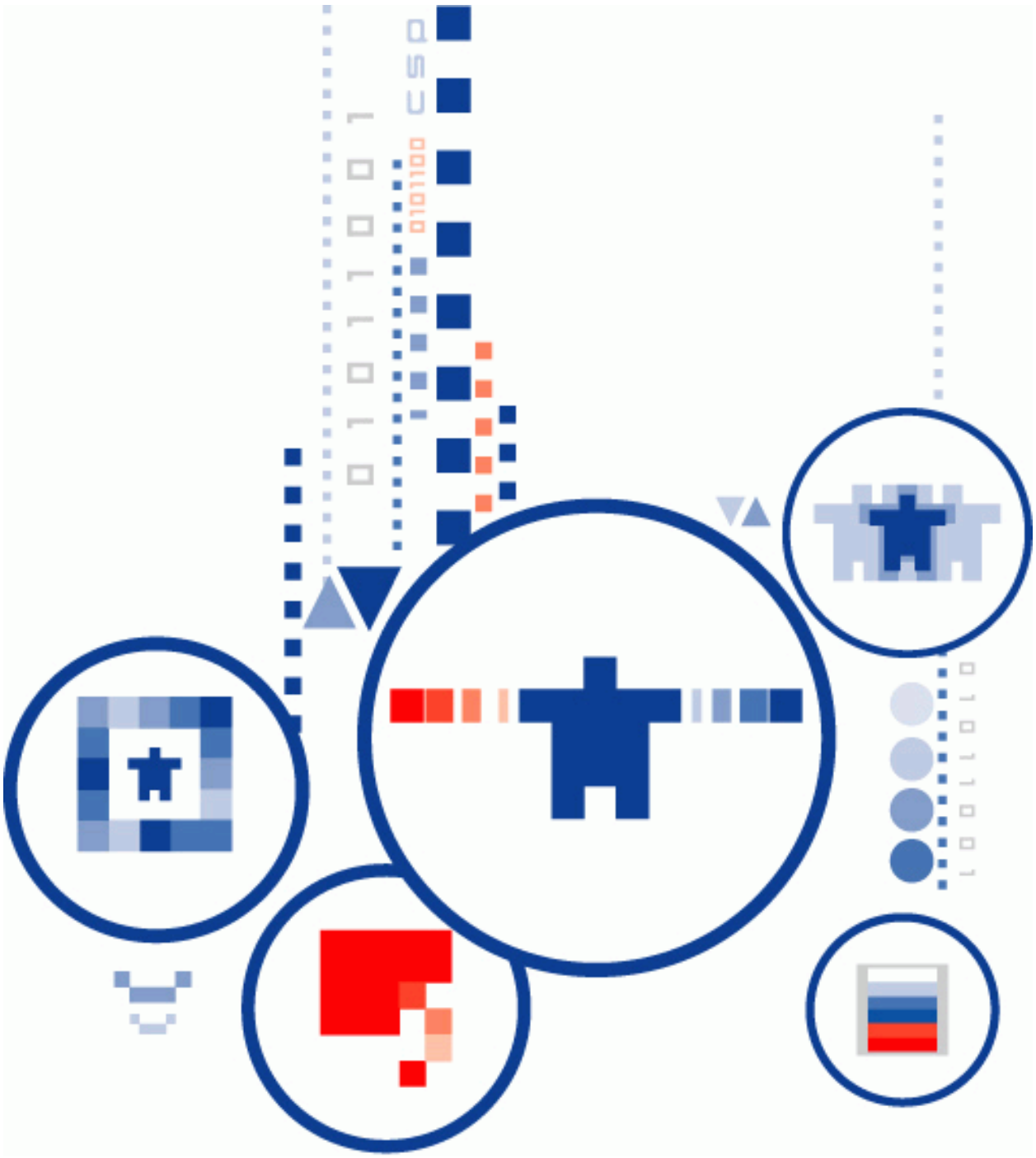

Инструкция Пользователя СЭП

ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Пользователей сервиса электронной подписи ООО «КРИПТО-ПРО» на базе ПАКМ "КриптоПро HSM" (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 ПАКМ "КриптоПро HSM":

ООО «КРИПТО-ПРО»

127018, Москва, ул. Сущевский вал, 18

Телефон: (495) 995 4820

http://www.CryptoPro.ru
https://saas.cryptopro.ru/cryptoproidp/Users
E-mail: info@CryptoPro.ru

Содержание

1. Общие положения

Сервис электронной подписи ООО «КРИПТО-ПРО» на базе ПАКМ "КриптоПро HSM" версии 2.0 (далее – СЭП) предназначен для создания и хранения ключей электронной подписи, 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.

1.1. Требования и подготовка рабочего места Пользователя

На рабочем месте Оператора под управлением MS Windows 7 или выше, macOS версии 10.10 и выше, *Unix-системы (совместимые ОС см. формуляр СКЗИ Криптопро CSP ЖТЯИ.00087-03 30 01) должен быть установлен СКЗИ «КриптоПро CSP» версии 4.0 или выше. Для подключения к СЭП необходимо использовать Интернет-браузер с поддержкой ГОСТ-TLS: Яндекс-браузер, Chromium-GOST, Internet Explorer. Для использования модуля Cloud необходимо установить СКЗИ «КриптоПро CSP» версии 5.0.

1.1.1. Настройка Internet Explorer

Для корректной работы с СЭП необходимо добавить адрес в доверенные сайты в настройках браузера. Для этого в свойствах браузера выбрать вкладку «***Безопасность***», в список надежных сайтов добавить узел https://saas.cryptopro.ru/и сохранить изменения свойств (см. Рисунок 1 – Добавление сайта в зону надежных сайтов).

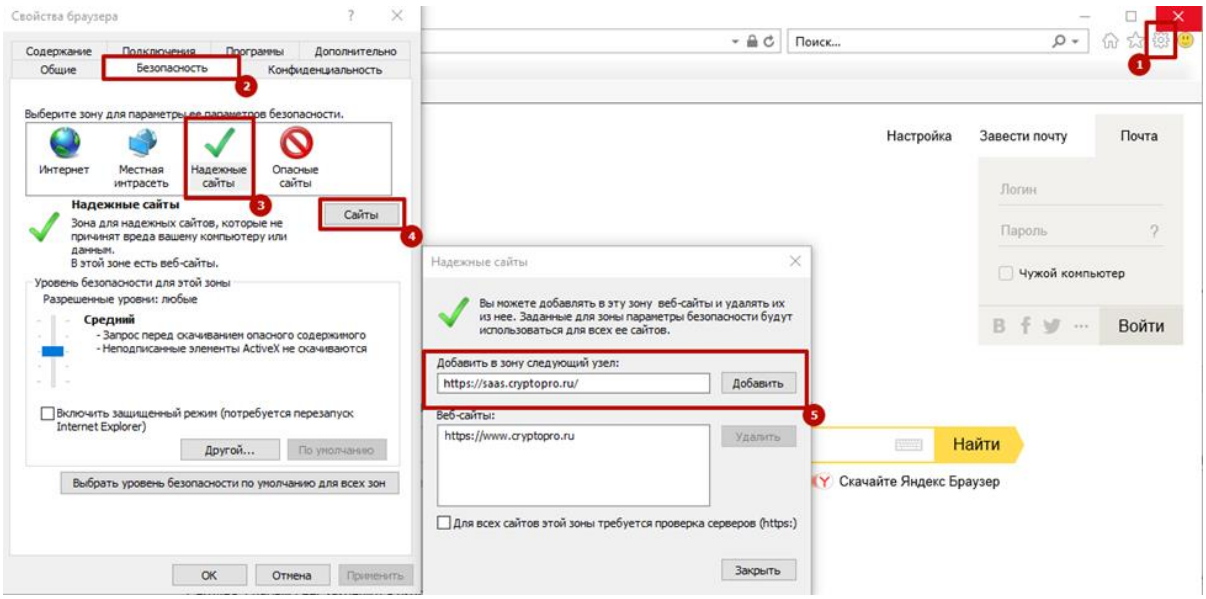

Рисунок 1 – Добавление сайта в зону надежных сайтов

В разделе "***Элементы ActiveX и модуль подключения***" проверить состояние настройки "***Использование элементов управления ActiveX, не помеченных как безопасные для использования***" - должно быть "***Включить***" (см. Рисунок 2 – Включение ActiveX). Для этого зайти в Internet Explorer меню «***Сервис***» - «***Свойства обозревателя***» – «***Безопасность***» - для зоны "***Надежные узлы***" нажать кнопку "***Другой***".

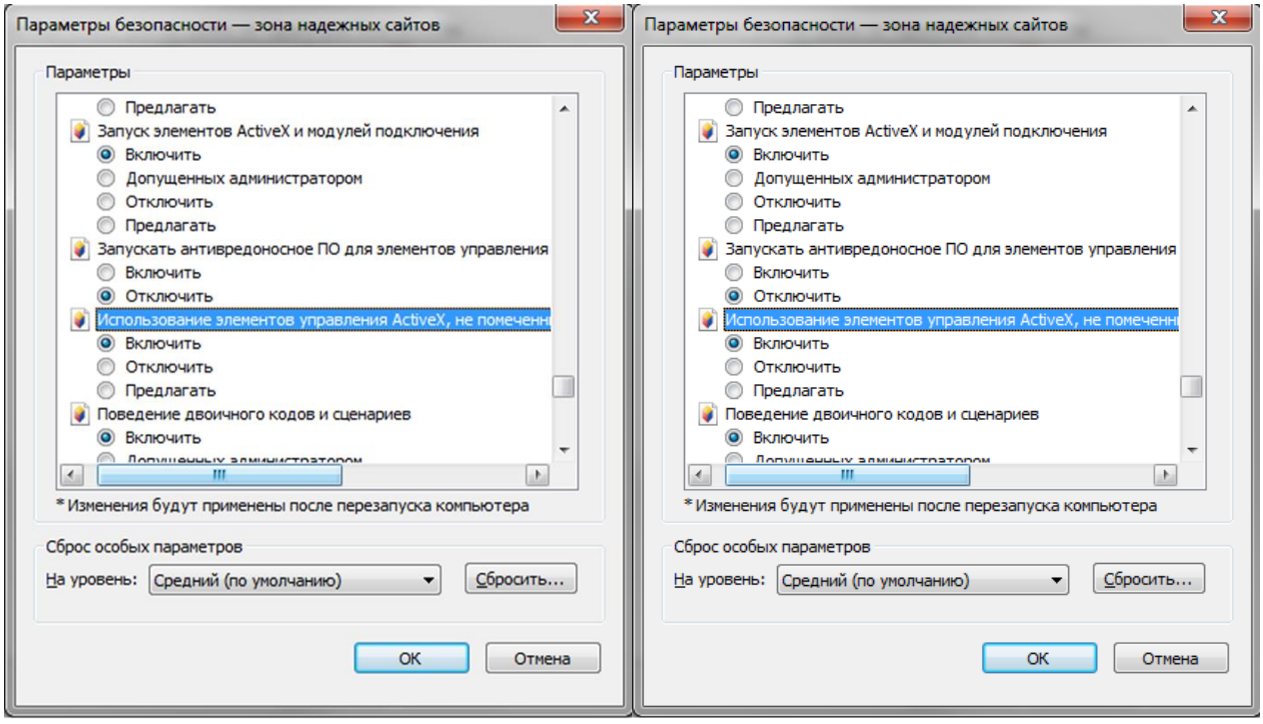

Рисунок 2 – Включение ActiveX

1.1.2. Настройка Яндекс-браузера

Перейдите в «***Настройки***» - «***Системные***».

Убедитесь, что в разделе «Сеть» включена опция «***Подключаться к сайтам, использующим шифрование по ГОСТ. Требуется КриптоПро CSP***».

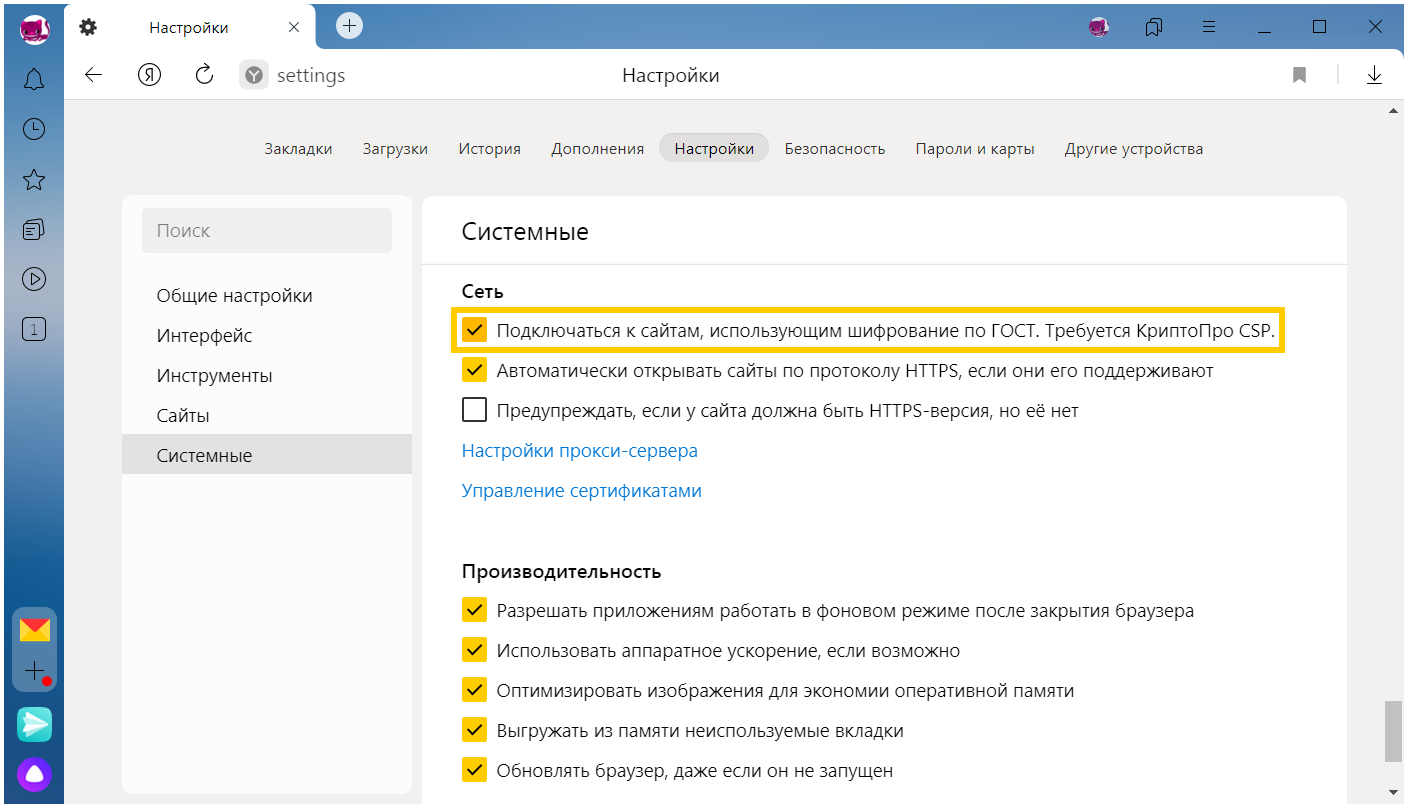

Рисунок 3 – Включение поддержки ГОСТ

1.2. Первый вход в СЭП (аутентификация по паролю)

Оператор СЭП после регистрации Пользователя выдает ему логин и пароль для входа.

Для работы в СЭП Пользователю требуется осуществить вход в веб-интерфейс Пользователя по адресу https://saas.cryptopro.ru/cryptopro

В окне аутентификации введите логин Пользователя, полученный от Оператора СЭП, и нажмите кнопку «***Далее***» (см. Рисунок 4 - Вход в СЭП. Окно ввода учётной записи)

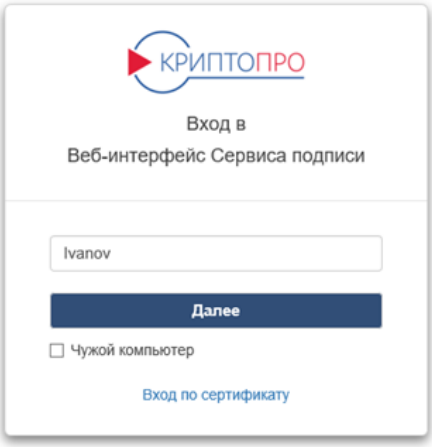

Рисунок 4 - Вход в СЭП. Окно ввода учётной записи

Если имя учётной записи введено верно, появится форма для ввода пароля, выданного Пользователю Оператором СЭП при регистрации (см. Рисунок 5 - Вход в СЭП).

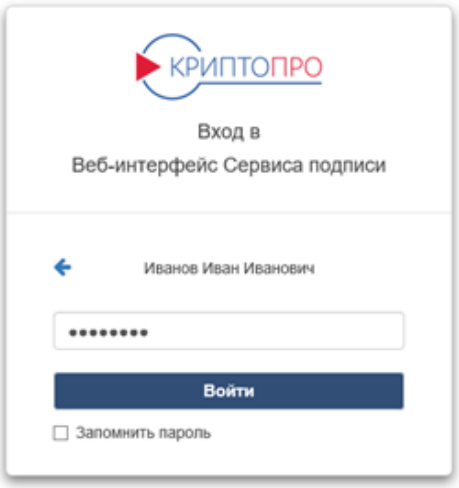

Рисунок 5 - Вход в СЭП

2. Настройка аутентификации

Для редактирования параметров настроек аутентификации СЭП Пользователю требуется осуществить вход в веб-интерфейс Пользователя по адресу https://saas.cryptopro.ru/cryptoproidp/Users.

2.1. Настройка аутентификации по логину/паролю.

Для настройки аутентификации Пользователя по логину и паролю необходимо в группе «Методы вторичной аутентификации» раскрыть блок «***Аутентификация по паролю***» и нажать кнопку «***Изменить***». Новый пароль отобразится на экране (см. Рисунок 6 - Изменение пароля).

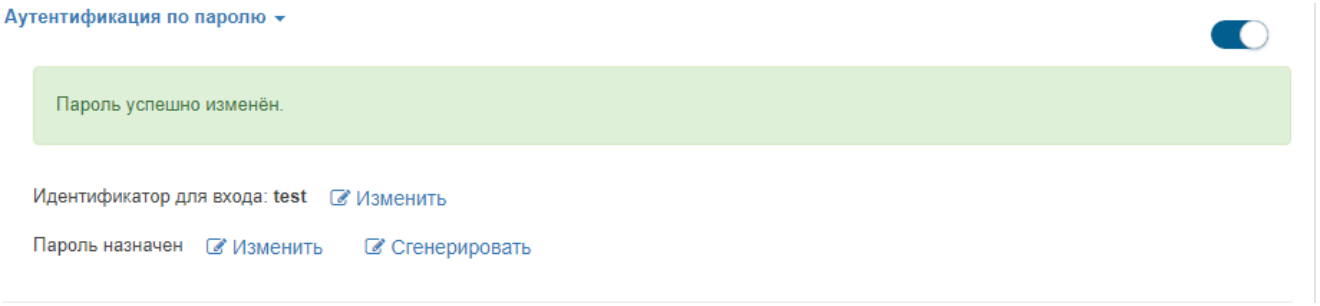

Рисунок 6 - Изменение пароля

2.2. Настройка аутентификации по сертификату

Для настройки первичной аутентификации пользователя по сертификату необходимо импортировать компоненты имени Пользователя из существующего сертификата с расширением *.cer/*.crt по кнопке «***Заполнить компоненты имени из сертификата***» (см. **Ошибка! Источник ссылки не найден.**).

Рисунок 7 - Загрузка сертификата

Для экспорта сертификата с расширением *.cer/*.crt/*.p7b откройте Криптопро CSP – «***Сервис***» - «***Просмотреть сертификаты в контейнере***» - «***Обзор***» - выберите нужный контейнер и нажмите «***Далее***»

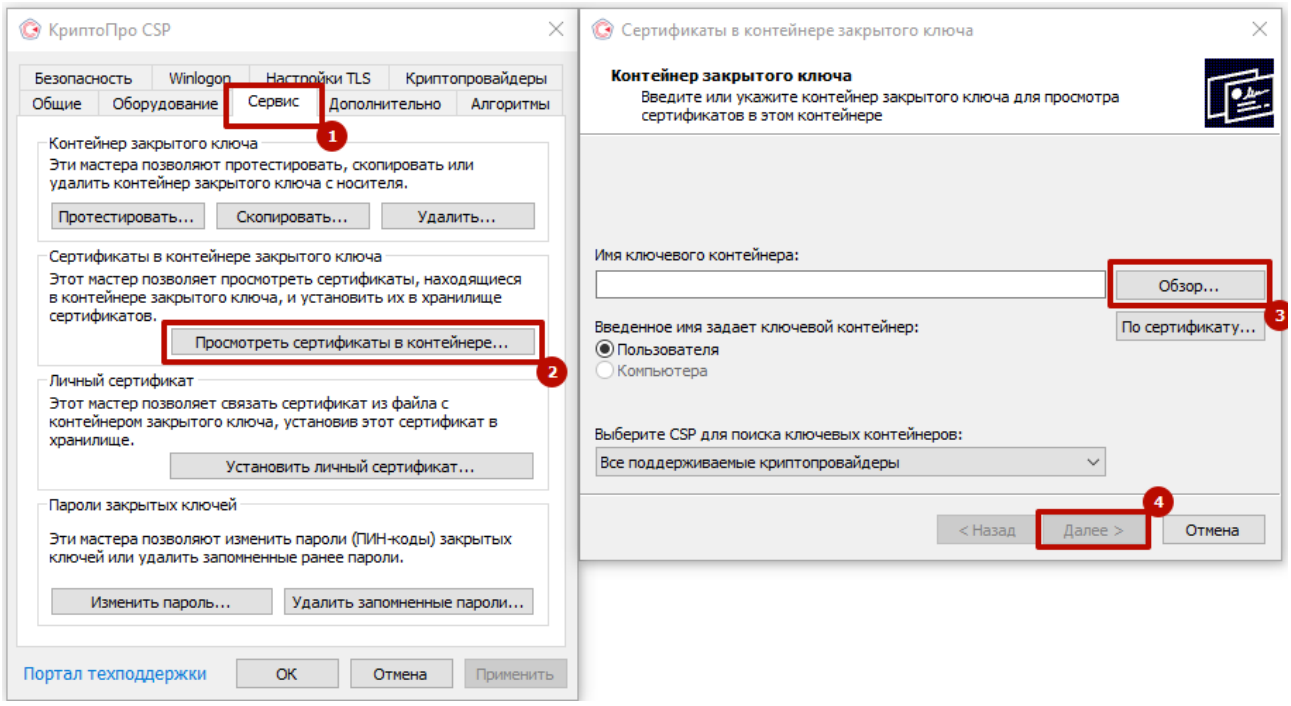

Рисунок 8 - Импорт сертификата через КриптоПро CSP

В открывшемся окне сертификата нажмите кнопку «***Свойства***», перейдите во вкладку «***Состав***» и нажмите «***Копировать в файл***» (см. Рисунок 9 - Экспорт сертификата)

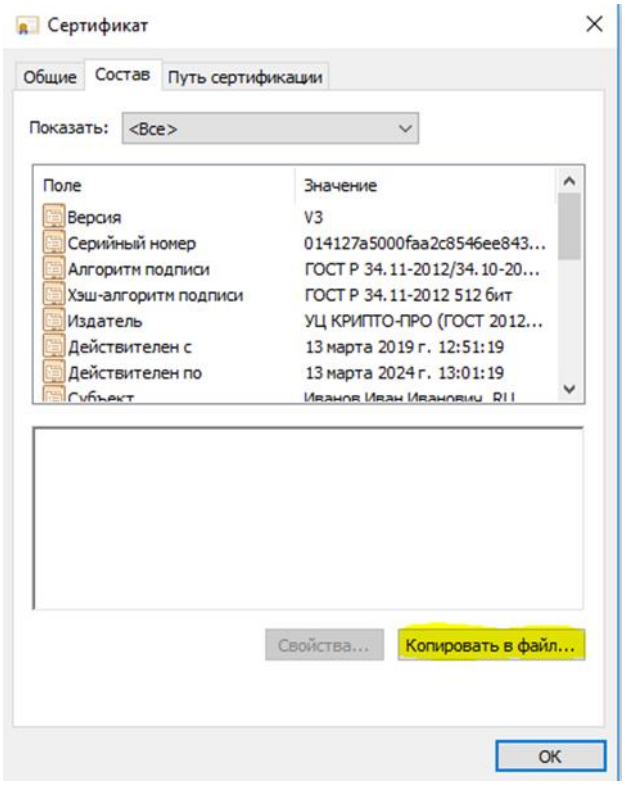

Рисунок 9 - Экспорт сертификата

На следующем шаге выберете «***Нет, не экспортировать закрытый ключ***».

Далее следуйте указаниям мастера импорта сертификатов, на этапе выбора места сохранения файла укажите удобную директорию и имя файла.

Сертификат должен быть установлен локально на компьютере пользователя, и требуется обеспечить доверие к данному сертификату со стороны сервера СЭП. Для этого отправьте цепочку сертификатов (выгруженный по инструкции сертификат в формате p7b) издателя на почту operdss@cryptopro.ru в формате zip/rar.

2.3. Настройка аутентификации с помощью мобильного приложения

Для настройки вторичной аутентификации Пользователя с помощью мобильного приложения «DSS Client» в группе «***Методы вторичной аутентификации***» раскройте блок «***Аутентификация с помощью мобильного приложения***» и нажмите кнопку «***Добавить устройство***» (см. Рисунок 10 - Аутентификация с помощью мобильного приложения).

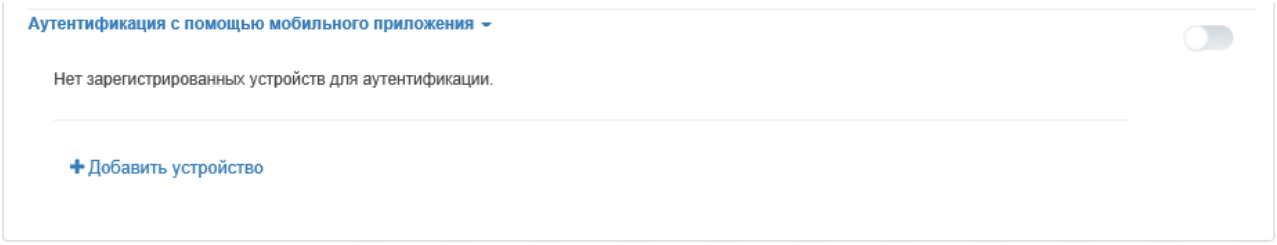

Рисунок 10 - Аутентификация с помощью мобильного приложения

Выберите способ отправки кода активации и отсканировать QR-код в мобильном приложении (см. Рисунок 11 - QR-код для DSS Client).

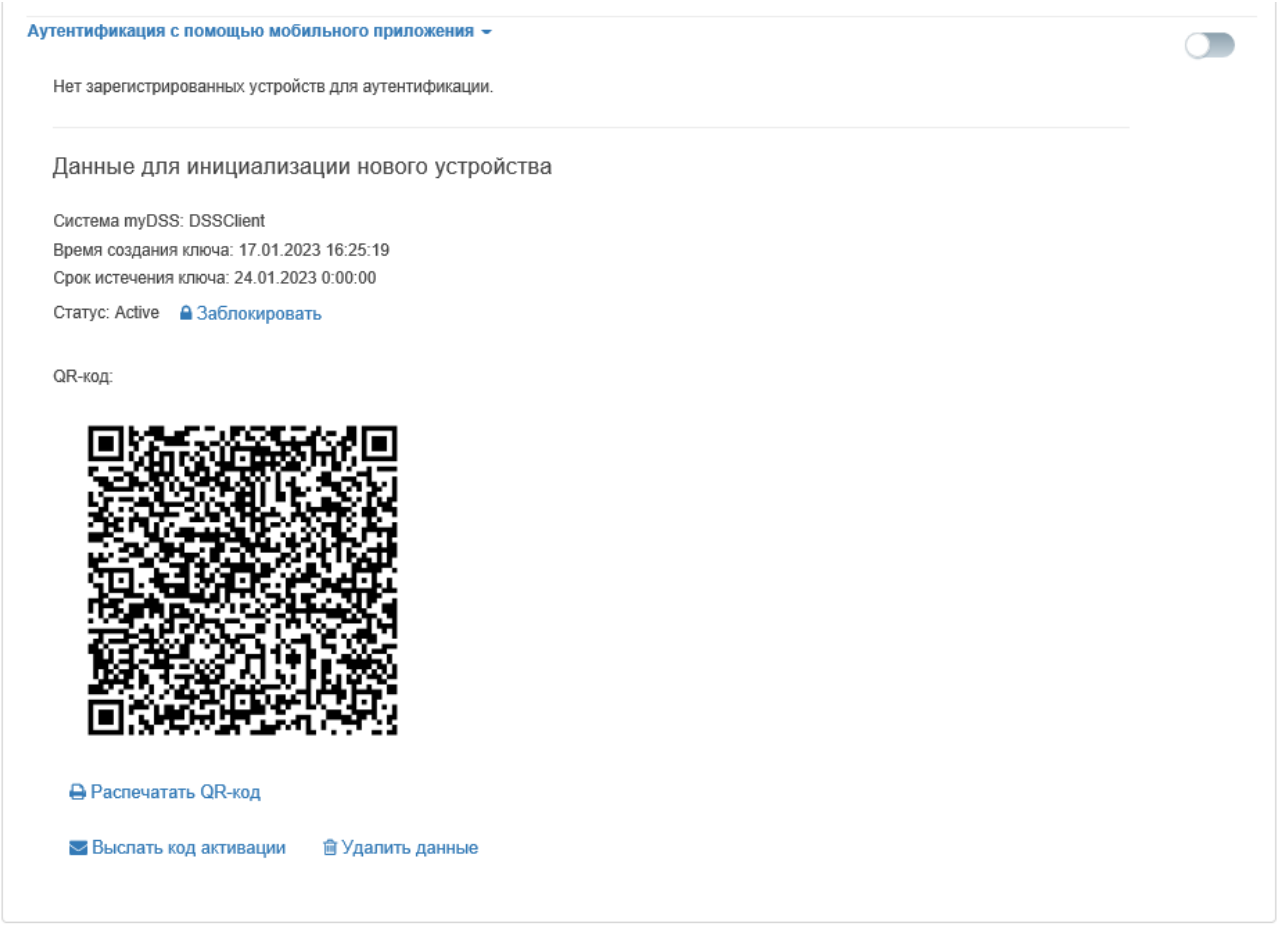

Рисунок 11 - QR-код для DSS Client

Для обеспечения работоспособности вторичной аутентификации с помощью мобильного приложения Пользователю необходимо установить мобильное приложение «DSS Client» из магазина Google Play, Apple App Store, AppGallery.

В мобильном приложении выберите способ привязки «через QR-код» и введите имя учетной записи.

При первом запуске мобильное приложение запросит разрешение на отправку уведомлений и установку способа защиты приложения (см. Рисунок 12 - Первый запуск мобильного приложения).

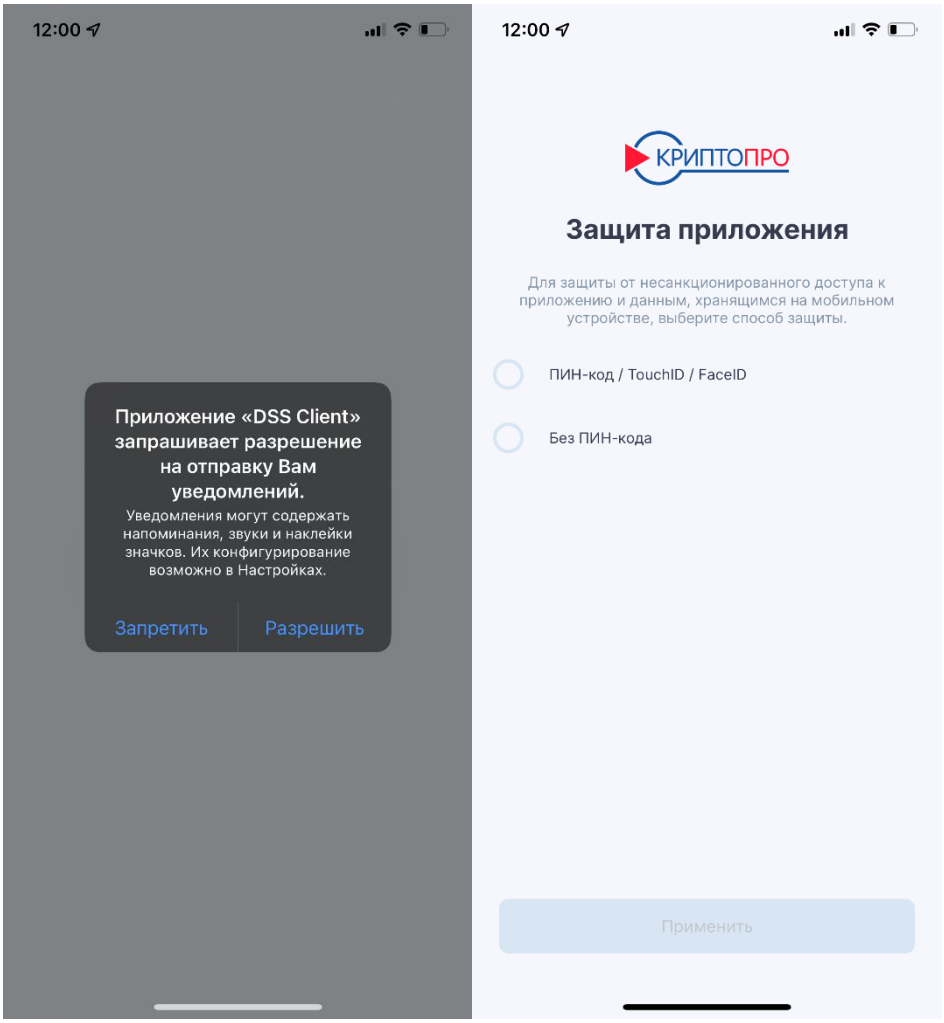

Рисунок 12 - Первый запуск мобильного приложения

На следующем шаге мобильное приложение попросит отсканировать QR-код. Как только QR-код будет успешно отсканирован, Пользователь должен ввести полученный им ранее при регистрации код активации (см. Рисунок 13 - Регистрация учетной записи в DSS Client).

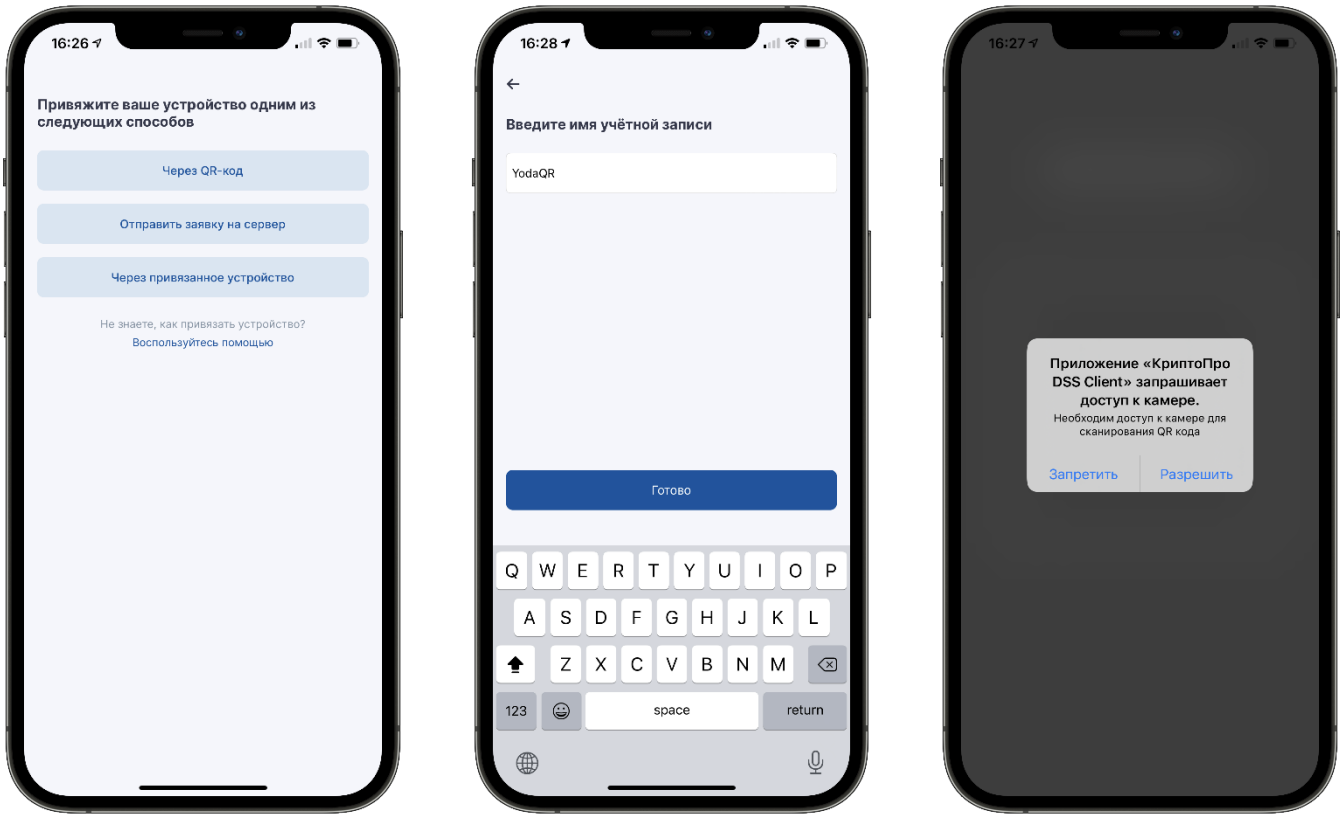

Рисунок 13 - Регистрация учетной записи в DSS Client

После ввода кода активации выберите способ защиты Вашей учетной записи и нажмите кнопку «***Применить***». Если Вы выбрали пункт «***ПИН-код / Face ID***», придумайте и введите в следующем окне ПИН-код. Данный ПИН-код необходимо будет вводить в дальнейшем при подтверждении операций, создании запросов на сертификаты, добавлении новых устройств и других действий, требующих аутентификации. Нажмите кнопку «***Подтвердить***». Если ранее в приложении не использовалась биометрия (например, при задании кода-пароля защиты приложения), разрешите приложению использовать биометрические данные (отпечаток пальца или скан формы лица). Биометрия может заменять ввод ПИН-кода при подтверждении операций и прочих действий, требующих аутентификации (см. Рисунок 14 - Защита мобильного приложения).

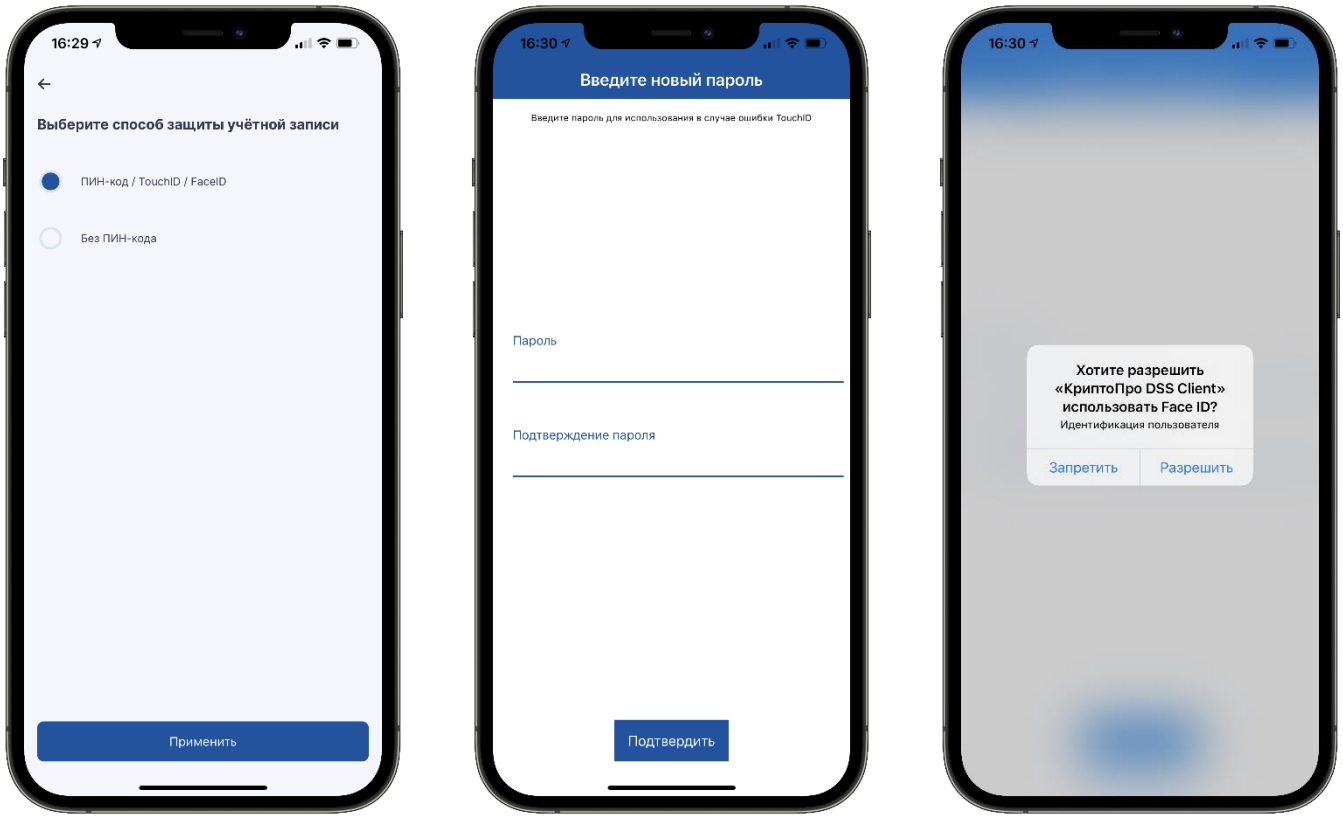

Рисунок 14 - Защита мобильного приложения

На экране мобильного устройства отобразится информация о Вашей учетной записи. Если данные верны, нажмите кнопку «***Подтвердить***», после чего привязка устройства будет завершена и его можно будет использовать для подтверждения подписи документов. В случае если данные не верны, следует отказаться от подтверждения привязки учетной записи и обратиться к Оператору. Если данные учётной записи верны, и Вы подтвердили привязку, на экране отобразится соответствующее информационное уведомление. Для перехода к подписи документов и подтверждению операций нажмите кнопку "***Ок***". Статус учетной записи в меню «***Настройки***» – «***Учетные записи***» изменится на «***Используется по умолчанию***» или «***Активный***», если Ваше мобильное устройство ранее уже привязывалось к другим учетным записям (см. Рисунок 15 - Информация об учетной записи пользователя).

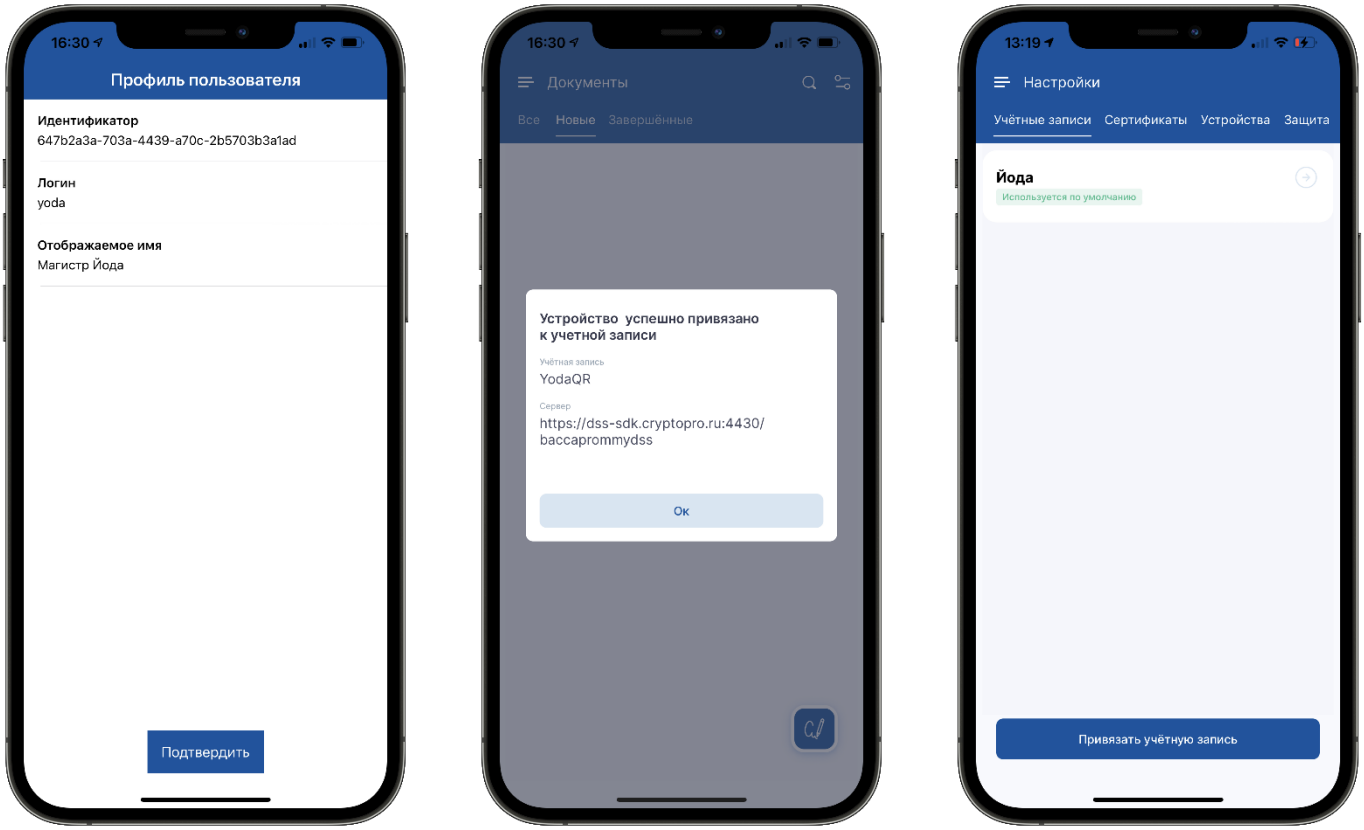

Рисунок 15 - Информация об учетной записи пользователя

2.4. Настройка доступа к операциям СЭП

После успешной настройки параметров аутентификации Пользователя необходимо определить операции, которые Пользователь должен подтверждать выбранным методом вторичной аутентификации.

Можно настроить доступ к следующим операциям в СЭП:

- Подпись документа
- Шифрование/расшифрование документа
- Удаление сертификата
- Смена ПИН-кода закрытого ключа
- Создание запроса на сертификат

3. Вход в веб-интерфейс СЭП

Аутентификация Пользователя в СЭП происходит с использованием методов первичной и вторичной аутентификации в СЭП. Оператор СЭП назначает Пользователю 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:

• «Аутентификация по сертификату» – первичная аутентификация Пользователя происходит по сертификату, предоставленному Пользователем Оператору СЭП.

• «Аутентификация по паролю» – первичная аутентификация Пользователя происходит по паролю, выданному Пользователю Оператором СЭП.

Возможные методы вторичной аутентификации Пользователя:

• «Аутентификация с помощью мобильного приложения» – вторичная аутентификация Пользователя происходит в мобильном приложении DSS Client.

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

В случае если Оператором СЭП определен метод первичной аутентификации «***Аутентификация по паролю***», Пользователю необходимо ввести имя учётной записи (логин) в поле ввода и нажать кнопку «***Далее***» (см. Рисунок 16 - Вход в СЭП. Окно ввода учётной записи).

Для работы в СЭП Пользователю требуется осуществить вход в веб-интерфейс Пользователя по адресу https://saas.cryptopro.ru/cryptopro

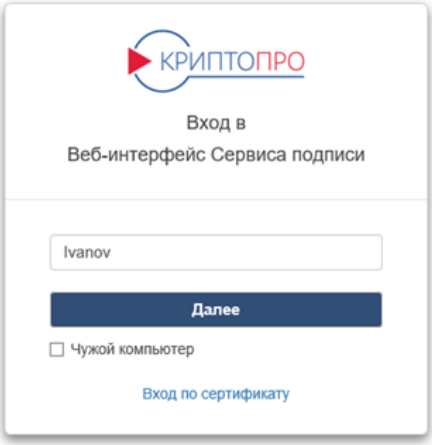

Рисунок 16 - Вход в СЭП. Окно ввода учётной записи

Если имя учётной записи введено верно, появится форма для ввода пароля, выданного Пользователю Оператором СЭП при регистрации (см. Рисунок 17 - Вход в СЭП).

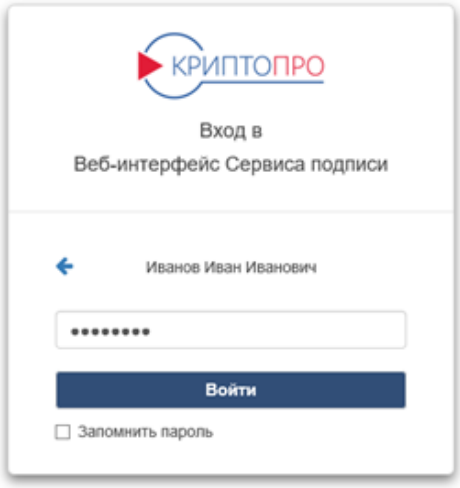

Рисунок 17 - Вход в СЭП

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

В случае если определен метод первичной аутентификации «Аутентификация по сертификату», Пользователю необходимо осуществить вход в веб-интерфейс Пользователя по адресу https://saas.cryptopro.ru/cryptopro, после чего выбрать «***Вход по сертификату***» (см. Рисунок 18 – Вход по сертификату).

В появившемся окне подтверждения сертификата выбрать сертификат Пользователя и нажать кнопку «***ОК***».

Рисунок 18 – Вход по сертификату

3.3. Вторичная аутентификация

Если Пользователю СЭП включено подтверждение операции входа в веб-интерфейс при помощи метода вторичной аутентификации – «***Аутентификация с***

помощью мобильного приложения», Пользователь должен подтвердить операцию входа в мобильном приложении «DSS Client».

При необходимости подтверждения операции с помощью мобильного приложения DSS Client СЭП выдаст соответствующий запрос (см. Рисунок 19 - Запрос аутентификации с помощью мобильного приложения DSS Client).

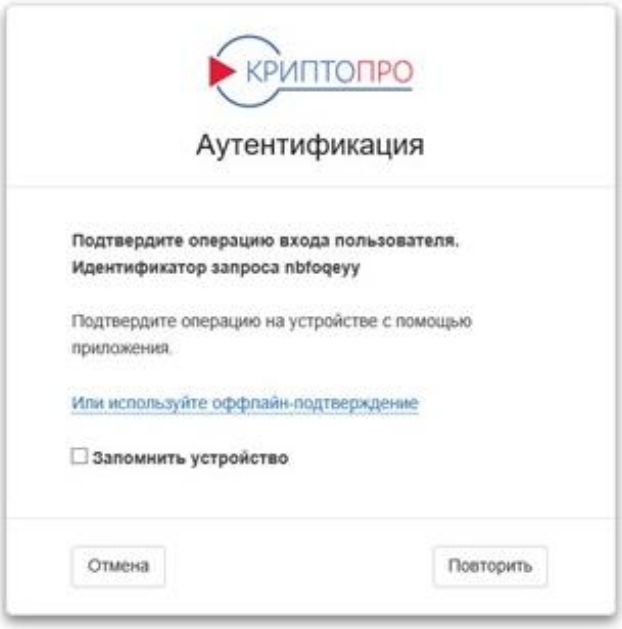

Рисунок 19 - Запрос аутентификации с помощью мобильного приложения DSS Client

После получения PUSH-уведомления о подтверждении операции в мобильном приложении DSS Client выбрать операцию для подтверждения и нажать на нее.

В открывшемся окне просмотрите следующие параметры операции, полученные с сервера:

- Учётная запись. Убедитесь, что подтверждаете операцию для нужной учетной записи.
- Идентификатор сессии. Убедитесь, что идентификаторы в веб-интерфейсе и в мобильном приложении совпадают.

В случае успешного подтверждения операции в мобильном приложении появится уведомление "***Операция успешно подтверждена***" (см. Рисунок 20 - Подтверждение операции). Для продолжения работы с приложением нажмите на произвольной области экрана.

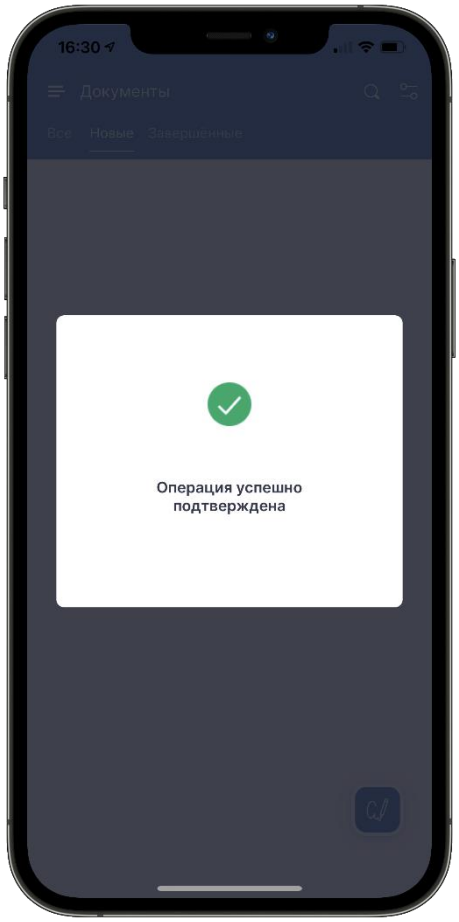

Рисунок 20 - Подтверждение операции

4. Меню web-интерфейса Пользователя СЭП

В меню web-интерфейса Пользователя доступны 8 разделов:

- Подписать
- Усовершенствовать подпись
- Зашифровать
- Расшифровать
- Проверить подпись
- Проверить сертификат
- Сертификаты
- Аудит

4.1. 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.

Для формирования электронной подписи электронного документа перейдите в раздел «***Подписать***» и выполните следующие действия:

1) Загрузите электронный документ, который требуется подписать, в СЭП, нажав кнопку «***Выбрать***» в секции «***Документ***».

2) Выберите нужный формат электронной подписи в секции «***Формат подписи***».

3) Выберите параметры электронной подписи в секции «***Параметры подписи***».

4) Выберите нужный сертификат Пользователя в секции «Сертификат».

5) Нажмите кнопку «Подписать»

6) Подтвердите операцию выполнения подписи в мобильном приложении DSS Client.

7) Документ будет загружен после подтверждения (см. Рисунок 21 - Документ успешно подписан).

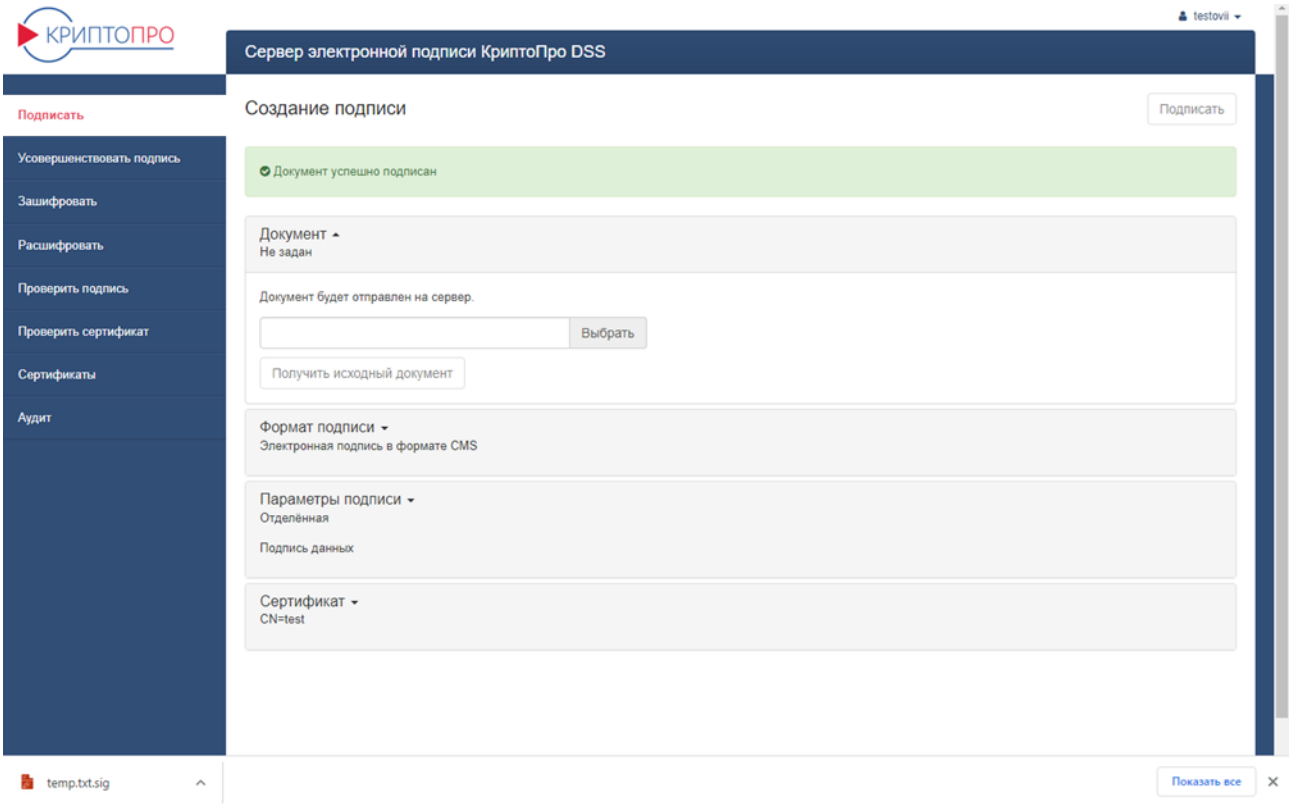

Рисунок 21 - Документ успешно подписан

Подтверждение операции подписи с помощью мобильного приложения

Если для Пользователя СЭП включено подтверждение операции подписи при помощи мобильного приложения, Пользователь должен подтвердить операцию подписи в мобильном приложении «DSS Client». При необходимости подтверждения операции с помощью мобильного приложения DSS Client СЭП выдаст соответствующий запрос (см. Рисунок 22 - Подтверждение операции подписи)

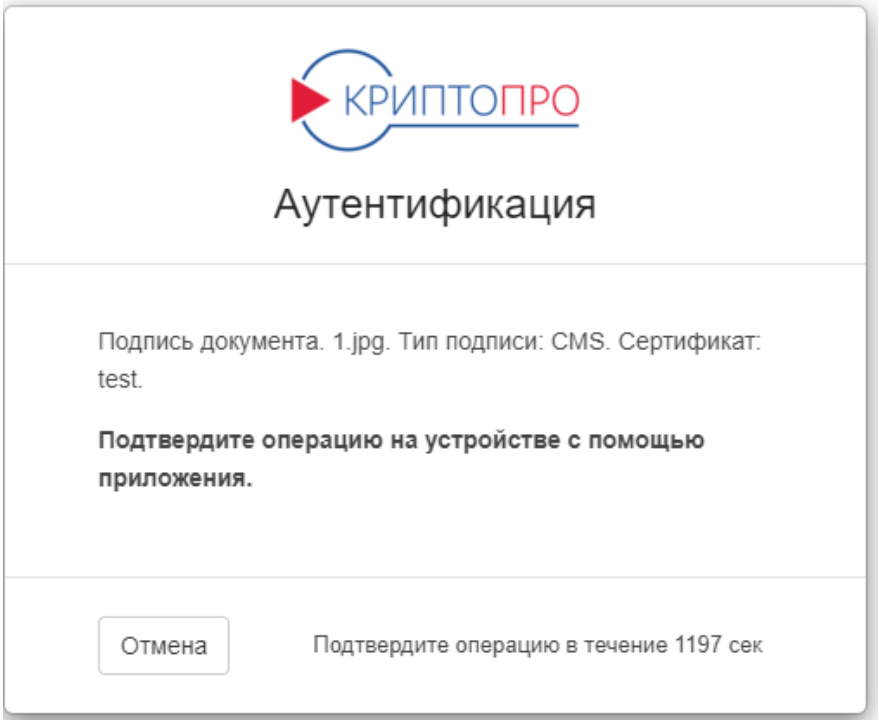

Рисунок 22 - Подтверждение операции подписи

После получения PUSH-уведомления о подтверждении операции в мобильном приложении DSS Client выберете операцию для подтверждения, нажав на нее.

В открывшемся окне просмотрите следующие параметры операции, полученные с сервера:

• Учётная запись. Убедитесь, что подтверждаете операцию для нужной учетной записи.

Сертификат. Убедитесь, что выбран верный сертификат, используемый при подписи документа.

• Сервер. Данный параметр заполняется автоматически и содержит адрес сервера, на котором производится подпись.

• Скачать документы. Переведите данный переключатель в активное положение, если требуется использовать офлайн-режим.

После того как Вы просмотрели все параметры операции, нажмите кнопку "Подтвердить" (см. Рисунок 23 - Информация об операции).

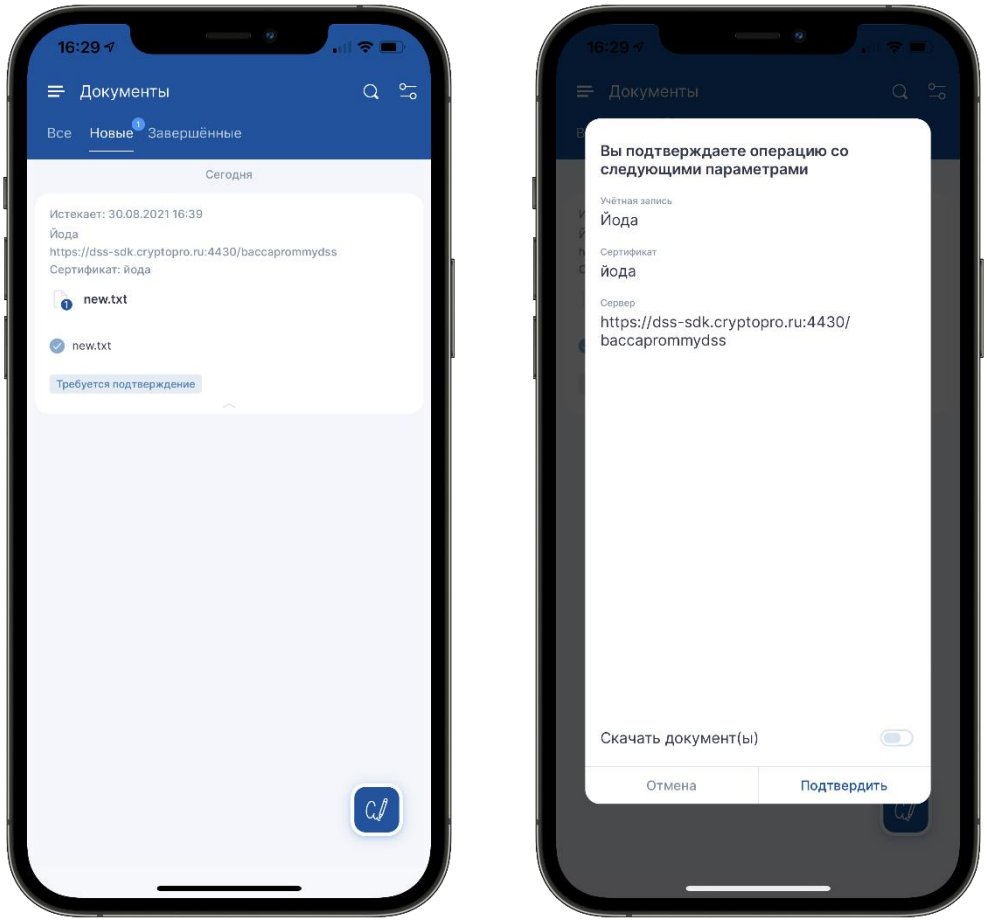

Рисунок 23 - Информация об операции

В открывшемся окне отобразится список документов, подпись которых требуется подтвердить. Ознакомьтесь с подписываемым документом(ами). После того как Вы ознакомились с документом, вернитесь назад и нажмите кнопку "Подтвердить". Если операцию необходимо отменить, нажмите кнопку "Отказаться". В случае успешного подтверждения операции документ будет подписан. В мобильном приложении появится уведомление "Операция успешно подтверждена" (см. Рисунок 24 - Подтверждение операции подписи). Для продолжения работы с приложением нажмите на произвольной области экрана.

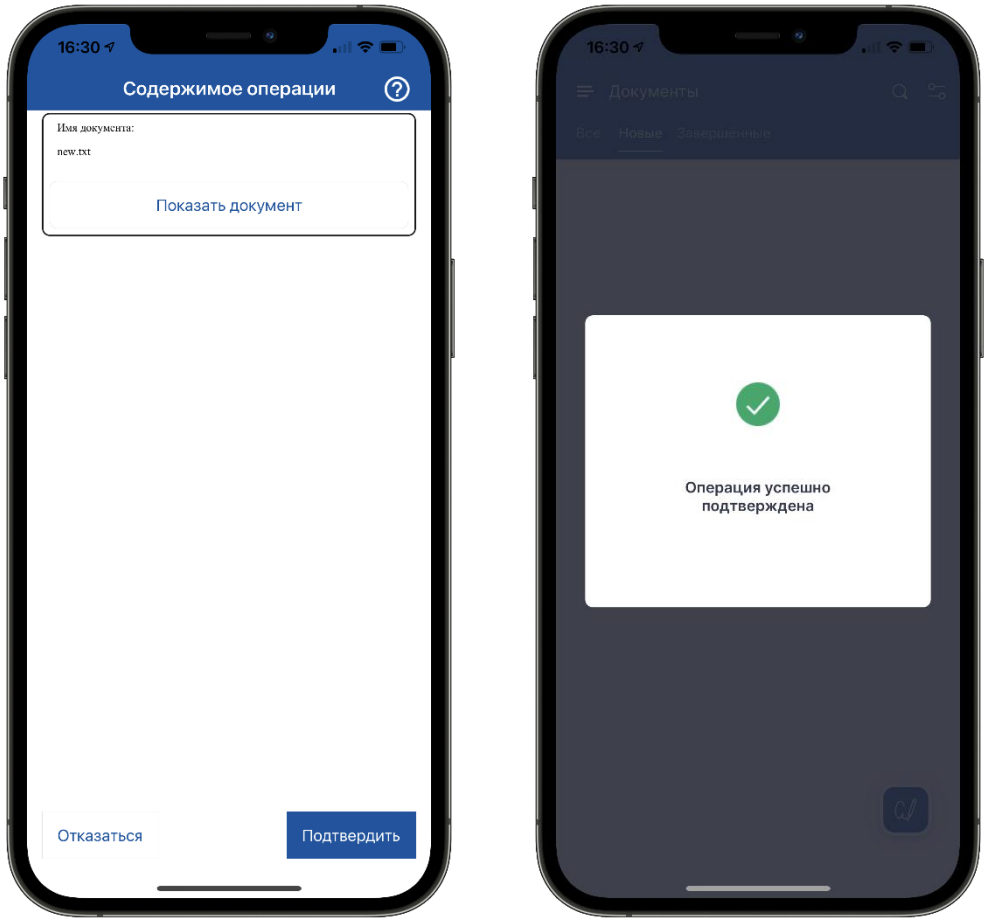

Рисунок 24 - Подтверждение операции подписи

4.2. 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 необходимо 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 есть необходимость удалить из подписи существующие штампы времени/статусы сертификатов.

4) Нажать кнопку «***Усовершенствовать***» (см. Рисунок 25 - Формирование усовершенствованной подписи).

5) Загрузить полученную усовершенствованную электронную подпись (см. Рисунок 26 - Загрузка файла усовершенствованной подписи документа).

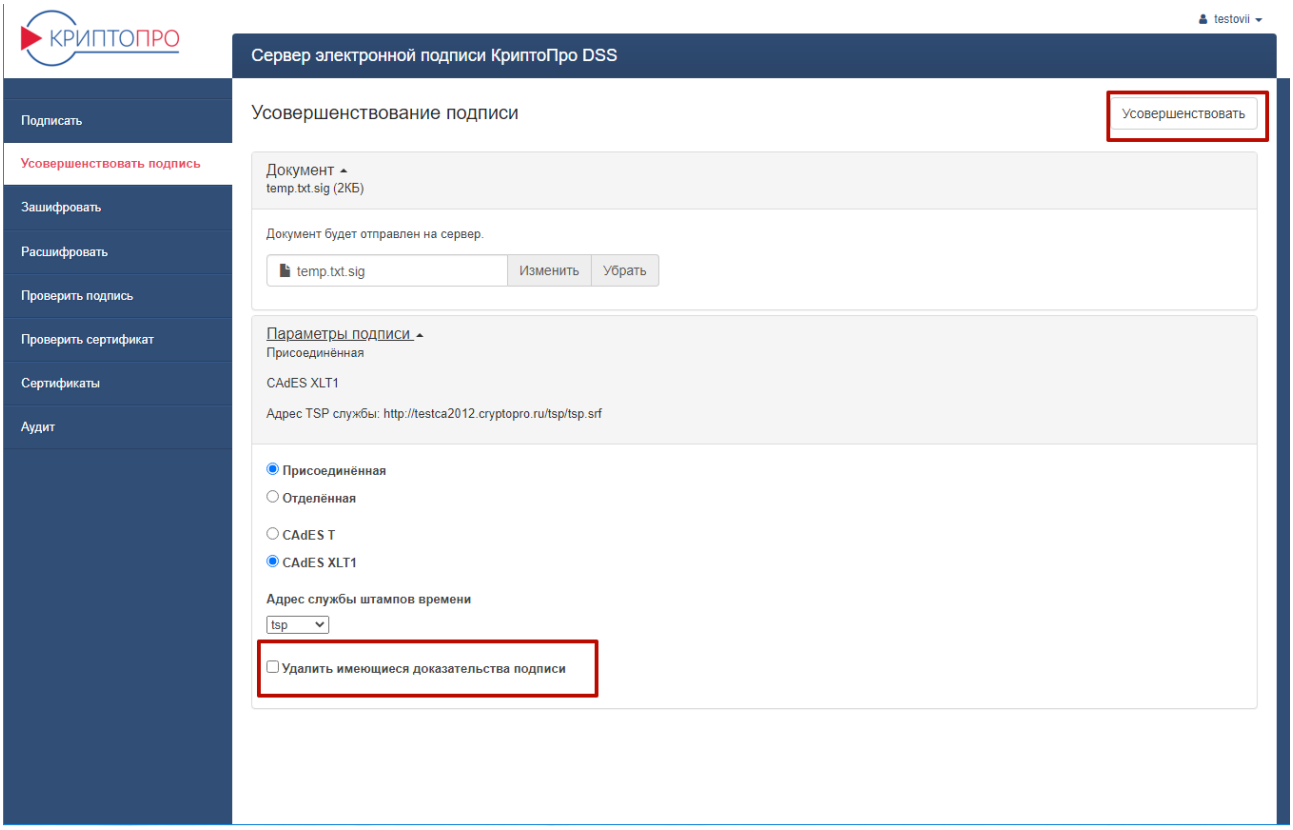

Рисунок 25 - Формирование усовершенствованной подписи

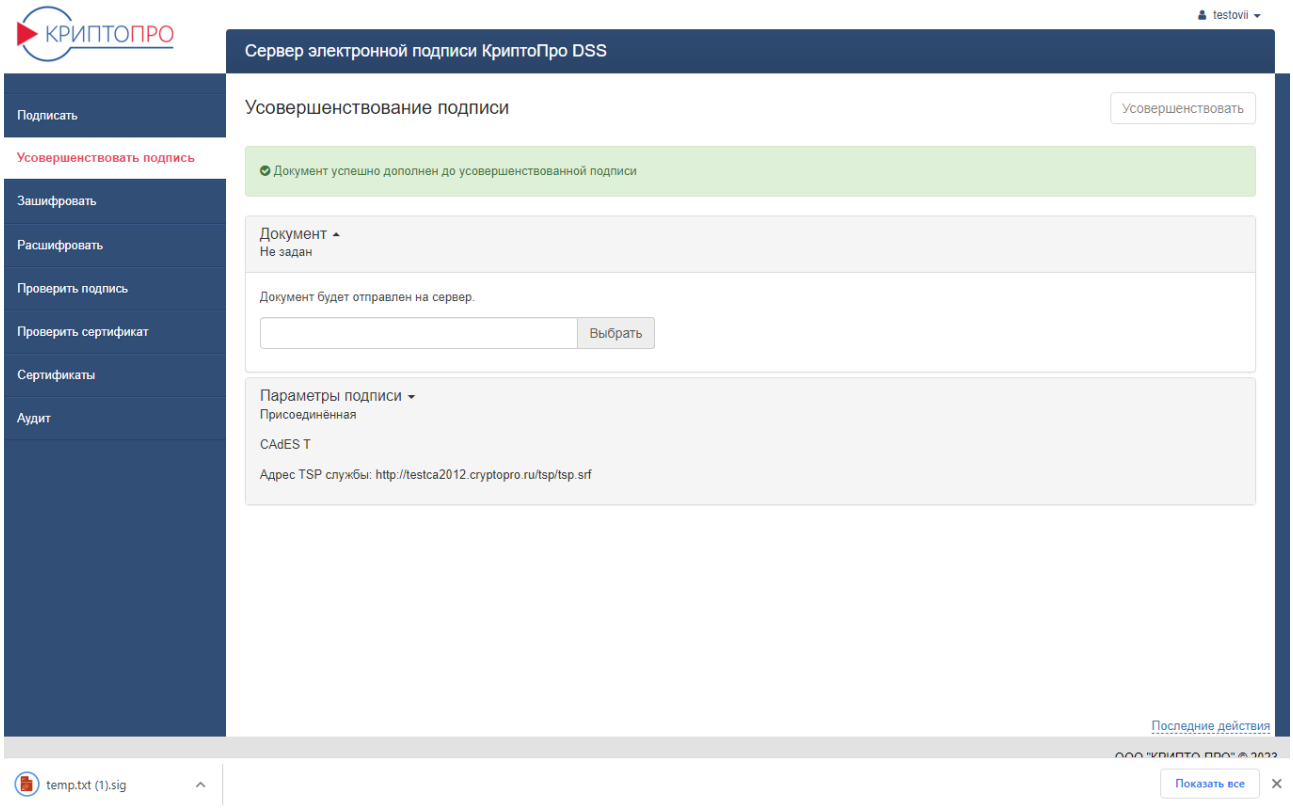

Рисунок 26 - Загрузка файла усовершенствованной подписи документа

4.3. Раздел «Зашифровать»

Раздел предназначен для адресного шифрования электронных документов. Для шифрования 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 требуется 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 27 - Параметры шифрования).

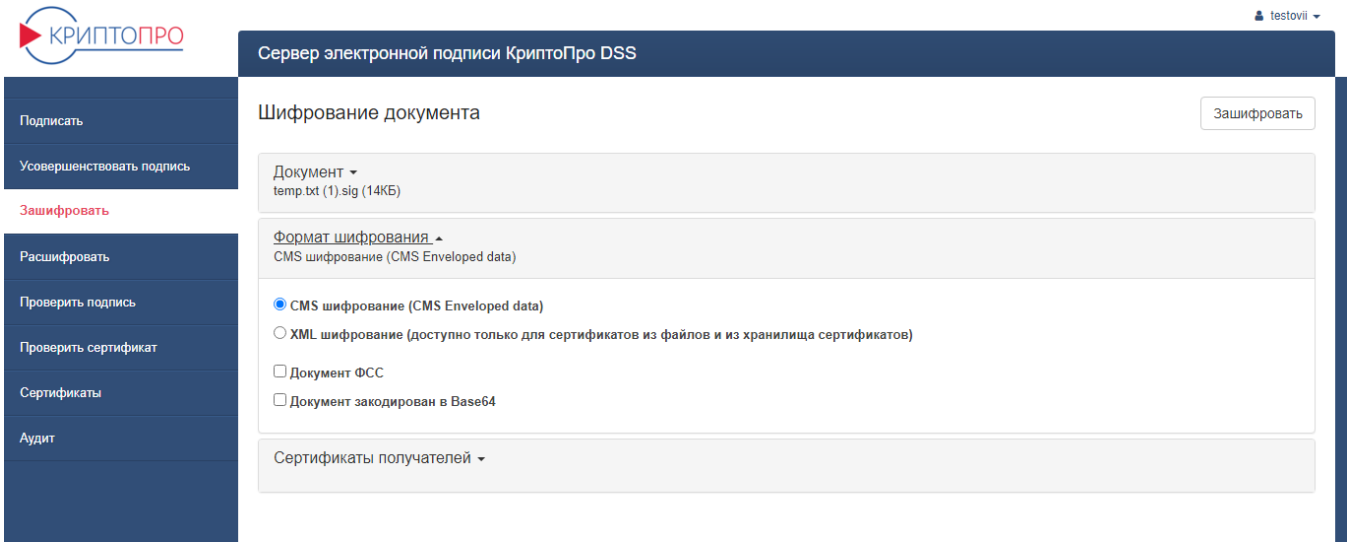

Рисунок 27 - Параметры шифрования

4) Загрузить полученный зашифрованный электронный документ (см. Рисунок 28 -Шифрование электронного документа).

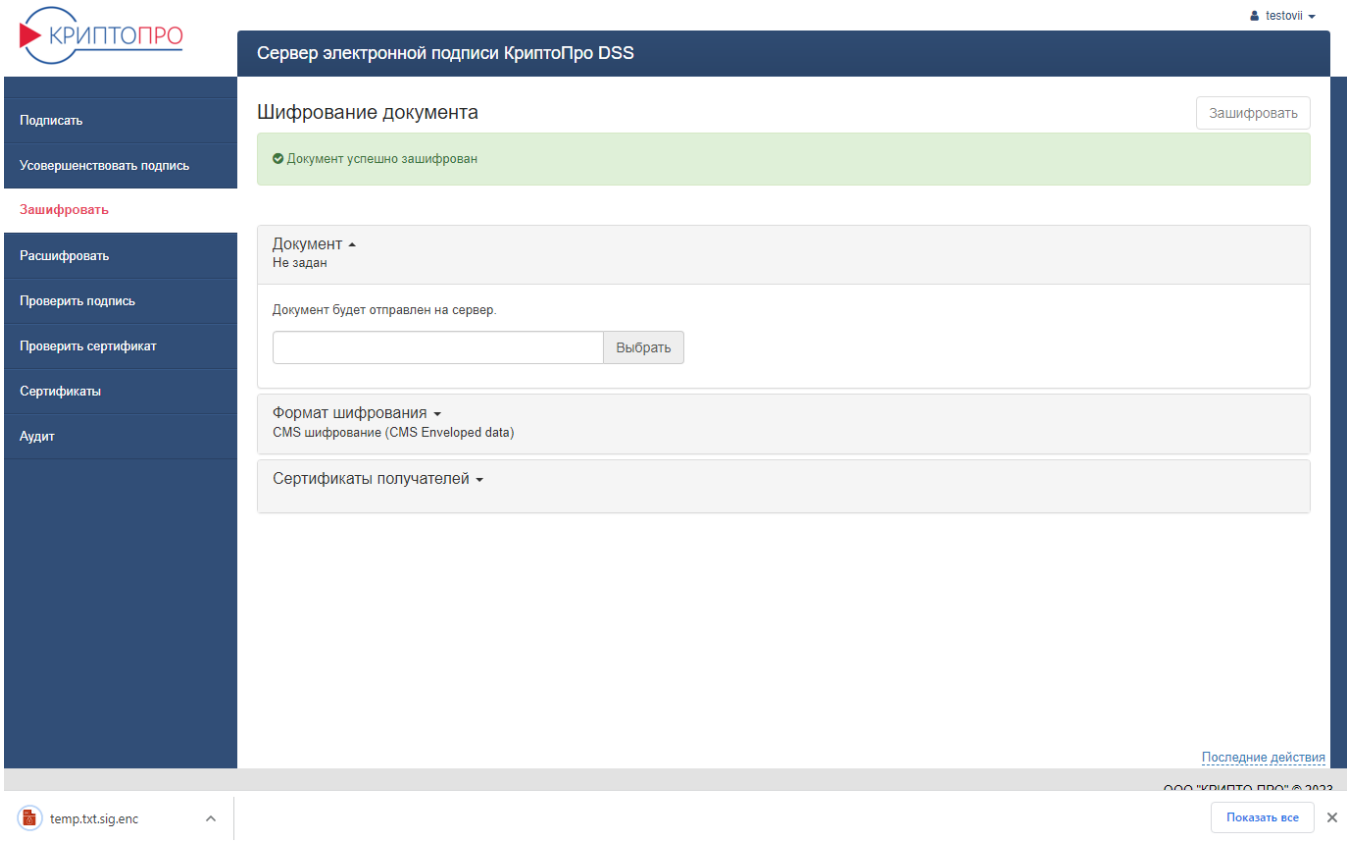

Рисунок 28 -Шифрование электронного документа

4.4. Раздел «Расшифровать»

Раздел предназначен для расшифрования электронных документов, зашифрованных для Пользователя. Для расшифрования электронного документа нужен зашифрованный файл электронного документа.

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

1) Загрузить зашифрованный для Пользователя файл электронного документа, который требуется 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***». (см. Рисунок 29 - Расшифрование электронного документа).

4) Загрузить расшифрованный электронный документ.

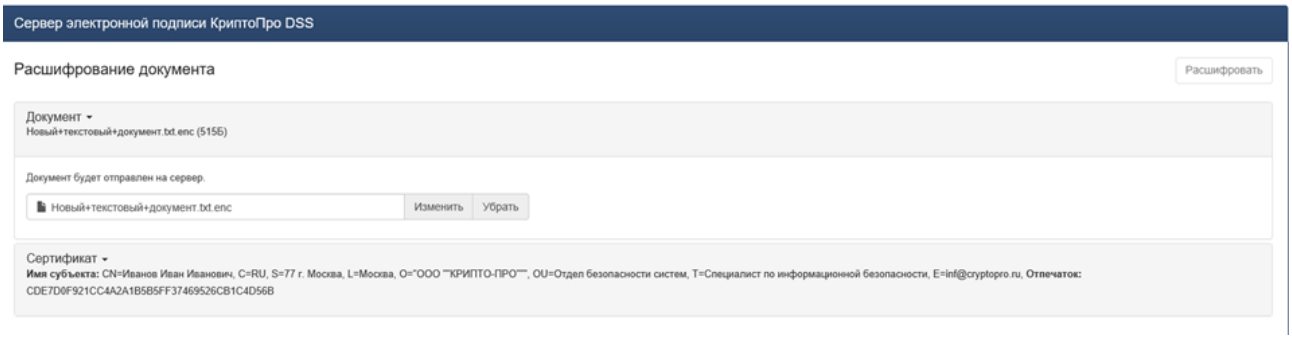

Рисунок 29 - Расшифрование электронного документа

4.5. 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 30 - Проверка подписи электронного документа).

6) Для присоединенной подписи также будет доступна кнопка «***Снять и проверить***», которая позволит получить исходный документ при корректной прохождении проверки.

7) Получить результат проверки подписи (см. Рисунок 31 - Результат проверки подписи).

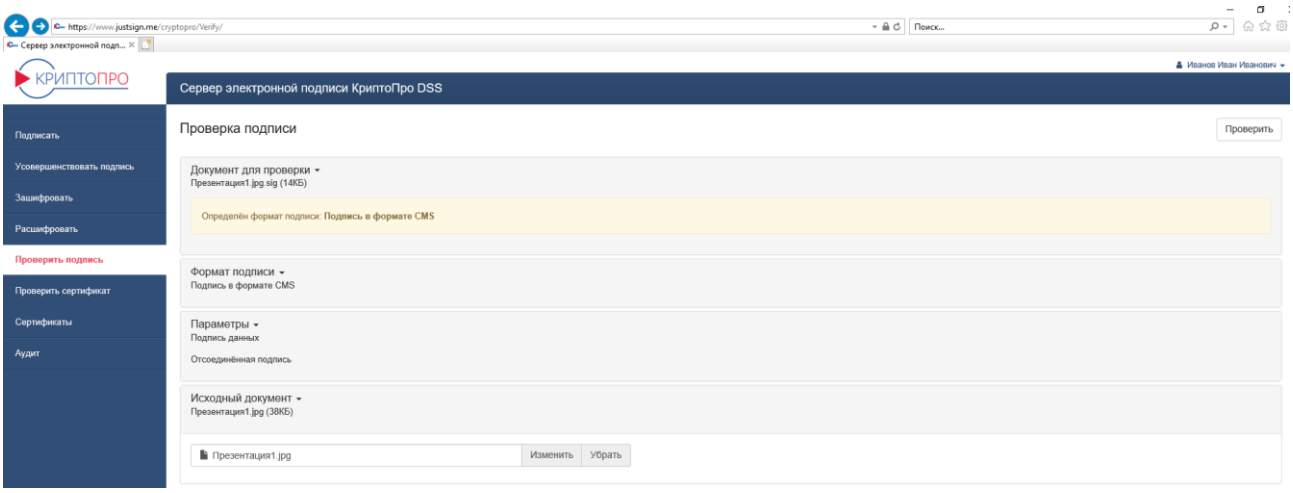

Рисунок 30 - Проверка подписи электронного документа

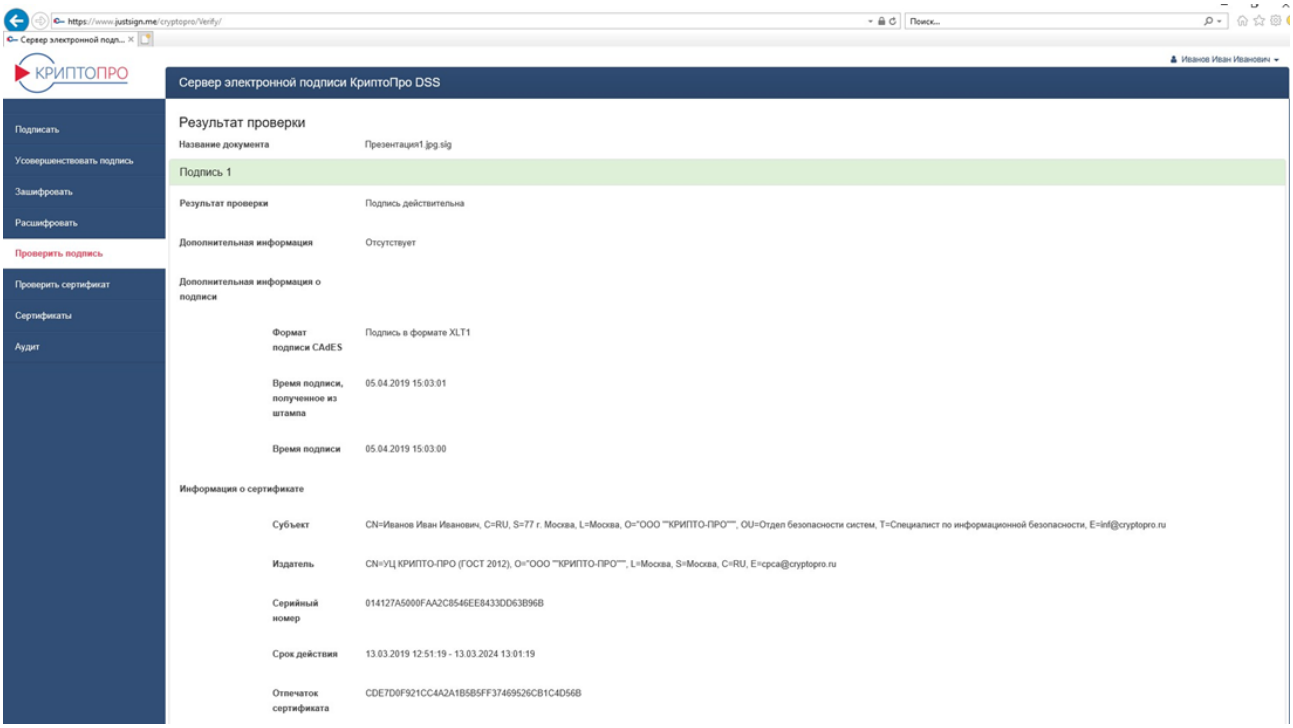

Рисунок 31 - Результат проверки подписи

4.6. 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 32 - Проверка статуса сертификата).

Получить результат проверки статуса сертификата (см. Рисунок 33 - Результат проверки статуса сертификата)

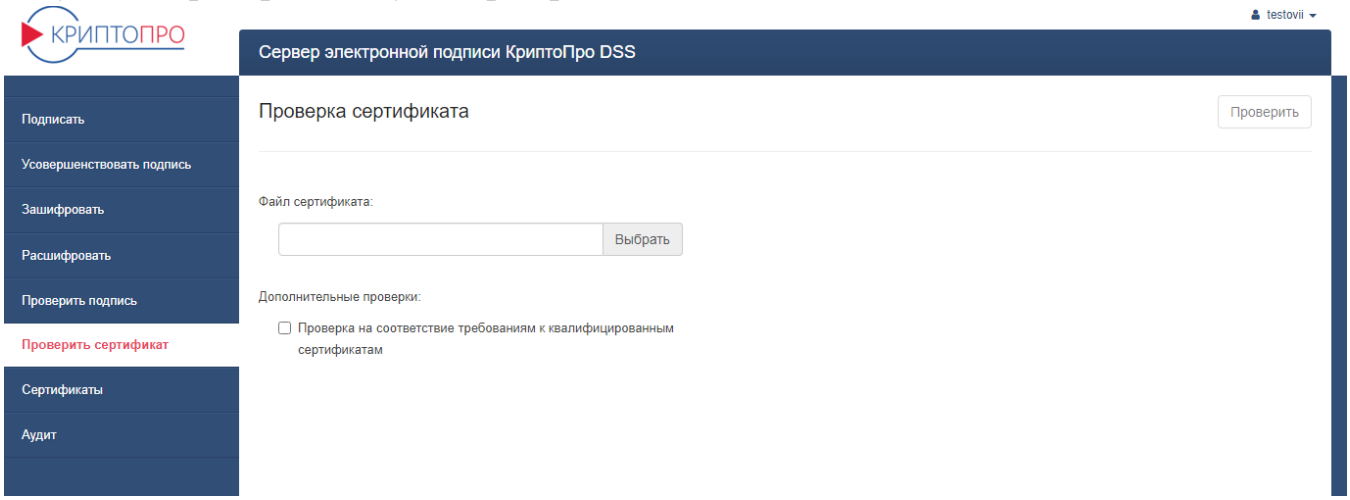

Рисунок 32 - Проверка статуса сертификата

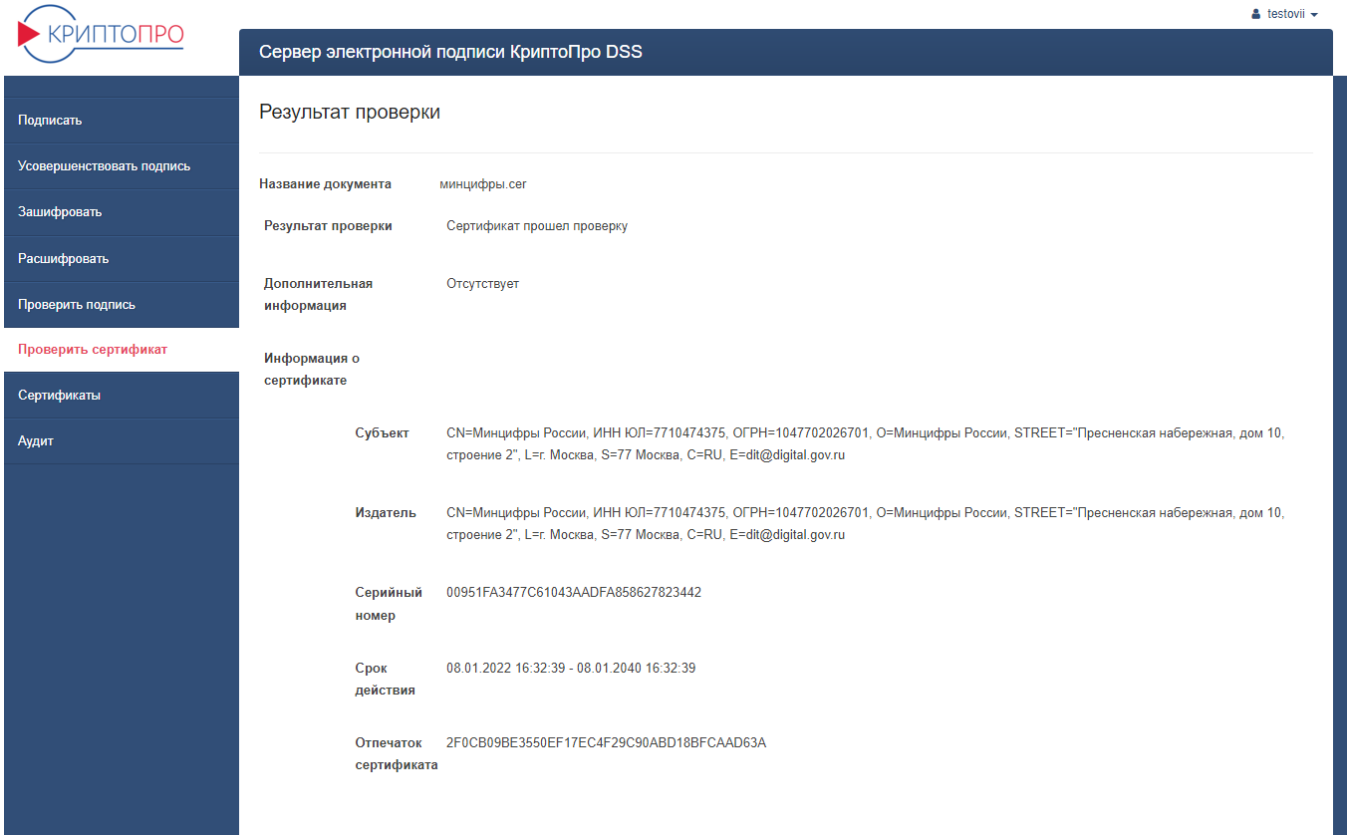

Рисунок 33 - Результат проверки статуса сертификата

4.7. Раздел «Сертификаты»

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

4.7.1. Создание запроса на сертификат

Для создания запроса на новый/первый сертификат Пользователя необходимо перейти в раздел «***Сертификаты***» и нажать кнопку «***Создать запрос на сертификат***» (см. Рисунок 34 – Вкладка «Сертификаты»).

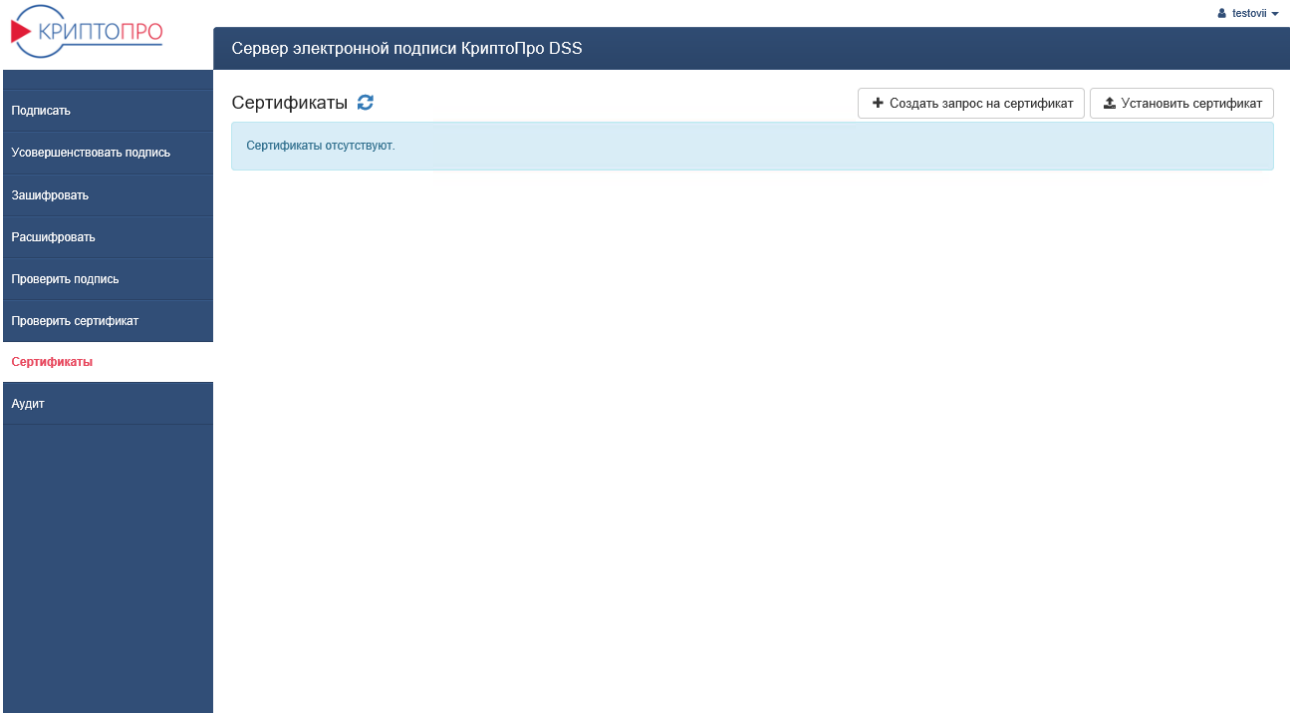

Рисунок 34 – Вкладка «Сертификаты»

Далее необходимо отредактировать данные Пользователя и нажать кнопку «***Создать запрос***» (см. Рисунок 35 - Создание запроса на сертификат), задать ПИН-код к ключу в СЭП и нажать кнопку «***ОК***».

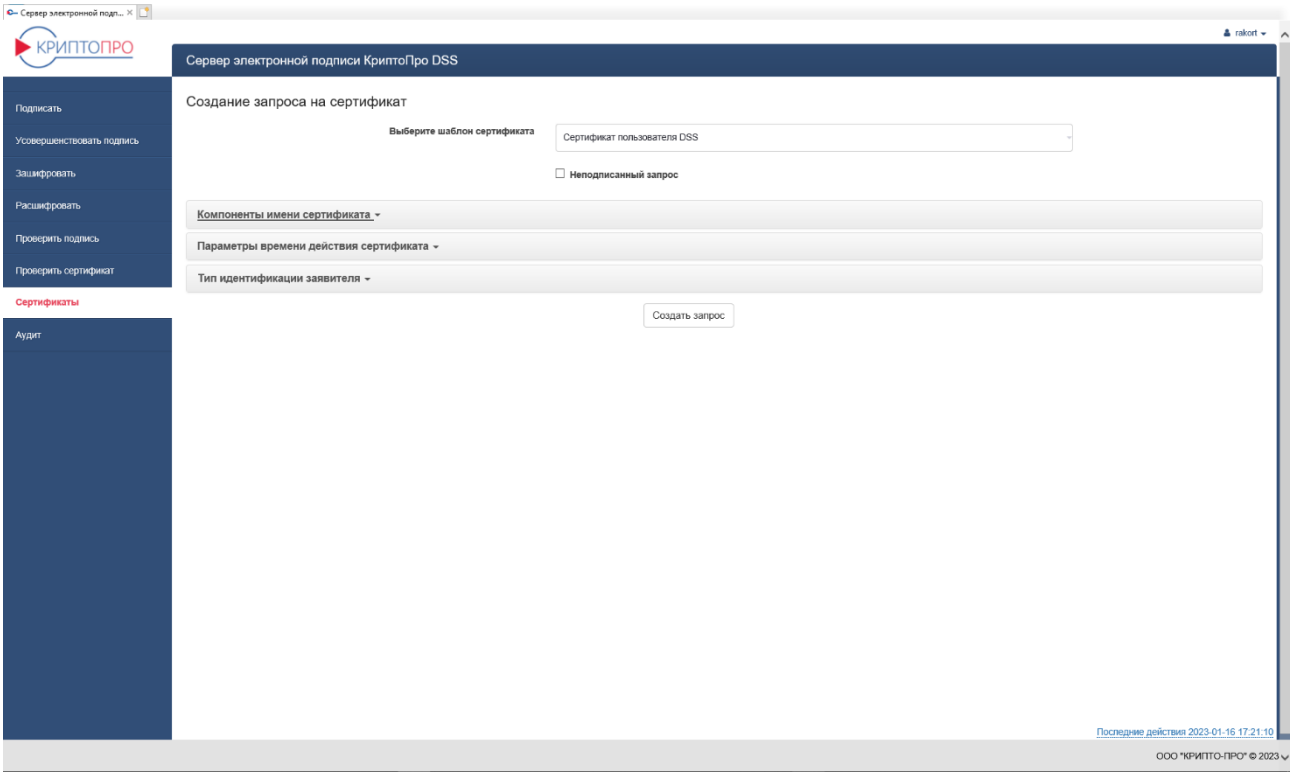

Рисунок 35 - Создание запроса на сертификат

При установке чекбокса «***Неподписанный запрос***» ключи пользователя будут храниться в мобильном устройстве.

После создания такого запроса его статус изменится на «***Ожидает подписи***» (см. Рисунок 36 - Неподписанный запрос).

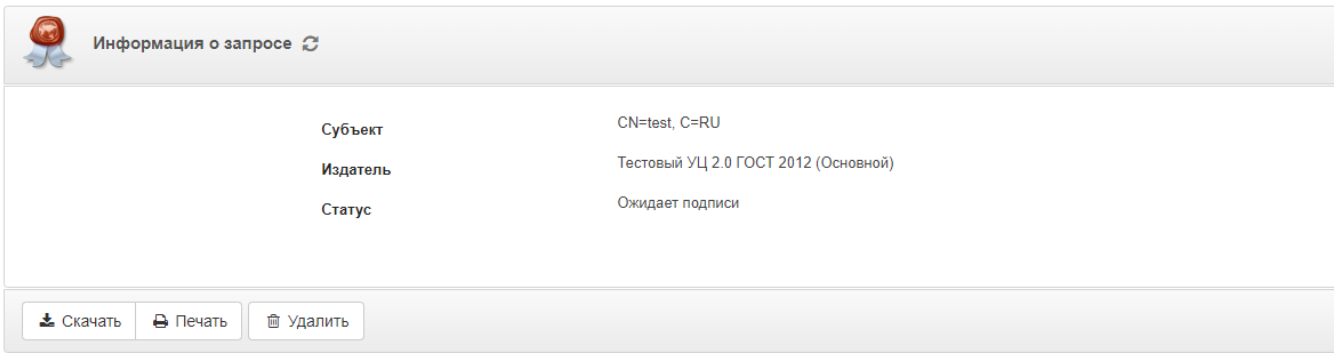

Рисунок 36 - Неподписанный запрос

Дальнейшие действия выполняются в мобильном приложении.

Необходимо открыть DSS Client перейти в «***Настройки***» - «***Сертификаты***» и нажать на созданный запрос со статусом «***Запрос на сертификат не подписан***».

Откроется информация о запросе, в данном окне нажмите кнопку «***Подписать запрос***». На следующем этапе откроется датчик случайных чисел, нажимайте на экран телефона для генерации ключей до тех пор, пока шкала в нижней части экране

не будет заполнена (см. Рисунок 37 - Подписание запроса в мобильном приложении).

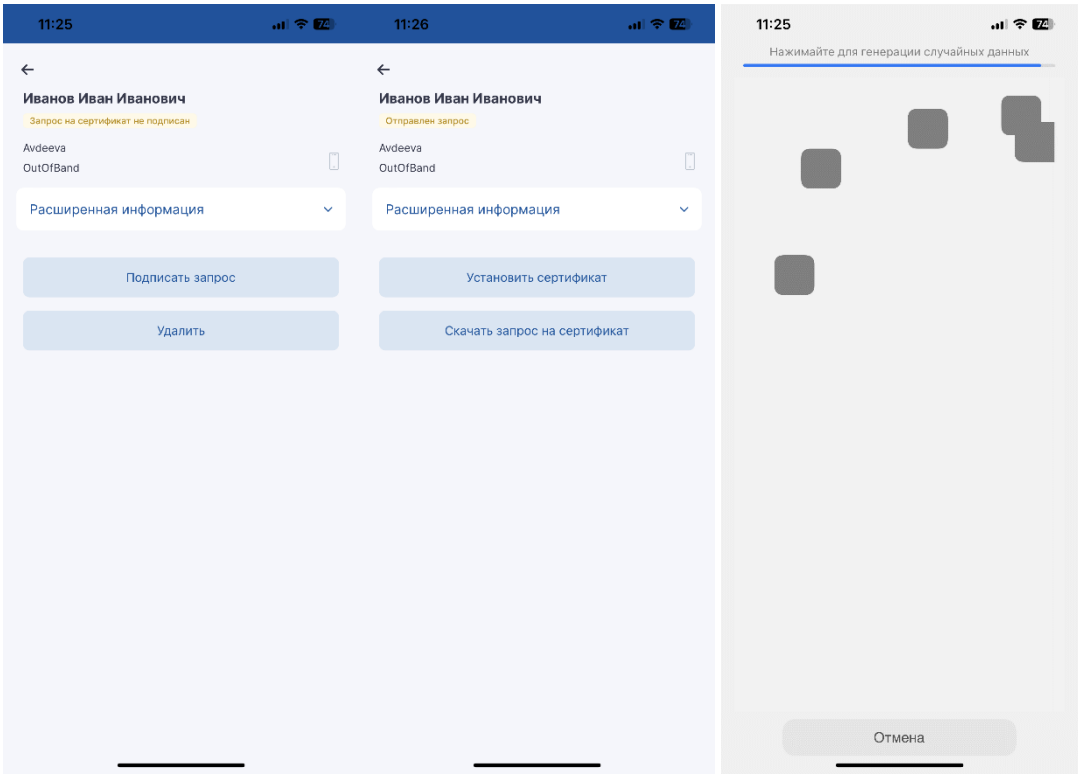

Рисунок 37 - Подписание запроса в мобильном приложении

После появления сообщения «***Запрос успешно подписан»*** запрос перейдет в мобильном приложении перейдет в статус «***Отправлен запрос***», а в веб-интерфейсе на «***Обрабатывается***» (см. Рисунок 38 - Информация о статусе запроса).

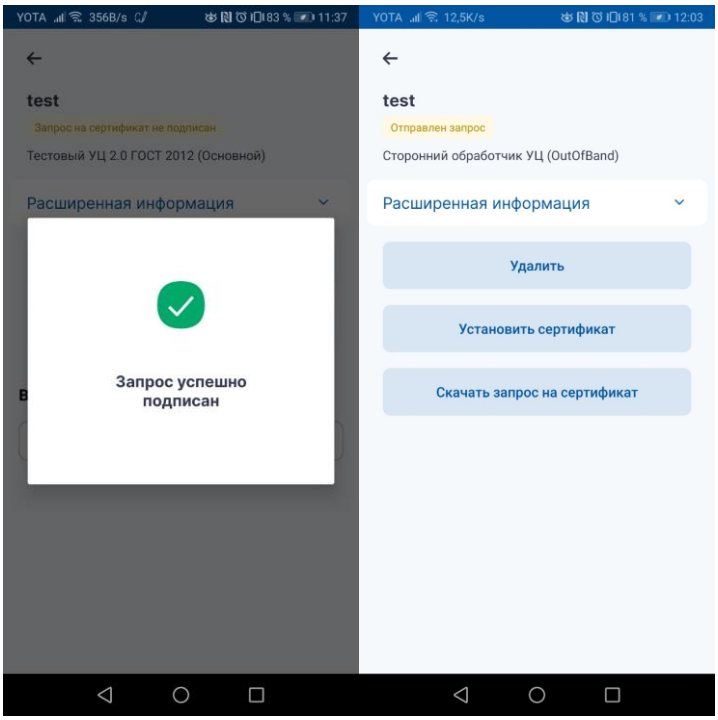

Рисунок 38 - Информация о статусе запроса

Данный запрос на сертификат можно:

- Скачать
- Распечатать
- Удалить

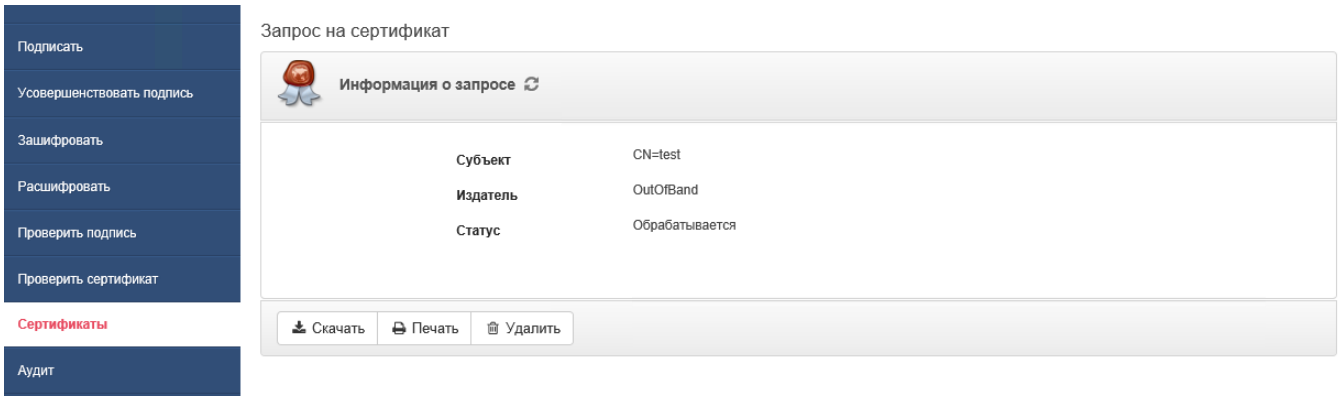

Рисунок 39 - Действия с запросом на сертификат

После получения сертификата его необходимо загрузить в СЭП. Для этого вернитесь на вкладку «***Сертификаты***» и нажмите кнопку «***Установить сертификат***» (см. Рисунок 34 – Вкладка «Сертификаты»).

В открывшемся окне нажмите «***Выбрать***» - выбрать файл сертификата на компьютере пользователя и нажмите «***Загрузить сертификат***» (см. Рисунок 40 - Загрузка нового сертификата).

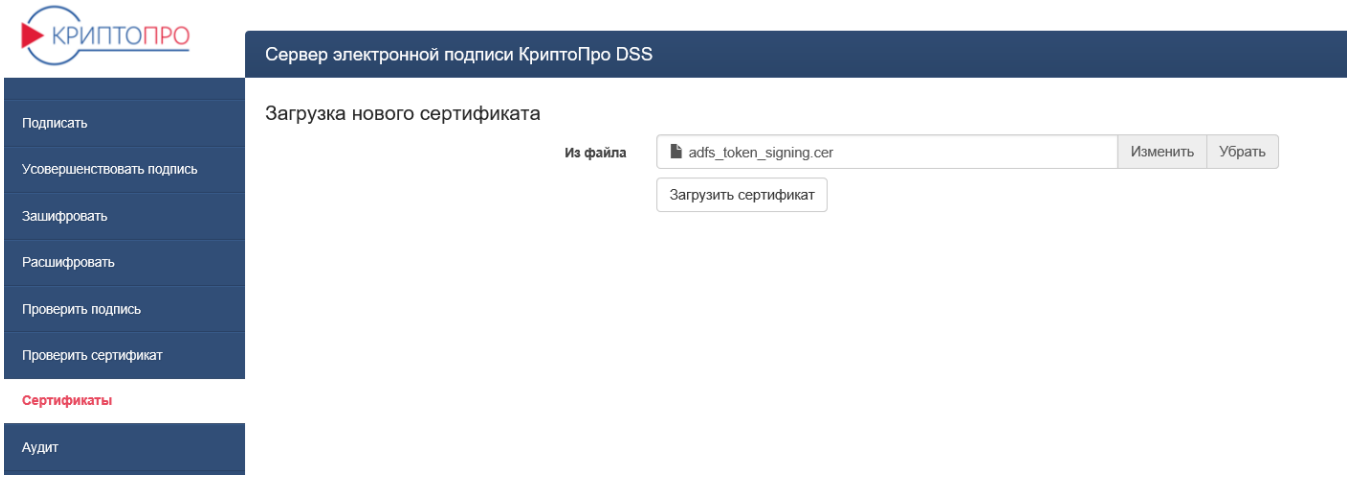

Рисунок 40 - Загрузка нового сертификата

4.7.2. Загрузка ключей из pfx

Экспорт ключей в pfx описан в разделе 5 данной инструкции (см. Экспорт ключа электронной подписи и сертификата ключа проверки электронной подписи)

Для загрузки ключей из pfx во вкладке «***Сертификаты***» нажмите «***Загрузить сертификат***» - «***Выбрать***» - выберите файл pfx на компьютере пользователя и нажмите «***Загрузить сертификат***» (см. Рисунок 40 - Загрузка нового сертификата).

4.8. Раздел «Аудит»

Раздел предназначен для отображения журнала событий, связанных с действиями Пользователей и Операторов в СЭП, совершенных над Пользователем с возможностью фильтрации по типам событий (см. Рисунок 41 - Журнал Аудита).

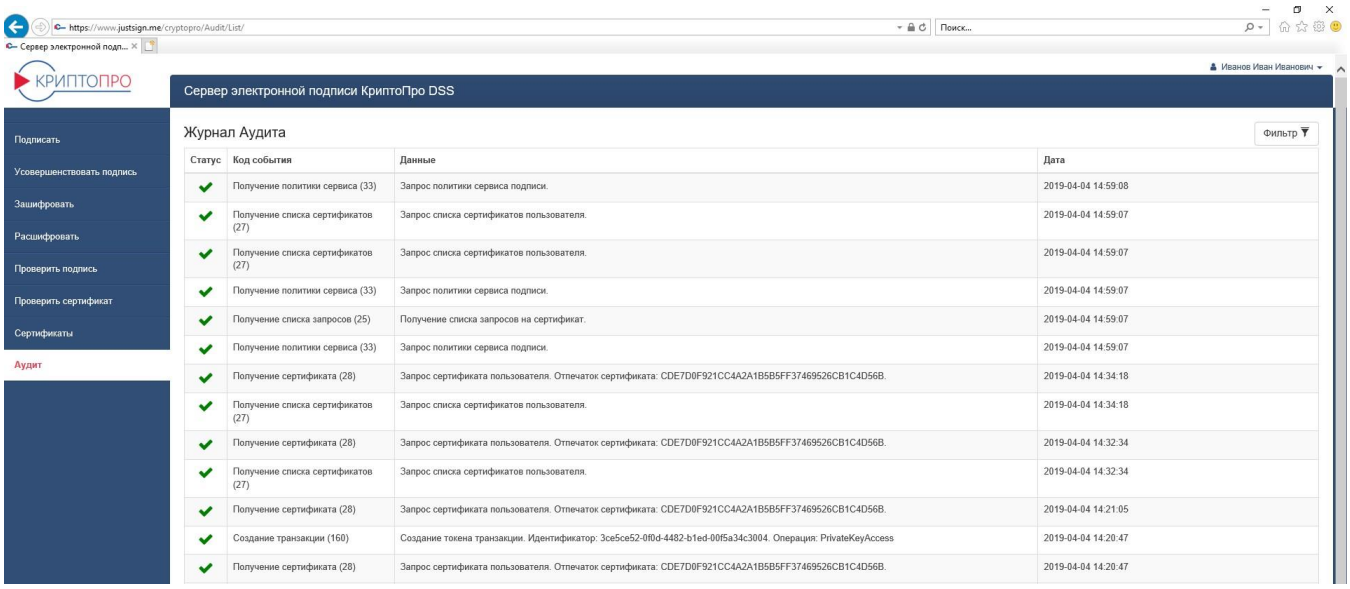

Рисунок 41 - Журнал Аудита

5. Экспорт ключа электронной подписи и сертификата ключа проверки электронной подписи

Импорт pfx описан в разделе 4.7.2 данной инструкции (см. Загрузка ключей из pfx).

5.1. ОС Windows

Для экспорта ключа подписи и сертификата ключа проверки электронной подписи необходимо запустить СКЗИ «КриптоПро CSP» перейти во вкладку «***Сервис***», нажать «***Просмотреть сертификаты в контейнере закрытого ключа***» (см. Рисунок 42 - Кнопка «Просмотреть сертификаты в контейнере»), через кнопку «***Обзор***» выбрать необходимый контейнер закрытого ключа (см. Рисунок 43 - Выбор ключевого контейнера).

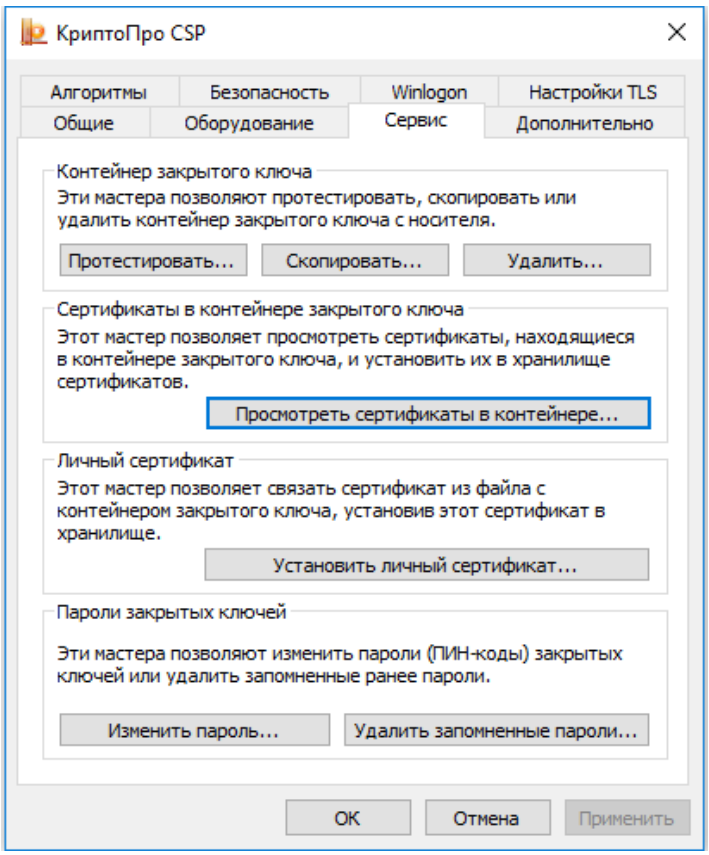

Рисунок 42 - Кнопка «Просмотреть сертификаты в контейнере»

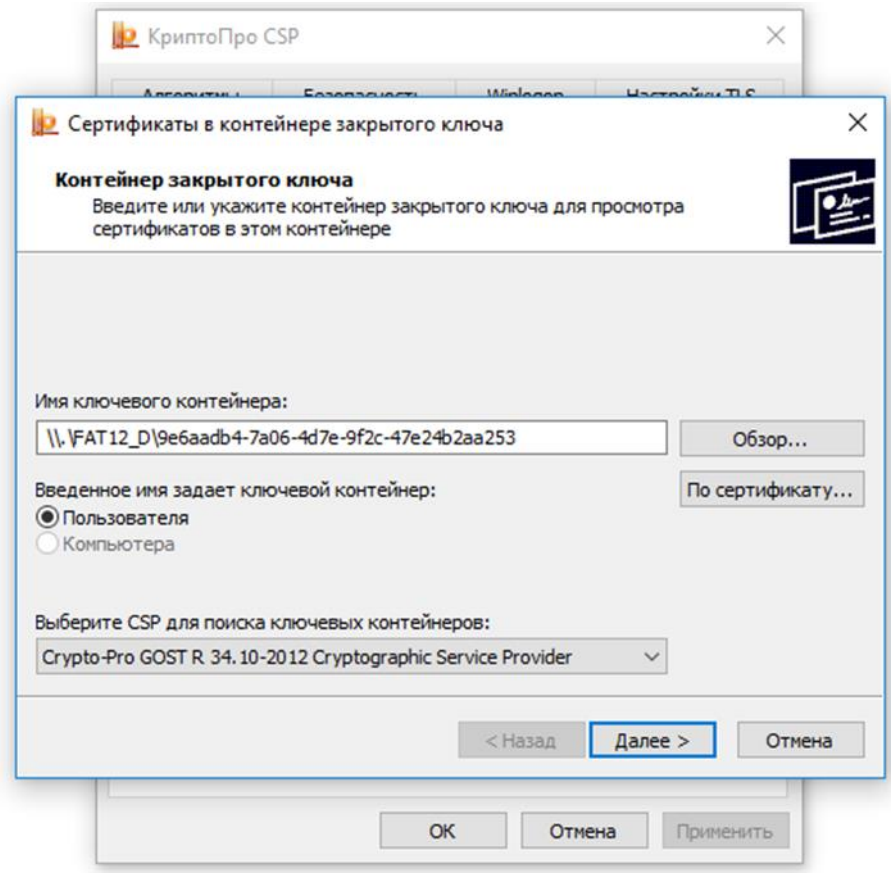

Рисунок 43 - Выбор ключевого контейнера

Нажать кнопку «***Свойства***», перейти во вкладку «***Состав***» и нажать «***Копировать в*** файл» (см.Рисунок 44 - Экспорт ключа).

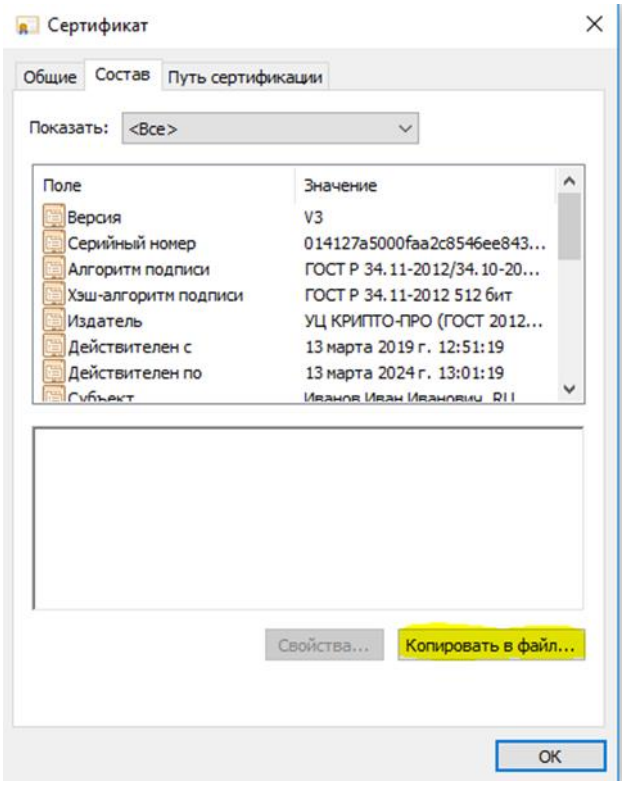

Рисунок 44 - Экспорт ключа

На следующем шаге выбрать «***Да, экспортировать закрытый ключ***» (см. Рисунок 45 - Экспортирование закрытого ключа).

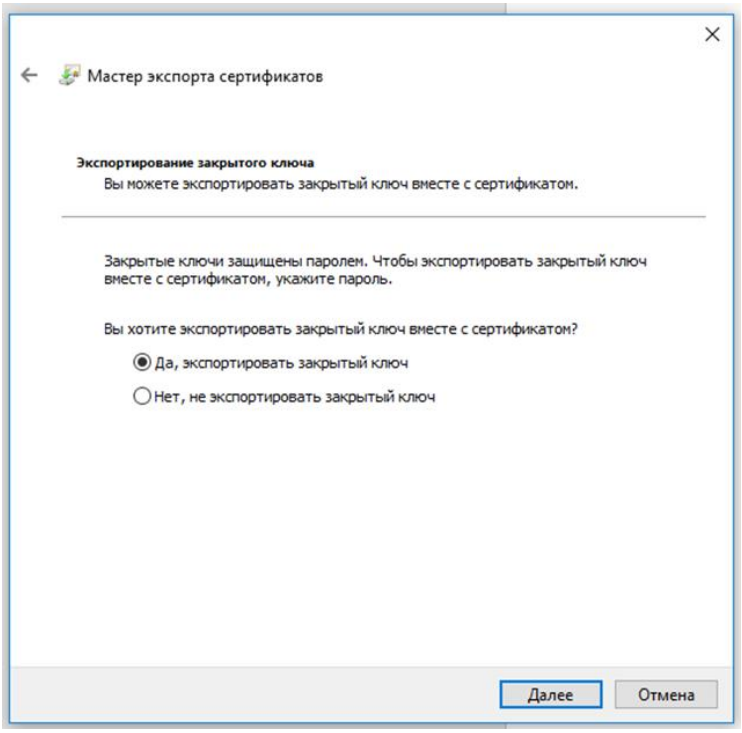

Рисунок 45 - Экспортирование закрытого ключа

На следующем шаге оставить все по умолчанию и нажать «***Далее***». Задать пароль, нажать «***Далее***». Выбрать директорию для сохранения файла (например, Рабочий стол) и задать имя файла, соглашаться с работой Мастера нажатием кнопки «***Дале***е» (см. Рисунок 46 - Экспорт ключа подписи и сертификата ключа проверки электронной подписи).

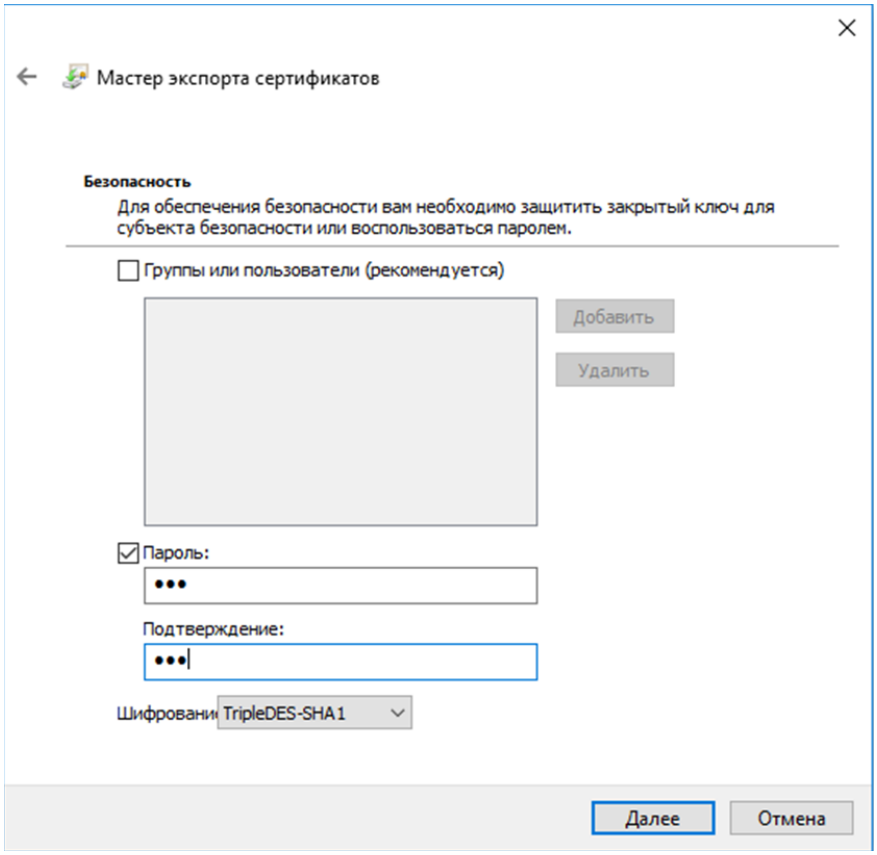

Рисунок 46 - Экспорт ключа подписи и сертификата ключа проверки электронной подписи

5.2. ОС Linux

Для экспорта ключа подписи и сертификата ключа проверки электронной подписи необходимо запустить cptools («Инструменты КриптоПро»).

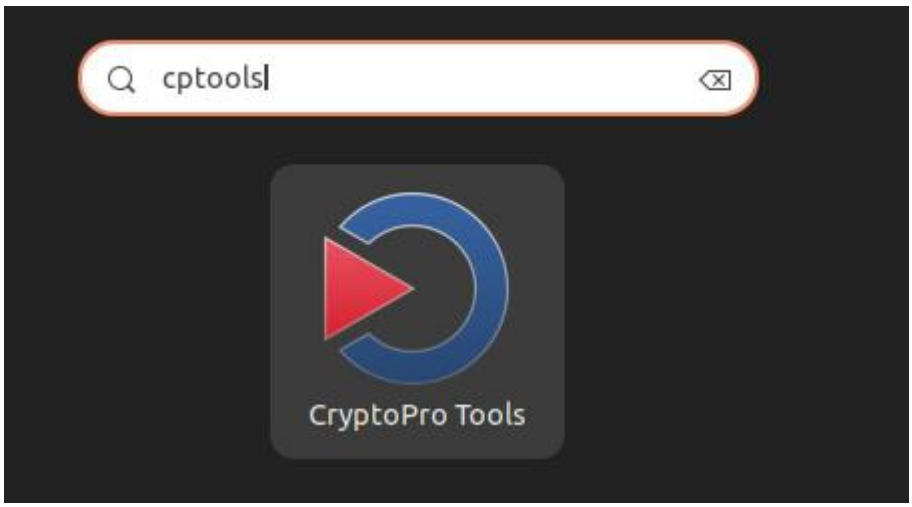

Рисунок 47 - Инструменты КриптоПро

Перейти во вкладку «***Сертификаты***» и выбрать нужный контейнер. Нажать кнопку «***Экспортировать ключи***».

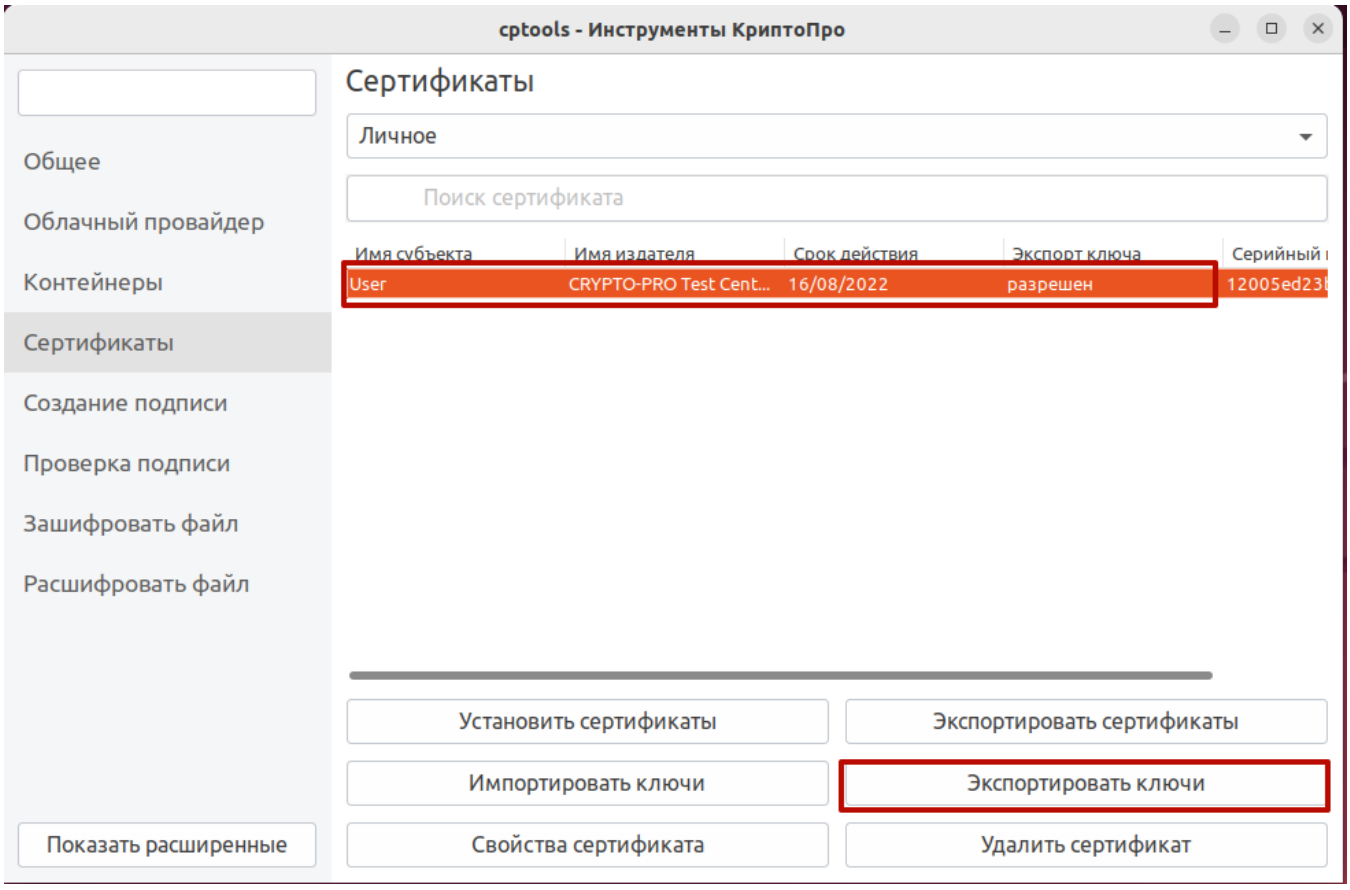

Рисунок 48 - Экспортировать ключи

Далее задать пароль на pfx и выбрать «***Экспортировать pfx в файл***» (см. Рисунок 49 - Параметры экспорта ключа)

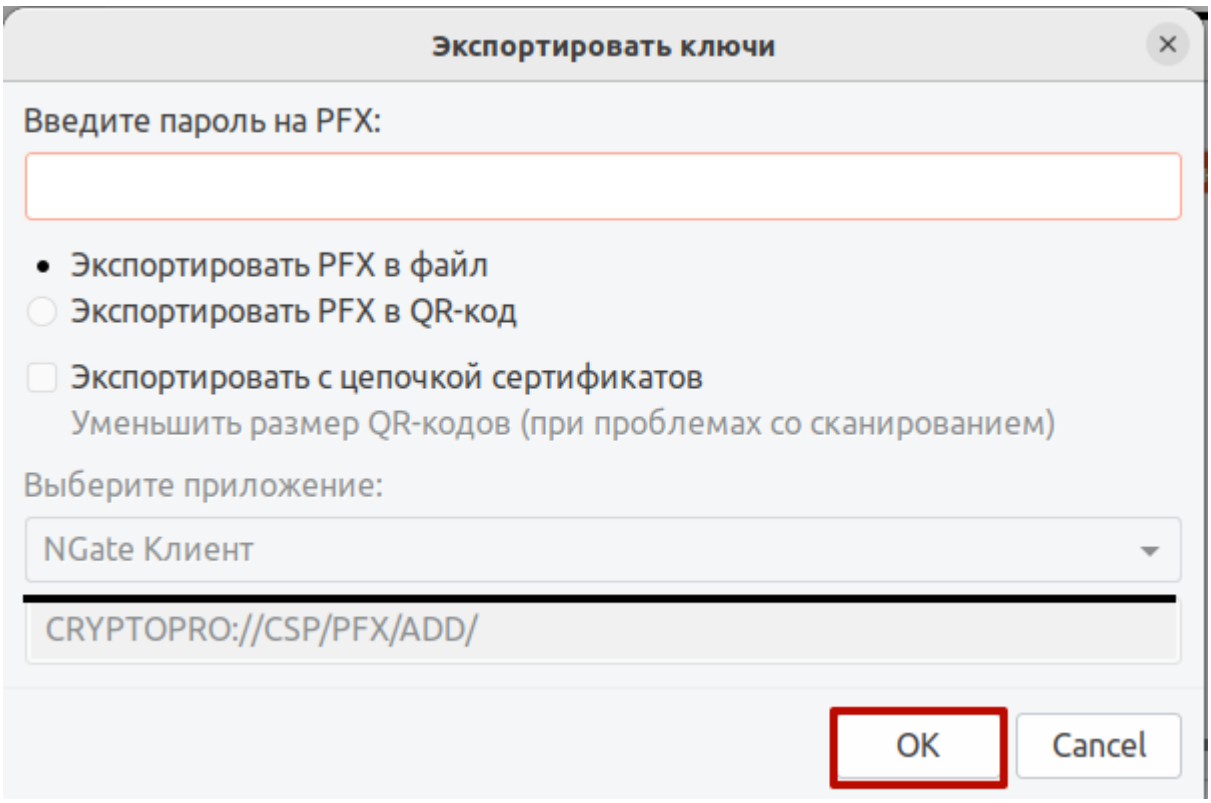

Рисунок 49 - Параметры экспорта ключа

На последнем этапе выберите место сохранения файла и имя.

5.3. ОС macOS

Необходимо использовать Криптопро CSP 5.0.

Для экспорта ключа подписи и сертификата ключа проверки электронной подписи необходимо последовательно открыть «Finder -> Программы -> Инструменты КриптоПро». Открыть вкладку «***Сертификаты***» и нажать кнопку «***Экспортировать ключи***» (см. Рисунок 50 - Экспортировать ключи).

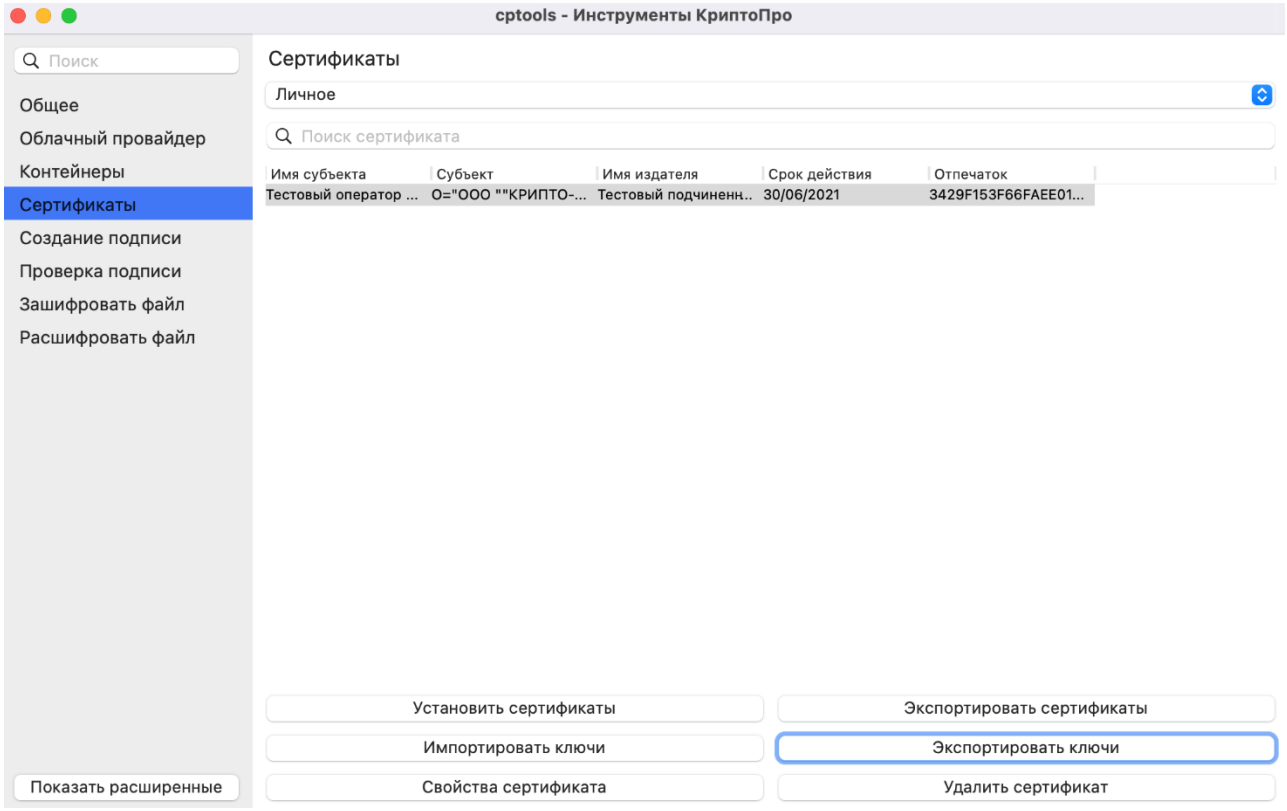

Рисунок 50 - Экспортировать ключи

Далее задать пароль на pfx и выбрать «***Экспортировать pfx в файл***» (см. Рисунок 51 - Меню экспорта)

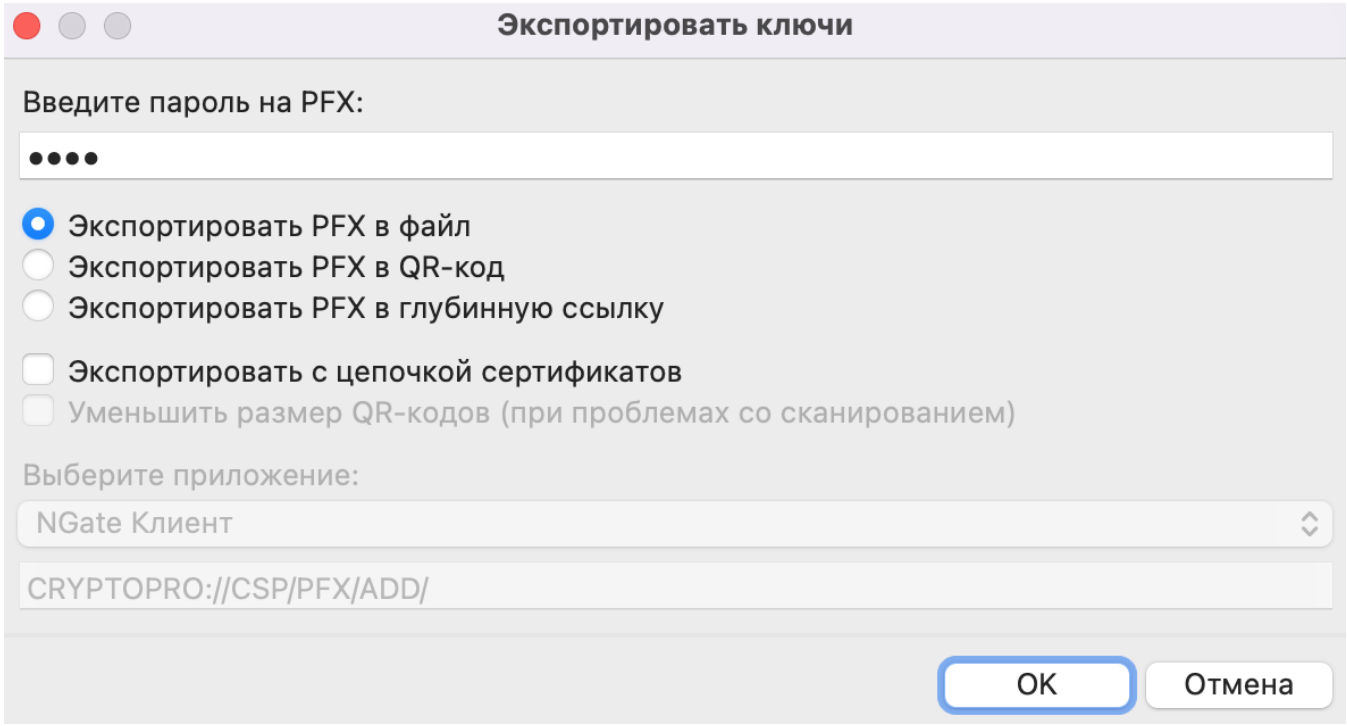

Рисунок 51 - Меню экспорта

Указать место сохранения и имя файла и нажать кнопку «***Save***» (см. Рисунок 52 - Сохранение pfx).

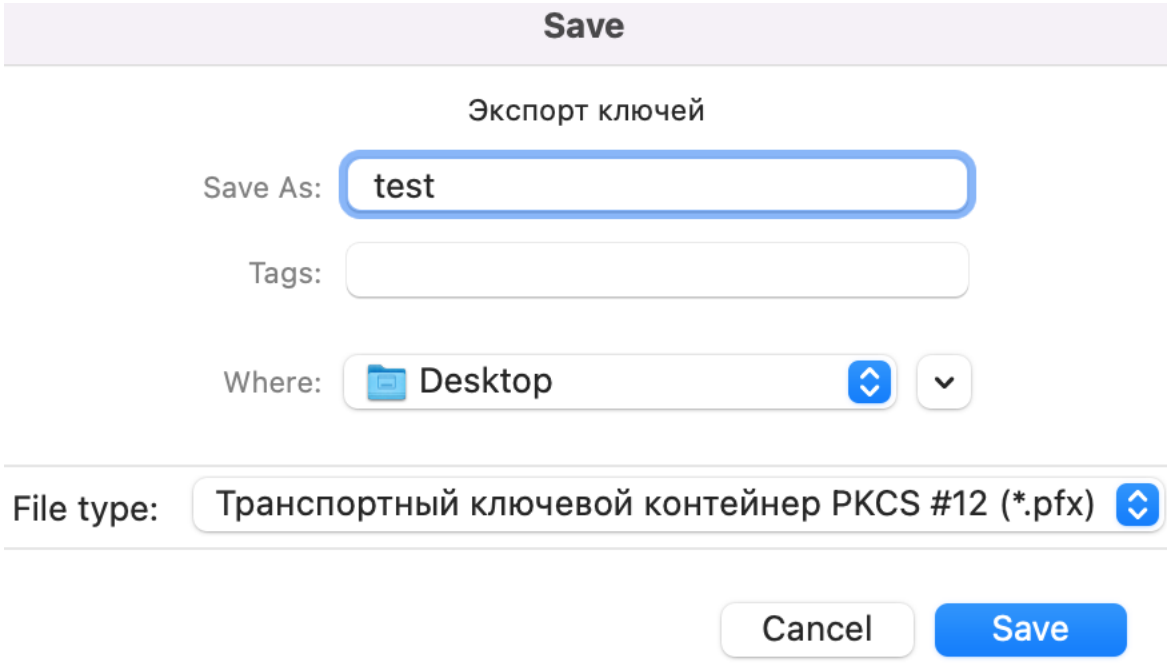

Рисунок 52 - Сохранение pfx

Экспорт успешно выполнен.

6. 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 «saas.cryptopro.ru»):

3) Сервер авторизации: https://saas.cryptopro.ru:4433/cryptoproidp/oauth;

4) Сервер DSS: https://saas.cryptopro.ru:4433/cryptopross/rest (см. Рисунок 53 - Настройки облачного провайдера), после чего нажать кнопку «***Установить сертификаты***».

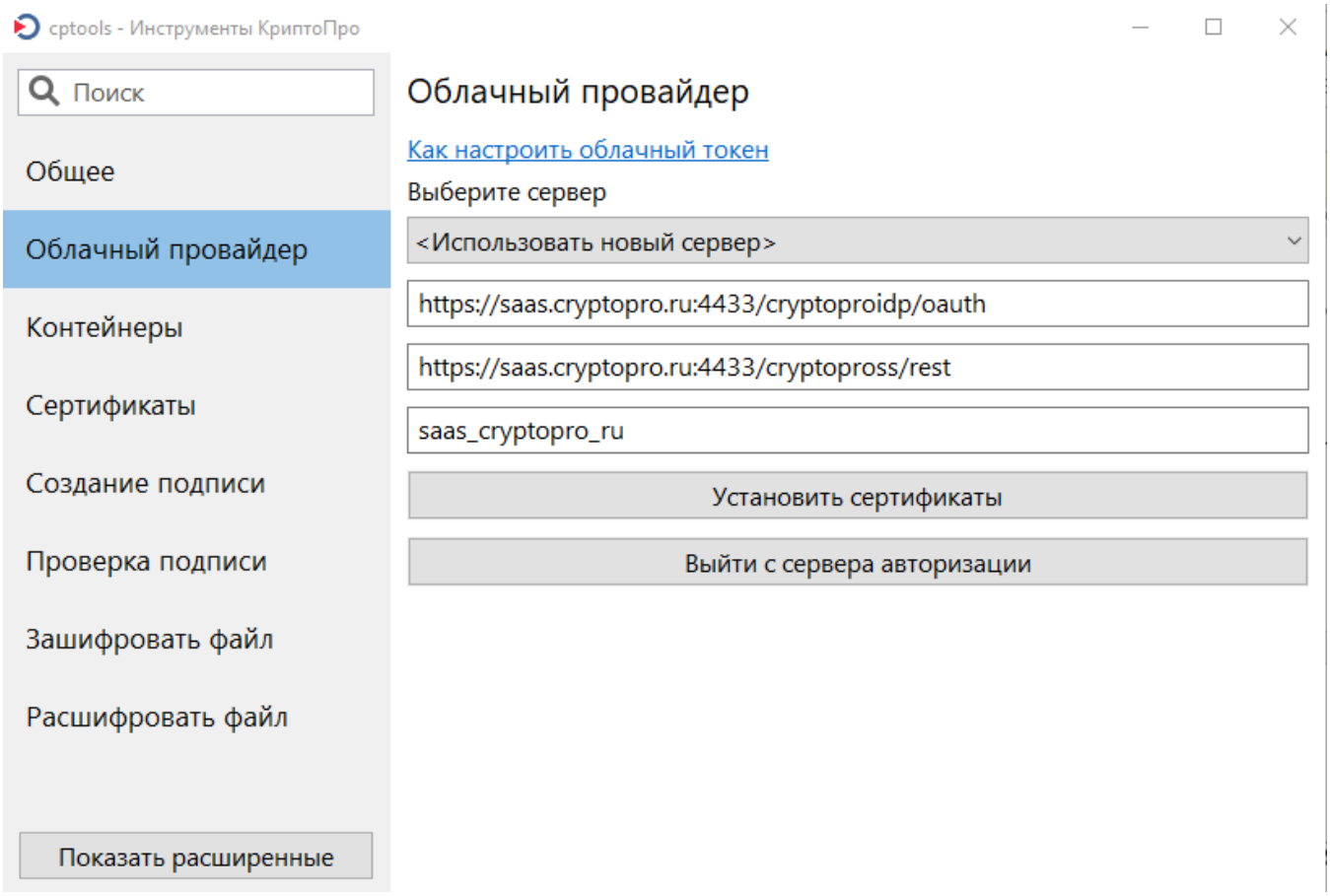

Рисунок 53 - Настройки облачного провайдера

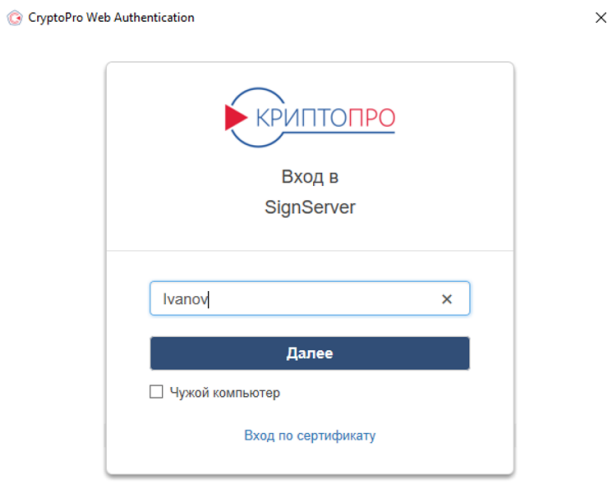

Рисунок 54 - Ввод учетной записи пользователя

Теперь необходимо пройти аутентификацию в СЭП. В окне «***CryptoPro Web Authentication***» для этого понадобится указать имя Пользователя в экземпляре СЭП и нажать кнопку «***Далее***» (см. Рисунок 54 - Ввод учетной записи пользователя).

После этого в появившуюся форму ввести пароль Пользователя и нажать

кнопку «***Войти***» (см. Рисунок 55 - Ввод пароля пользователя).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом.

На следующем шаге будет отображено сообщение об успешной установке сертификатов Пользователя.

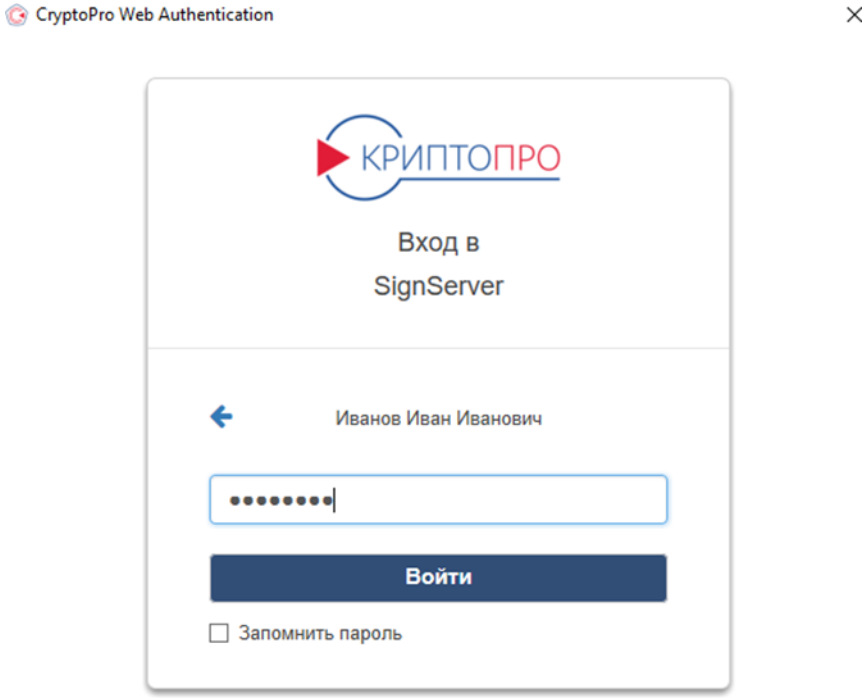

Рисунок 55 - Ввод пароля пользователя

«Облачный» ключевой контейнер можно увидеть во вкладке «***Контейнеры***» (см. Рисунок 56 - «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.

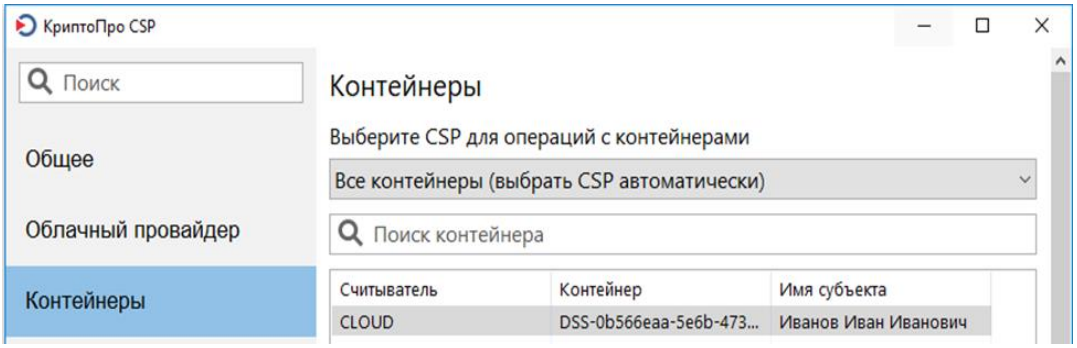

Рисунок 56 - «Облачный» контейнер

7. Работа с порталами органов государственной власти

7.1. Установка КриптоПро ЭЦП Browser plug-in

Необходимо перейти на страницу:
https://www.cryptopro.ru/products/cades/plugin
и скачать актуальную версию КриптоПро ЭЦП Browser plug-in.
Далее перейти на тестовую страницу:
https://www.cryptopro.ru/sites/default/files/products/cades/demopage/main.html
и попробовать подписать данные.

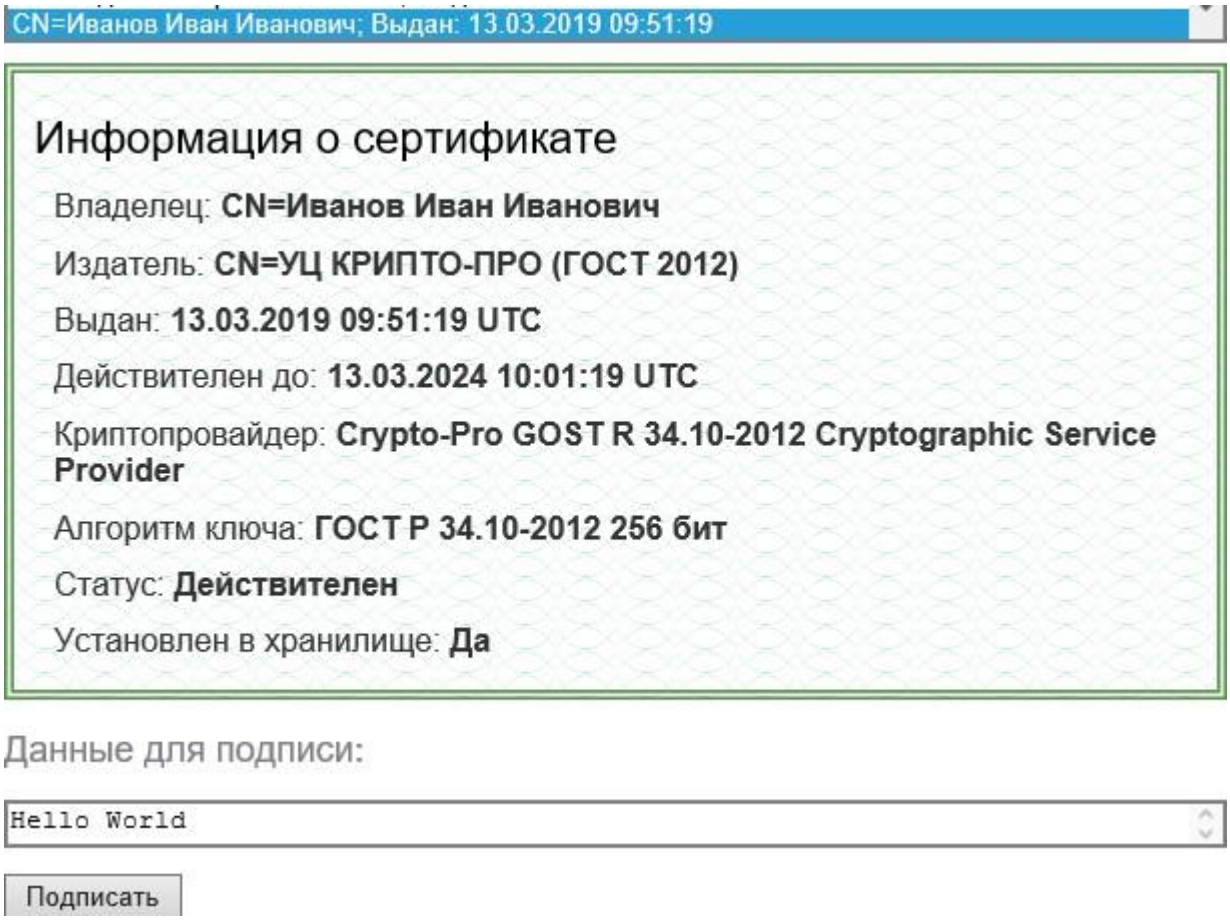

Рисунок 57 - Подпись данных

Далее необходимо пройти аутентификацию в СЭП. В окне «***CryptoPro Web Authentication***» укажите имя Пользователя в экземпляре СЭП и нажмите кнопку «***Далее***» (см. Рисунок 54 - Ввод учетной записи пользователя).

После этого в появившуюся форму введите пароль Пользователя и нажмите кнопку «Войти» (см. Рисунок 55 - Ввод пароля пользователя).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом (см Рисунок 15 - Информация об учетной записи пользователя).

Результатом является успешное подписание данных (см. Рисунок 58 - Результат подписи данных).

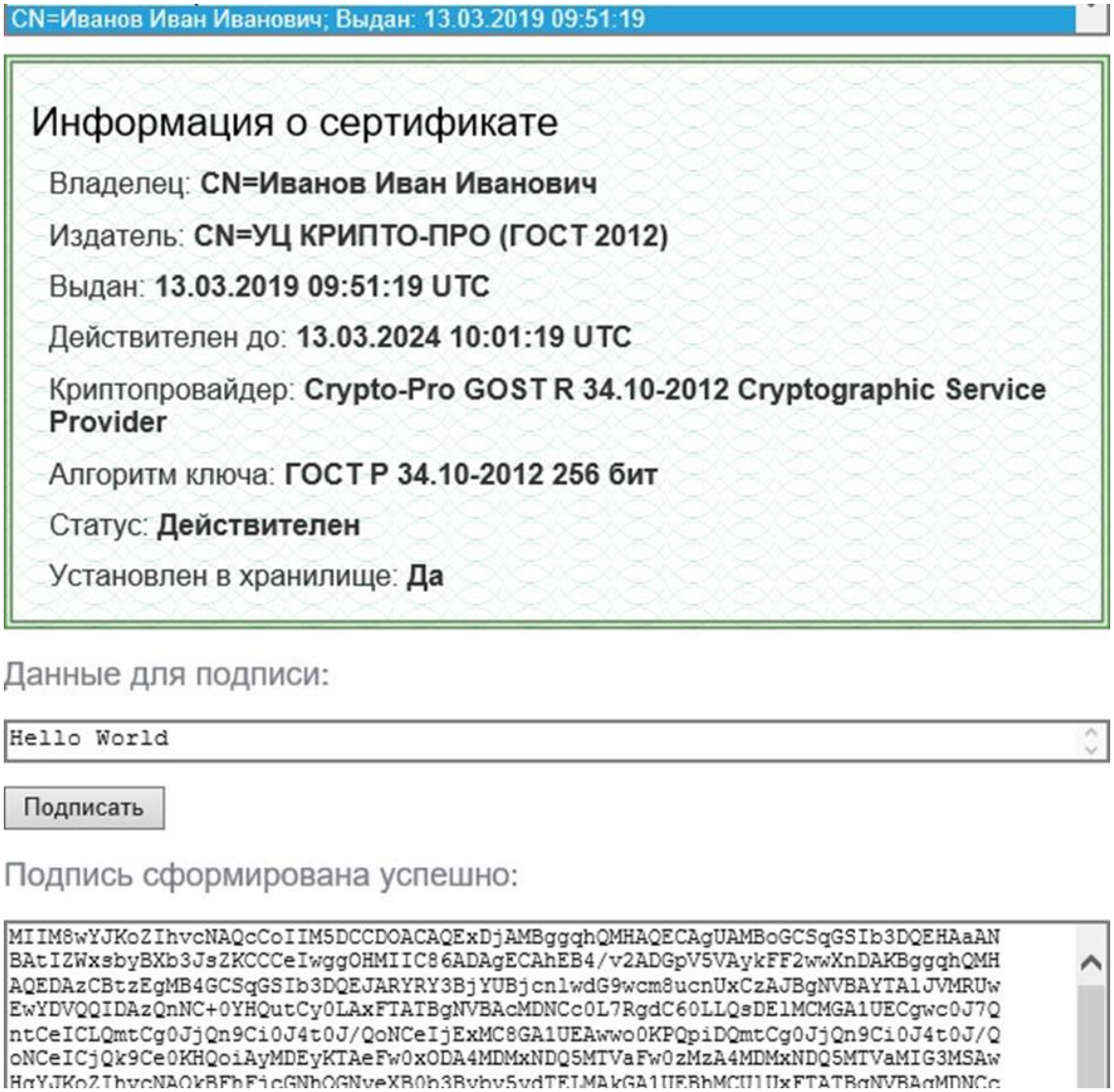

Рисунок 58 - Результат подписи данных

7.2. Работа с порталом nalog.ru

Необходимо перейти по адресу https://lkfl2.nalog.ru/lkfl/login, выбрать «***Войти с помощью ЭП***».

Выполнить все рекомендации, приведенные на странице «***Вход в Личный кабинет***». Выбрать сертификат и нажать «***Войти***».

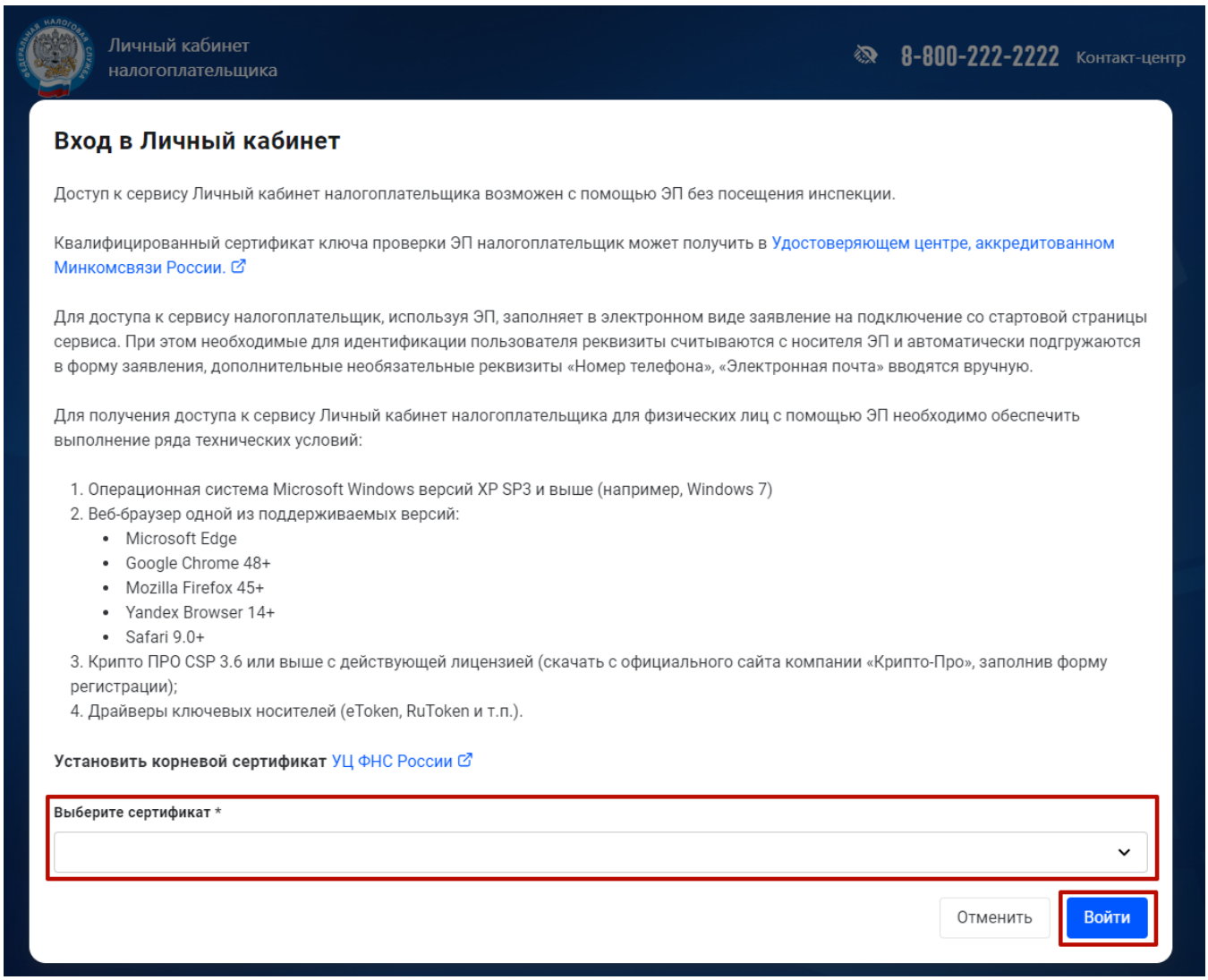

Рисунок 59 - Вход в личный кабинет nalog.ru

Далее необходимо пройти аутентификацию в СЭП. В окне «***CryptoPro Web Authentication***» для этого укажите имя Пользователя в экземпляре СЭП и нажмите кнопку «***Далее***» (см. Рисунок 54 - Ввод учетной записи пользователя).

После этого в появившуюся форму введите пароль Пользователя и нажмите кнопку «Войти» (см. Рисунок 55 - Ввод пароля пользователя).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом (см. Рисунок 60 - Вход в личный кабинет gosuslugi.ru).

7.3. Работа с порталом www.gosuslugi.ru

Необходимо перейти на страницу www.gosuslugi.ru, перейти в раздел «***Личный кабинет***», выбрать «***Вход с помощью электронной подписи***» -> «***Готово***».

Для входа в личный кабинет необходимо установить плагин:

https://ds-plugin.gosuslugi.ru/plugin/upload/Index.spr

Если плагин установлен, то появится окно выбора сертификата (см. Рисунок 60 - Вход в личный кабинет gosuslugi.ru).

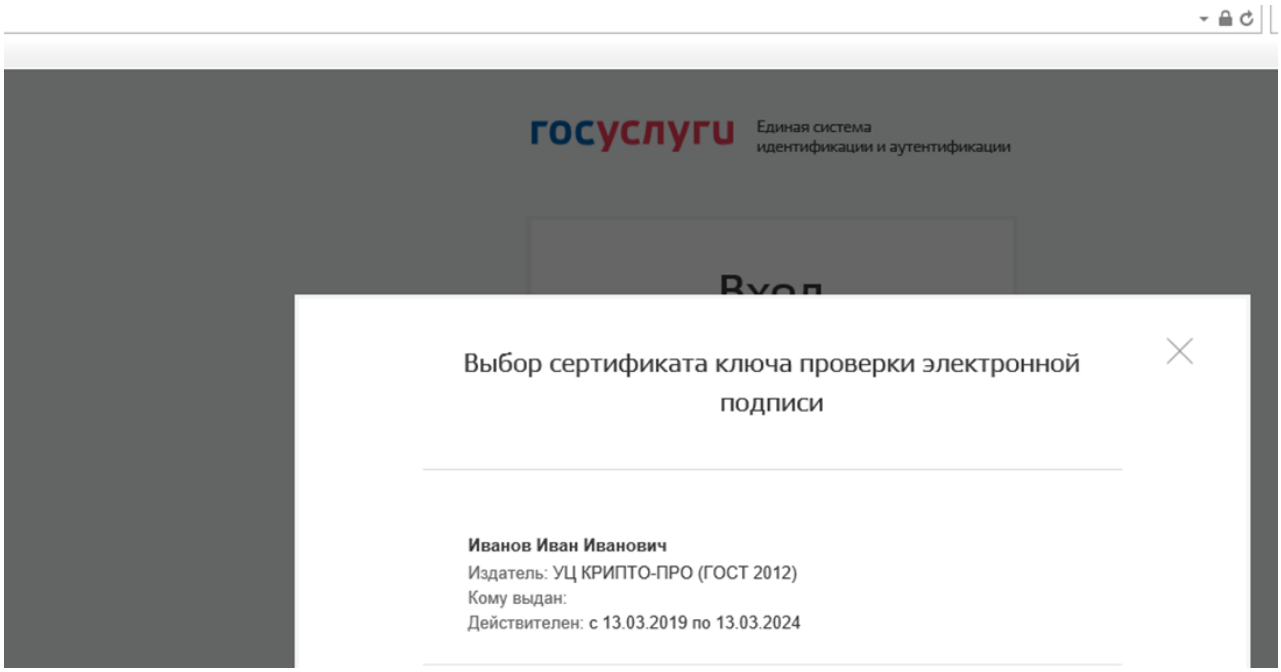

Рисунок 60 - Вход в личный кабинет gosuslugi.ru

Далее необходимо пройти аутентификацию в СЭП. В окне «***CryptoPro Web Authentication***» для этого укажите имя Пользователя в экземпляре СЭП и нажмите кнопку «***Далее***» (см. Рисунок 54 - Ввод учетной записи пользователя).

После этого в появившуюся форму введите пароль Пользователя и нажмите кнопку «Войти» (см. Рисунок 55 - Ввод пароля пользователя).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом.

8. Интеграция СЭП с использованием методов REST API

Для обеспечения возможности интеграции с СЭП сторонних прикладных систем, с использованием методов REST API, необходимо отправить запрос на почту operdss@cryptopro.ru, в котором требуется перечислить список методов, планируемых к использованию. С полным списком можно ознакомиться в руководстве разработчика КриптоПро DSS: https://dss.cryptopro.ru/docs/articles/intro.html

9. Безопасность при работе в СЭП

Для создания квалифицированной электронной подписи Пользователем УЦ используется СЭП на базе ПАМК «КриптоПро HSM» версии 2.0.

Ключи электронной подписи Пользователя УЦ формируются и хранятся в СЭП в неизвлекаемом формате, т.е. недоступном для выгрузки и сохранения на съемные носители, мобильные устройства и рабочие места Пользователя УЦ.

При создании ключа электронной подписи в СЭП Пользователем УЦ может быть установлен индивидуальный PIN-код доступа к ключевому контейнеру, содержащему ключ электронной подписи.

Использование ключа электронной подписи должно подтверждаться владельцем соответствующего сертификата ключа проверки электронной подписи (Пользователем УЦ) с помощью:

- ключа аутентификации в мобильном приложении DSS Client из состава ПО «Модуль аутентификации DSS Client для ПАК «КриптоПро DSS» версии 2.0 (далее – Мобильное приложение) на мобильном устройстве Пользователя УЦ;
- а также (опционально) индивидуальным PIN-кодом доступа к ключевому контейнеру, содержащему используемый ключ электронной подписи Пользователя УЦ.

Работа Мобильного приложения обеспечивается при соответствии мобильного устройства Пользователя УЦ следующим техническим требованиям:

- операционная система iOS версий: 8/9/10/11 и выше;
- операционная система Android версий: 7.0 и выше.

Мобильное приложение должно устанавливаться из официальных источников:

- для ОС iOS: магазин приложений «App Store»;
- для ОС Huawei магазин приложений «AppGallery»;
- для ОС Android: магазин приложений «Google Play».

В целях исключения доступа посторонних лиц к Мобильному приложению Пользователям УЦ рекомендуется установить пароль для доступа к мобильному устройству и разблокировки экрана. В случае наличия в мобильном устройстве функции распознавания отпечатка пальца, ее также рекомендуется включить.

Для обеспечения безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи Пользователь УЦ должен:

• Хранить в тайне индивидуальный PIN-код доступа к ключевому контейнеру, аутентификационную информацию для доступа к СЭП, обеспечить сохранность персональных мобильных устройств, используемых для подтверждения использования ключа электронной подписи при подписании

электронного документа, принимать все возможные меры для предотвращения их потери, раскрытия и несанкционированного использования.

• Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

• Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия соответствующего сертификата ключа проверки электронной подписи и не применять данный ключ электронной подписи:

1) при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
2) в случае компрометации аутентификационной информации и утраты мобильных устройств, на которых установлено мобильное приложения DSS Client;
3) в случае, если Пользователю УЦ стало известно, что этот ключ электронной подписи используется или использовался ранее другими лицами, в том числе если Пользователь УЦ получил сообщение от СЭП о выполнении каких-либо операций от его имени в, то время, когда он их не выполнял.

• Использовать и регулярно обновлять средства антивирусной защиты в мобильных устройствах и на рабочих местах Пользователя УЦ.

10. Перечень рисунков