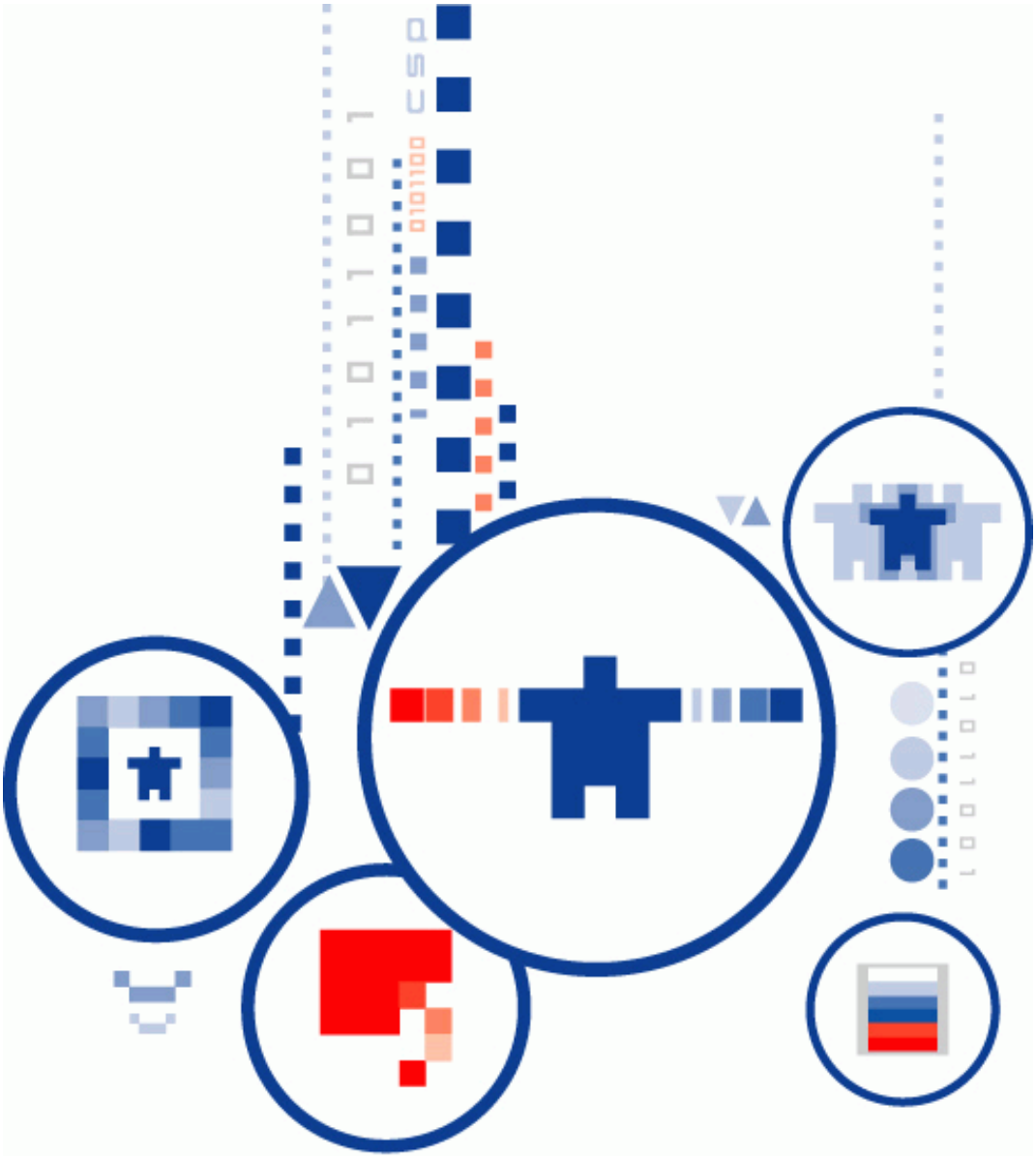

Программный комплекс

«КриптоПро Ключ»

Руководство Пользователя

ЖТЯИ.00118-01 93 01

Аннотация

Данный документ предназначен для Пользователей ПК «КриптоПро Ключ» (далее – Пользователей СЭП) и определяет порядок действий Пользователя при выполнении операций создания, 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.

Информация о разработчике:

ООО «Крипто-Про»
127 018, Москва, Улица Сущевский Вал, д.18, эт.17
Телефон: (495) 995 4820
https://www.cryptopro.ru/
E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Подготовка рабочего места Пользователя

В данном документе рассмотрены случаи, когда Пользователь осуществляет работу в СЭП с использованием Веб-интерфейса. В зависимости от используемого способа аутентификации Пользователя в Веб-интерфейсе и настроек сервера СЭП может потребоваться установка браузера, поддерживающего российские криптографические алгоритмы, а также СКЗИ КриптоПро CSP и КриптоПро ЭЦП Browser plug-in.

2. Аутентификация Пользователя

СЭП предоставляет методы первичной и вторичной аутентификации. Каждому Пользователю Оператором СЭП назначается как минимум один метод первичной аутентификации и, опционально, методы вторичной аутентификации. Заданные методы первичной и вторичной аутентификации, а также перечень операций, подтверждаемых Пользователем с их помощью, сообщаются Пользователю Оператором СЭП.

Возможные методы первичной аутентификации Пользователя:

- «*Только идентификация*» – первичная аутентификация Пользователя происходит посредством ввода наименования учетной записи Пользователя в СЭП (логин).
- «*Аутентификация по сертификату*» – первичная аутентификация Пользователя происходит по сертификату, выданному Пользователю Оператором. Если у Пользователя уже есть сертификат, он может быть использован для аутентификации при соблюдении следующих условий:
  - СЭП должен доверять издателю сертификата Пользователя;
  - компоненты имени сертификата, с использованием которого производится аутентификация Пользователя в СЭП, должны соответствовать компонентам личной информации Пользователя;
- «*Аутентификация по паролю*» – первичная аутентификация Пользователя происходит по паролю, выданному Пользователю Оператором СЭП либо сгенерированным\придуманным Пользователем самостоятельно при наличии соответствующих настроек СЭП.

Возможные методы вторичной аутентификации Пользователя:

- «*Аутентификация с помощью мобильного приложения*» – подтверждение действий Пользователя СЭП в мобильном приложении.
- «*Аутентификация по SMS*» – подтверждение действий Пользователя в СЭП по коду в SMS, отправляемых СЭП на мобильный телефон Пользователя; метод доступен только в случае, если задан номер мобильного телефона Пользователя. В тестовом СЭП не выполняется отправка реальных SMS-сообщений; используется эмуляция, посредством записи текста SMS-сообщений в текстовые файлы. Адрес, по которому публикуются файлы, предоставляется в списке данных для подключения.
- «*Аутентификация по протоколу OATH*» – подтверждение действий Пользователя в СЭП по одноразовому паролю OTP-токена; метод доступен только в случае, если заданы параметры OTP-токена.
- «*Аутентификация по электронной почте*» – подтверждение действий

Пользователя в СЭП по коду в сообщениях электронной почты, отправляемых СЭП на адрес электронной почты Пользователя; метод доступен только в случае, если задан адрес электронной почты Пользователя.

Для работы в СЭП Пользователю необходимо осуществить вход в Веб-интерфейс Пользователя с выбранным при регистрации методом аутентификации.

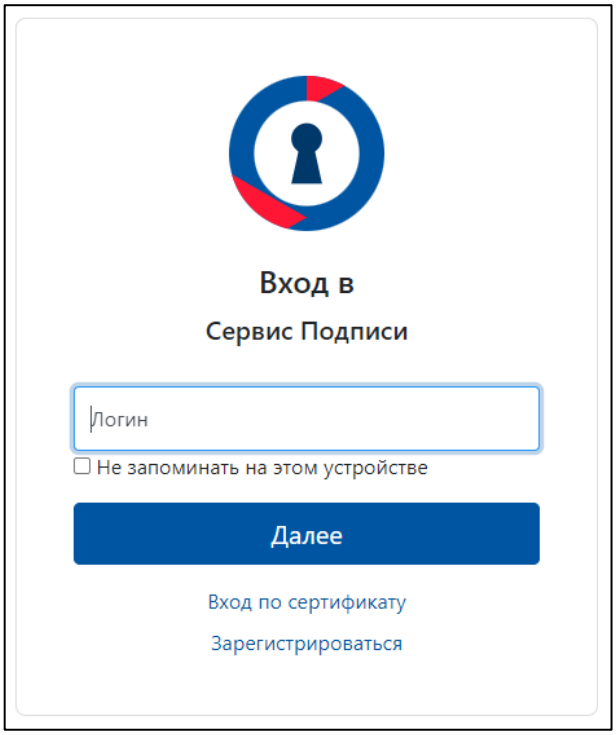

Рисунок 1. — Окно аутентификации

2.1. Методы первичной аутентификации

2.1.1. Вход в Веб-интерфейс СЭП (только идентификация)

В случае если Оператором (или Пользователем) был выбран метод первичной аутентификации «*Только идентификация*» Пользователю необходимо ввести имя учетной записи (логин) или адрес электронной почты в поле ввода и нажать кнопку «*Далее*» (см. Рисунок 2 — Вход в СЭП. Окно ввода).

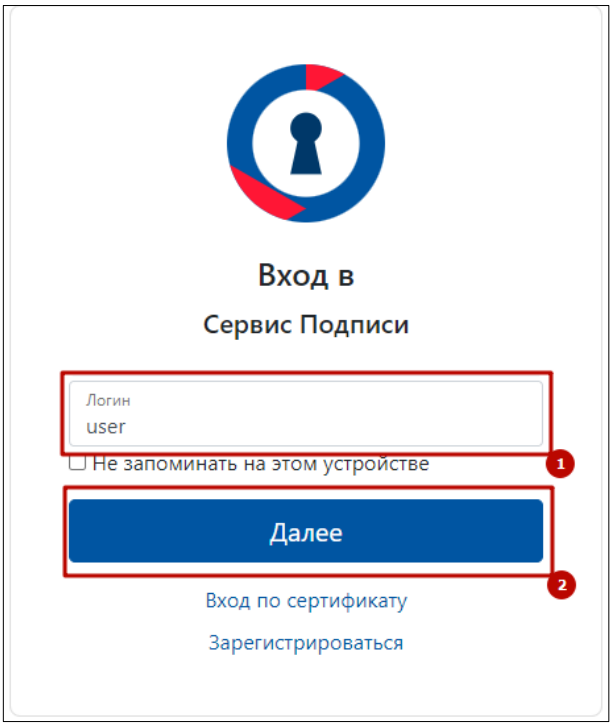

Рисунок 2 — Вход в СЭП. Окно ввода логина

Если Оператором (или Пользователем) было задано подтверждение Пользователем операции входа в Веб-интерфейс СЭП при помощи метода вторичной аутентификации, Пользователь должен подтвердить операцию входа соответствующим методом вторичной аутентификации.

Если все процедуры аутентификации Пользователя пройдены успешно, будет отображен интерфейс Пользователя СЭП (см. Рисунок 3 — Веб-интерфейс Пользователя). В случае если у Пользователя есть зарегистрированные в СЭП сертификаты, то они будут отображены в Веб-интерфейсе.

Внимание: если вход при помощи метода «Только идентификация» выполняется без подтверждения (например, в мобильном приложении), часть функций Веб-интерфейса может быть недоступна.

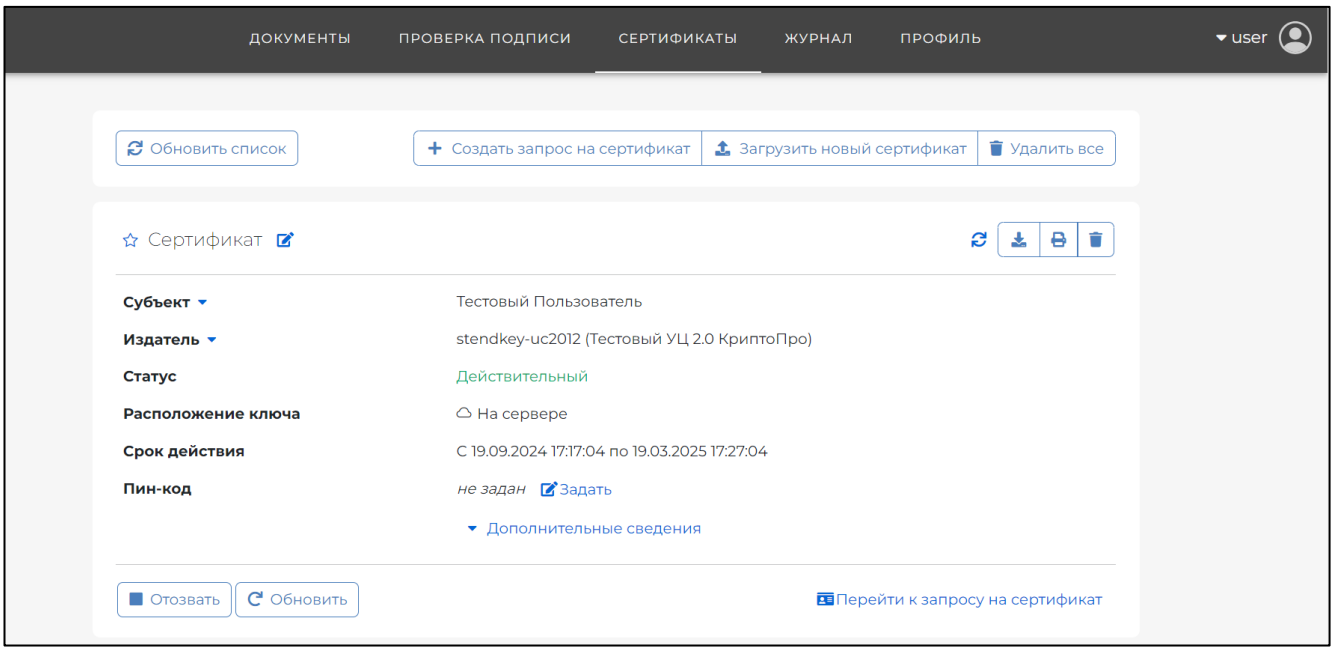

Рисунок 3 — Веб-интерфейс Пользователя

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

В случае если Оператором (или Пользователем) был 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*». В зависимости от настроек, Пользователю может потребоваться ввести ПИН-код доступа к ключевому контейнеру, и затем нажать кнопку «*ОК*».

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

Если все процедуры аутентификации Пользователя пройдены успешно, будет отображен интерфейс Пользователя СЭП (см. Рисунок 3 — Веб-интерфейс Пользователя). В случае если у Пользователя есть зарегистрированные в СЭП сертификаты, то они будут отображены в веб-интерфейсе Пользователя.

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

В случае если Оператором (или Пользователем) был выбран метод первичной аутентификации «*Аутентификация по паролю*», Пользователю

необходимо ввести имя учетной записи (логин) или адрес электронной почты в поле ввода и нажать кнопку «*Далее*» (см. Рисунок 2 — Вход в СЭП. Окно ввода).

Если имя учетной записи или адрес электронной почты введено верно и найдены в СЭП, появится форма для ввода пароля, выданного Пользователю Оператором при регистрации Пользователя, или назначенного Пользователем самостоятельно.

В появившейся форме Пользователю необходимо ввести пароль и нажать на кнопку «*Войти*» (см. Рисунок 4 — Вход в СЭП. Окно ввода пароля). Если Оператором задано подтверждение Пользователем операции входа в веб-интерфейс СЭП при помощи метода вторичной аутентификации, Пользователь должен подтвердить операцию входа соответствующим методом вторичной аутентификации.

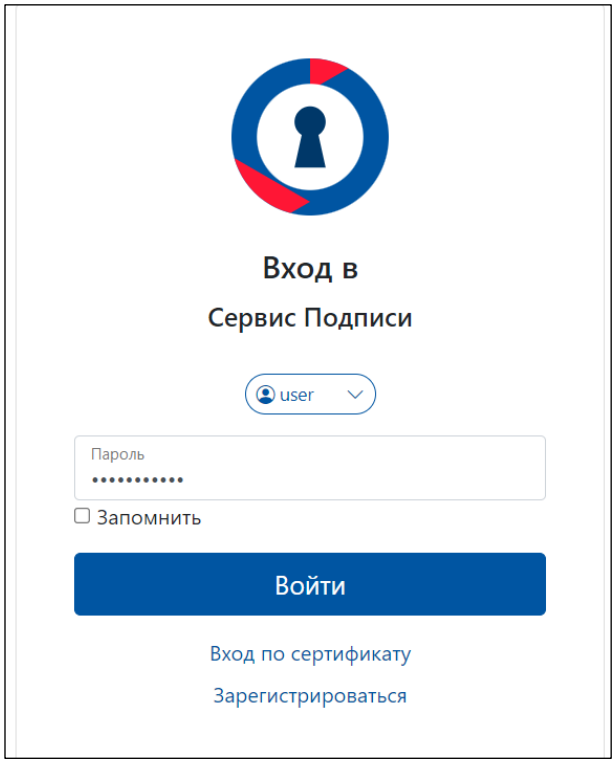

Рисунок 4 — Вход в СЭП. Окно ввода пароля

Если все процедуры аутентификации Пользователя пройдены успешно, будет отображен интерфейс Пользователя СЭП (см. Рисунок 3 — Веб-интерфейс Пользователя). В случае если у Пользователя есть зарегистрированные в СЭП сертификаты, то они будут отображены в веб-интерфейсе Пользователя.

2.2. Методы вторичной аутентификации

Заданные Оператором (или Пользователем) методы вторичной аутентификации применяются при подтверждении операций Пользователя в

СЭП. В случае если какая-либо операция требует подтверждения методом вторичной аутентификации, появится соответствующее уведомление от СЭП.

Следует отметить, что идентификатор запроса не является фиксированным – при осуществлении новой операции Пользователем в СЭП будет формироваться новый идентификатор запроса.

2.2.1. 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 (см. Рисунок 5 — Окно ввода одноразового кода подтверждения).

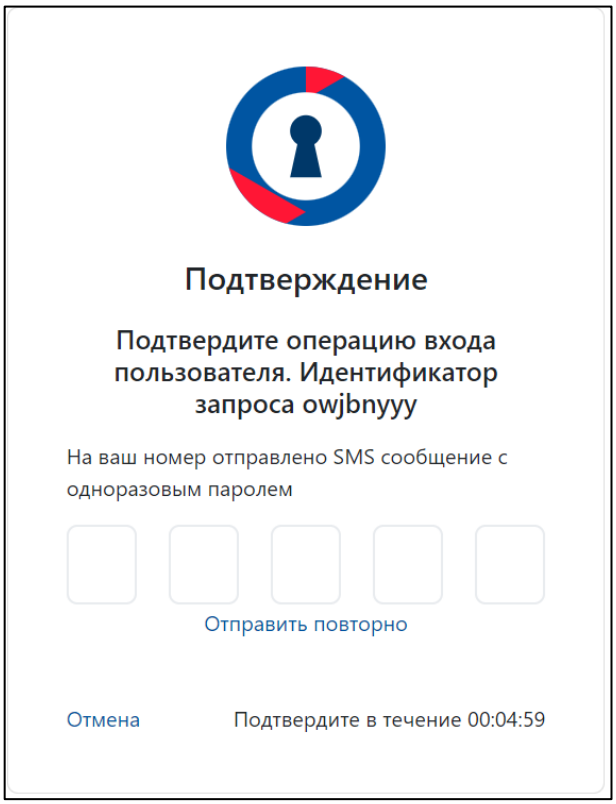

Рисунок 5 — Окно ввода одноразового кода подтверждения

Перечисленные способы аутентификации являются вспомогательными и не могут быть использованы как единственные.

2.2.2. Вторичная аутентификация с помощью мобильного приложения

В случае если для подтверждения операции используется метод вторичной аутентификации «Аутентификация с помощью мобильного приложения», для прохождения процедуры аутентификации Пользователю нужно установить мобильное приложение, предоставляемое по запросу на support@cryptopro.ru или полученное из магазина приложений.

После установки мобильного приложения будет предложено привязать устройство:

1. Через QR-код.
2. Отправить заявку на сервер.
3. Через привязанное устройство.

При наличии QR-кода для регистрации необходимо выбрать «*Через QR-код*». На следующем шаге необходимо ввести «Имя учетной записи» и нажать «Готово». После нажатия кнопки появится окно сканирования QR-кода, необходимо навести камеру на qr-код (см. Рисунок 6 — Мобильное приложение. Сканирование QR-кода).

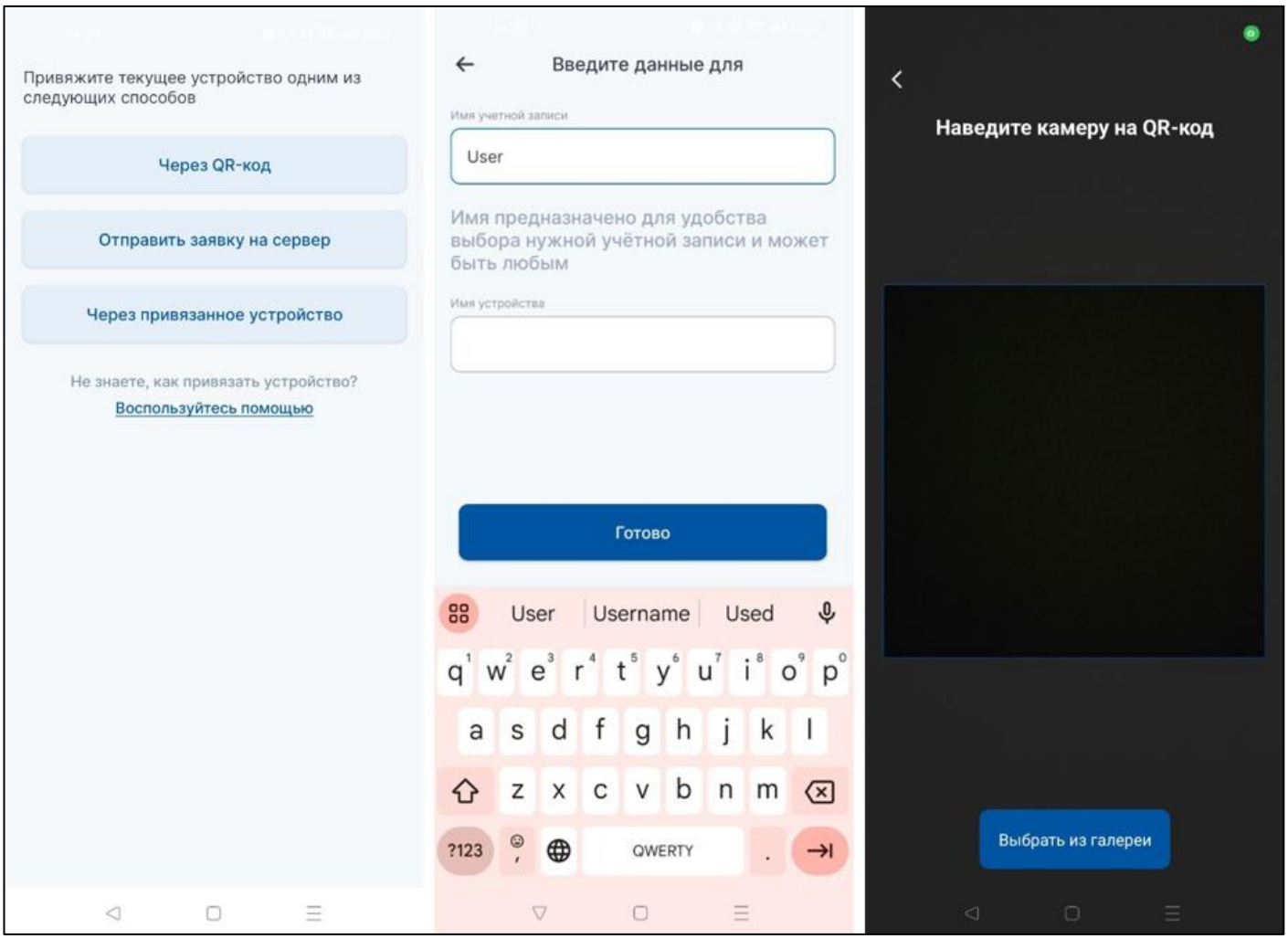

Рисунок 6 — Мобильное приложение. Сканирование QR-кода

После успешного сканирования QR-кода появится окно задания пароля для доступа к учетной записи. Необходимо указать пароль для учетной записи в мобильном приложении и подтвердить его. На следующем этапе будет предложено установить биометрический способ входа в учетную запись.

На следующем этапе появится окно с учетными данными Пользователя, данная информация загружается с сервера Ключа. Если данные указаны корректно, то нужно нажать «*Продолжить*». Появится информация, что регистрация успешно завершена (см. Рисунок 7 — Мобильное приложение. Завершение регистрации).

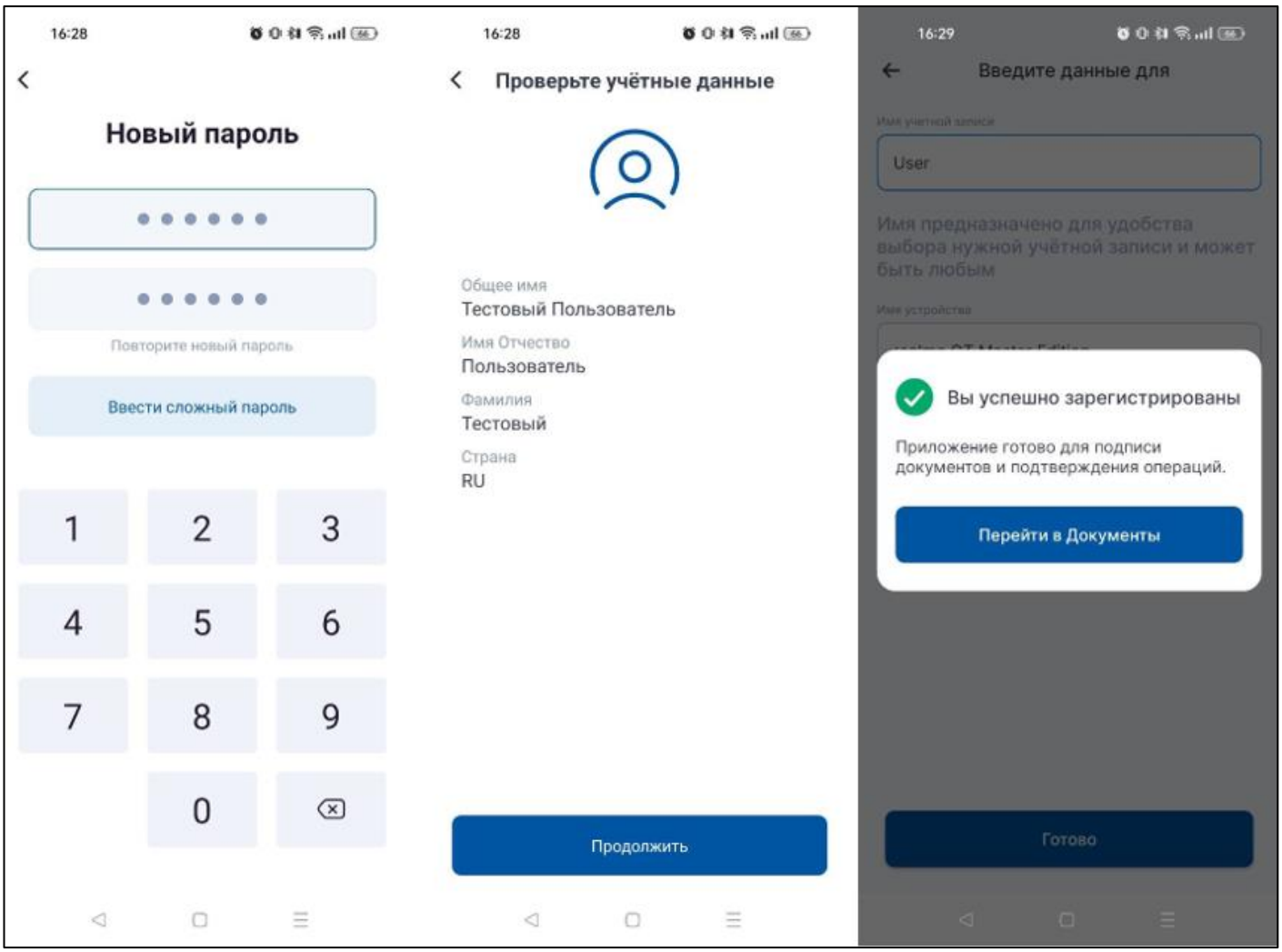

Рисунок 7 — Мобильное приложение. Завершение регистрации

После регистрации устройства его можно использовать для подтверждения операций и хранения ключей.

В случае запроса подтверждения операции через мобильное приложение в веб-интерфейсе СЭП появится информация о необходимости подтверждения операции (см. Рисунок 8 — Окно запроса на подтверждение операции в приложении), на мобильное устройство поступит Push-уведомление, что запрошено подтверждение операции и в мобильном приложении во вкладке «*Документы*» появится запись с информацией об операции.

Для подтверждения операции в списке доступных для подтверждения операций на вкладке «*Документы*» необходимо выбрать нужную операцию и нажать кнопку «*Подтвердить*». Появится сообщение об успешном выполнении операции (см. Рисунок 9 — Подтверждение операции в мобильном приложении).

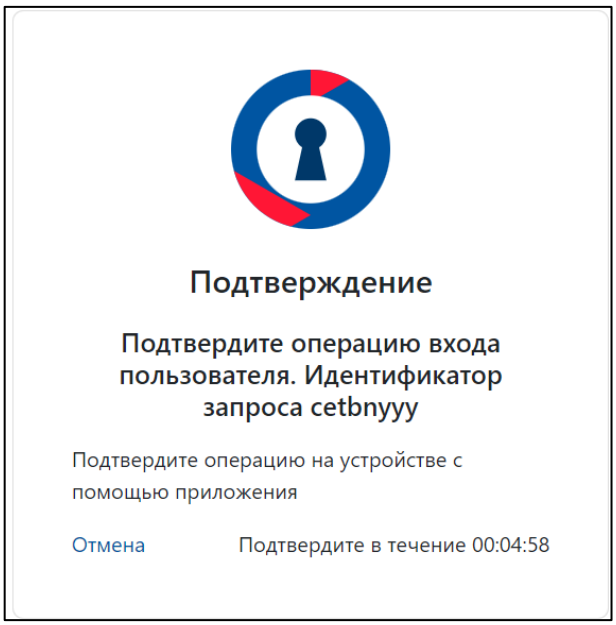

Рисунок 8 — Окно запроса на подтверждение операции в приложении

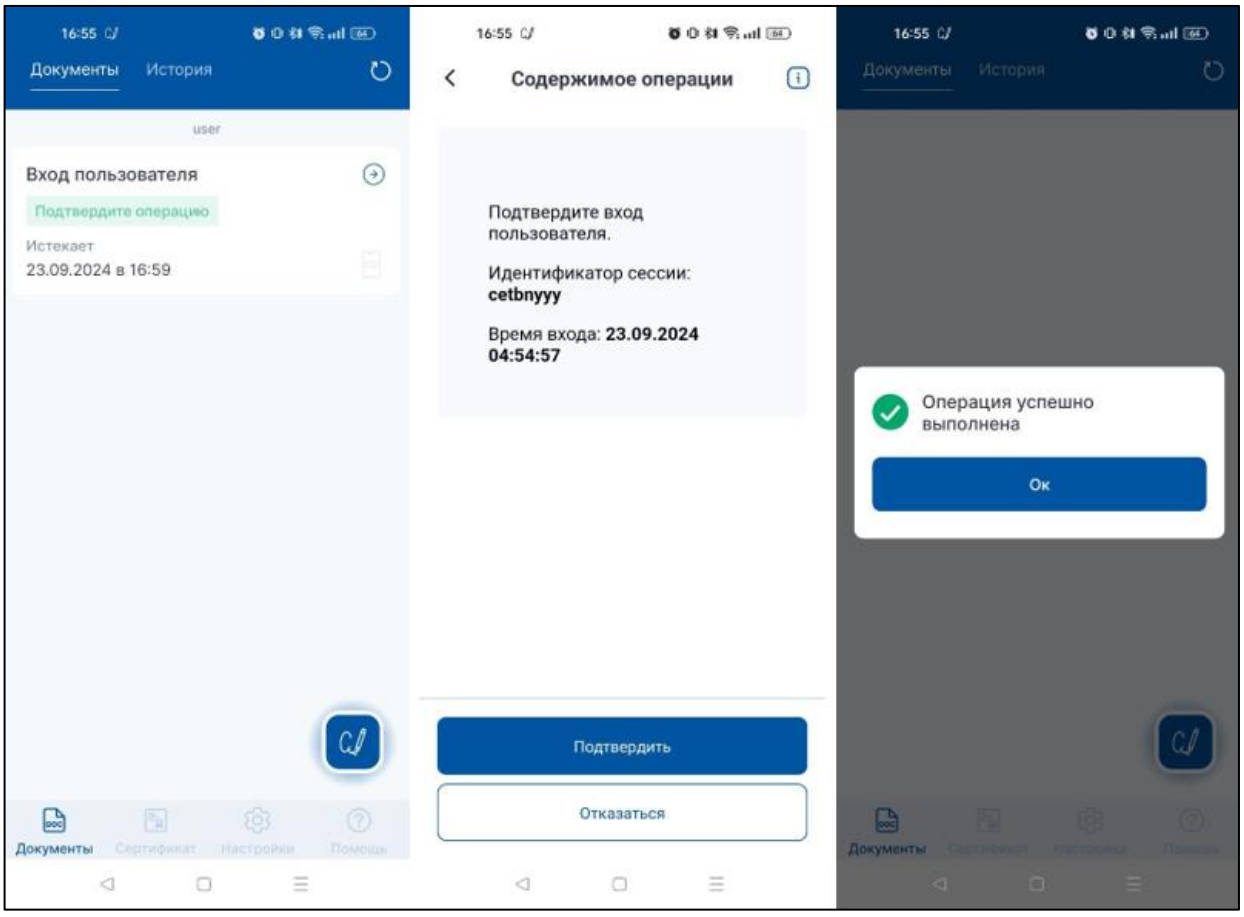

Рисунок 9 — Подтверждение операции в мобильном приложении

3. Документы

Раздел предназначен для выполнения криптографических операций, таких как:

- Создание электронной подписи;
- Шифрование/Расшифрование;
- Усовершенствование подписи.

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 «*Документы*» и загрузить документ или по кнопке «*Выбрать файлы*», или переместив нужный файл в окно загрузки (см. Рисунок 10 — Загрузка документа)

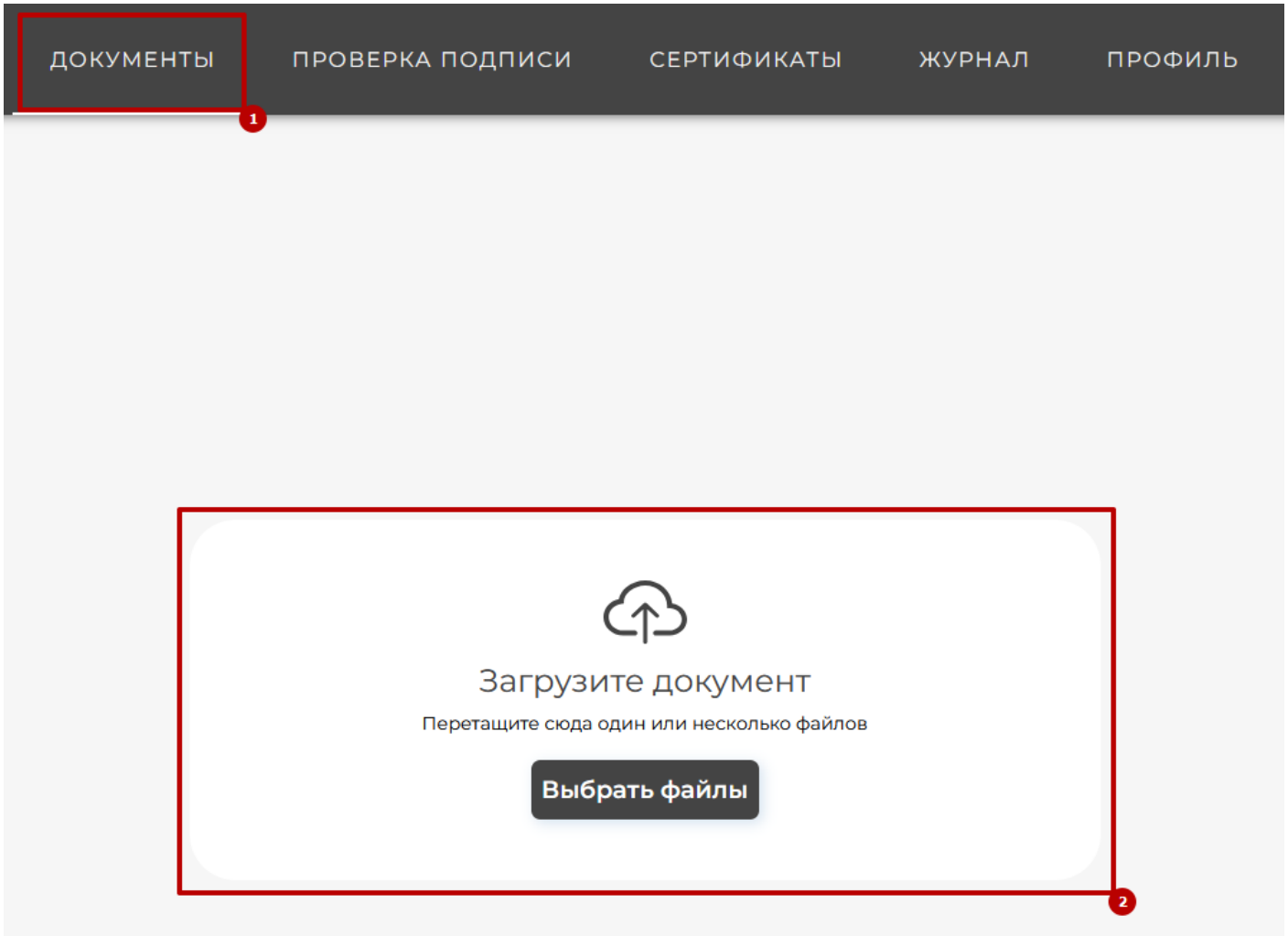

Рисунок 10 — Загрузка документа

После успешной загрузки документа содержимое документа появится:

1. Содержимое документа (если поддерживается отображение)
2. Окно с возможностью загрузки дополнительных документов
3. Возможность выбора действия с документами – Подпись документов, Шифрование документов, Расшифрование документов, Усовершенствование подписи.
4. Возможность удаления загруженных документов

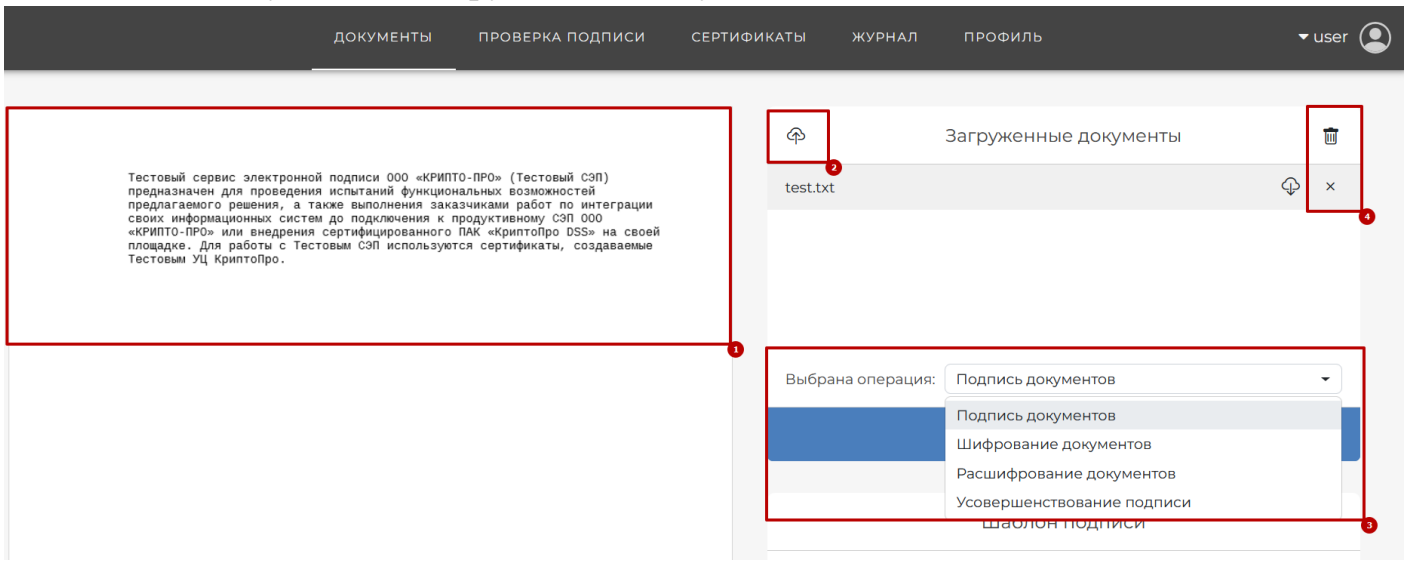

Рисунок 11 — Загрузка документа

3.1. Подписание документов

Для подписания документов необходимо выбрать опцию «*Подписание документов*», в окне «*Шаблон подписи*» отобразятся доступные шаблоны[1]. Если подходящего шаблона нет, то можно выбрать опцию «*Вручную*» и задать необходимые параметры. Далее необходимо выбрать сертификат для подписи и нажать кнопку «*Подписать*» (см. Рисунок 12 — Указание параметров подписи документов).

[1] Шаблоны настраиваются администратором СЭП

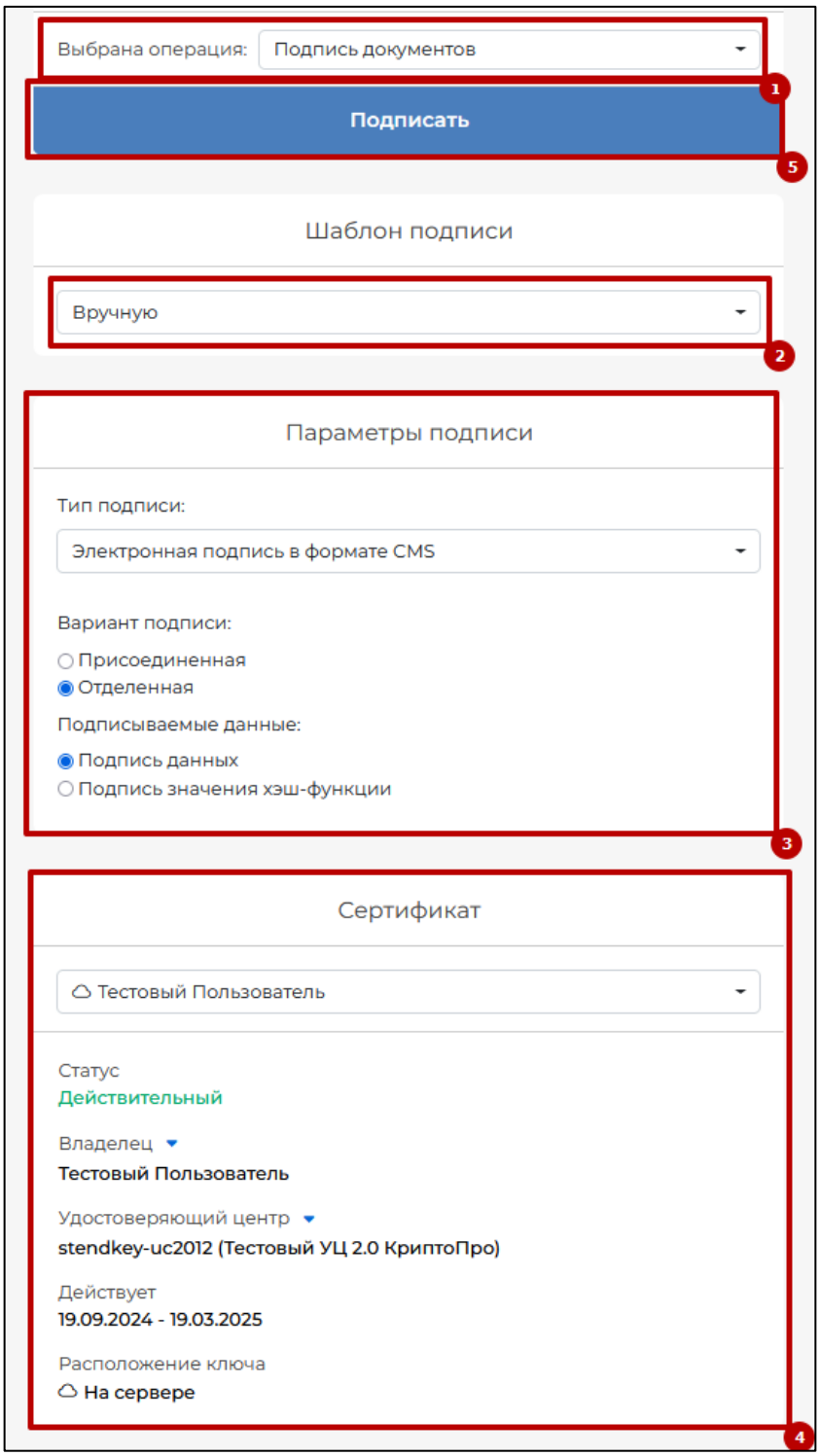

Рисунок 12 — Указание параметров подписи документов

Если на ключ с сертификатом установлен пин-код, то в веб-интерфейсе появится окно ввода пин-кода (см. Рисунок 13 — Ввод пин-кода).

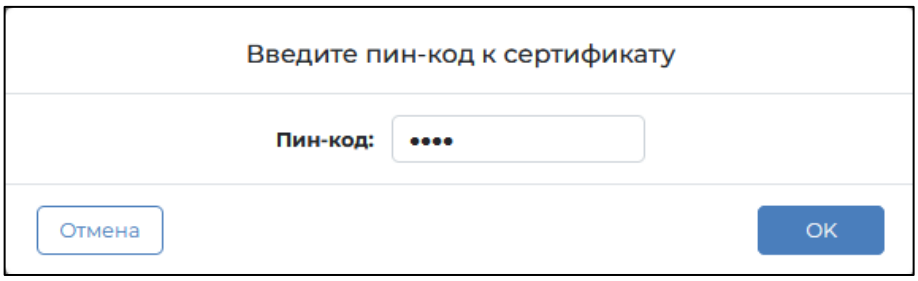

Рисунок 13 — Ввод пин-кода

Если операция требует подтверждения в мобильном приложении, то произойдет перенаправление на страницу подтверждения операции. После этого операцию будет необходимо подтвердить в мобильном приложении (см. подраздел 3.5).

После успешного завершения появится окно с сообщением, что документы успешно подписаны (см. Рисунок 14 — Завершение операции подписи).

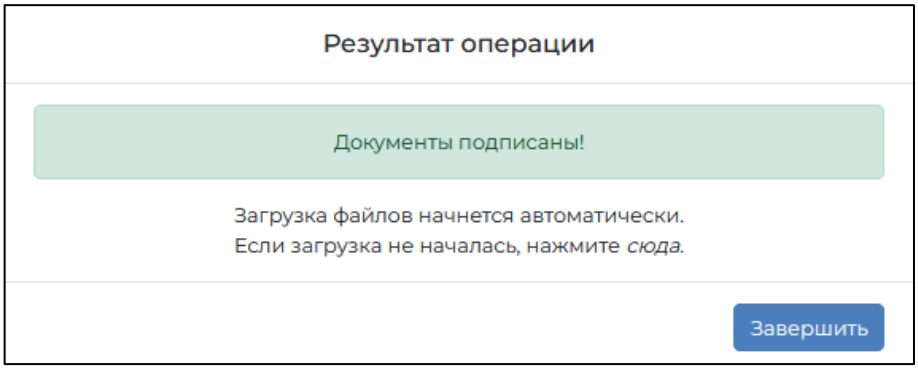

Рисунок 14 — Завершение операции подписи

3.2. Шифрование документов

Для шифрования документов необходимо выбрать опцию «*Шифрование документов*», в окне «*Параметры шифрования*» требуется указать нужный тип шифрования и выбрать параметры.

Сертификаты получателей можно загрузить по кнопке «*Загрузить сертификаты получателей*» (см. Рисунок 15 — Указание параметров шифрования документов), либо выбрать из личных сертификатов(см. Рисунок 15 — Указание параметров шифрования документов).

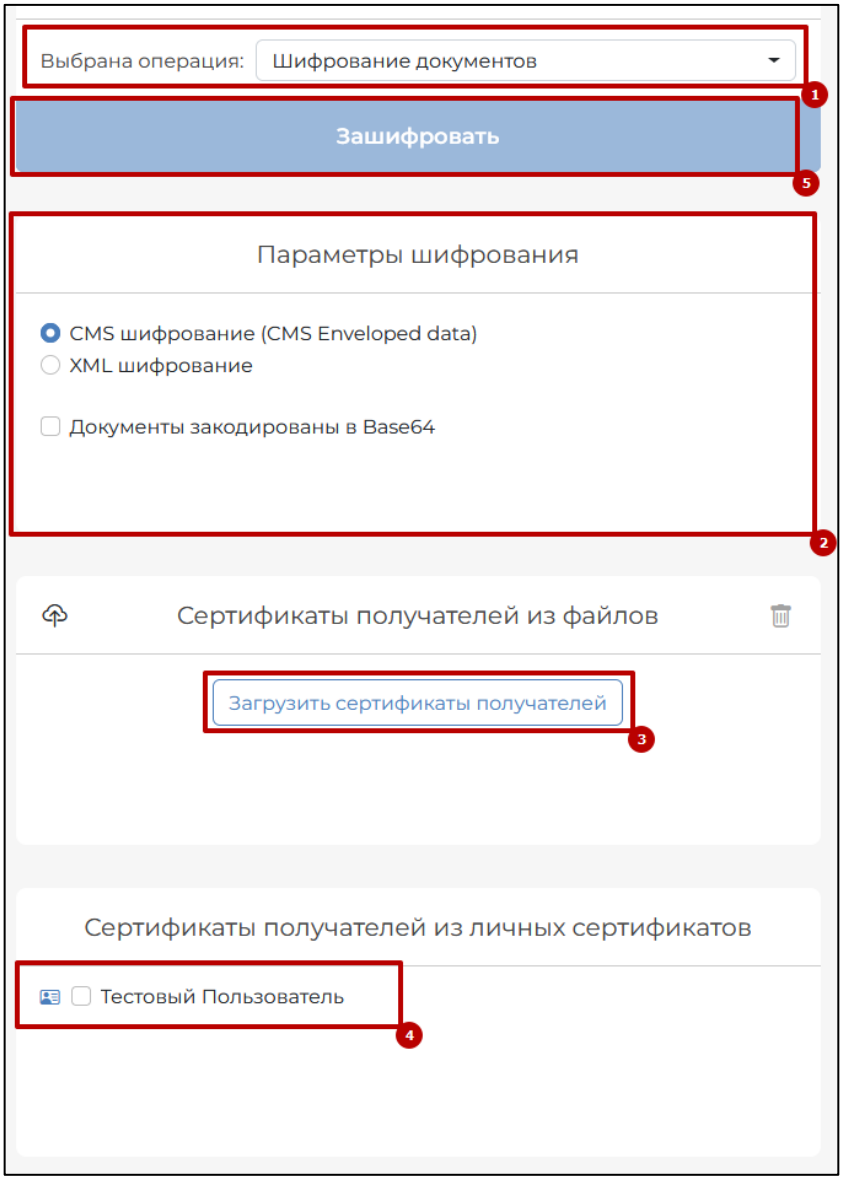

Рисунок 15 — Указание параметров шифрования документов

После настройки параметров шифрования необходимо нажать кнопку «Зашифровать».

После успешного завершения появится окно с сообщением, что документы успешно зашифрованы (см. Рисунок 16 — Завершение операции шифрования).

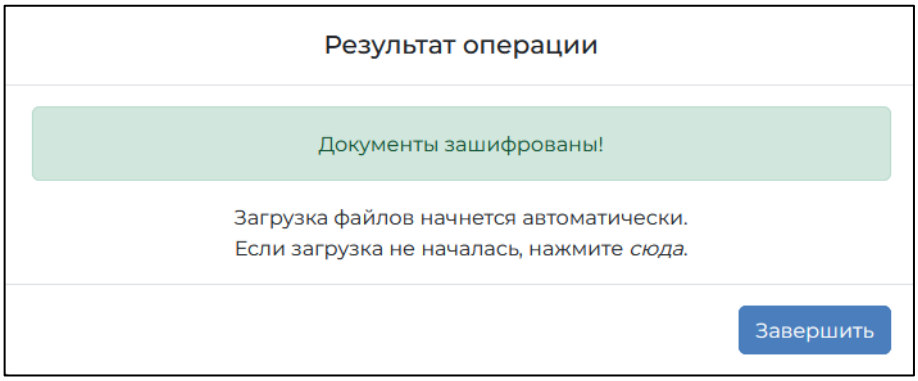

Рисунок 16 — Завершение операции шифрования

3.3. Расшифрование документов

Для расшифрования документов необходимо выбрать опцию «*Расшифрование документов*», в окне «*Параметры расшифрования*» требуется указать нужный тип расшифрования выбрать параметры.

Сертификаты расшифрования будут выбраны автоматически из списка доступных.

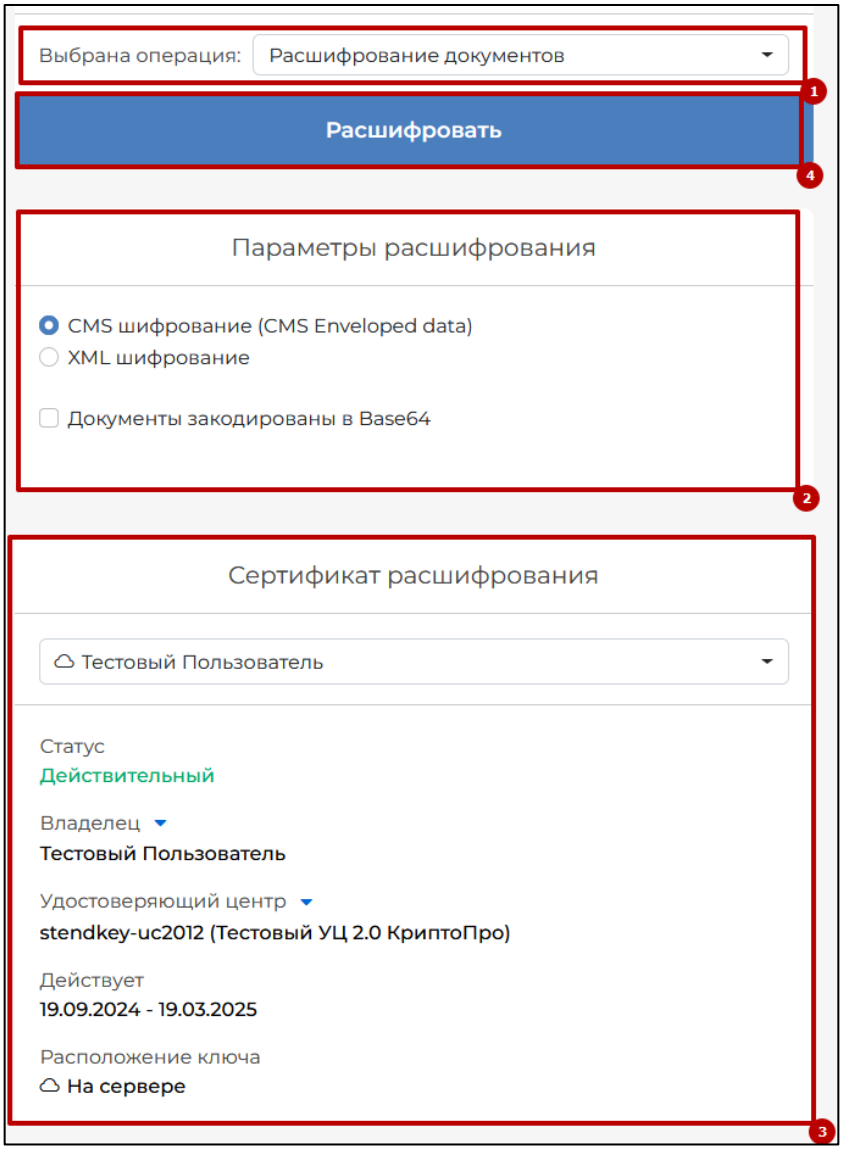

Рисунок 17 — Указание параметров расшифрования документов

Если на ключ с сертификатом установлен пин-код, то в веб-интерфейсе появится окно ввода пин-кода (см. Рисунок 13 — Ввод пин-кода).

Если операция требует подтверждения в мобильном приложении, то произойдет перенаправление на страницу подтверждения операции. После этого операцию будет необходимо подтвердить в мобильном приложении (см. подраздел 3.5).

После успешного завершения появится окно с сообщением, что документы успешно расшифрованы (см. Рисунок 18 — Завершение операции расшифрования).

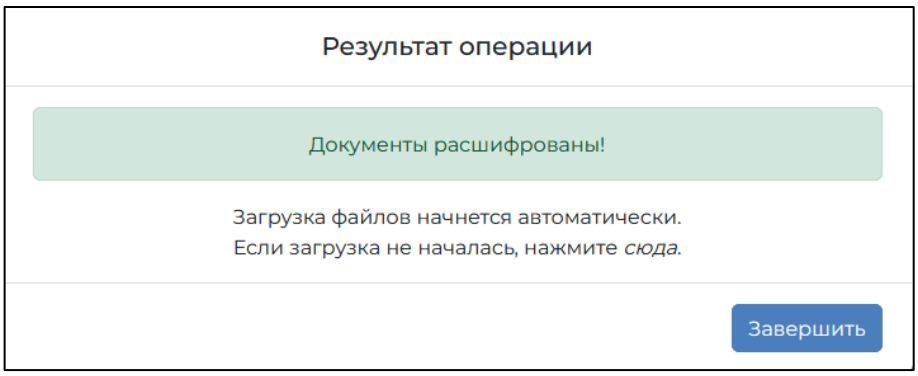

Рисунок 18 — Завершение операции расшифрования

3.4. Усовершенствование подписи

Для усовершенствования подписи необходимо выбрать опцию «*Усовершенствование подписи*», в окне «*Параметры усовершенствования*» требуется указать тип подписи, который необходимо получить (Cades или XMLDSig) и параметры выбранной подписи и нажать кнопку «*Усовершенствовать*».

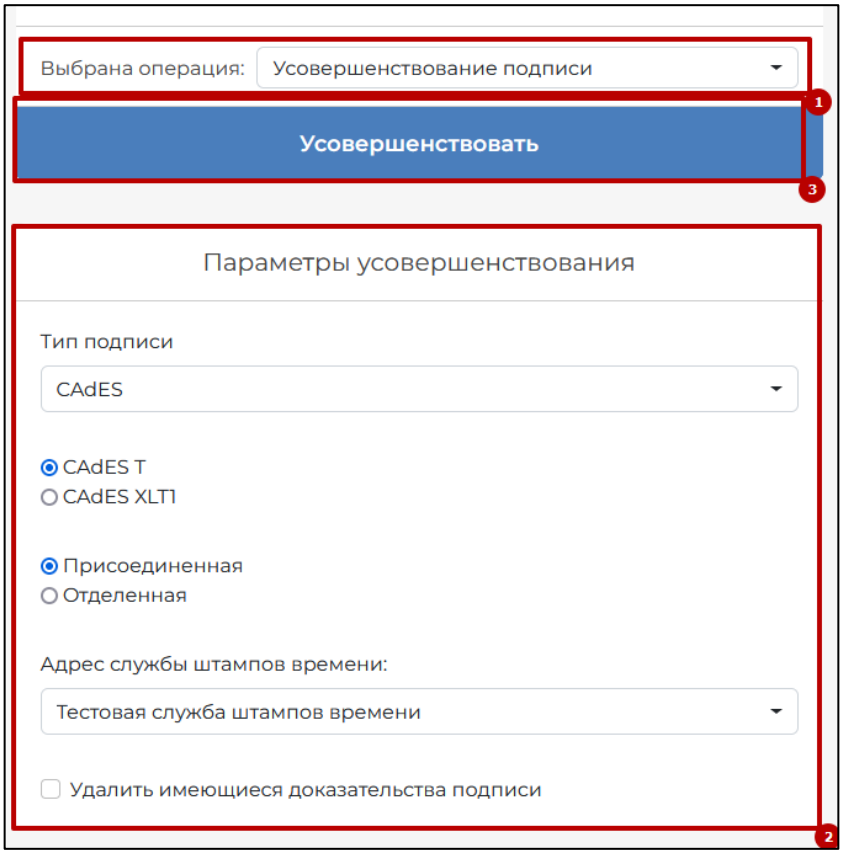

Рисунок 19 — Указание параметров усовершенствования

После успешного завершения появится окно с сообщением, что документы успешно усовершенствованы (см. Рисунок 20 — Завершение операции усовершенствования).

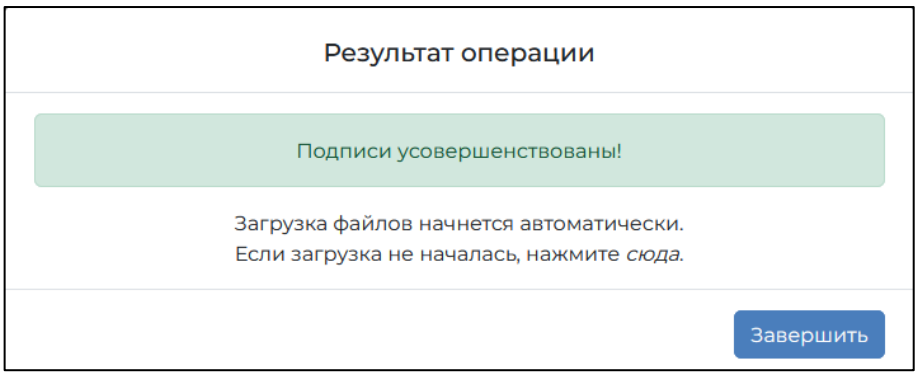

Рисунок 20 — Завершение операции усовершенствования

3.5. Подтверждение операций в мобильном приложении

Действия, описанные в подразделах 3.1, 3.3, 3.4, требуют подтверждения операции в мобильном приложении, если при создании сертификата был создан ключ подписи, хранимый в мобильном приложении или в распределенном виде. Подробнее о типах хранения ключей см. документ «ЖТЯИ.00118-01 96 01 КриптоПро Ключ. Общее описание».

После перехода на страницу подтверждения операции Пользователю необходимо выполнить следующие действия (см. Рисунок 21 — Подтверждение операции в мобильном приложении):

1. Перейти в мобильное приложение по пришедшему PUSH-уведомлению либо открыть мобильное приложение самостоятельно и перейти в раздел «Документы». Выбрать появившуюся операцию.
2. Ознакомиться с подписываемыми документами при помощи кнопки «Показать документ» и иной информацией об операции, установить чекбокс «Подтверждаю ознакомление с платежными документами» и нажать кнопку «Подписать».
3. Ввести пароль, созданный при привязке мобильного устройства к учетной записи (Подробнее о сценариях привязки см. документ «ЖТЯИ.00118-01 96 01 КриптоПро Ключ. Общее описание»).

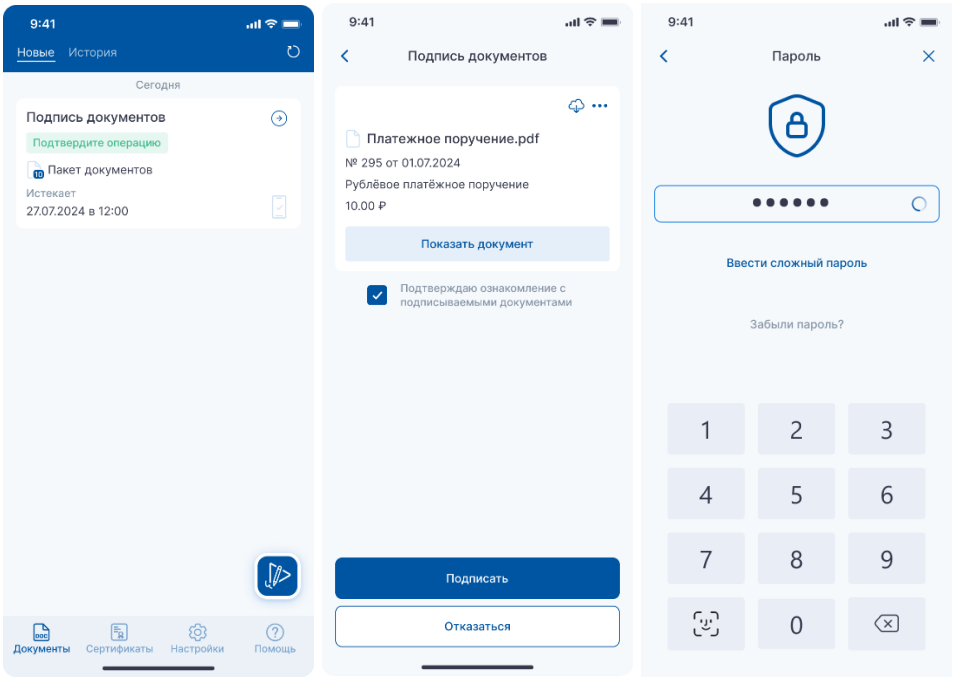

Рисунок 21 — Подтверждение операции в мобильном приложении

4. Проверка подписи и сертификатов

4.1. Проверка подписи

Внимание: данный раздел доступен только в случае настроенного взаимодействия со службой проверки сертификатов и электронной подписи КриптоПро SVS 2.0.

Раздел предназначен для проверки подписи электронных документов. Для проверки подписи электронного документа нужен файл подписи электронного документа и файл электронного документа (для отсоединенной подписи). Для проверки подписи электронного документа необходимо перейти в раздел «*Проверка подписи*» и выполнить следующие действия:

1. Загрузить файл подписи электронного документа по кнопке «переместите документ(-ы) или нажмите, чтобы выбрать» или переместите документ в область окна (см. Рисунок 22 — Загрузка документов для проверки).

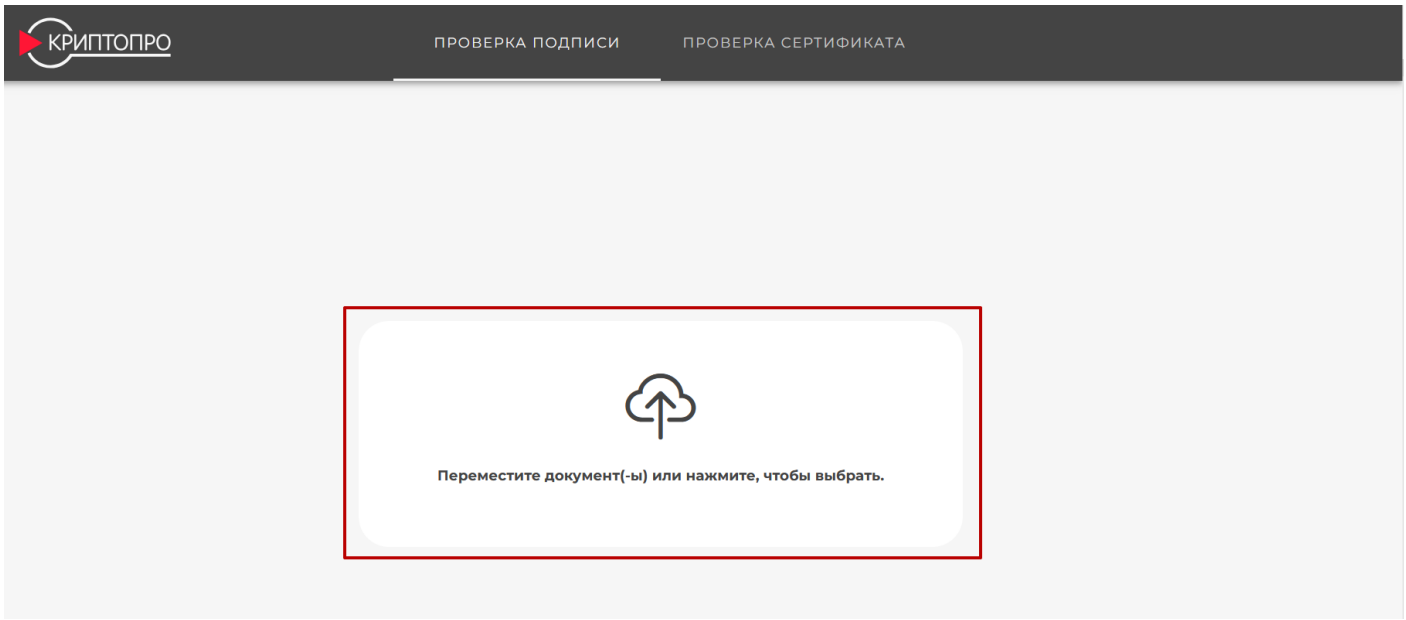

Рисунок 22 — Загрузка документов для проверки

2. Формат подписи будет определен автоматически. При необходимости изменения формата подписи необходимо в области «Параметры подписи» выбрать «Задается вручную» и указать параметры (см. Рисунок 23 — Параметры подписи).

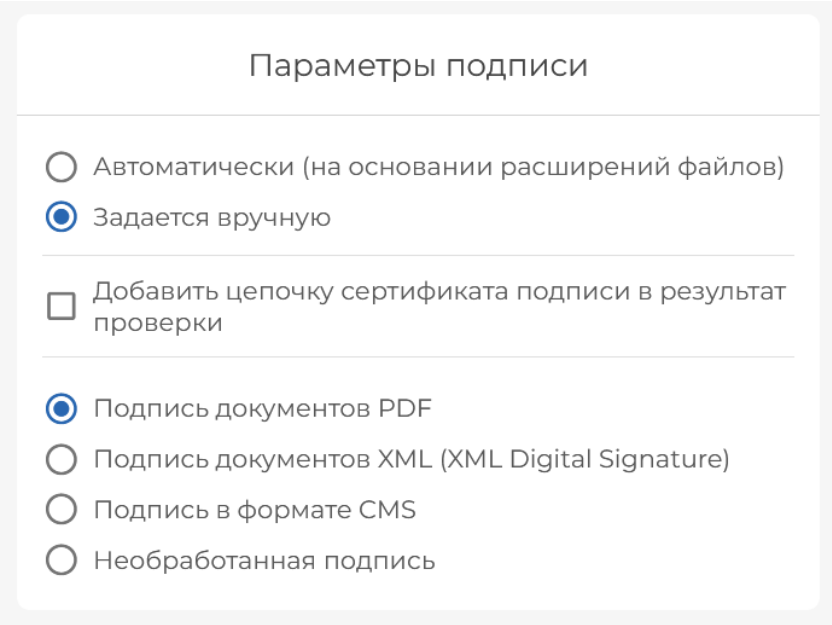

Рисунок 23 — Параметры подписи

3. Нажать кнопку «*Проверить*».

На странице отобразится информация о результате проверки каждого загруженного документа. Если было загружено несколько документов, то для получения подробной информации нужно нажать на имя документа в разделе «*Список подписей*».

Для загрузки файла отчета нужно нажать на кнопку «*Файл отчета*». В загруженном файле будет подробная информация с результатом проверки всех загруженных подписей (см. Рисунок 24 — Результат проверки).

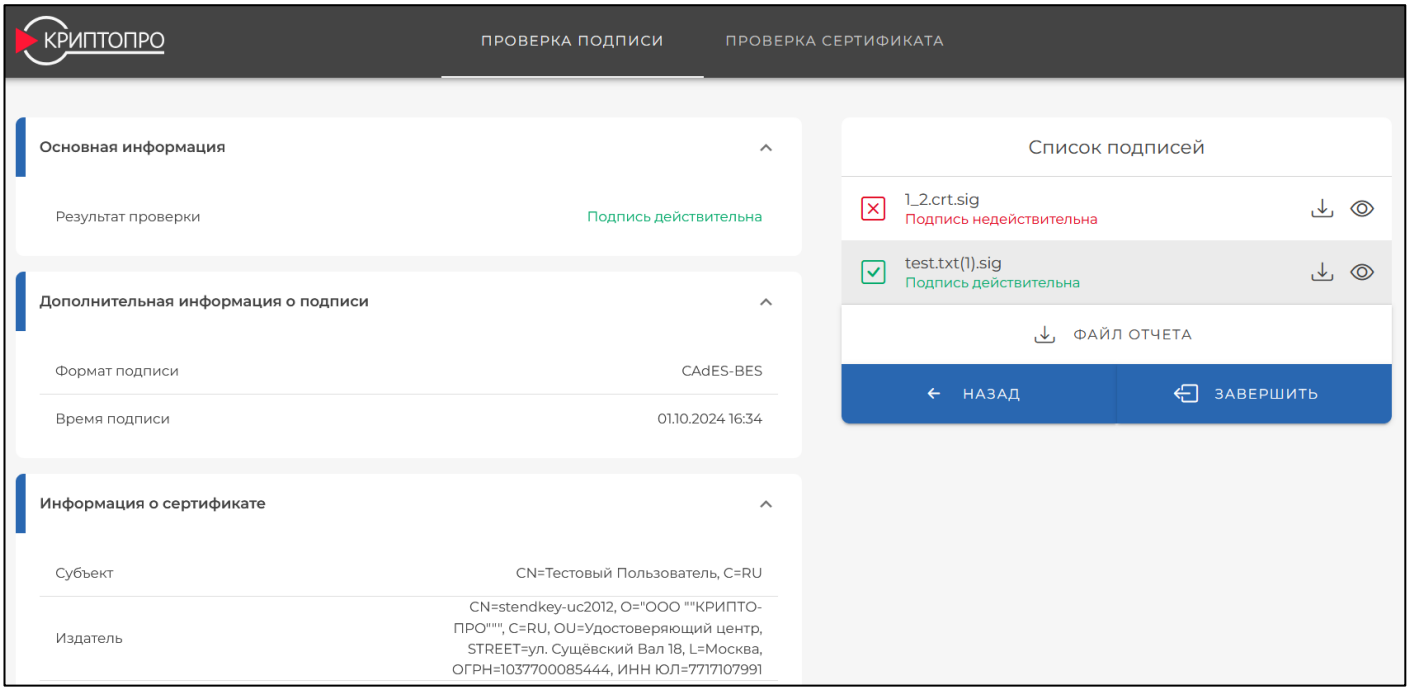

Рисунок 24 — Результат проверки подписей

4.2. Проверка сертификата

Для проверки сертификата нужно открыть вкладку «*Проверка сертификата*» и выполнить следующие действия:

1. Загрузить файл сертификата по кнопке «*переместите файл(-ы) или* нажмите, *чтобы выбрать*» или переместить документ в область окна (см. Рисунок 25 — Загрузка сертификатов для проверки).

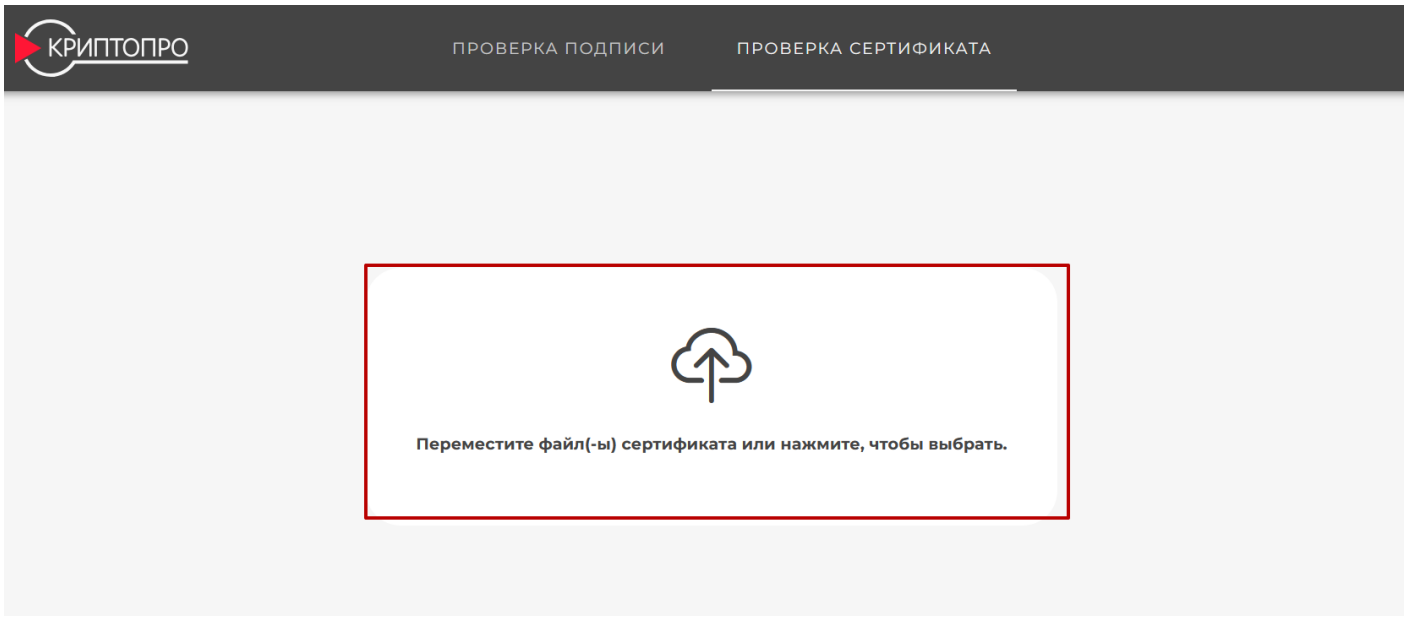

Рисунок 25 — Загрузка сертификатов для проверки

2. После загрузки сертификата появятся параметры проверки (см. Рисунок 26 — Опции проверки сертификатов).

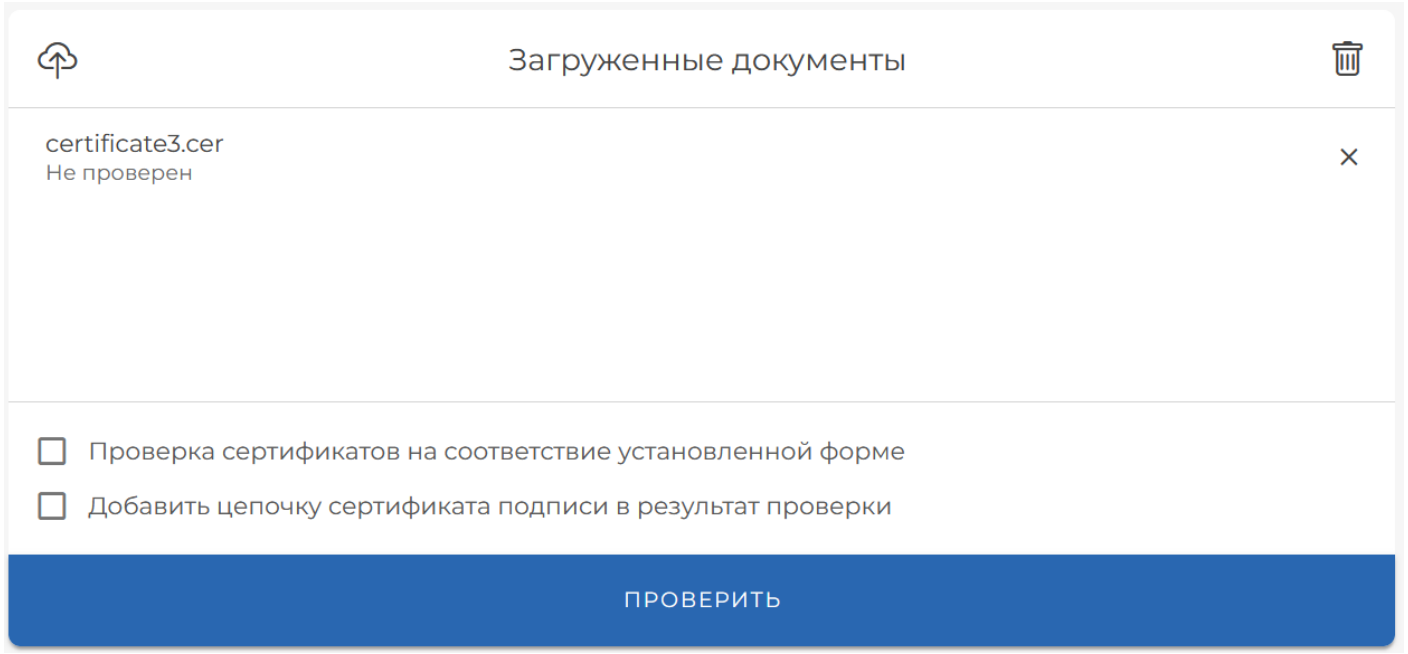

Рисунок 26 — Опции проверки сертификатов

3. Нажать кнопку «*Проверить*»

Результат проверки сертификата будет отображен на странице (см. Рисунок 27 — Результат проверки сертификата).

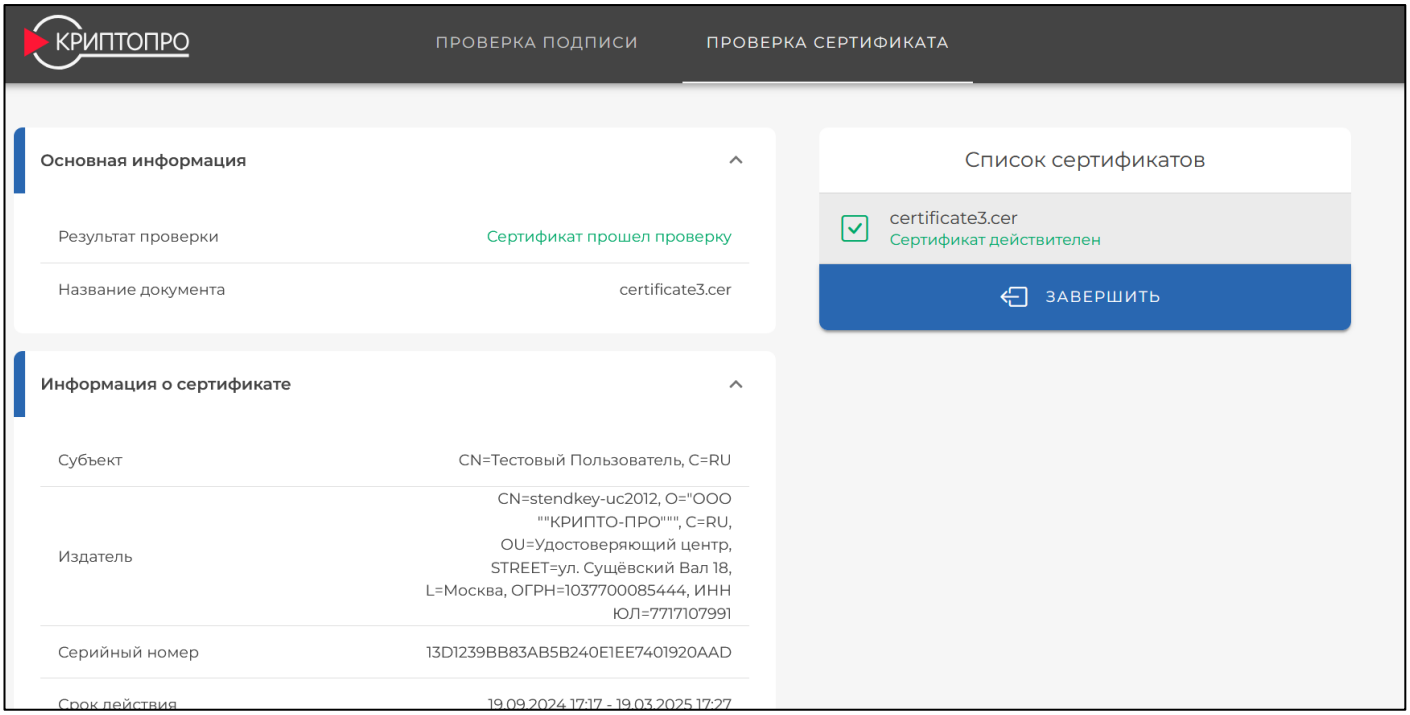

Рисунок 27 — Результат проверки сертификата

5. Сертификаты

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

5.1. Создание запроса на сертификат с автоматическим выпуском сертификата в Тестовом УЦ с хранением ключей на мобильном устройстве (тестовый вариант)

Для хранения ключей в мобильном приложении у Пользователя должно быть привязано мобильное устройство.

Для создания запроса на новый/первый сертификат Пользователя нужно перейти в раздел «*Сертификаты*» и нажать кнопку «*Создать запрос на сертификат*» (см. Рисунок 28 — Заполнение данных запроса на сертификат).

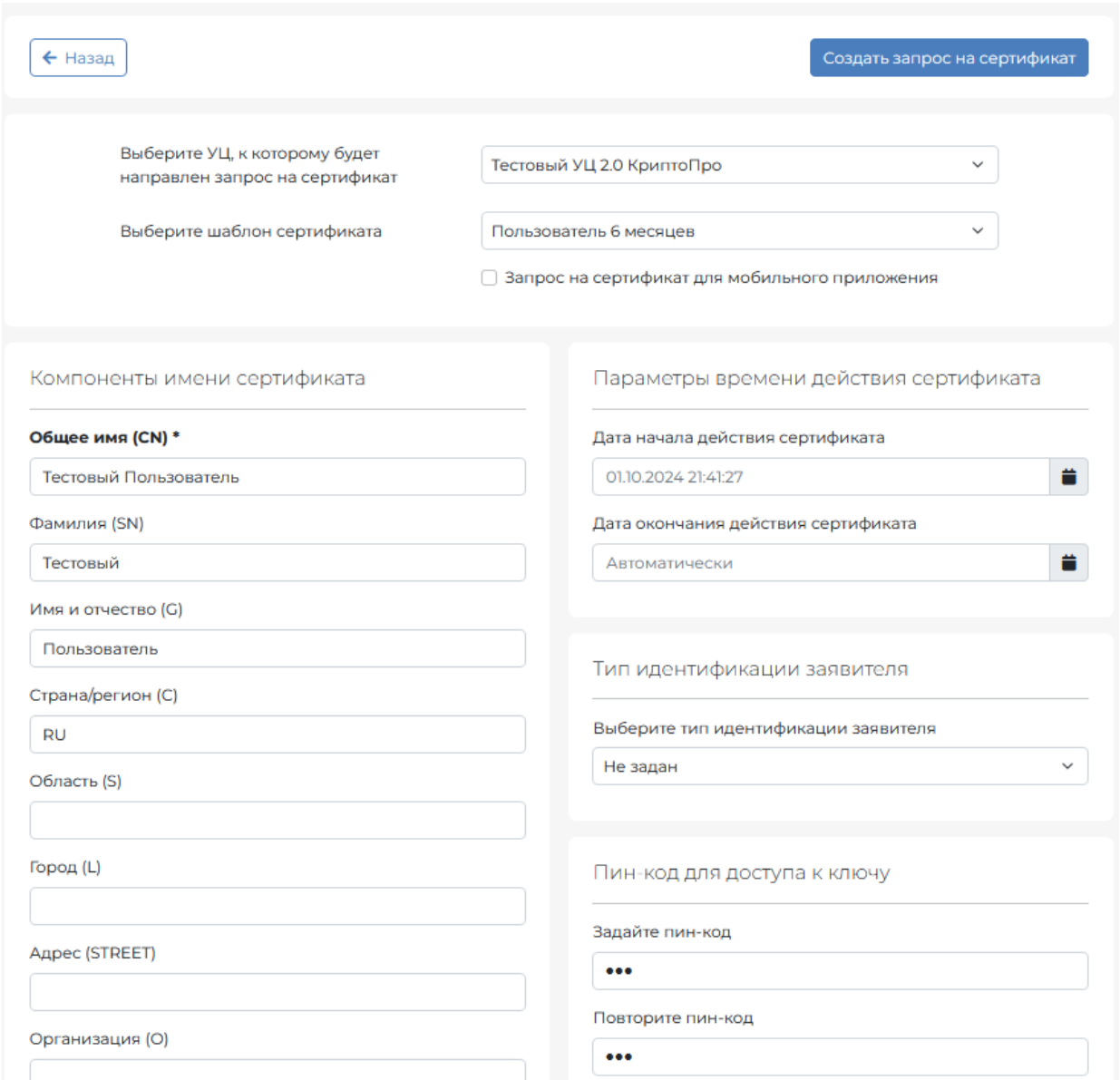

Рисунок 28 — Заполнение данных запроса на сертификат

Далее необходимо выбрать Удостоверяющий центр для выпуска сертификата Пользователя (по умолчанию «*Тестовый УЦ 2.0 КриптоПро*», отредактировать данные Пользователя, выбрать шаблон сертификата (по умолчанию «*Пользователь 6 месяцев*») и нажать кнопку «*Создать запрос на сертификат*» (см. Рисунок 28 — Заполнение данных запроса на сертификат) и установить чек-бокс «*Запрос на сертификат для мобильного приложения*» (см. Рисунок 29 — Запрос на сертификат с хранением ключей в мобильном приложении).

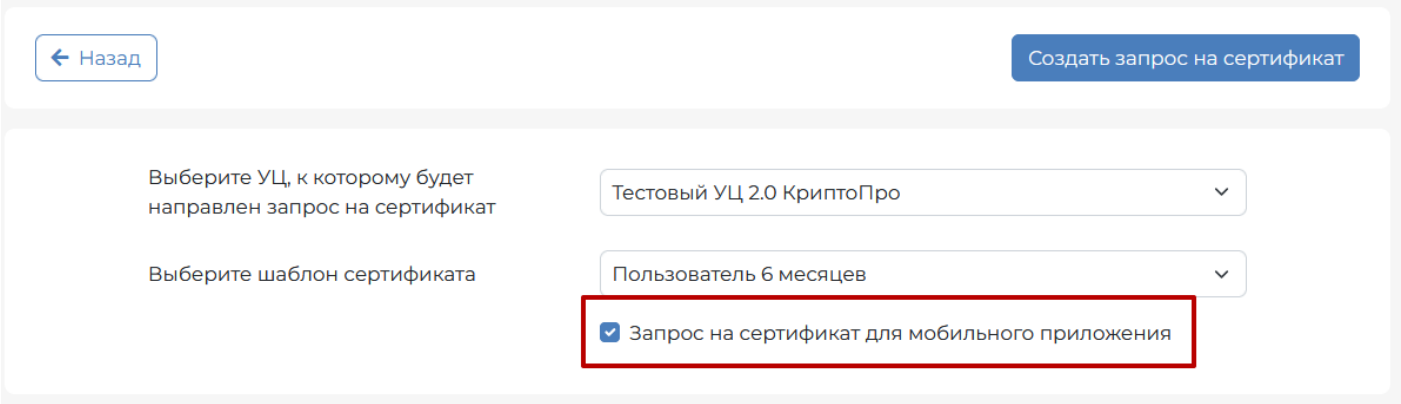

Рисунок 29 — Запрос на сертификат с хранением ключей в мобильном приложении

Появится окно с информацией о запросе на сертификат. Статус запроса – «*Ожидает подписи*» (см. Рисунок 30 — Запрос на сертификат с хранением в мобильном устройстве).

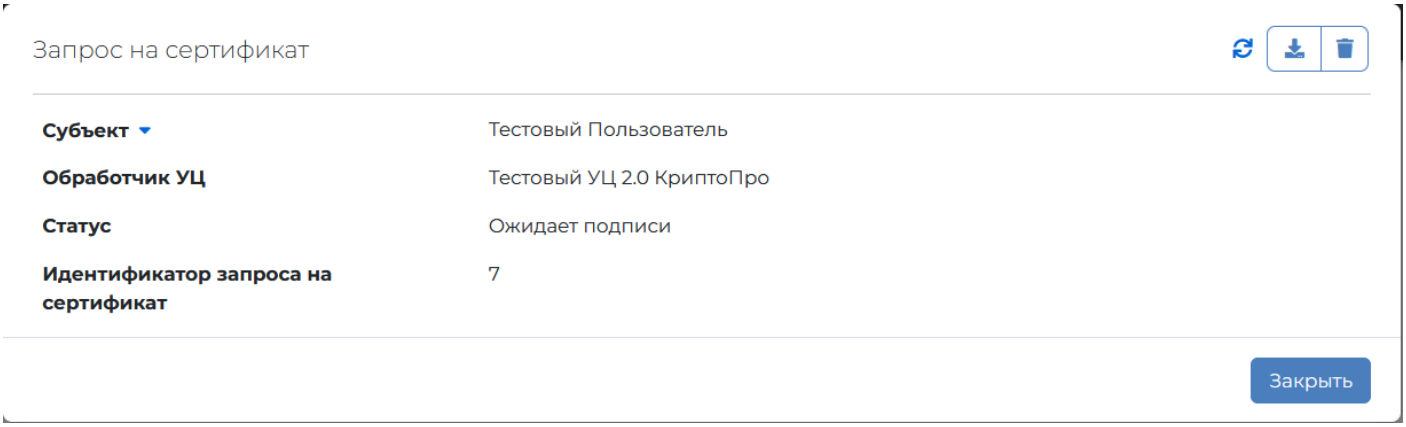

Рисунок 30 — Запрос на сертификат с хранением в мобильном устройстве

Дальнейшие действия выполняются на мобильном устройстве.

1. Откройте мобильное приложение.
2. Перейдите во вкладку «*Сертификаты*». В списке сертификатов будет запрос со статусом «*Запрос на сертификат не подписан*».
3. Нажмите кнопку «Создать ключ подписи».

4. Будет предложено выбрать место хранения ключей. Выберите ключевой носитель «*Это устройство*».
5. В следующем окне откроется биологический датчик случайных чисел. Необходимо нажимать на экран до тех пор, пока полоска снизу не будет заполнена и не появится сообщение «*Запрос успешно подписан*» (см. Рисунок 31 — Подписание запроса на сертификат).
6. Статус запроса изменится на «*Активен*», при нажатии на сертификат отобразятся доступные действия с ним и подробная информация (см. Рисунок 32 — Успешное подписание запроса и выпуск сертификата).

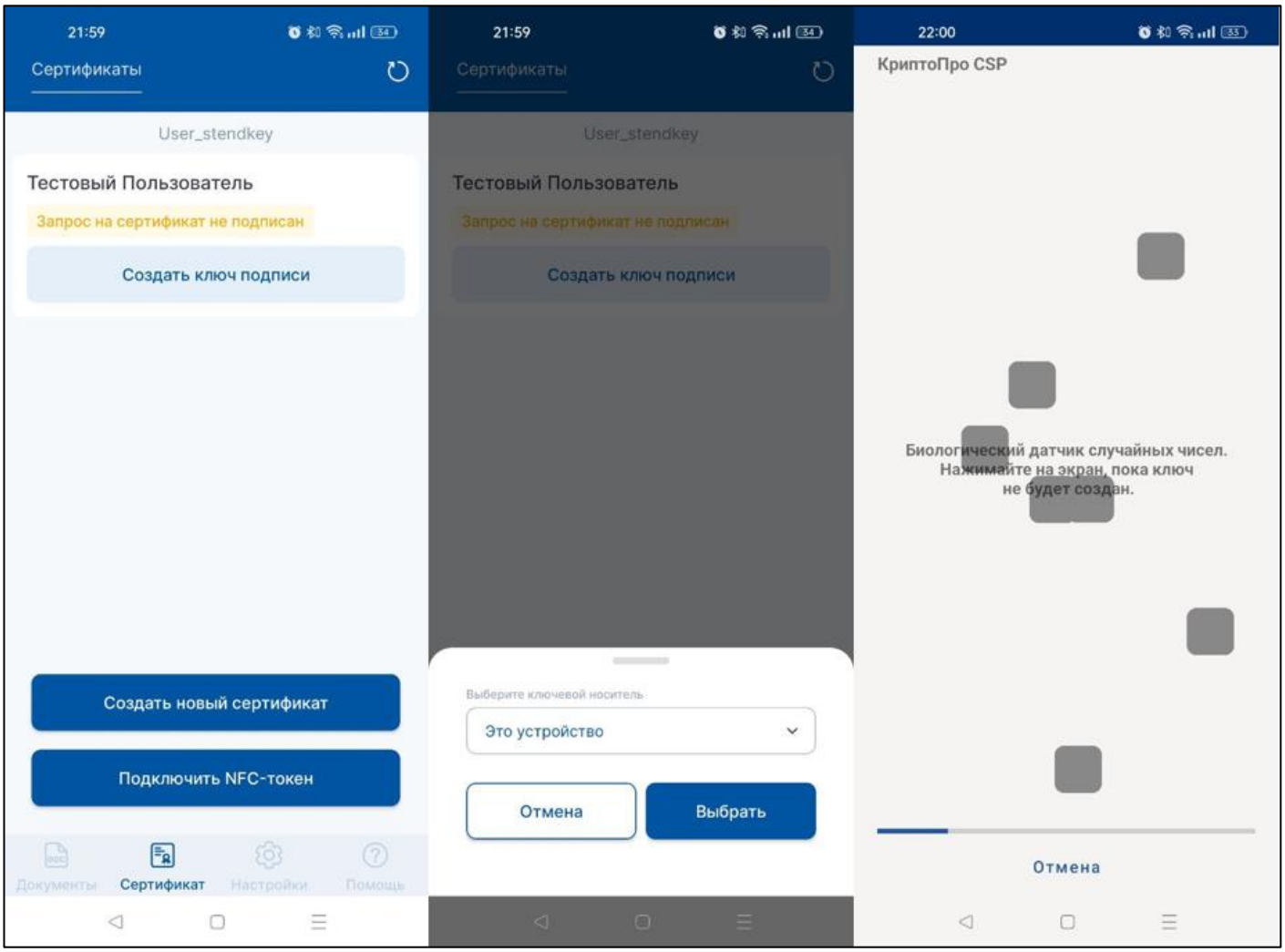

Рисунок 31 — Подписание запроса на сертификат

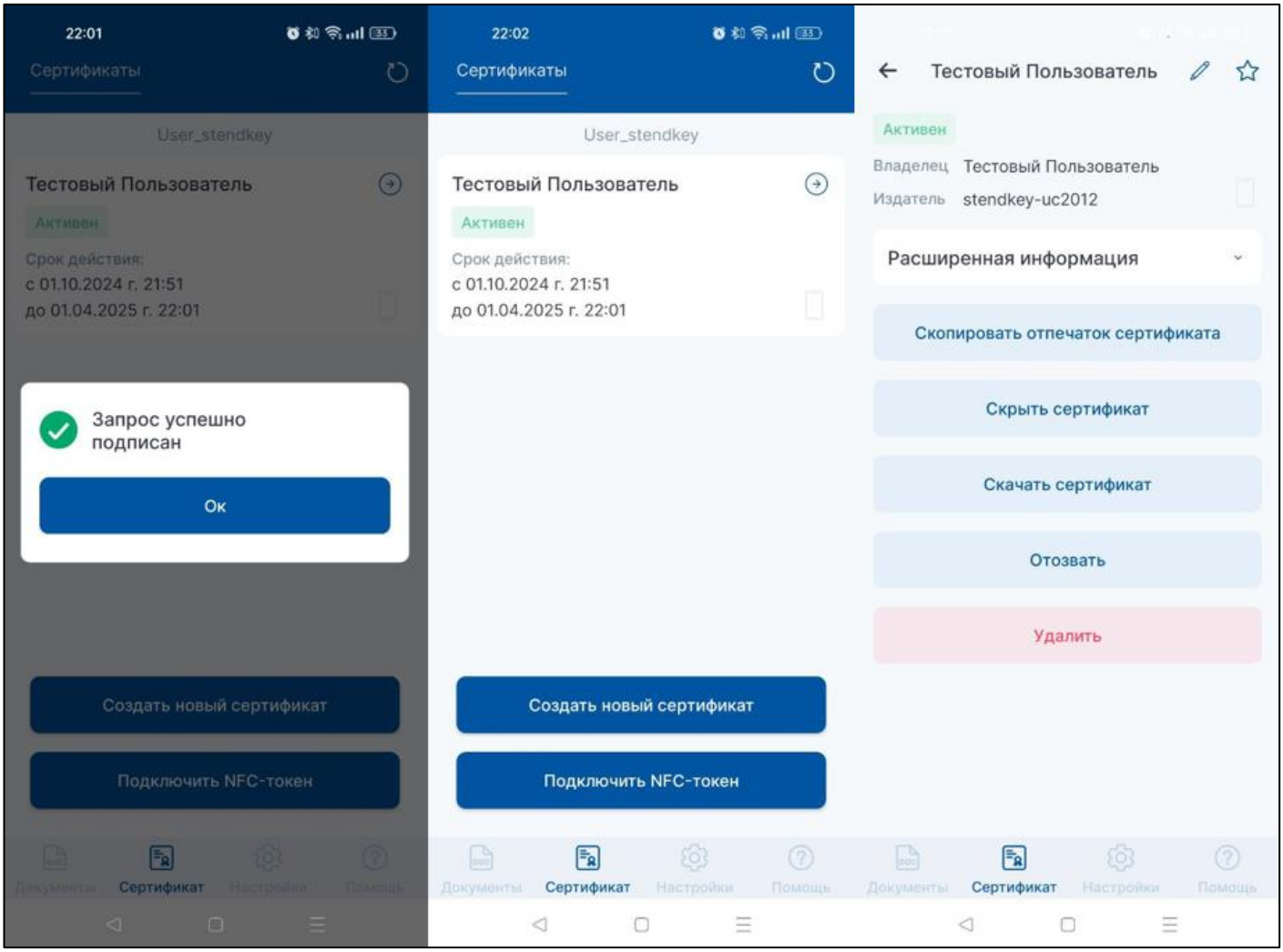

Рисунок 32 — Успешное подписание запроса и выпуск сертификата

5.2. Создание запроса на сертификат с выпуском сертификата в стороннем УЦ с хранением ключей в мобильном приложении

Для создания запроса на новый/первый сертификат Пользователя нужно перейти в раздел «*Сертификаты*» и нажать кнопку «*Создать запрос на сертификат*» (см. Рисунок 28 — Заполнение данных запроса на сертификат).

Далее необходимо выбрать Удостоверяющий центр для выпуска сертификата Пользователя – Сторонний УЦ, отредактировать данные Пользователя, выбрать шаблон сертификата («*Сертификат Пользователя КриптоПро Ключ*»), поставить чек-бокс *«Запрос на сертификат для мобильного приложения»* и нажать кнопку «*Создать запрос на сертификат*») (см. Рисунок 33 — Создание запроса на сертификат с выпуском в стороннем УЦ и хранением в мобильном приложении).

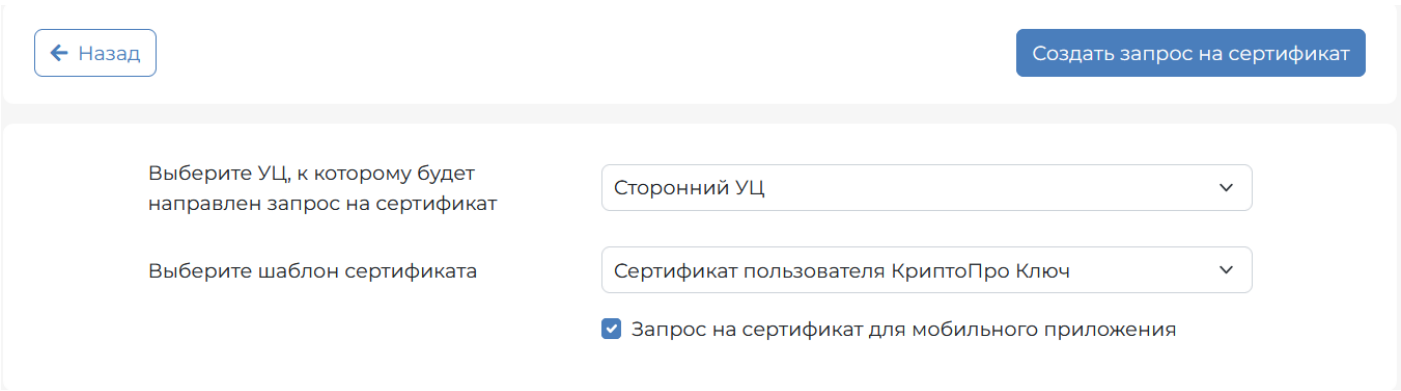

Рисунок 33 — Создание запроса на сертификат с выпуском в стороннем УЦ и хранением в мобильном приложении

Появится окно с информацией о запросе на сертификат. Статус запроса – «*Ожидает подписи*» (см. Рисунок 30 — Запрос на сертификат с хранением в мобильном устройстве).

Дальнейшие действия выполняются на мобильном устройстве

1. Откройте мобильное приложение.
2. Перейдите во вкладку «*Сертификаты*», в списке сертификатов будет запрос со статусом «*Запрос на сертификат не подписан*»
3. Нажмите кнопку «Создать ключ подписи».
4. Будет предложено выбрать место хранения ключей. По умолчанию «*Это устройство*» - ключевая информация сохранен будет сохранена в память устройства в зашифрованном виде.
5. В следующем окне откроется датчик случайных чисел, необходимо нажимать на экран до тех пор, пока полоска снизу не будет заполнена и не появится сообщение «*Запрос успешно подписан*» (см. Рисунок 31 — Подписание запроса на сертификат).
6. Статус запроса изменится на «*Отправлен запрос*».

Запрос на сертификат можно скачать следующими способами:

- из мобильного приложения: Вкладка «*Сертификат*» - запрос на сертификат – «*Скачать запрос на сертификат*» (см. Рисунок 34 — Подписанный запрос на сертификат в мобильном приложении)

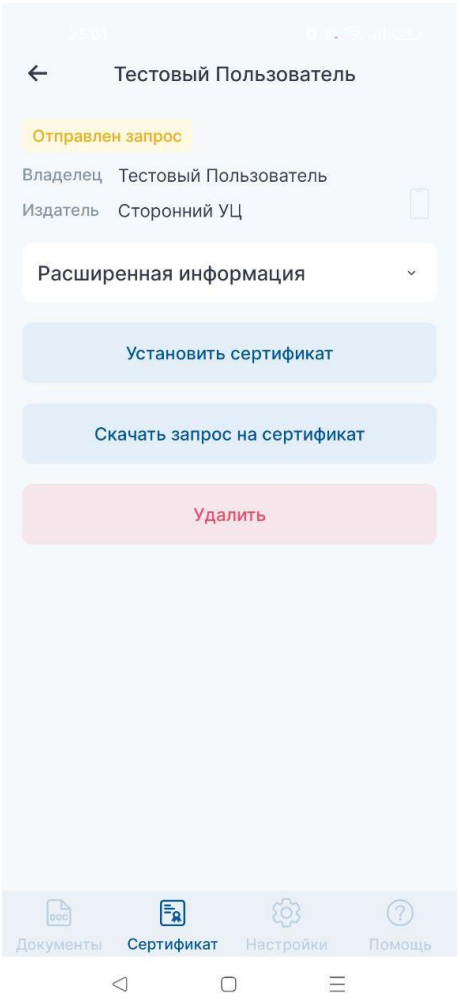

Рисунок 34 — Подписанный запрос на сертификат в мобильном приложении

- в Веб-интерфейсе СЭП. Вкладка «*Сертификаты*» - запрос на сертификат – «*Скачать*» (см. Рисунок 35 — Запрос на сертификат с выпуском в стороннем УЦ).

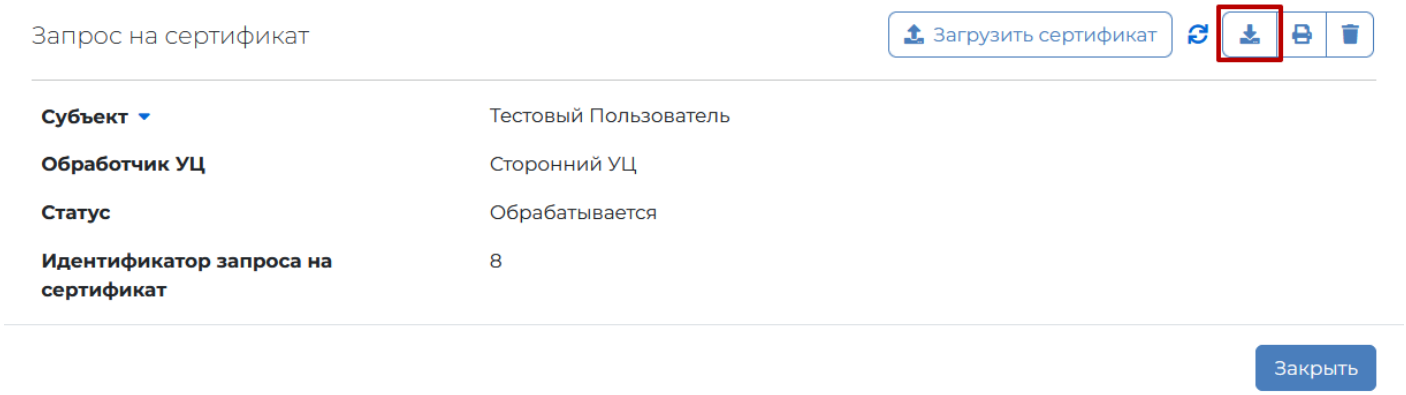

Рисунок 35 — Запрос на сертификат с выпуском в стороннем УЦ

Данный запрос необходимо отправить в Удостоверяющий центр.

В данном руководстве приведен пример использования тестового УЦ КриптоПро https://testgost2012.cryptopro.ru/certsrv/. Информацию о подходящих УЦ для определенного СЭП необходимо запросить у Оператора.

Для выпуска необходимо перейти на страницу УЦ и нажать кнопку «*Отправить готовый запрос PKCS#10 или PKCS#7 в кодировке Base64*». На странице будет отображено поле, в которое нужно вставить текст запроса. Для этого нужно открыть загруженный запрос любым текстовым редактором, скопировать содержимое и вставить в поле «*Base-64-шифрованный запрос сертификата (CMC или PKCS #10 или PKCS #7*)» и нажать кнопку «*Выдать*» (см. Рисунок 36 — Выпуск сертификата в УЦ testgost2012.cryptopro.ru).

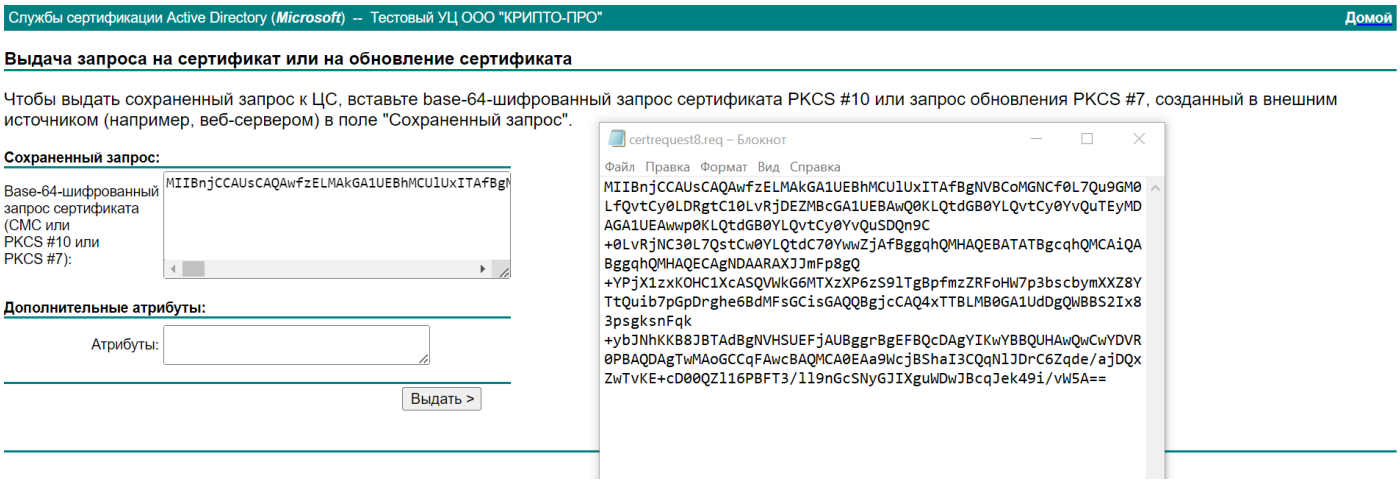

Рисунок 36 — Выпуск сертификата в УЦ testgost2012.cryptopro.ru

Появится сообщение, что запрошенный сертификат был выдан. Его можно скачать по кнопке «*Загрузить сертификат*» (см. Рисунок 37 — Загрузка сертификата testgost2012.cryptopro.ru).

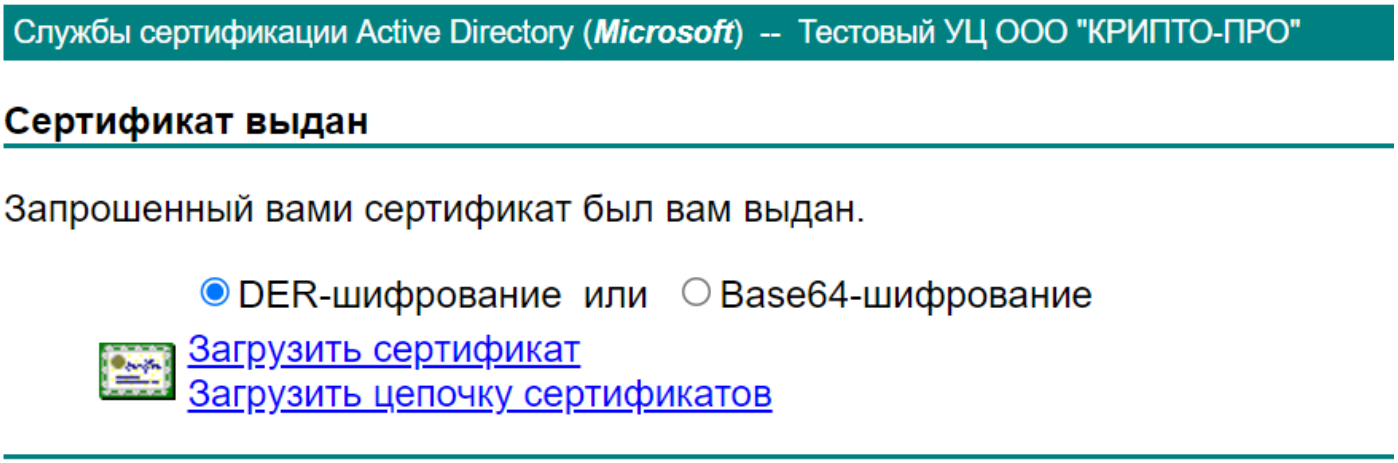

Рисунок 37 — Загрузка сертификата testgost2012.cryptopro.ru

Данный сертификат нужно загрузить в СЭП. Для этого нужно вернуться в Веб-интерфейс СЭП, перейти во вкладку «*Сертификаты*», в списке

сертификатов и запросов найти созданный ранее запрос и нажать кнопку «*Загрузить сертификат*». В появившемся окне нажать кнопку «*Обзор*» и выбрать ранее загруженный файл сертификата. Нажать кнопку «*Загрузить*» (см. Рисунок 38 — Загрузка сертификата стороннего УЦ).

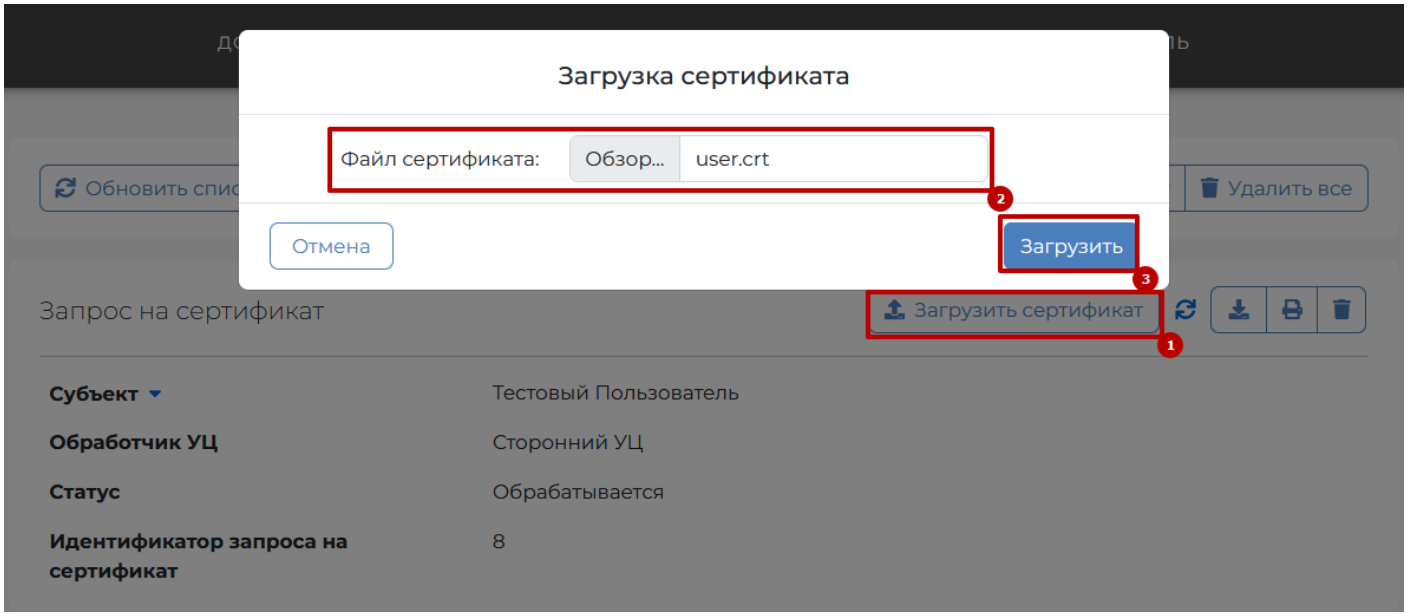

Рисунок 38 — Загрузка сертификата стороннего УЦ

При успешной загрузке сертификата он отобразится в списке доступных (см. Рисунок 39 — Информация о сертификате, выпущенном в стороннем УЦ).

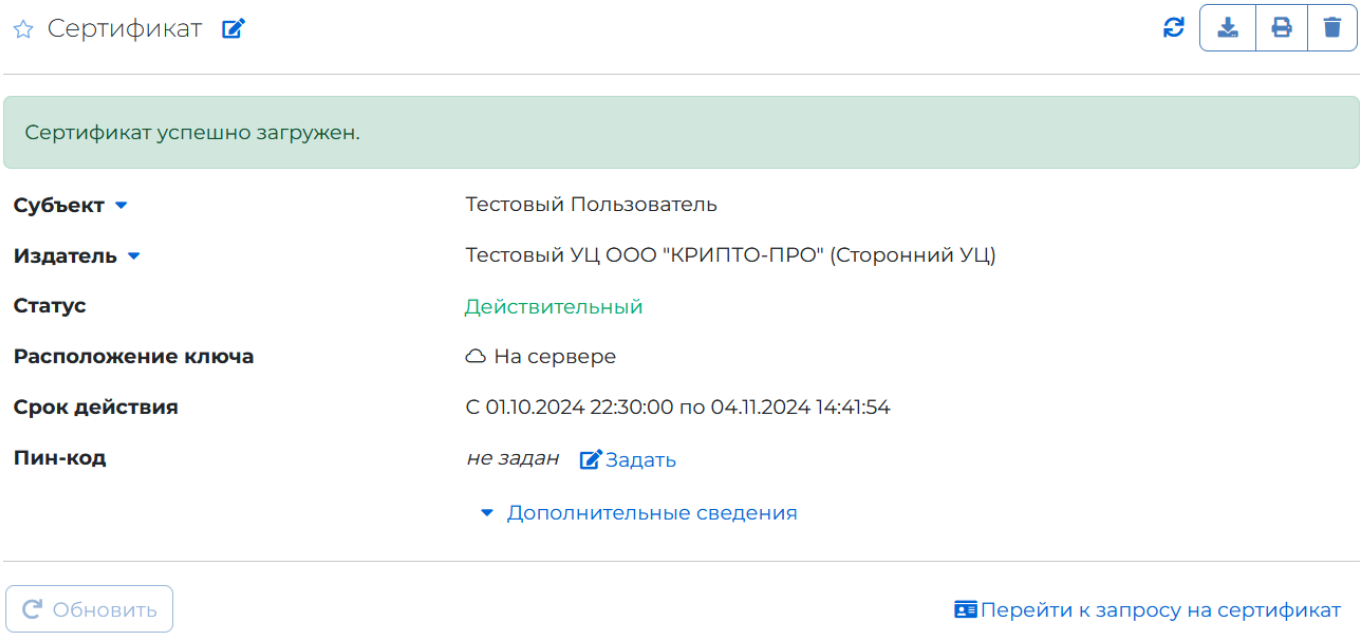

Рисунок 39 — Информация о сертификате, выпущенном в стороннем УЦ

Данный сертификат можно использовать для выполнения криптографических операций.

6. Профиль

Раздел предназначен для управления настройками профиля пользователя. Доступны следующие разделы:

- Редактирование компонентов имени пользователя (см. 6.1)
- Добавление и редактирование контактных данных (см. 6.2)
- Настройка аутентификации (см. 6.3)
- Настройка оповещений (см. 6.4)
- Просмотр и редактирование разрешений (см. 6.5).

6.1. Компоненты имени пользователя

Данный раздел предназначен для редактирования компонентов имени пользователя. Для изменения данных нужно, находясь на вкладке «профиль», открыть раздел «Профиль» и нажать «Редактировать» (см. Рисунок 40 — Компоненты имени).

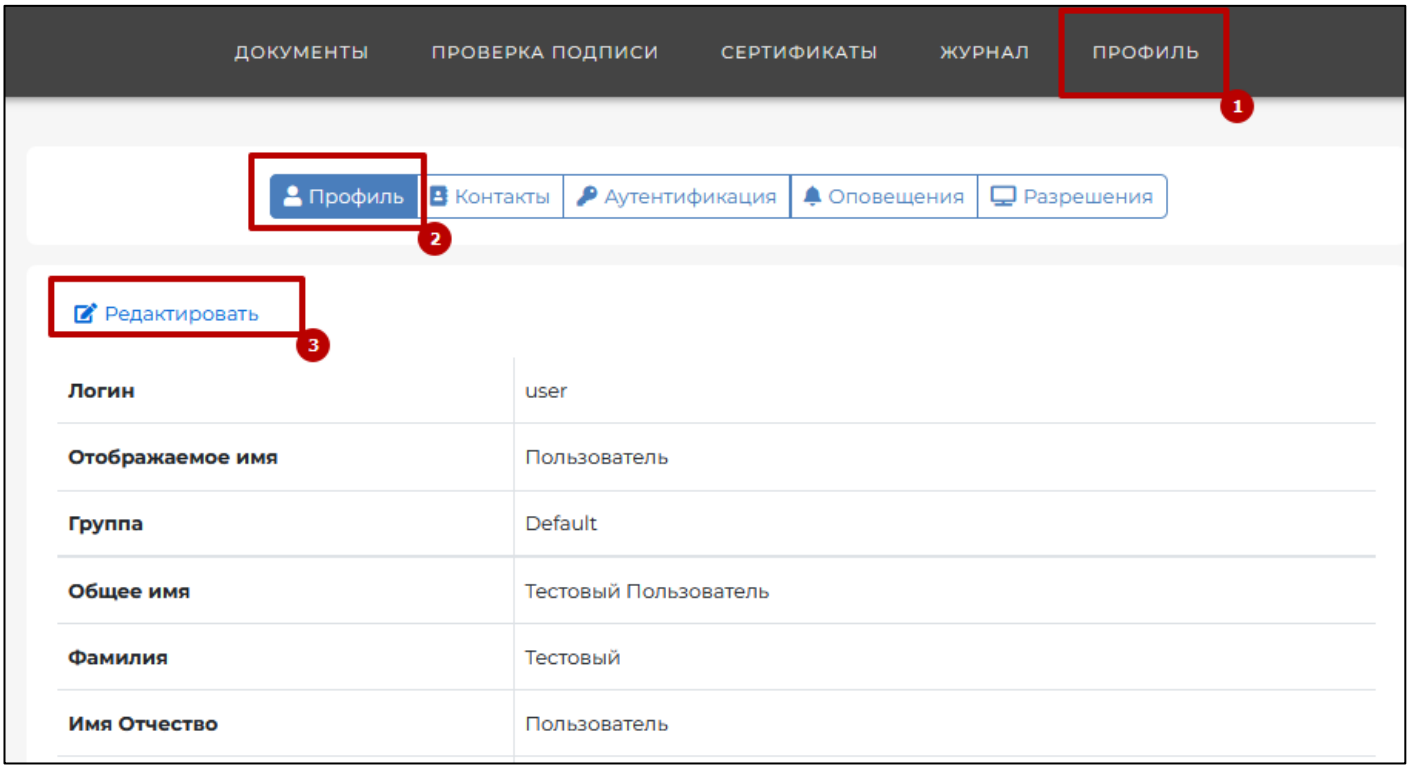

Рисунок 40 — Компоненты имени

После завершения редактирования для сохранения данных нужно нажать кнопку «**Сохранить**». Для отмены изменений нужно нажать кнопку «**Отмена**».

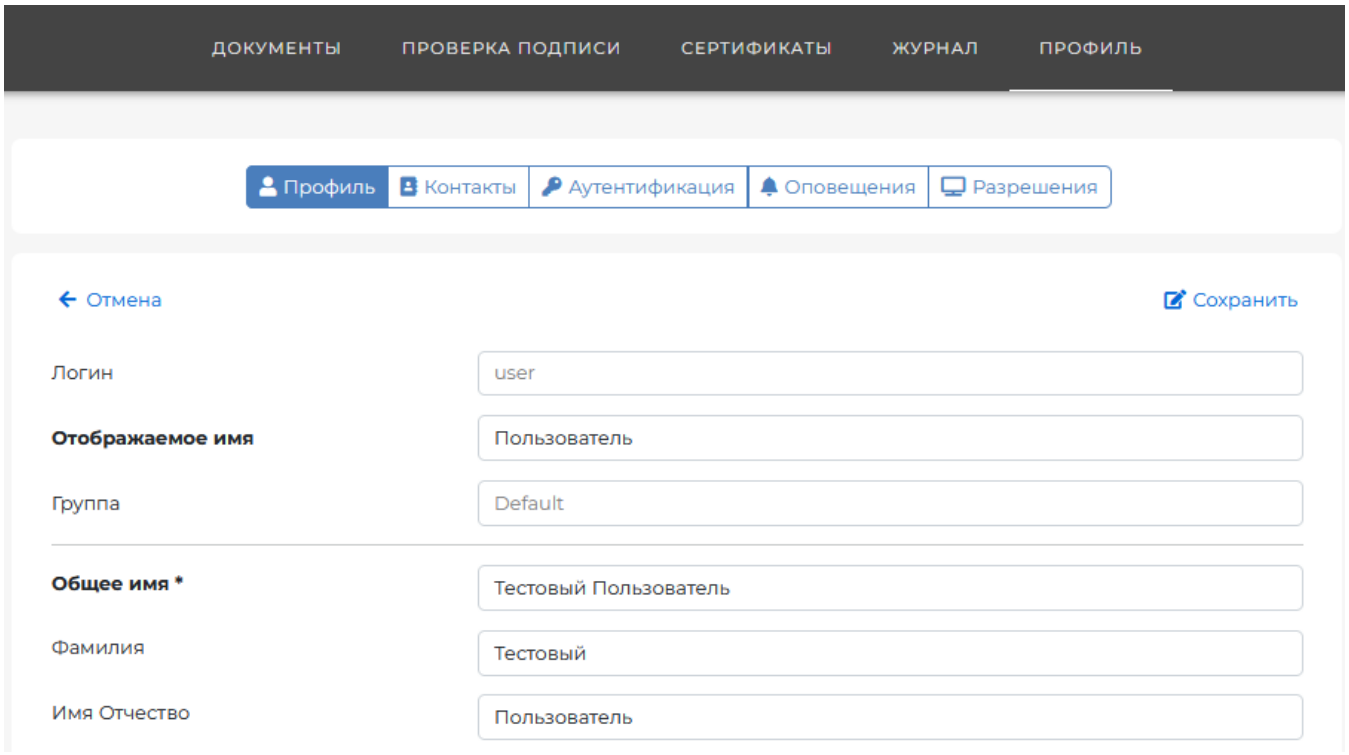

Рисунок 41 — Изменение компонентов имени

Замечание: если возможности редактирования нет, то необходимо обратиться к Оператору.

6.2. Контакты

Раздел предназначен для управления контактной информацией пользователя.

Для добавления номера телефона нужно открыть «*Контакты*» и ввести номер телефона в разделе «*Номера телефонов*» и нажать кнопку «*Добавить*» (см. Рисунок 42 — Добавление номера телефона).

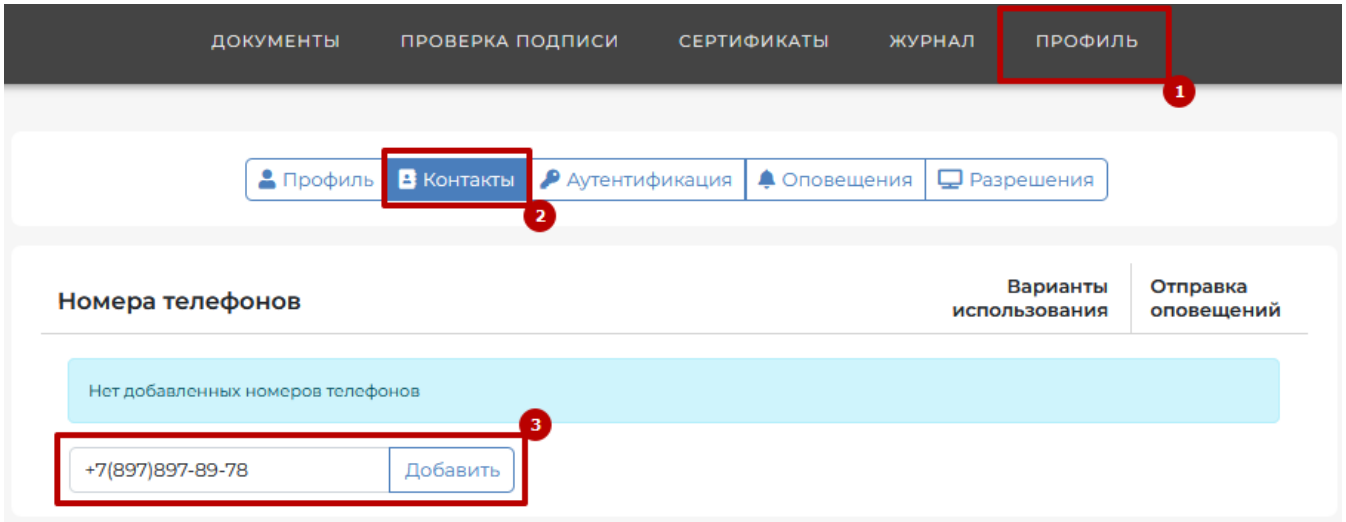

Рисунок 42 — Добавление номера телефона

Для добавления адреса email нужно открыть «*Контакты*» и ввести email в разделе «*Адреса электронной почты*» и нажать кнопку «*Добавить*» (см. Рисунок 43 — Добавление email)

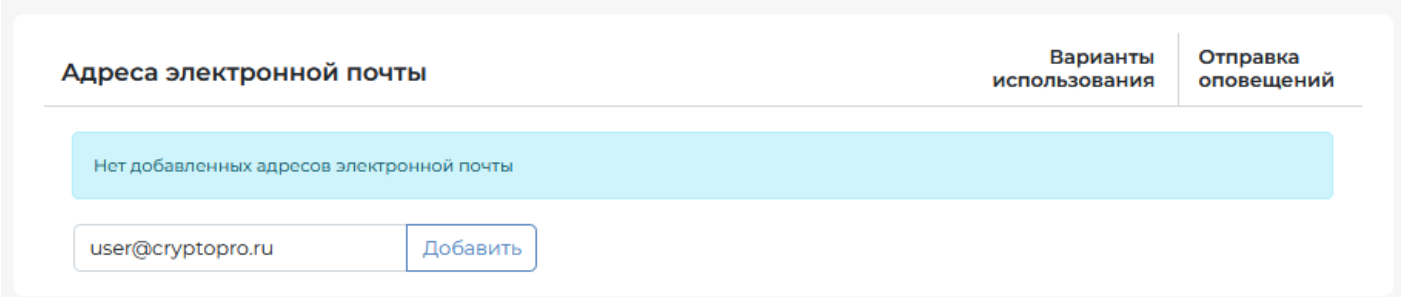

Рисунок 43 — Добавление email

После добавления контактной информации, в зависимости от настроек экземпляра, телефон/email можно использовать для получения оповещения, одноразовых паролей для подтверждения операций или в качестве идентификатора входа.

6.3. Аутентификация

В СЭП предусмотрены методы первичной аутентификации (применяются для аутентификации входа Пользователя в интерфейс СЭП) и методы вторичной аутентификации (применяются для подтверждения действий Пользователя в СЭП).

Доступны следующие методы первичной аутентификации Пользователя:

- «*Только идентификация*» – отсутствие первичной аутентификации (только ввод логина Пользователя при входе в СЭП).
- «*Аутентификация по сертификату*» – аутентификация Пользователя по сертификату; метод доступен только если Пользователю назначен сертификат.
- «*Аутентификация по паролю*» – аутентификация Пользователя по паре «логин-пароль»; пароль может быть сгенерирован Оператором в интерфейсе СЭП и передан Пользователю, либо создан самим пользователем.

Доступны следующие методы вторичной аутентификации Пользователя:

- «*Аутентификация по SMS*» – подтверждение действий Пользователя в СЭП по коду в SMS, отправляемых СЭП на мобильный телефон Пользователя; метод доступен только в случае, если задан номер мобильного телефона Пользователя.
- «*Аутентификация по протоколу OATH*» – подтверждение действий

Пользователя в СЭП по одноразовому паролю OTP-токена; метод доступен только в случае, если заданы параметры OTP-токена.

- «*Аутентификация по электронной почте*» – подтверждение действий Пользователя в СЭП по коду в сообщениях электронной почты, отправляемых СЭП на адрес электронной почты Пользователя; метод доступен только в случае, если задан адрес электронной почты Пользователя.
- «*Аутентификация с помощью мобильного приложения*» – подтверждение действий пользователя СЭП в мобильном приложении.

6.3.1. Настройка первичной аутентификации

6.3.2. Настройка аутентификации по сертификату

Для создания сертификата первичной аутентификации можно импортировать компоненты имени Пользователя из существующего сертификата по кнопке «*Заполнить компоненты имени из сертификата*» (см. Рисунок 44. — Назначение сертификата для первичной аутентификации).

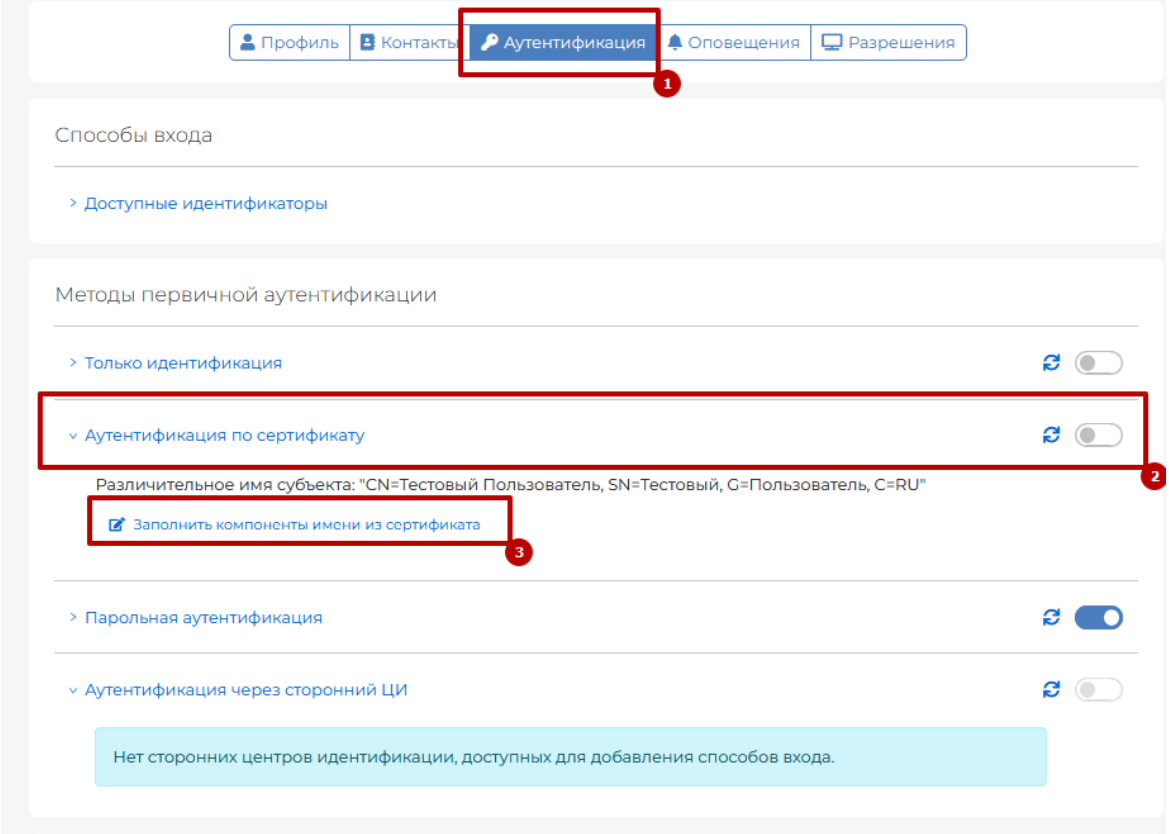

Рисунок 44. — Назначение сертификата для первичной аутентификации

Для включения первичной аутентификации по сертификату необходимо установить переключатель «*Аутентификация по сертификату*» в группе «*Первичная аутентификация*» в активное положение.

6.3.3. Настройка аутентификации по паролю

Для изменения пароля нужно в разделе «*Методы первичной аутентификации*» раскрыть блок «*Аутентификация по паролю*» и нажать кнопку «*Сгенерировать новый*» - для автоматической генерации пароля или «*Изменить*» - для указания собственного пароля (см. Рисунок 45. — Изменение пароля для первичной аутентификации).

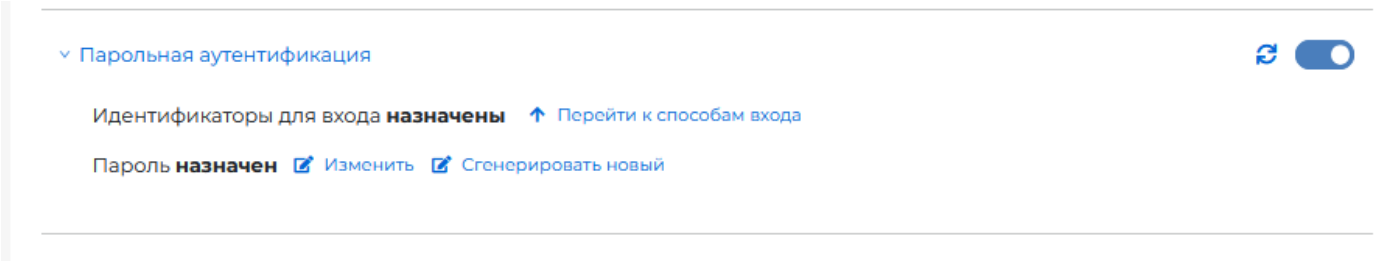

Рисунок 45. — Изменение пароля для первичной аутентификации

Для генерации случайного пароля нужно нажать кнопку «*Сгенерировать новый*». Появится окно ввода старого пароля, после ввода предыдущего пароля отобразится новый пароль (см. Рисунок 46 - Успешная генерация пароля).

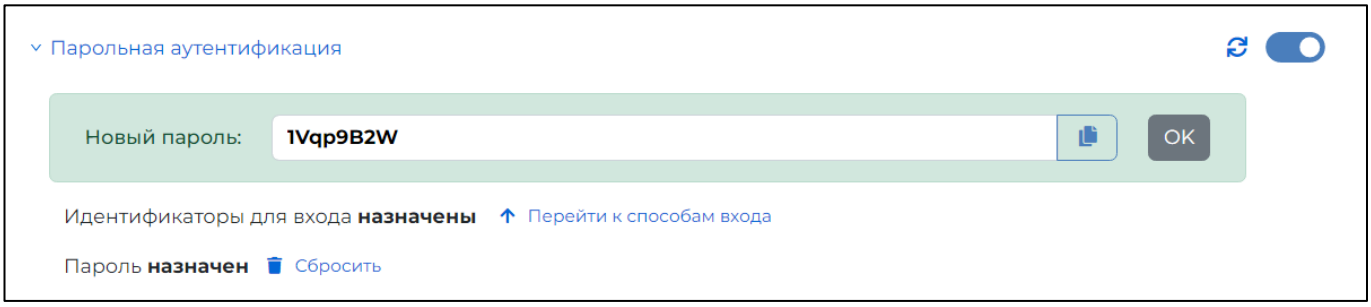

Рисунок 46 - Успешная генерация пароля

Для задания собственного пароля нужно нажать кнопку «*Изменить*». Появится окно, где необходимо указать старый пароль и задать, и подтвердить новый (см. Рисунок 47 — Изменение пароля).

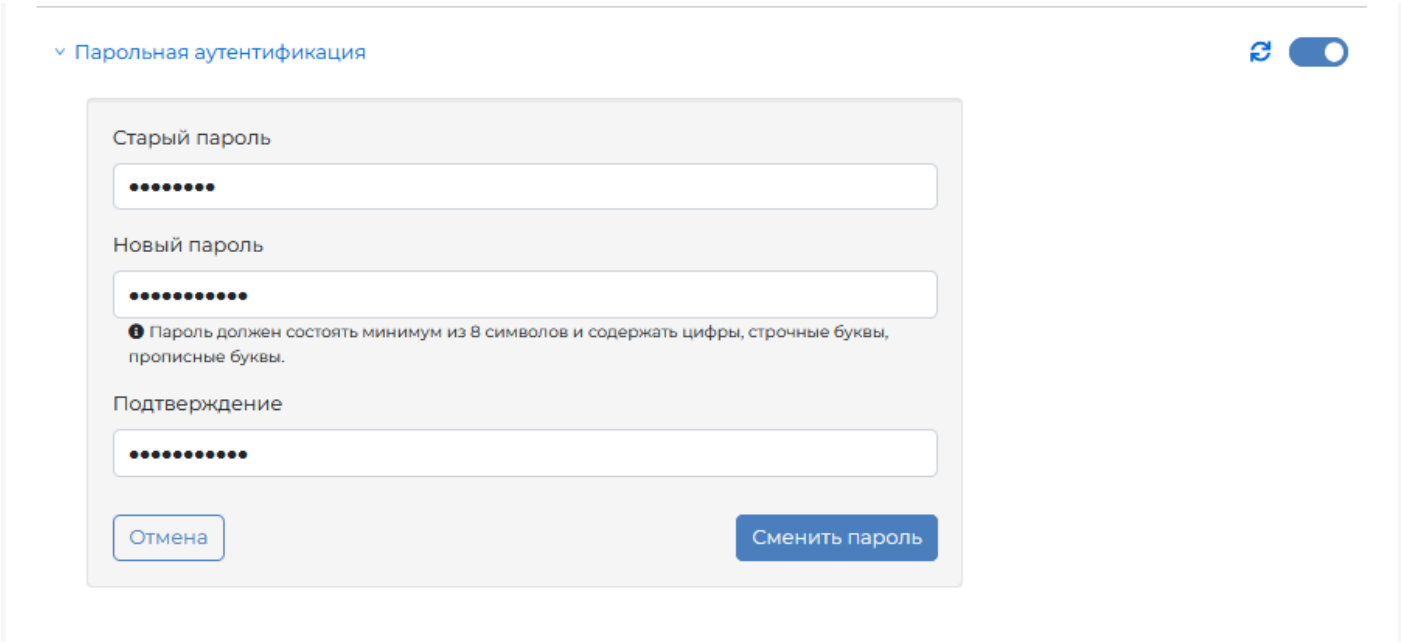

Рисунок 47 — Изменение пароля

Если пароль был забыт, то необходимо обратиться к Оператору для генерации нового пароля.

6.3.4. Настройка вторичной аутентификации

6.3.5. Настройка аутентификации по SMS

Для настройки вторичной аутентификации по SMS следует в группе «*Методы вторичной аутентификации*» раскрыть блок «*Аутентификация по SMS*» и нажать кнопку «*Назначить*». Если ранее Пользователю не был указан контактный номер телефона, то отобразится информация о необходимости добавления контактного номера телефона. Для добавления номера необходимо нажать кнопку «*Добавить*».

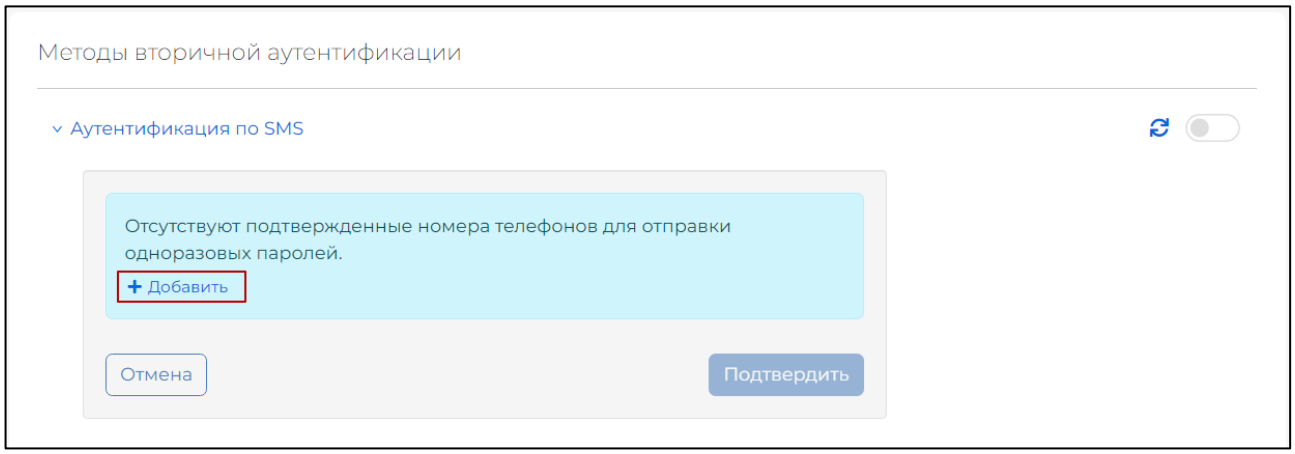

Рисунок 48 — Аутентификация по SMS

После чего произойдет перенаправление на страницу «*Контакты*». После ввода контактного номера телефона нужно нажать кнопку «*Добавить*».

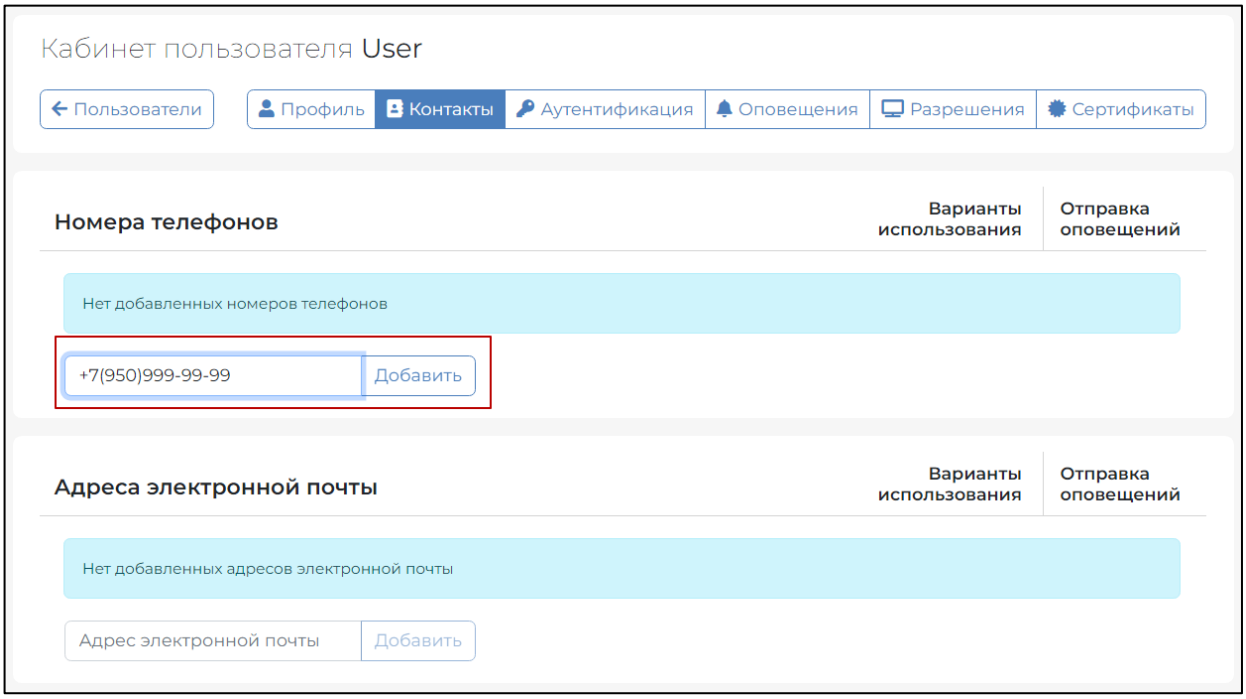

Рисунок 49 — Добавление номера телефона

После успешного добавления номера телефона появится сообщение: «*Номер телефона успешно добавлен*». Перейдите во вкладку «*Аутентификация*».

Раскройте блок «*Аутентификация по SMS*» в «*Методах вторичной аутентификации*» и нажмите кнопку «*Назначить*». Добавленный ранее номер телефона теперь будет доступен для выбора. Для выбора добавленного номера телефона для получения одноразовых паролей нажмите кнопку «*Подтвердить*».

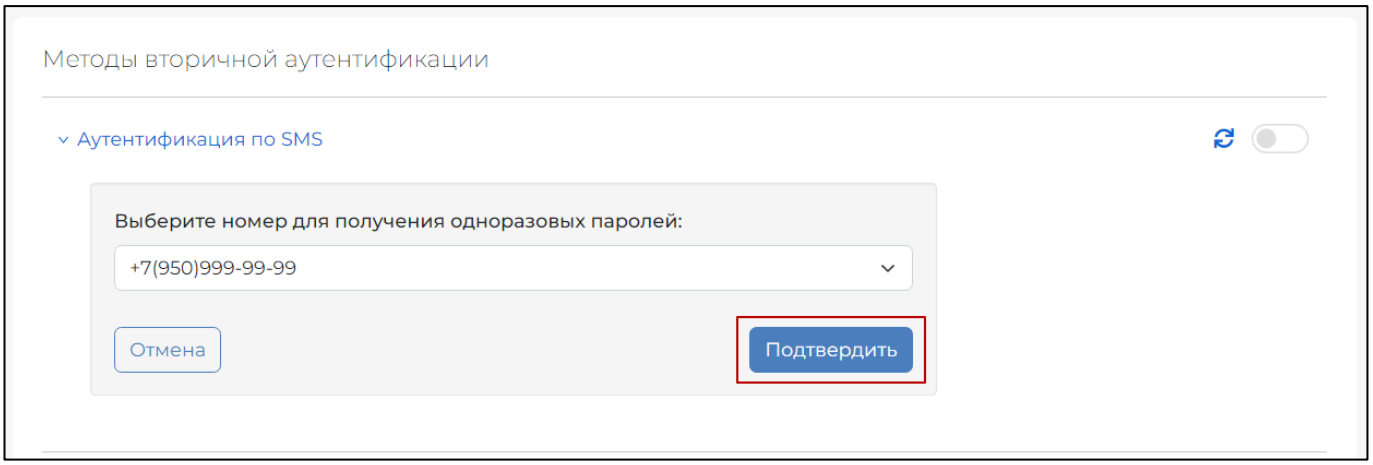

Рисунок 50 — Выбор номера телефона для получения одноразовых паролей

Для включения вторичной аутентификации по SMS необходимо установить переключатель «*Аутентификация по SMS*» в группе «*Вторичная аутентификация*» в активное положение.

6.3.6. Настройка аутентификации по протоколу OATH

Для настройки вторичной аутентификации по протоколу OATH (токену TOTP/HOTP, например, eToken Pass) нужно в группе «*Методы вторичной аутентификации*» раскрыть блок «*Аутентификация по протоколу OATH*» и нажать ссылку «*Добавить токен*» (см. Рисунок 51 — Настройка аутентификации по протоколу OATH).

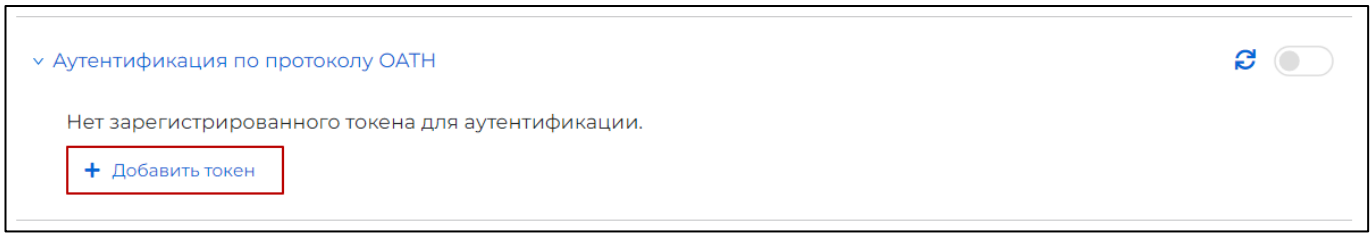

Рисунок 51 — Настройка аутентификации по протоколу OATH

Далее необходимо выбрать способ генерации одноразовых паролей: брелок или мобильное приложение.

1. Брелок.

В появившемся поле ввода параметров аутентификации по протоколу OATH следует указать серийный номер OTP-токена, первый и второй пароли OTP, после чего нажать кнопку «*Сохранить*» (см. Рисунок 52 — Ввод параметров аутентификации по протоколу OATH).

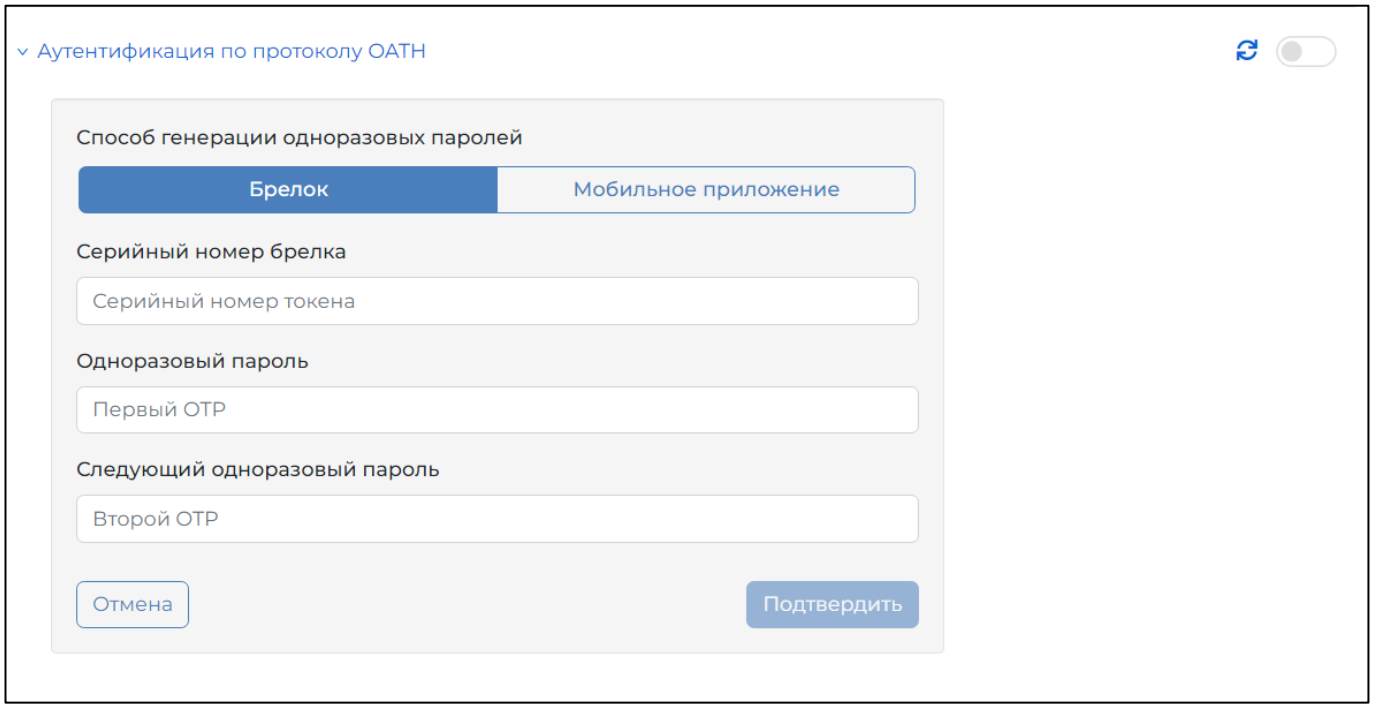

Рисунок 52 — Ввод параметров аутентификации по протоколу OATH

2. Мобильное приложение

Для получения данных инициализации для настройки мобильного приложения нажмите кнопку «*Подтвердить*». Необходимые данные отобразятся на экране.

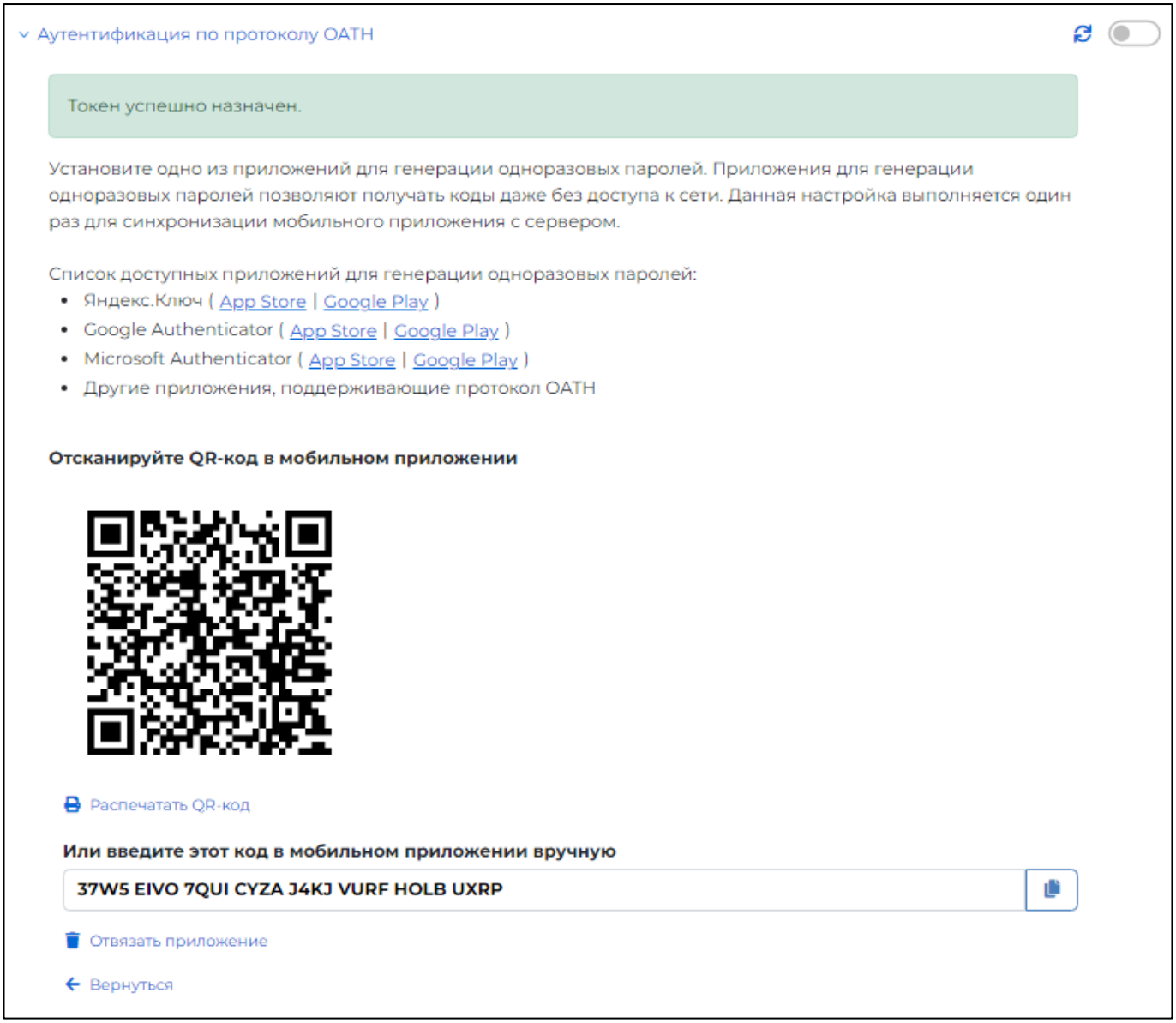

Рисунок 53 — Назначение oath-токена для мобильного приложения

Для включения вторичной аутентификации по протоколу OATH необходимо установить переключатель «*Аутентификация по протоколу OATH*» в группе «*Вторичная аутентификация*» в активное положение.

6.3.7. Настройка аутентификации по электронной почте

Для настройки вторичной аутентификации по электронной почте следует в группе «*Методы вторичной аутентификации*» раскрыть блок «Аутентификация по электронной почте» и нажать кнопку «*Назначить*». Если ранее не был указан контактный номер телефона, то отобразится информация о необходимости

добавления контактного номера телефона. Для добавления номера необходимо нажать кнопку «*Добавить*» (см. Рисунок 54 — Аутентификация по email).

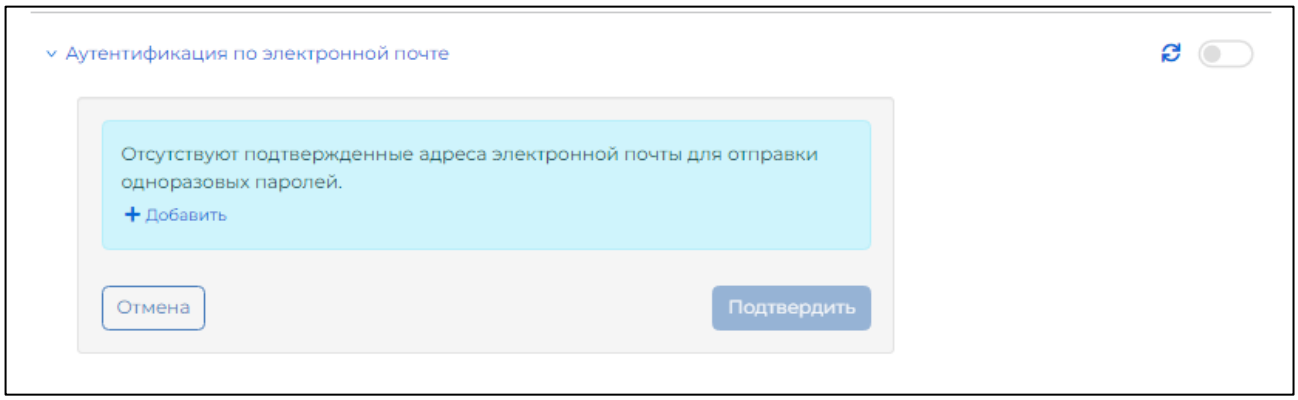

Рисунок 54 — Аутентификация по email

После чего произойдет перенаправление на страницу «*Контакты*». После ввода адреса email нужно нажать кнопку «*Добавить*».

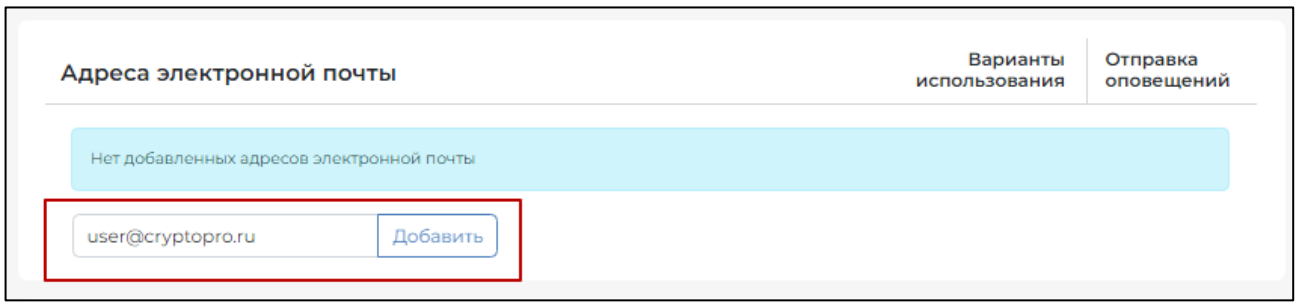

Рисунок 55 — Добавление адреса электронной почты

После успешного добавления адреса электронной почты появится сообщение: «*Адрес электронной почты успешно добавлен*». Перейдите во вкладку «*Аутентификация*».

Раскройте блок «*Аутентификация по электронной почте*» в «*Методах вторичной аутентификации*» и нажмите кнопку «*Назначить*». Добавленный ранее адрес электронной почты теперь будет доступен для выбора. Для выбора добавленного адреса электронной почты для получения одноразовых паролей нажмите кнопку «*Подтвердить*» (см. Рисунок 55 — Добавление адреса электронной почты).

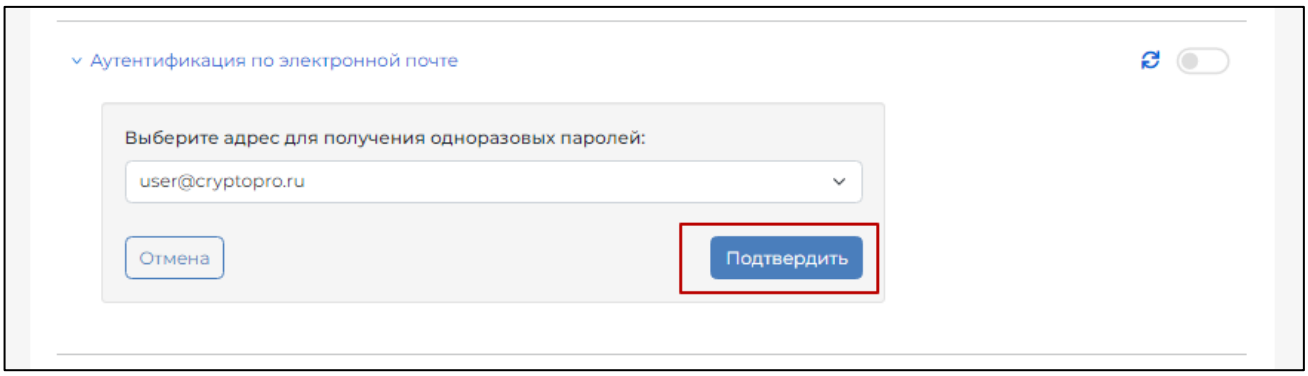

Рисунок 56 — Выбор адреса email для получения одноразовых паролей

Для включения вторичной аутентификации по email необходимо установить переключатель «*Аутентификация по электронной почте*» в группе «*Вторичная аутентификация*» в активное положение.

6.3.8. Настройка аутентификации с помощью мобильного приложения

Для настройки вторичной аутентификации с помощью мобильного приложения нужно в группе «*Методы вторичной аутентификации*» раскрыть блок «*Аутентификация с помощью мобильного приложения*» и нажать кнопку «*Добавить устройство*» (см. Рисунок 57 — Настройка аутентификации с помощью мобильного приложения).

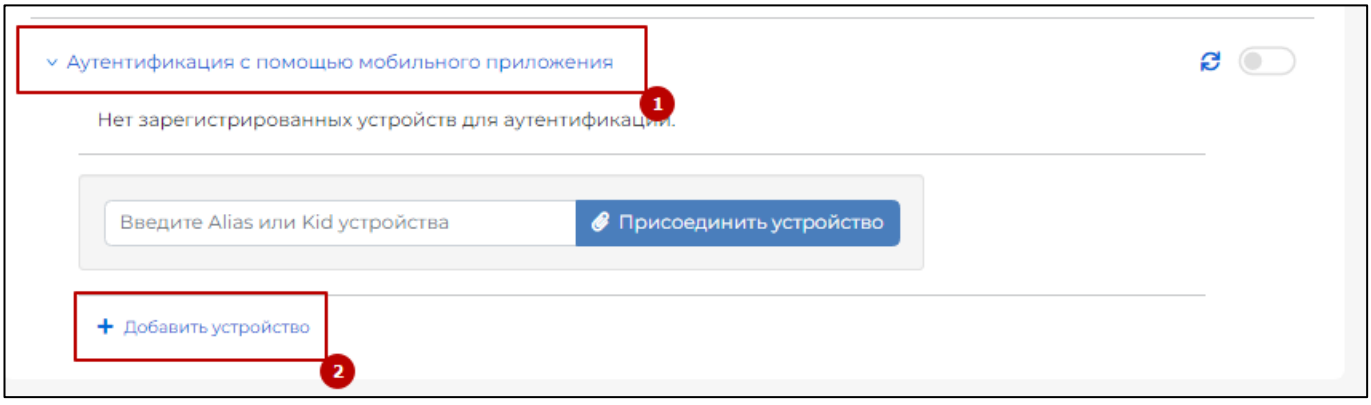

Рисунок 57 — Настройка аутентификации с помощью мобильного приложения

Далее отобразится QR-код, который необходимо отсканировать в мобильном приложении.

Рисунок 58 — Данные для инициализации устройства

Для включения вторичной аутентификации по мобильному приложению нужно установить переключатель «*Аутентификация по мобильному приложению*» в группе «*Вторичная аутентификация*» в активное положение.

6.3.9. Настройка подтверждения и доступа к операциям СЭП

После успешной настройки параметров аутентификации необходимо определить операции, которые необходимо подтверждать выбранным методом вторичной аутентификации и доступ к операциям в СЭП.

Операции, доступ к котором может быть ограничен:

- Подпись документа.
- Шифрование/расшифрование документа.
- Создание запроса на сертификат.
- Удаление сертификата.

- Обновление сертификата.
- Отзыв сертификата.
- Смена ПИН-кода закрытого ключа.

Можно установить подтверждение следующих операций:

- Выпуск маркера (вход в ЦИ).
- Подпись документа.
- Расшифрование документа.
- Создание запроса на сертификат.
- Смена ПИН-кода закрытого ключа.
- Обновление сертификата.
- Отзыв сертификата.
- Удаление сертификата.
- Доступ к закрытому ключу.

Подтверждение и доступ Пользователя к операциям в СЭП настраиваются в параметрах настройки аутентификации (см. Рисунок 59 — Настройка подтверждения операций и Рисунок 60 — Настройка доступа к операциям СЭП).

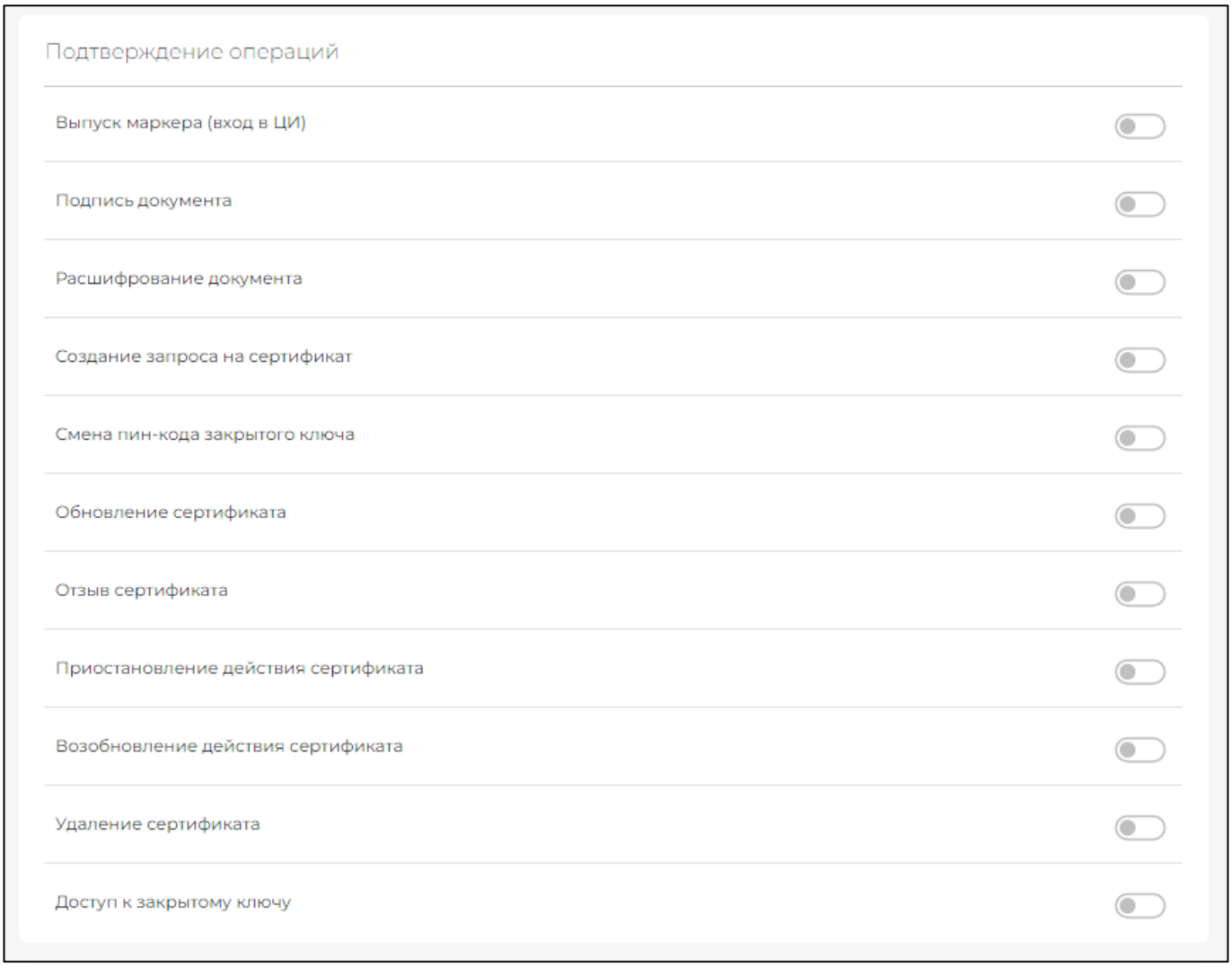

Рисунок 59 — Настройка подтверждения операций

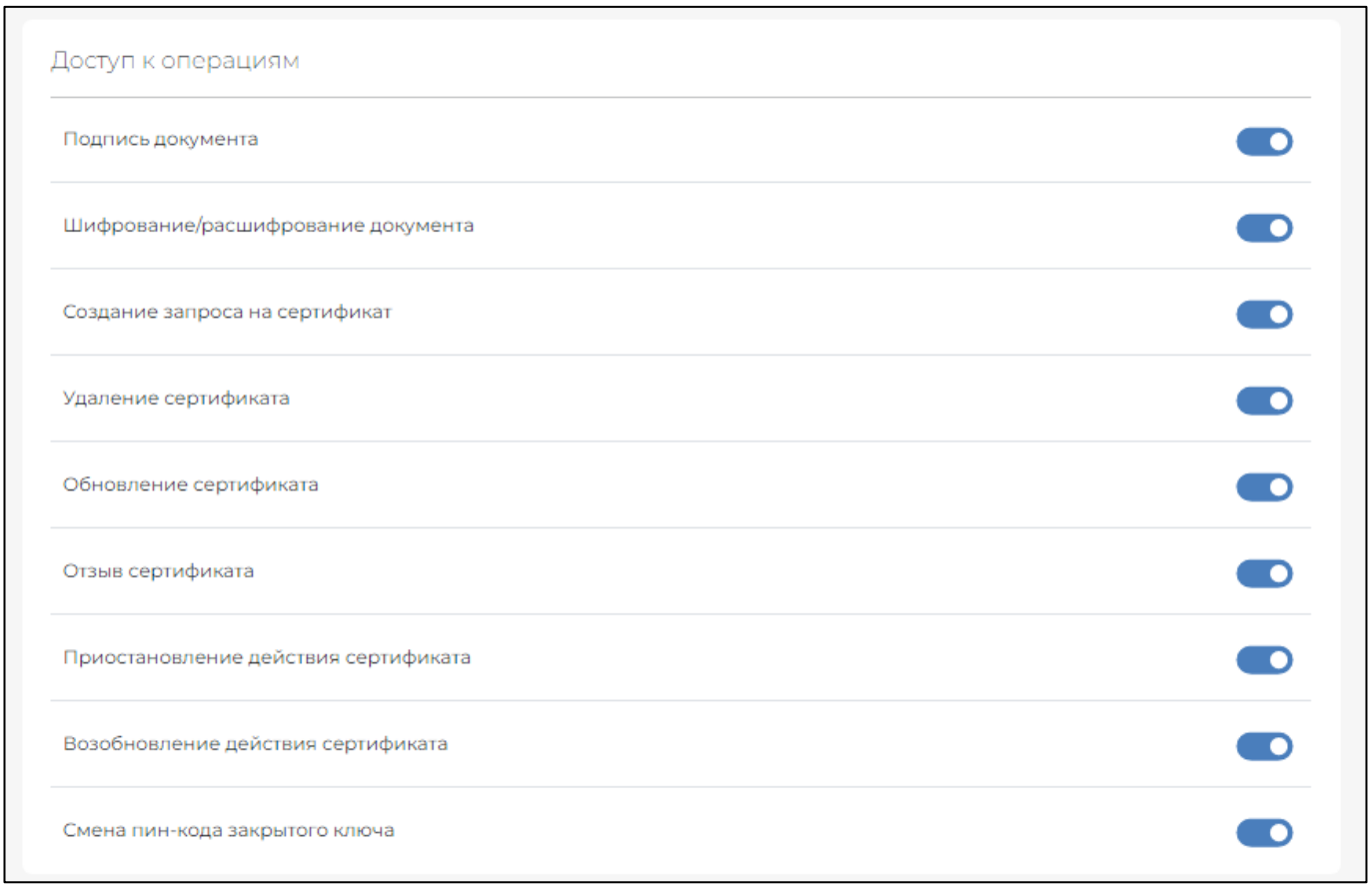

Рисунок 60 — Настройка доступа к операциям СЭП

Замечание: если редактирование доступа и подтверждения операций недоступно, то нужно обратиться к Оператору.

6.4. Оповещение

Раздел позволяет управлять Оповещениями Пользователя. Доступные способы получения уведомлений для пользователя:

- SMS;
- Email;
- PUSH.

Для изменения данных нужно, находясь на вкладке «Профиль», открыть раздел «Оповещения» и активировать один или несколько переключателей напротив события, о котором необходимо включить оповещение (см. Рисунок 61 — Настройка оповещения).

Перед настройкой оповещения необходимо убедиться, что заполнена контактная информация того типа, для которого планируется активировать переключатель (см. подраздел 6.2).

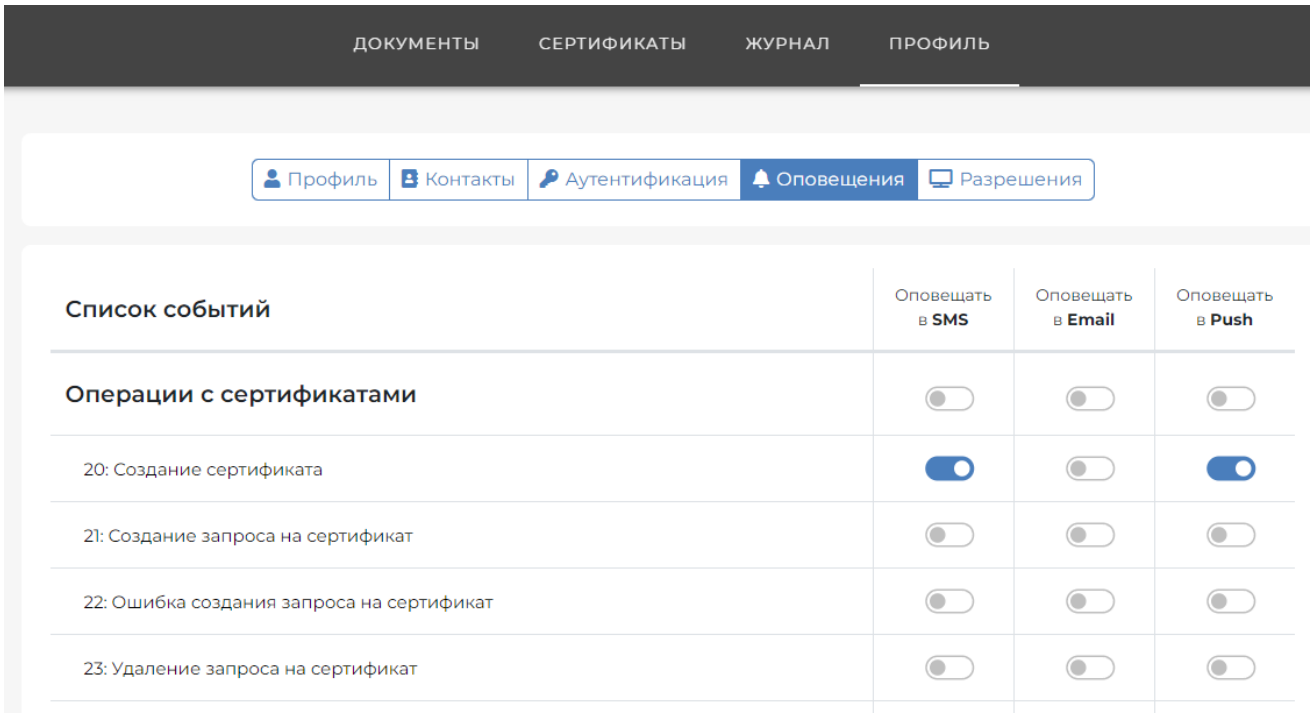

Рисунок 61 — Настройка оповещения

6.5. Разрешения

Раздел позволяет отзывать разрешения, выданные прикладным системам на доступ к сервисам КриптоПро Ключ для данного Пользователя.

Для отзыва разрешения необходимо выбрать приложение, для которого нужно отозвать разрешение и нажать кнопку «*Отозвать*». Как правило, в данном списке уже присутствует разрешение, выданное Веб-интерфейсу. В случае отзыва данного разрешения Пользователю придется пройти процедуру аутентификации на Веб-интерфейсе повторно.

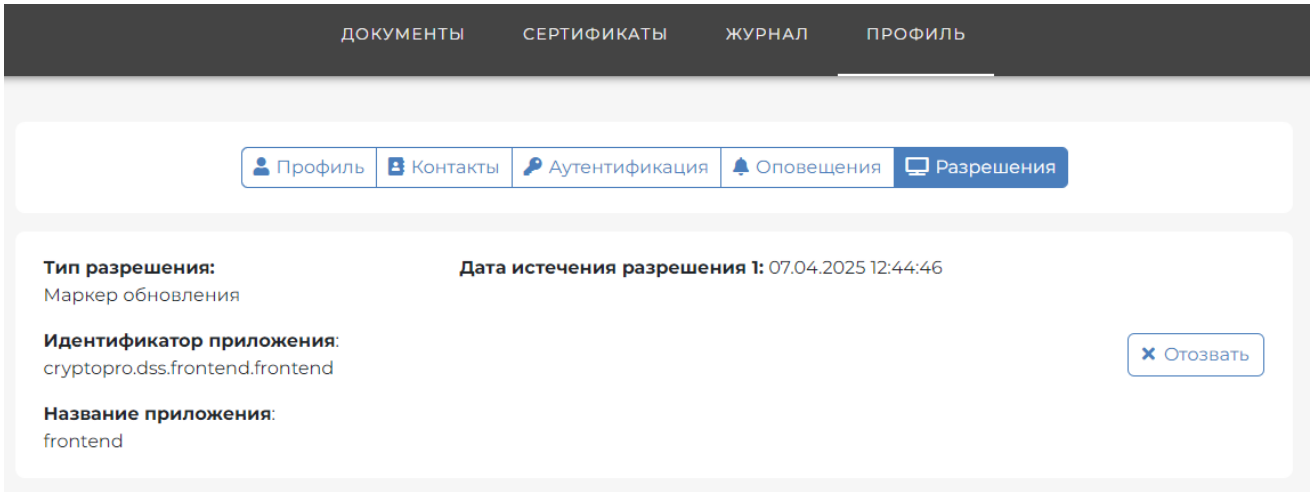

Рисунок 62 — Разрешения

7. Контроль целостности мобильного приложения

В целях исключения рисков преднамеренной и непреднамеренной модификации мобильного приложения (МП), установленного Пользователем на мобильное устройство из магазина приложений, Пользователю следует выполнить процедуру контроля целостности полученного мобильного приложения, если таковая не была выполнена Администратором (безопасности). Описание процедуры контроля целостности приложения приведено в документе «ЖТЯИ.00118-01 91 01 Руководство Администратора» в разделе «Развертывание КриптоПро Ключ».

Перечень рисунков