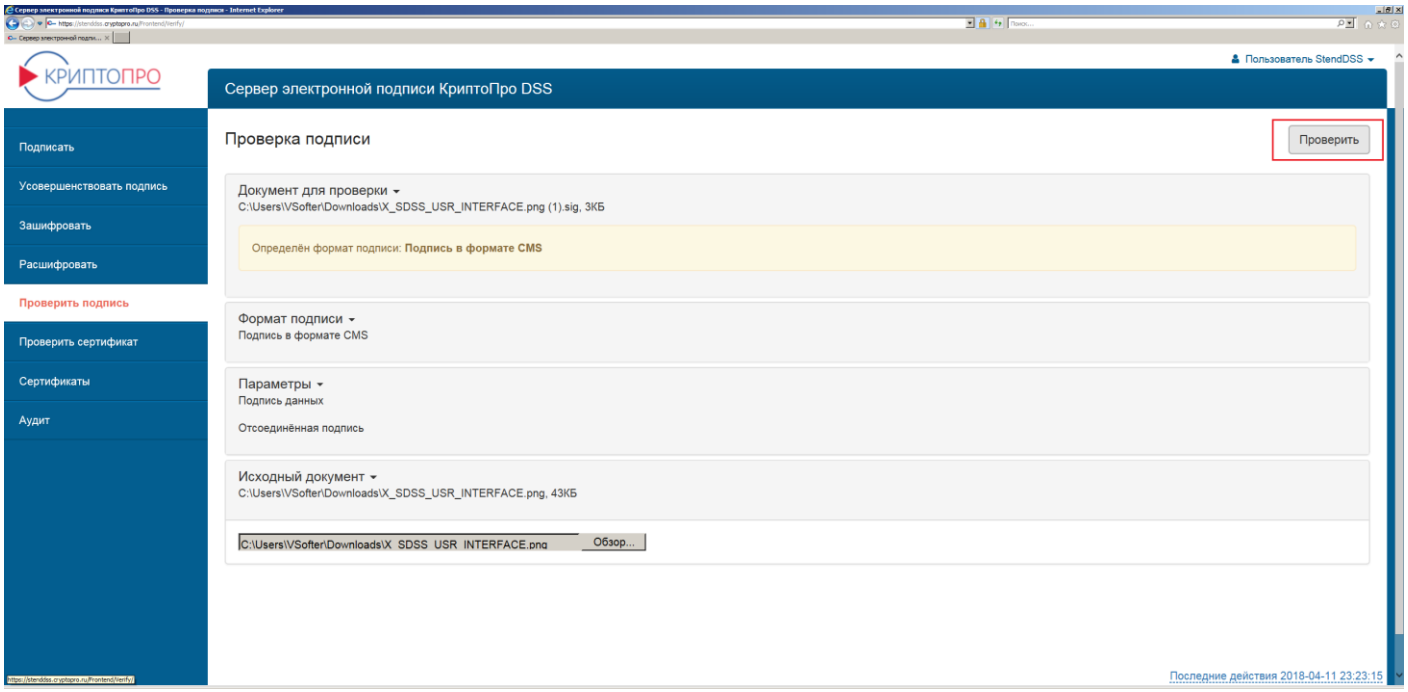


Рисунок 17. Проверка подписи электронного документа

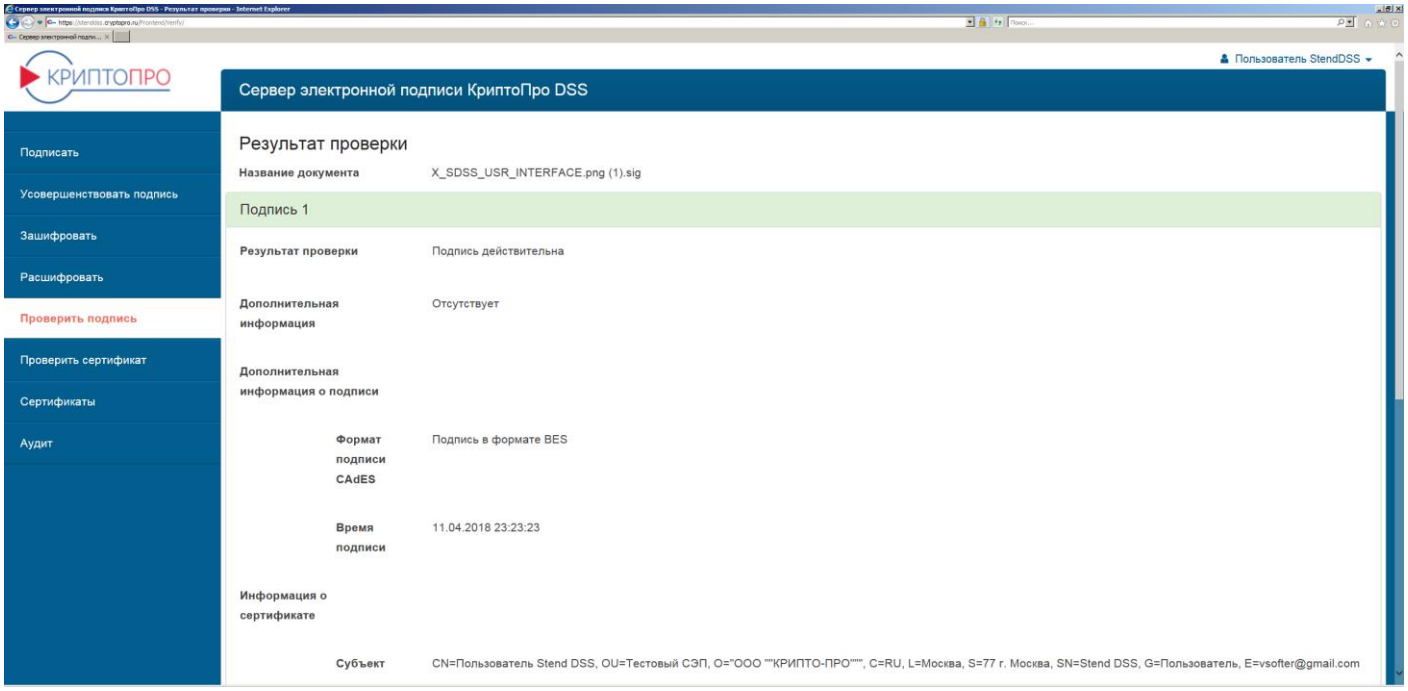


Рисунок 18. Результат проверки подписи электронного документа

3.6. Раздел «Проверить сертификат»

Раздел предназначен для проверки статуса сертификатов. Для проверки статуса сертификата нужен файл сертификата.

Для проверки статуса сертификата необходимо перейти в раздел «*Проверить сертификат*» и выполнить следующие действия:

1) Загрузить файл сертификата в СЭП, нажав кнопку «*Обзор*» в секции «*Файл сертификата*».
2) Нажать кнопку «*Проверить*» (см. **Рисунок 19. Проверка статуса сертификата**).
3) Получить результат проверки статуса сертификата (см. **Рисунок 20. Результат проверки статуса сертификата**).

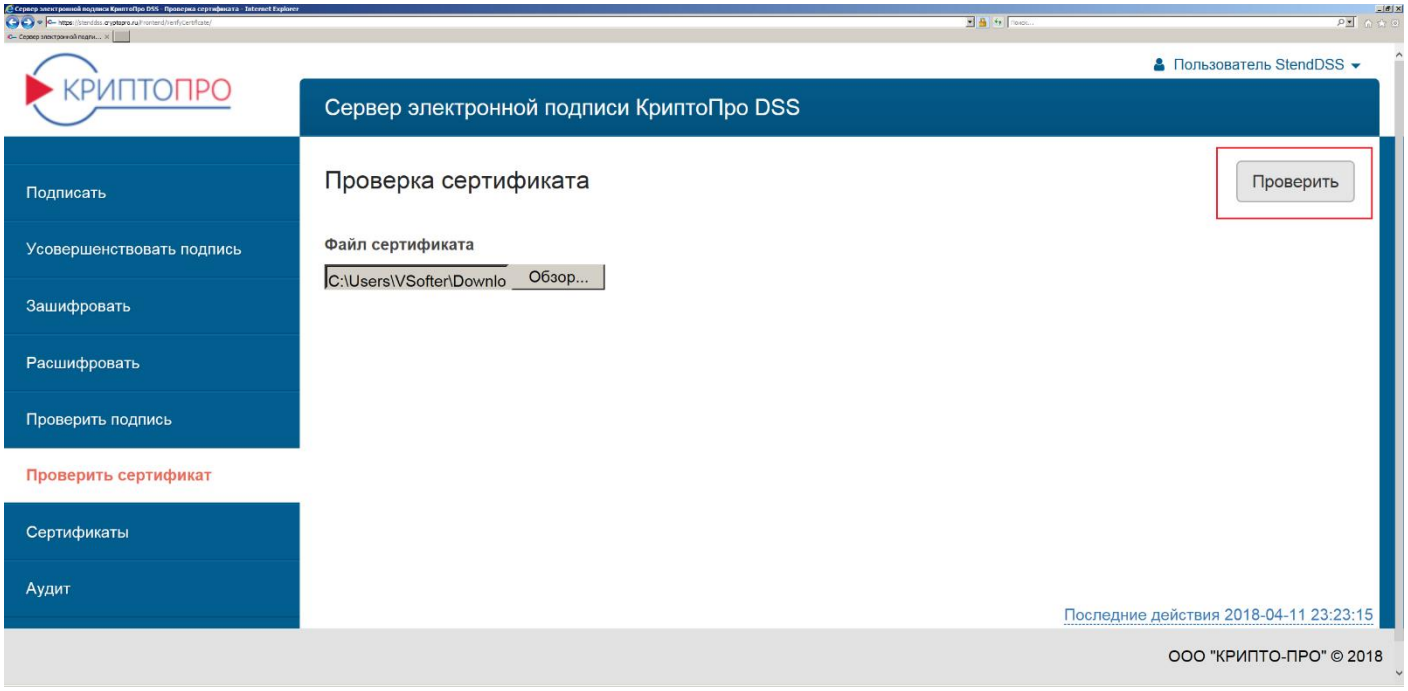


Рисунок 19. Проверка статуса сертификата

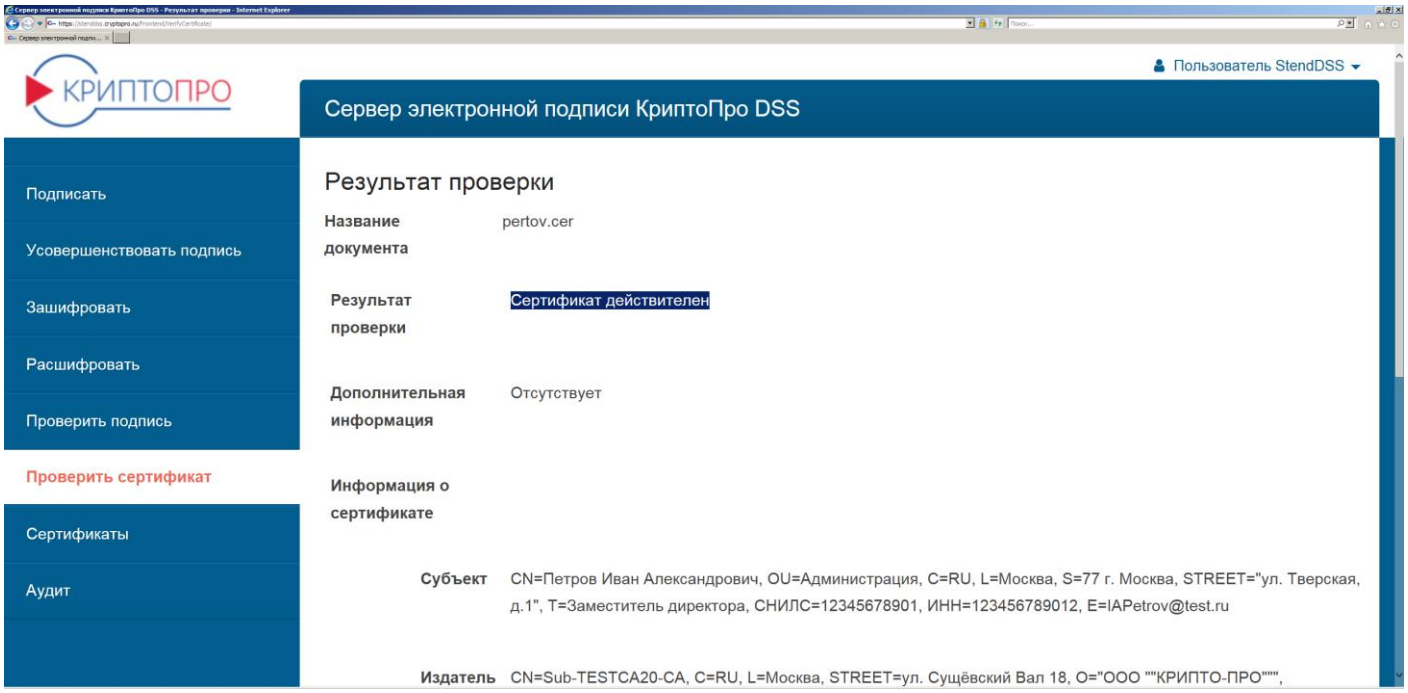


Рисунок 20. Результат проверки статуса сертификата

3.7. Раздел «Сертификаты»

Раздел предназначен для создания запросов на сертификат, управления сертификатами Пользователя.

Для создания запроса на новый/первый сертификат Пользователя нужно перейти в раздел «Сертификаты» и нажать кнопку «Создать запрос на сертификат» (см. **Рисунок 21. Создание запроса на сертификат**).

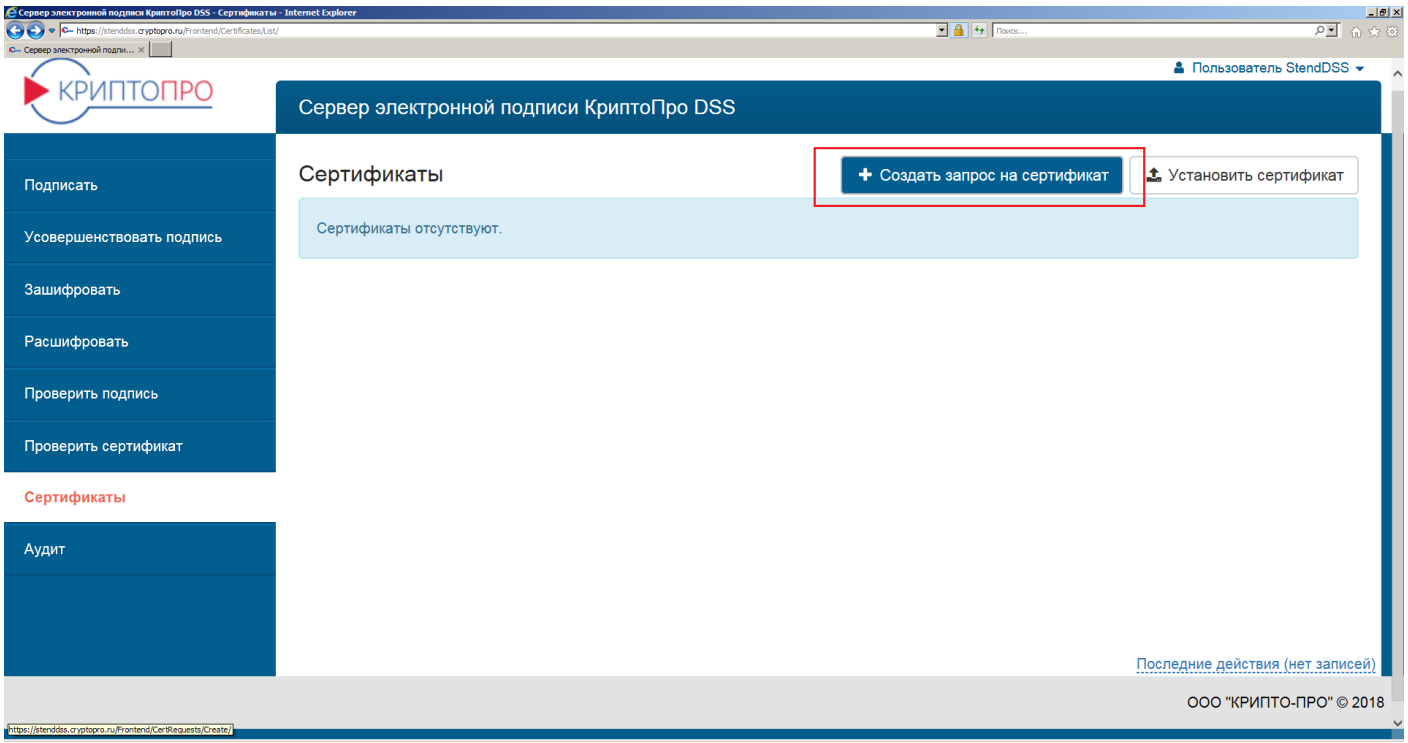


Рисунок 21. Создание запроса на сертификат

Далее необходимо выбрать Удостоверяющий центр для выпуска сертификата Пользователя (по умолчанию «*Тестовый УЦ 2.0 для DSS Подчиненный*»), отредактировать данные Пользователя, выбрать шаблон сертификата (по умолчанию «*Пользователь DSS*»), нажать кнопку «*Создать запрос*», задать ПИН-код к ключу в СЭП и нажать кнопку «*ОК*» (см. **Рисунок 22. Задание ПИН-кода для доступа к закрытому ключу**).

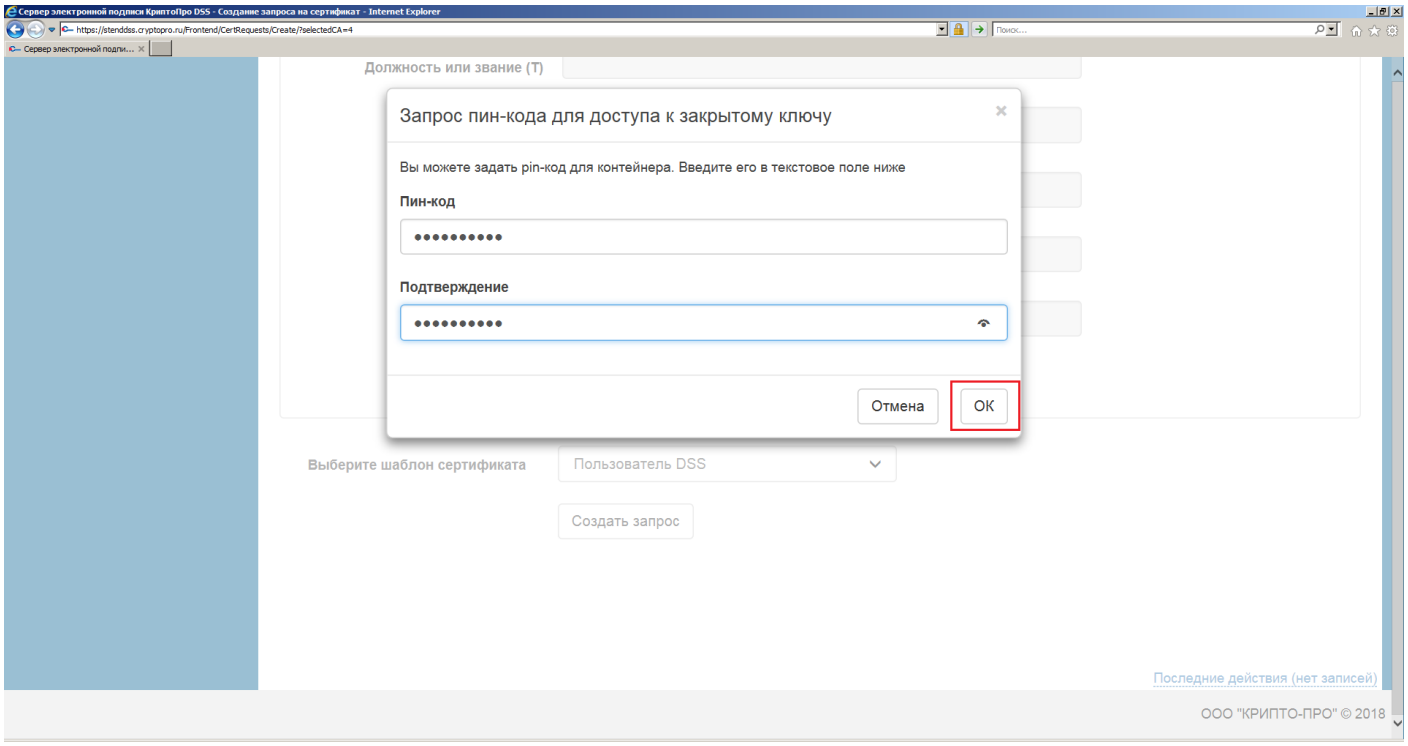


Рисунок 22. Задание ПИН-кода для доступа к закрытому ключу

После того, как Оператор СЭП одобрит созданный запрос на сертификат, выпущенный сертификат появится в списке сертификатов Пользователя, и его можно будет использовать для операций в СЭП (см. **Рисунок 23. Сертификат Пользователя**).

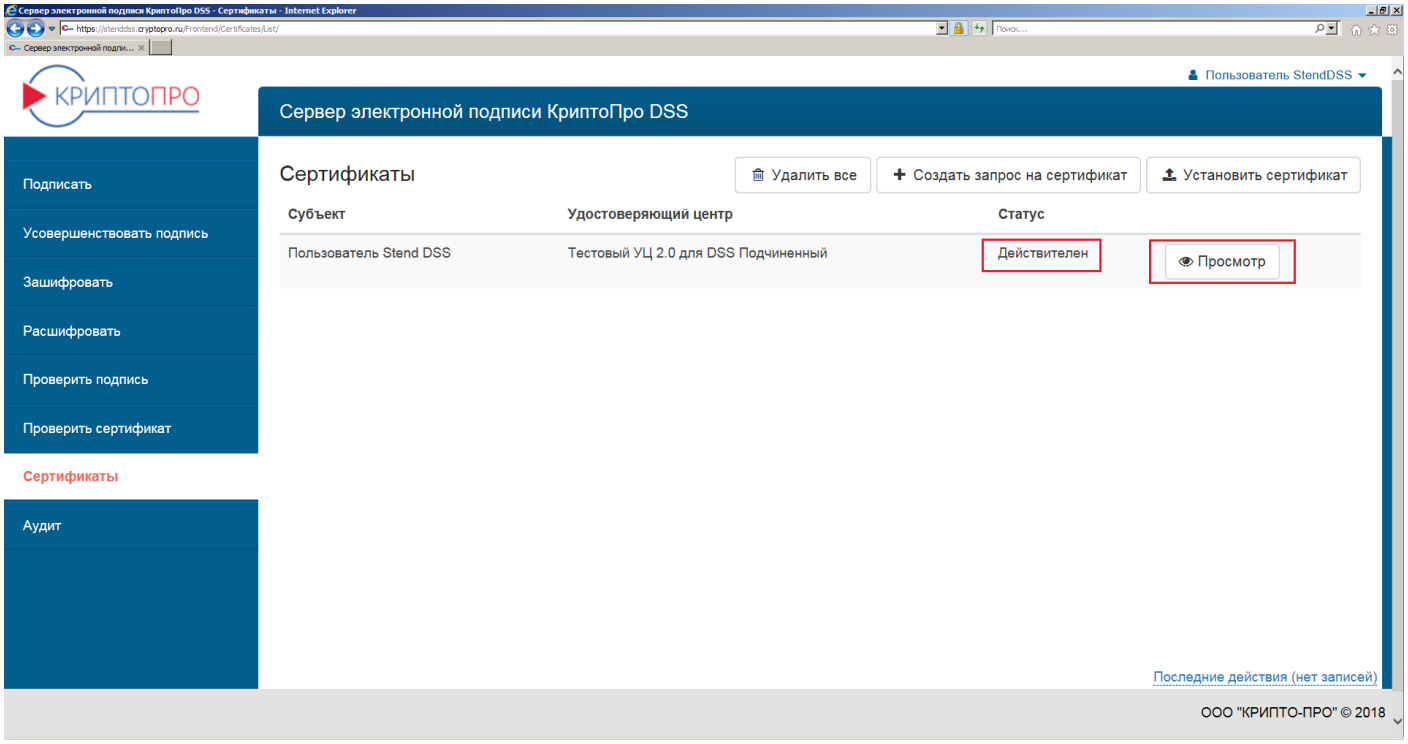


Рисунок 23. Сертификат Пользователя

При нажатии кнопки «Просмотр» будет отображён интерфейс управления сертификатом Пользователя. Пользователю доступны следующие операции с сертификатом (см. **Рисунок 24. Управление сертификатом Пользователя**):

- «*Скачать*» – скачать файл сертификата (*.cer).
- «*Печать*» – вывести бумажную копию сертификата на печать.
- «*Изменить дружественное имя*» – изменить дружественное имя сертификата (в случае если у Пользователя несколько сертификатов в СЭП).
- «*Удалить*» – удалить сертификат из СЭП.
- «*Отозвать*» – отозвать сертификат (нужно будет указать ПИН-код к ключевому контейнеру в СЭП, причину отзыва, дату отзыва).
- «*Приостановить*» – приостановить действие сертификата (необходимо будет указать ПИН-код к ключевому контейнеру в СЭП, причину приостановления, дату приостановления, дату окончания приостановления и действие после приостановления).
- «*Возобновить*» – возобновить действие приостановленного сертификата.
- «*Обновить*» – обновить сертификат в случае (скорого) истечения срока его действия.
- «*Назначить сертификатом по умолчанию*» – выбрать данный сертификат по умолчанию из всех сертификатов Пользователя.

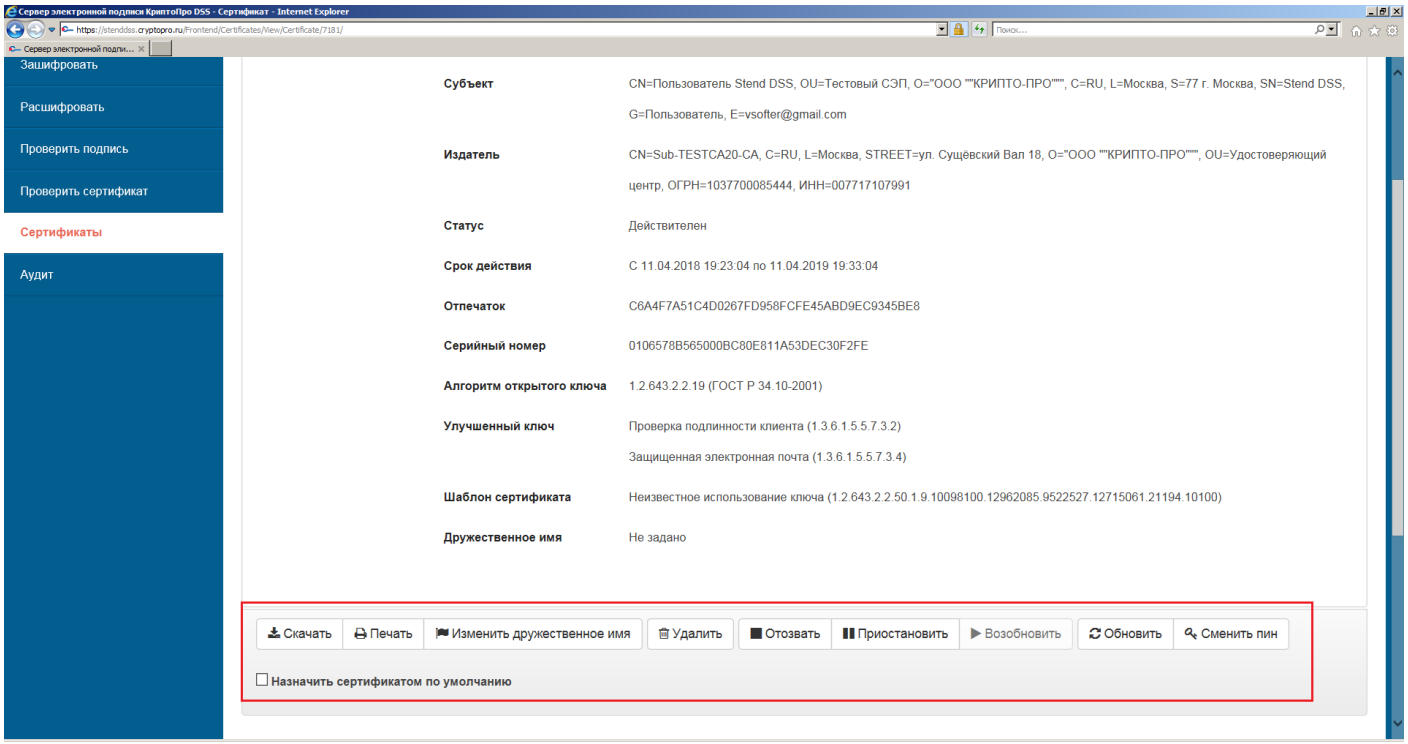


Рисунок 24. Управление сертификатом Пользователя

3.8. Раздел «Аудит»

Раздел предназначен для отображения журнала событий, связанных с действиями Пользователей и Операторов в СЭП с возможностью фильтрации по типам событий (см. **Рисунок 25. Журнал Аудита**).

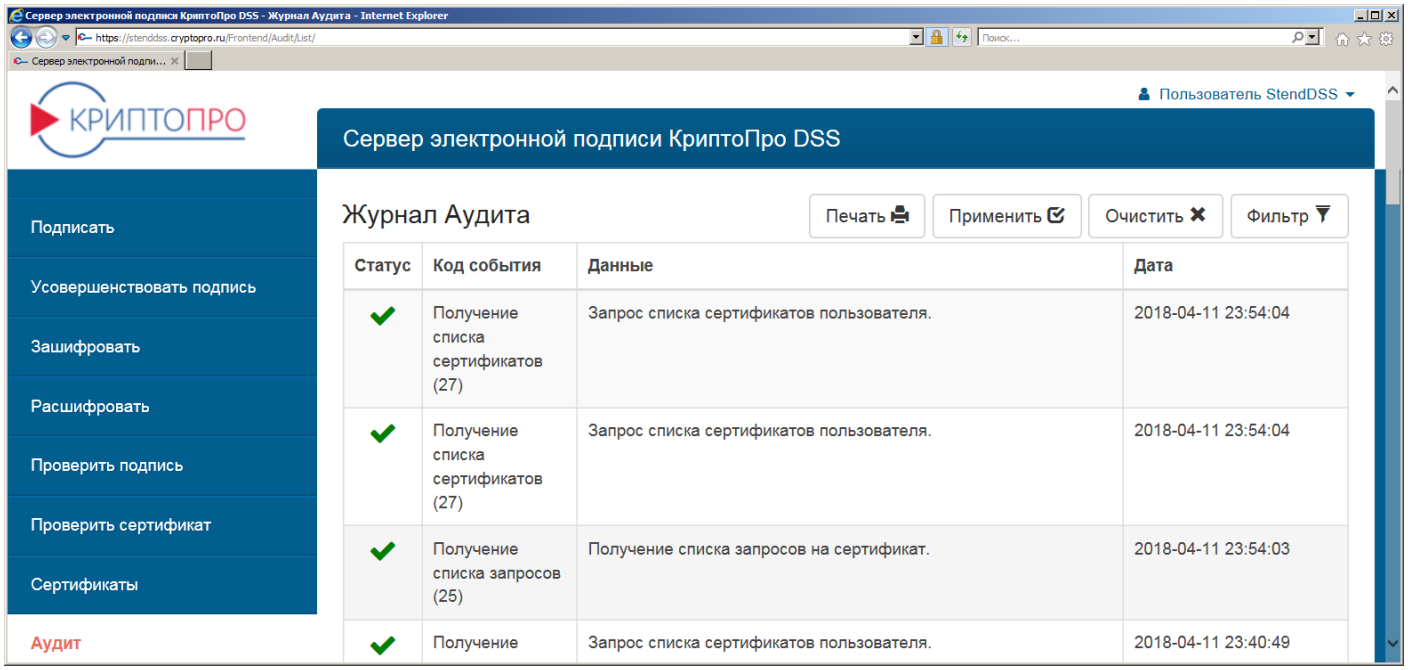


Рисунок 25. Журнал Аудита

4. Использование «облачного» токена в СКЗИ «КриптоПро CSP 5.0»

Пользователи могут использовать «облачные» ключи, хранящиеся в СЭП, в приложениях, в которые встроено СКЗИ «КриптоПро CSP» (например, программы шифрования и электронной подписи файлов, системы электронного документооборота и др.), в которых используются механизмы аутентификации/электронной подписи, порталы органов государственной власти (www.nalog.ru, www.gosuslugi.ru)).

Импорт «облачных» ключей из СЭП доступен в СКЗИ «КриптоПро CSP» версии 5.0 и выше. Для импорта «облачного» ключа необходимо выполнить следующие действия на АРМ Пользователя СЭП:

1) Открыть приложение «*Инструменты КриптоПро*» (по умолчанию «Пуск» → «Все программы» → «КРИПТО-ПРО» → «Инструменты КриптоПро»).
2) Выбрать пункт «Облачный провайдер» в меню приложения «*Инструменты КриптоПро*» и указать следующие параметры (например, для экземпляра СЭП с идентификатором «**test**»):
   - **Сервер авторизации**: «https://stenddss.cryptopro.ru/**test**idp/oauth»;
   - **Сервер DSS**: «https://stenddss.cryptopro.ru/**test**ss/rest» (см. **Рисунок 26. Настройки облачного провайдера**), после чего нажать кнопку «*Установить сертификаты*».

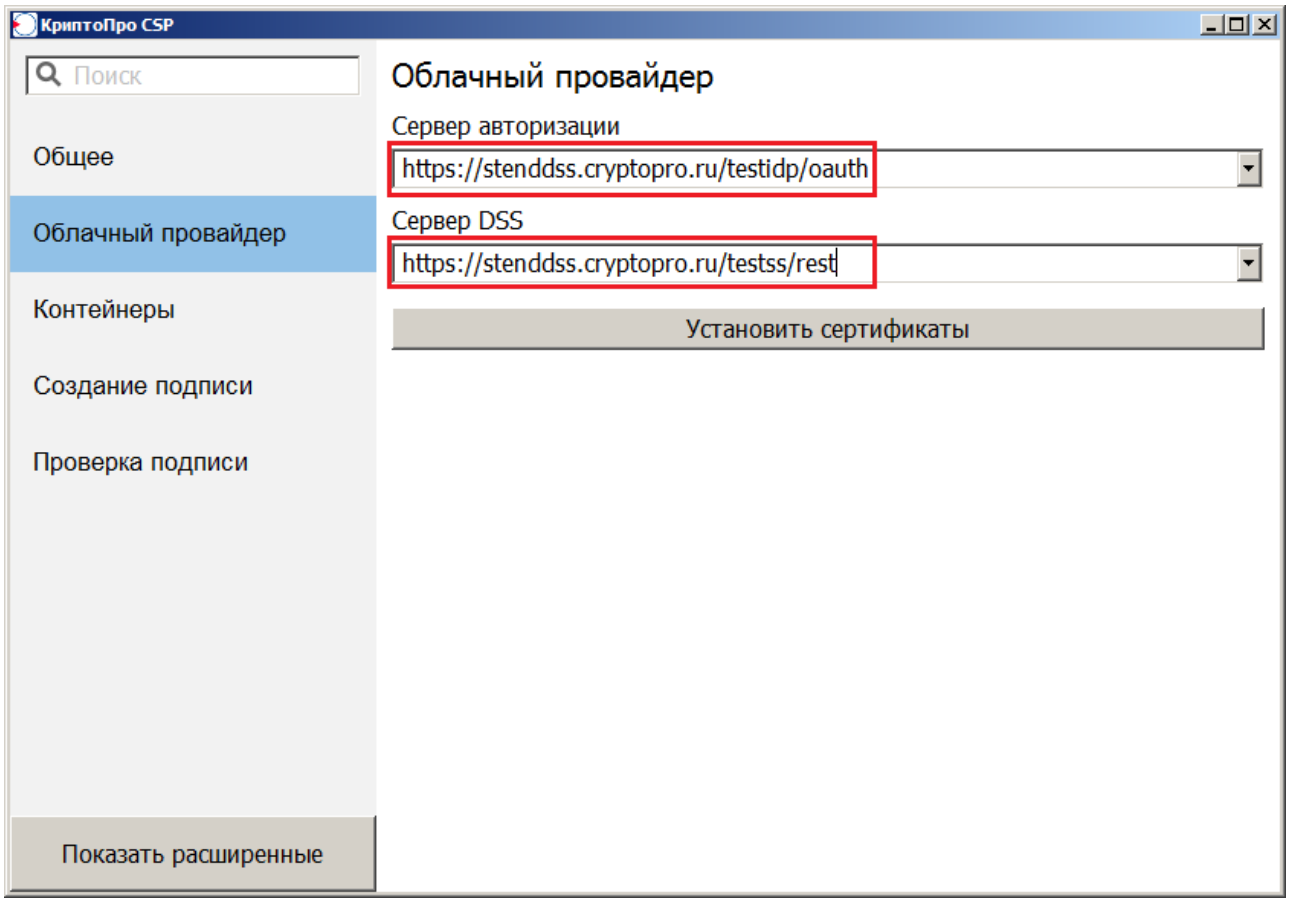


Рисунок 26. Настройки облачного провайдера

Теперь необходимо пройти авторизацию в СЭП. В окне «CryptoPro Web Authentication» для этого нужно указать имя Пользователя в экземпляре СЭП и нажать кнопку «*Далее*» (см. **Рисунок 27. Ввод учетной записи Пользователя**).

После этого в появившуюся форму ввести пароль Пользователя и нажать кнопку «*Войти*» (см. **Рисунок 28. Ввод пароля Пользователя**).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом (см. ***Вторичная аутентификация с помощью мобильного приложения***).

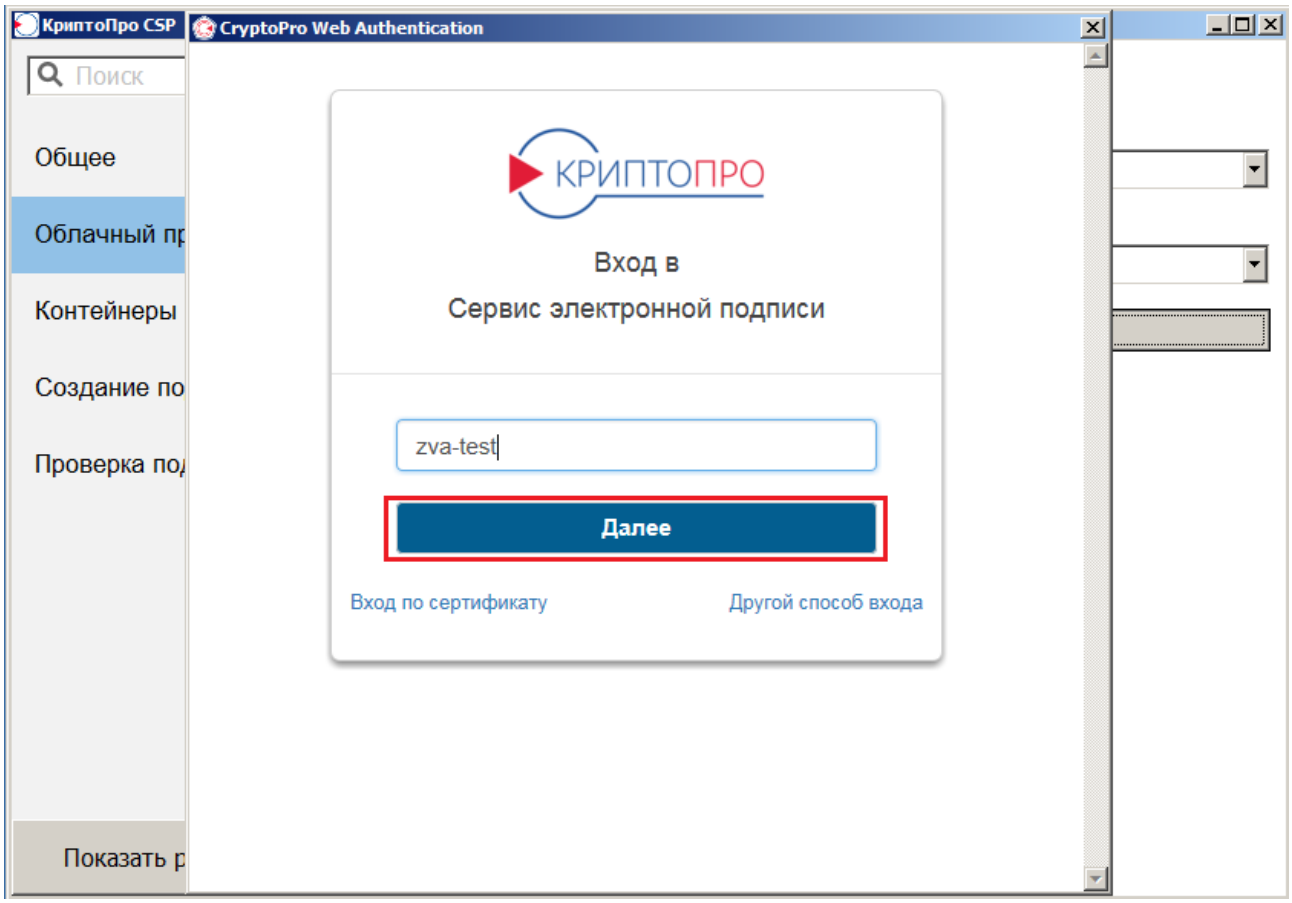


Рисунок 27. Ввод учетной записи Пользователя

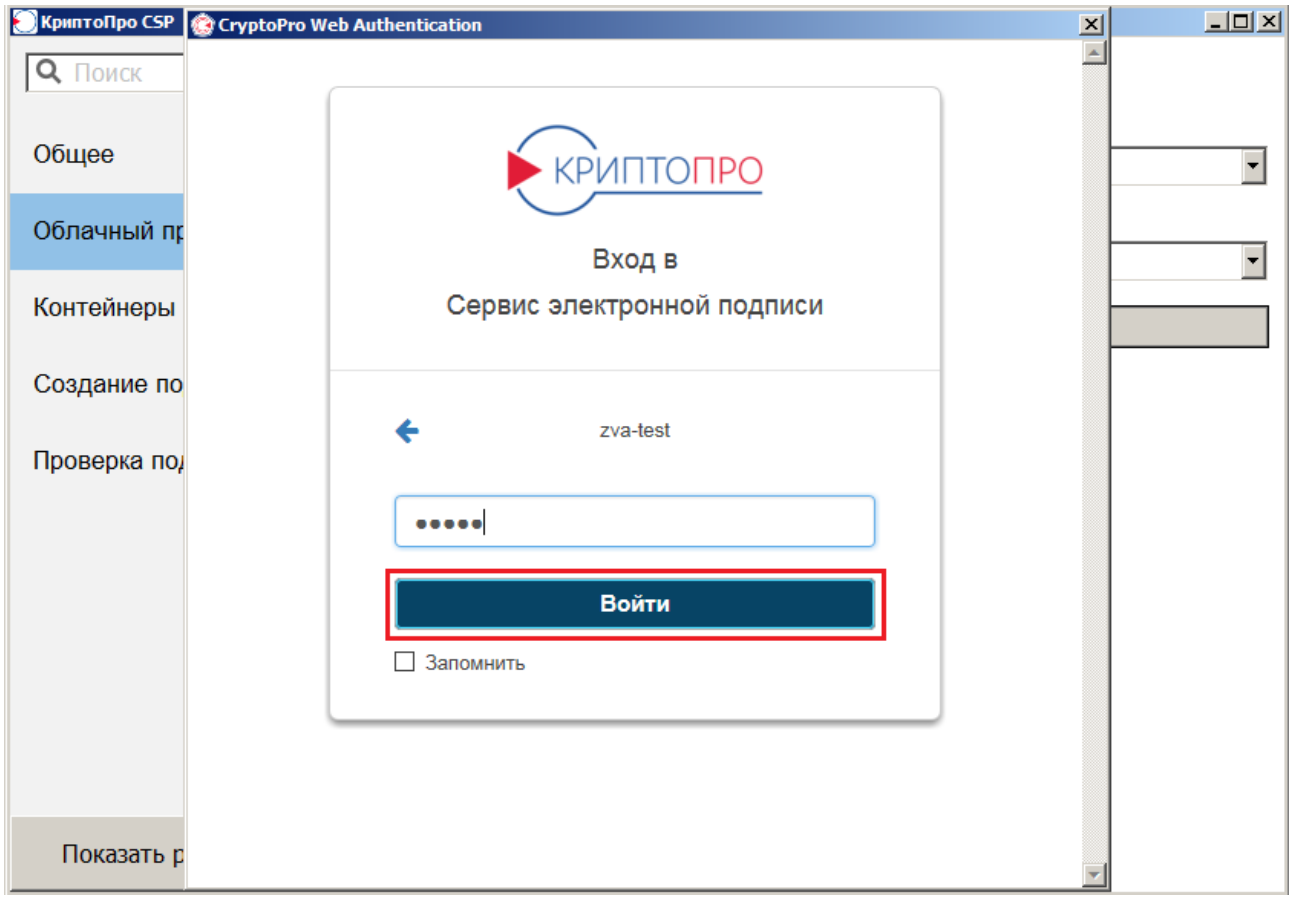


Рисунок 28. Ввод пароля Пользователя

Если аутентификация Пользователя прошла успешно, будет отображено сообщение об успешной установке сертификатов Пользователя (см. **Рисунок 29. Успешная установка сертификатов Пользователя**).

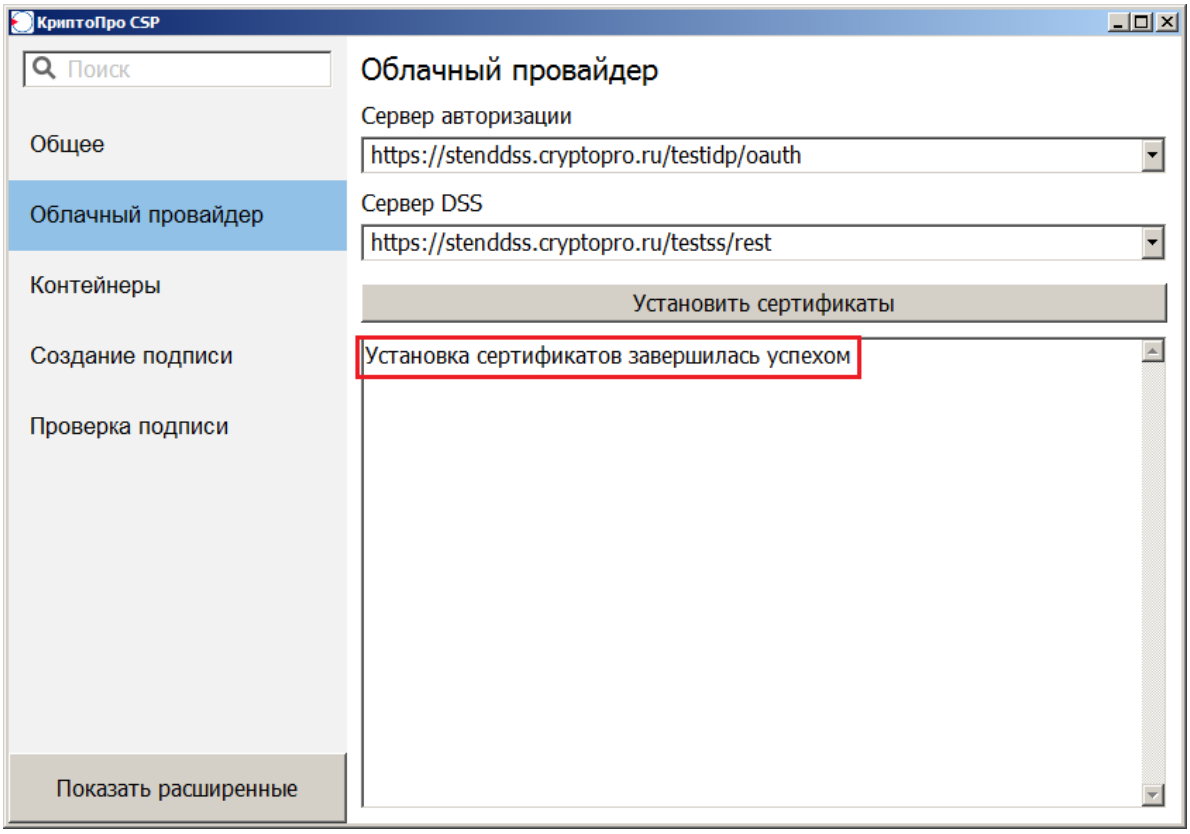


Рисунок 29. Успешная установка сертификатов Пользователя

«Облачный» ключевой контейнер можно увидеть во вкладке «*Контейнеры*» (см. **Рисунок 30. «Облачный» контейнер**).

Далее «облачный» ключевой контейнер можно использовать так же, как и локальный, во всех приложениях, в которые встроено СКЗИ «КриптоПро CSP» (при каждом обращении к данному контейнеру необходимо будет проходить аутентификацию Пользователя в СЭП, как указано выше), в том числе, веб-порталах, информационных системах и т.д.

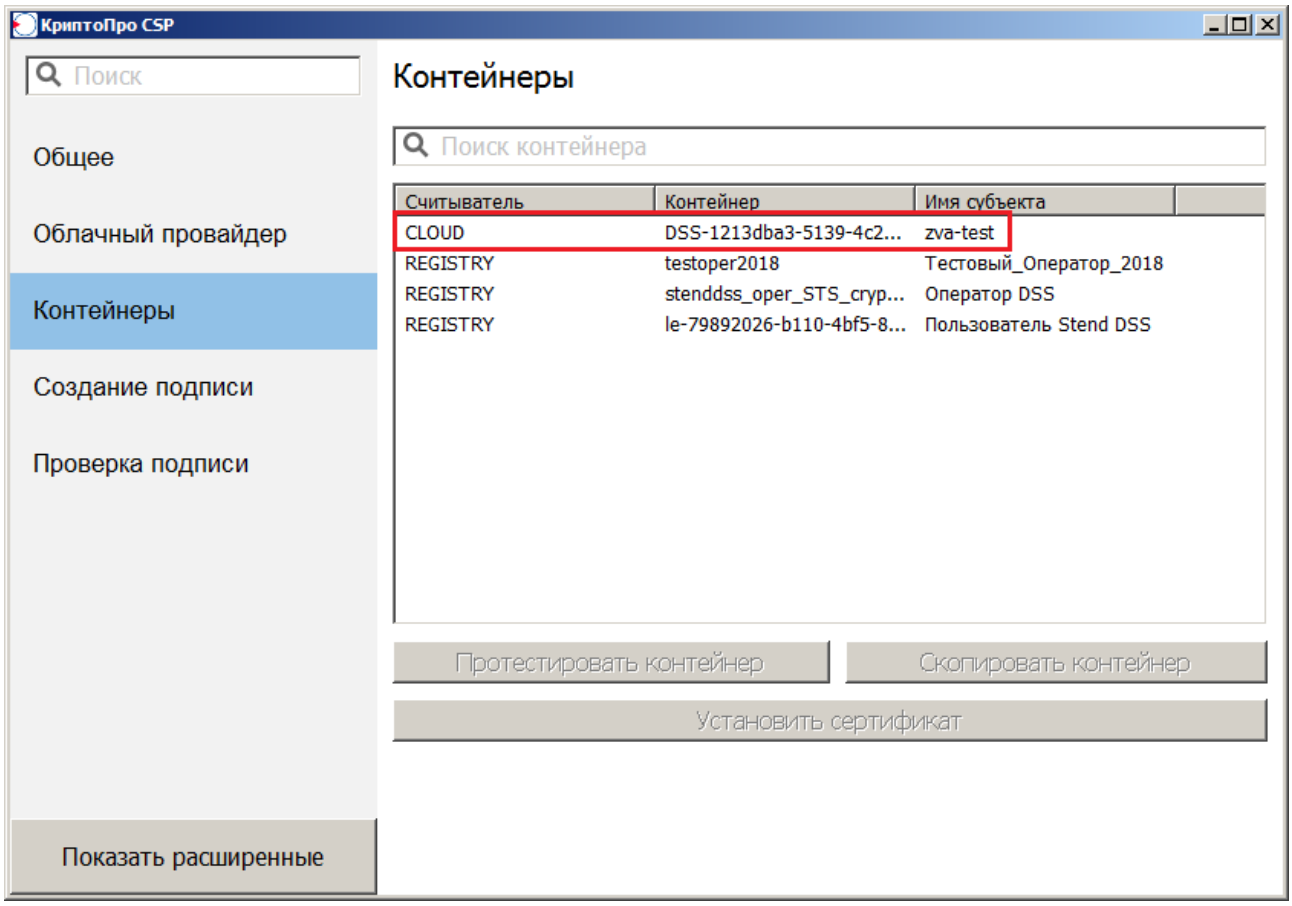


Рисунок 30. «Облачный» контейнер

Перечень рисунков