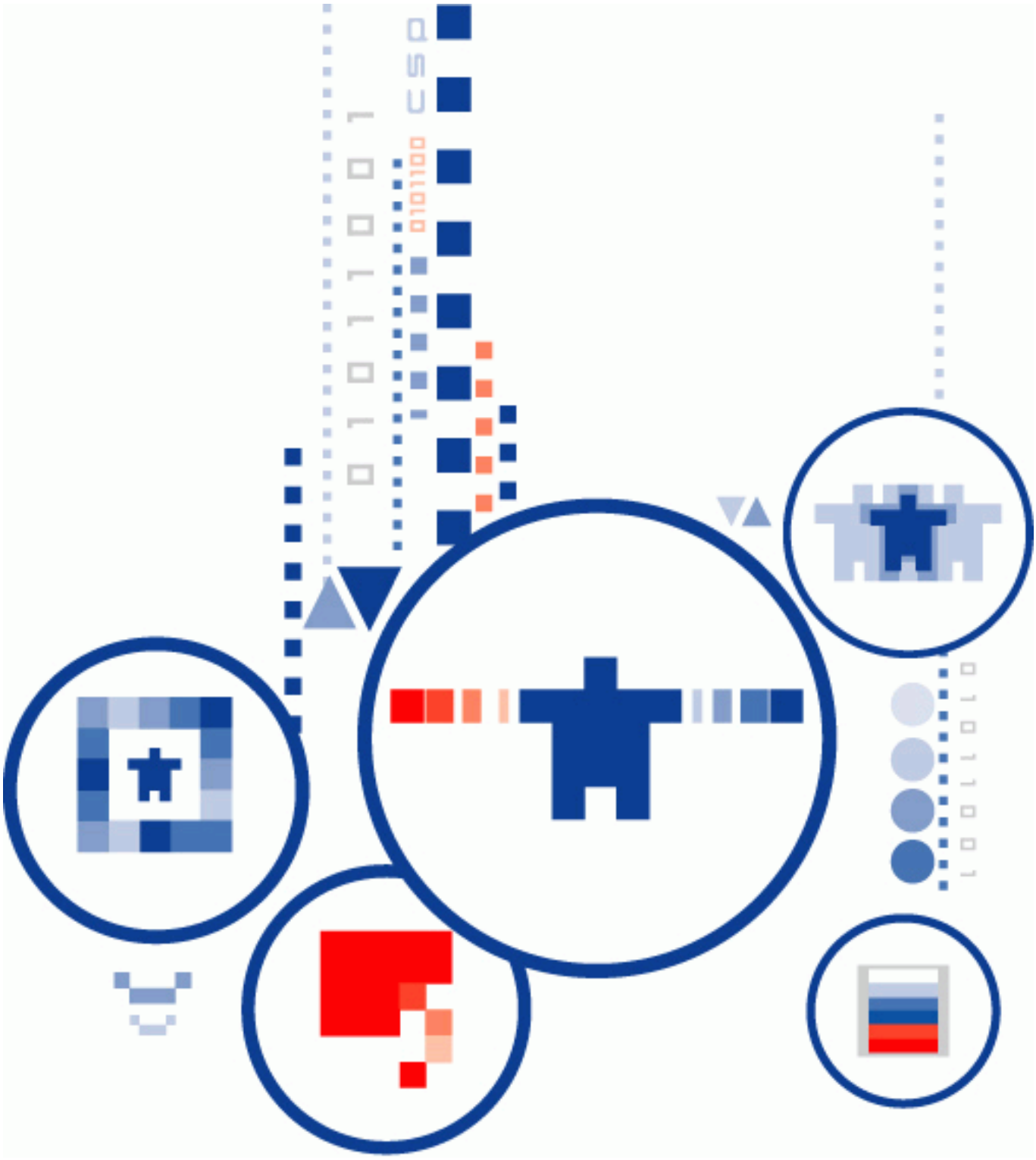
УТВЕРЖДЁН
ЖТЯИ.00082-01 90 03 06-ЛУ

ЖТЯИ.00082-01 90 03 06



Модуль аутентификации myDSS для ПАК «КриптоПро DSS»

версии 1.0

Аннотация

Настоящая инструкция содержит описание порядка использования программного комплекса «КриптоПро myDSS» в составе ПО "Модуль аутентификации myDSS для ПАК «КриптоПро DSS»" и мобильного приложения myDSS для вторичной аутентификации и подтверждения транзакций (создания электронной подписи, формирования запроса на создание сертификата ключа подписи и прочих операций, требующих дополнительного подтверждения) в ПАК «КриптоПро DSS».

Инструкция может быть использована Пользователями и Операторами Сервиса электронной подписи ООО «КРИПТО-ПРО» (СЭП КриптоПро) и в прочих системах электронной подписи на базе ПАК «КриптоПро DSS».

Информация о разработчике «КриптоПро myDSS»:

ООО «КРИПТО-ПРО»

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

Телефон: (495) 995 4820

http://www.CryptoPro.ru

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

E-mail: info@CryptoPro.ru

Содержание

1. Общие положения.

Программный комплекс «КриптоПро myDSS» состоит из серверной части - ПО "Модуль аутентификации myDSS для ПАК «КриптоПро DSS»" и мобильного приложения myDSS.

Модуль аутентификации myDSS для ПАК «КриптоПро DSS» обеспечивает взаимодействие с мобильными приложениями посредством отправки PUSH-нотификаций.

Мобильное приложение myDSS для смартфона под управлением Apple iOS или Google Android обеспечивает строгую криптографическую аутентификацию пользователей ПАК «КриптоПро DSS», безопасное online-взаимодействие, отображение документа и подтверждение операций, что позволяет выполнить требования, предъявляемые регулятором к средствам электронной подписи, и использовать в СЭП квалифицированную электронную подпись для систем дистанционного банкинга, порталов госуслуг, систем ЭДО, электронных торговых площадках и т.п. При этом клиентская часть myDSS может также быть встроена в мобильное приложение прикладной информационной системы, интегрированной с ПАК «КриптоПро DSS».

Настоящая инструкция определяет порядок действия Оператора СЭП для подключения Пользователям вторичной аутентификации с использованием мобильного приложения myDSS и действия Пользователей по установке и использованию приложения myDSS.

Для работы приложения myDSS необходимо устройство под управлением операционной системы Google Android версии 4.0 и новее, или Apple iOS версии 8.0 и новее.

2. Подключение Пользователю вторичной аутентификации с использованием мобильного приложения

Настройка метода вторичной аутентификации пользователя СЭП с применением мобильного приложения myDSS осуществляется Оператором в следующем порядке:

1. Подключиться к личному кабинету Оператора по адресу: https://stenddss.cryptopro.ru/sts/admins/ (*тут и далее указаны адреса общего*

экземпляра тестового СЭП КРИПТО-ПРО, адреса систем и экземпляров СЭП отдельных Заказчиков могут отличаться и должны уточняться в КРИПТО-ПРО);

2. Перейти в раздел «***Пользователи***»;
3. Выбрать нужного Пользователя и зайти в меню «***Настройки аутентификации***», нажав на значок (см. Рисунок 1):

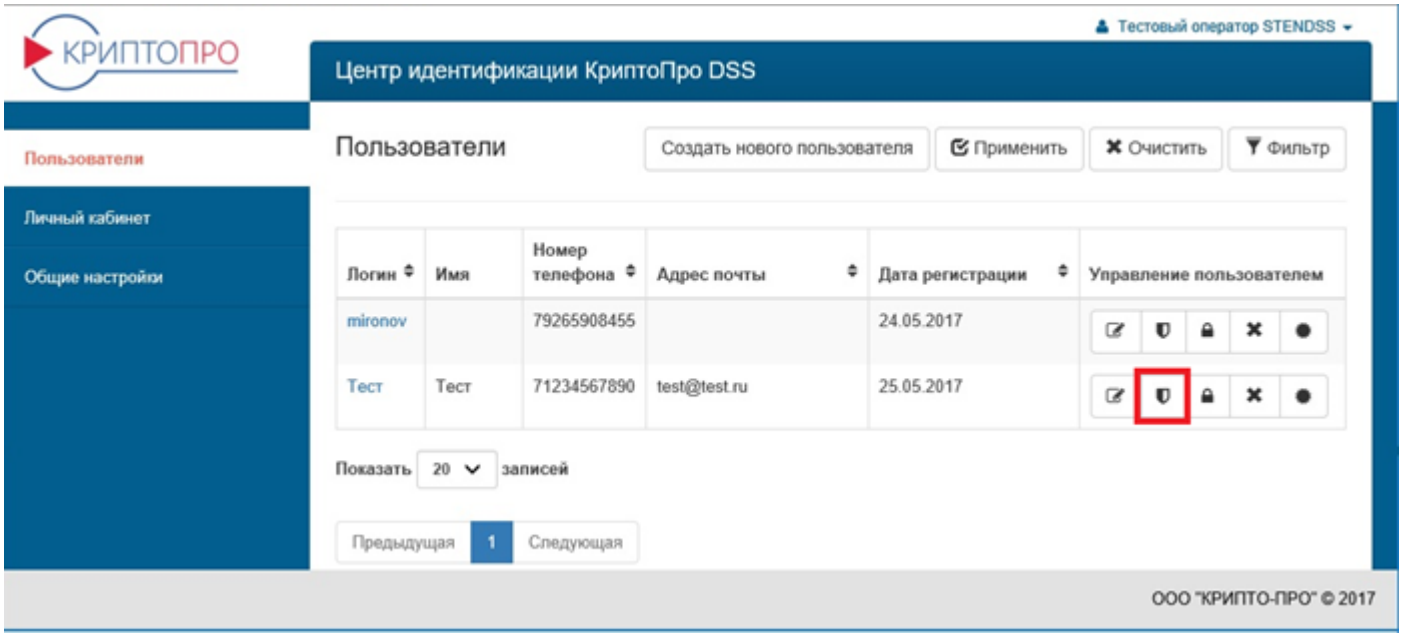


Рисунок 1. Переход к настройке аутентификации

4. Выбрать в списке методов вторичной аутентификации «Аутентификация с помощью мобильного приложения»;
5. Выбрать метод отправки кода активации ключа: путём направления по электронной почте, либо отправки СМС-сообщения пользователю и нажать кнопку «**ОК**» (см. Рисунок 2):

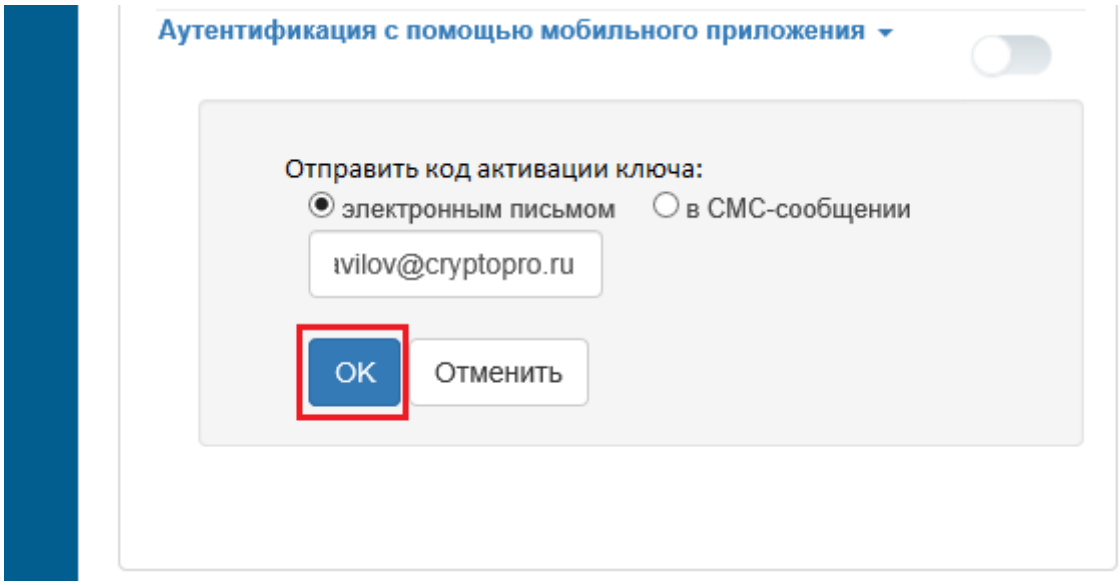


Рисунок 2. Ввод адреса электронной почты для отправки кода активации

6. Активировать возможность аутентификации с помощью мобильного приложения, кликнув по рычажку справа от наименования метода аутентификации (см. Рисунок 3**. Активация аутентификации с помощью мобильного приложения**):

Рисунок 3. Активация аутентификации с помощью мобильного приложения

7. В настройках метода появляется идентификатор пользователя, срок истечения действия ключа и QR-код, который необходимо передать пользователю (см. Рисунок 4):

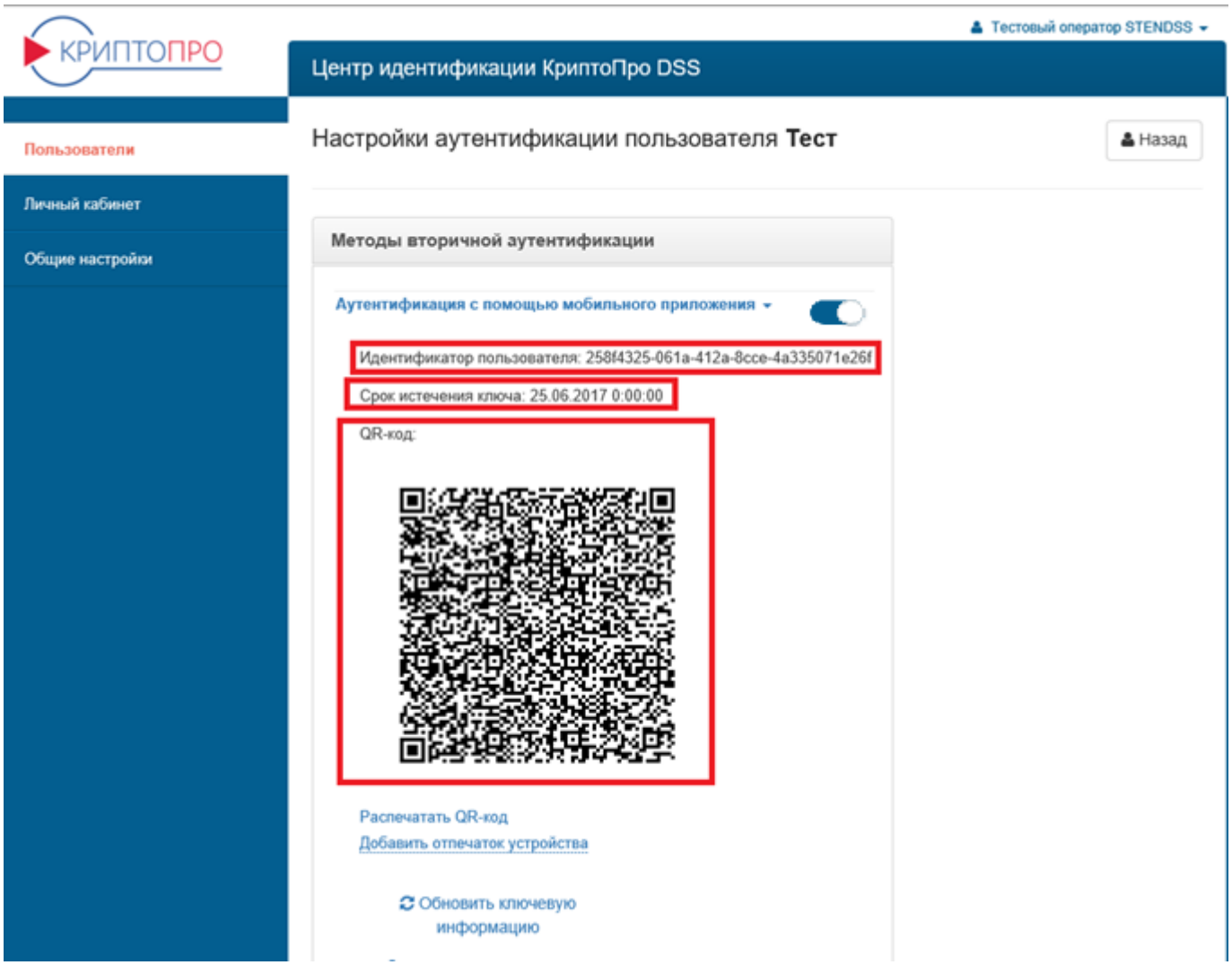


Рисунок 4. Генерация QR-кода

8. QR-код распечатать и передать пользователю под роспись в запечатанной бумажной форме.
9. Включением тумблера выбрать операции пользователя, которые необходимо подтверждать с применением мобильного приложения (см. Рисунок 5):

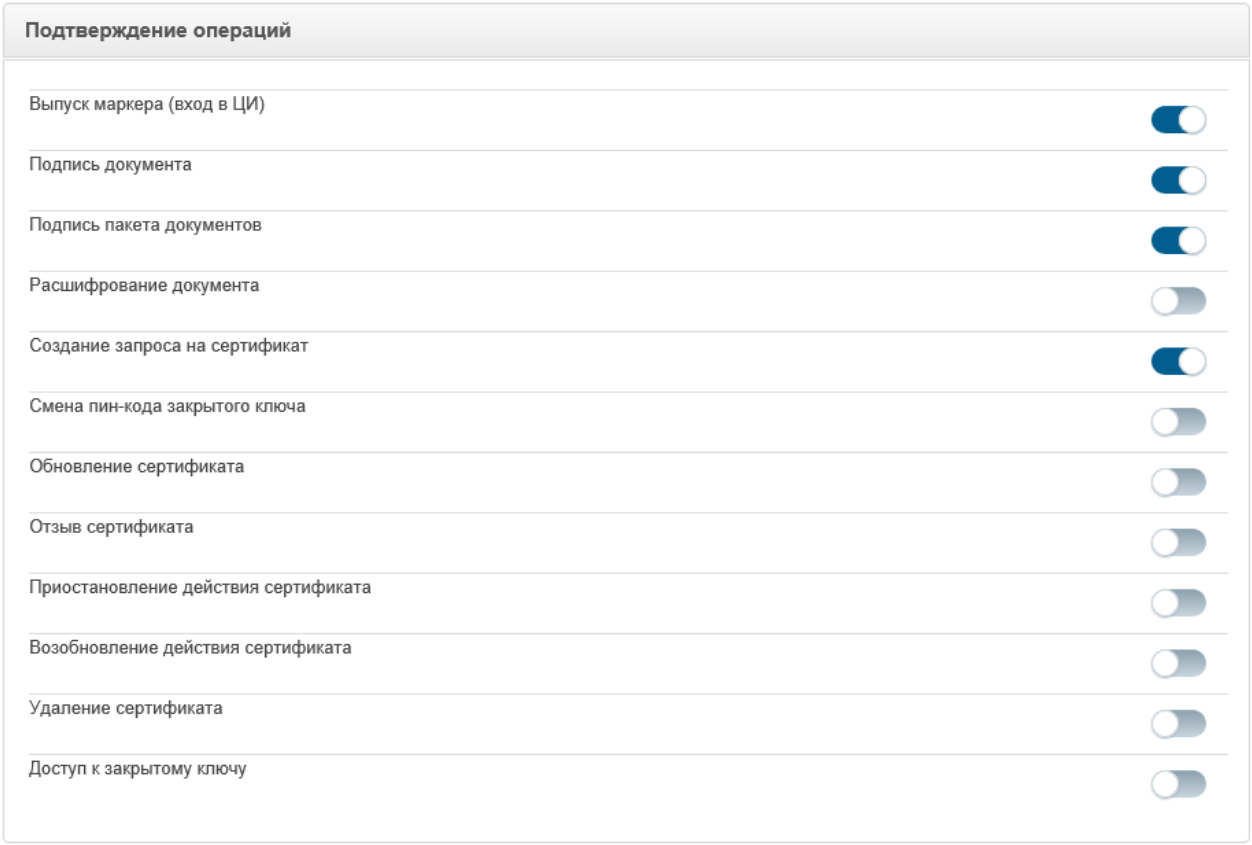


Рисунок 5. Выбор операций, требующих подтверждения

3. Настройка мобильного устройства Пользователя СЭП для использования приложения

3.1. Установка приложения на устройствах под управлением iOS

1. На мобильном устройстве открыть приложение «**APP Store**»;
2. В строке поиска в приложении «**APP Store**» набрать «mydss» и нажать кнопку поиска;
3. В результатах поиска найти приложение «myDSS КриптоПро»;
4. Нажать на кнопку «Загрузить»
5. Нажать кнопку «Установить»
6. После завершения установки на экране мобильного устройства появится значок установленного приложения (см. Рисунок 6):

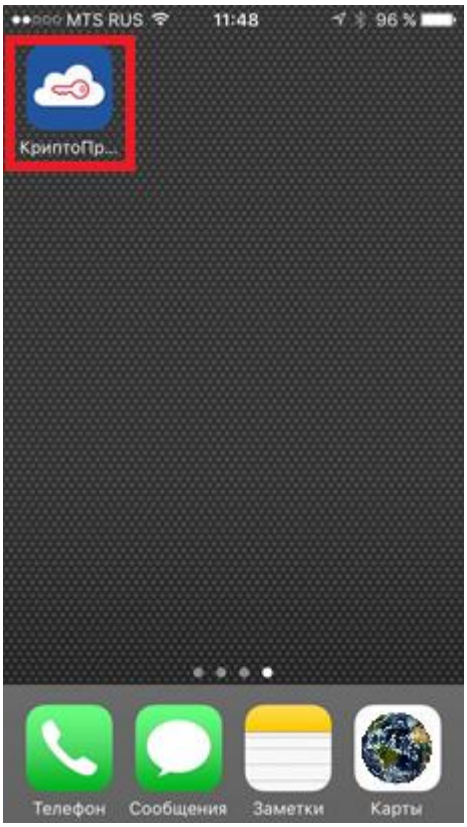


Рисунок 6. Установленное приложение myDSS на iOS устройстве

7. Далее перейти к п. 4.

3.2. Установка приложения на устройствах под управлением Android

1. На мобильном устройстве открыть приложение «**Play Маркет**»;
2. В строке поиска в приложении «**Play Маркет**» набрать «mydss» и нажать кнопку поиска;
3. В результатах поиска найти приложение «myDSS КриптоПро»;
4. Нажать на кнопку «Установить»;
5. После завершения установки на экране мобильного устройства появится значок установленного приложения (см. Рисунок 7):

Рисунок 7. Установленное приложение myDSS на Android устройстве

6. Далее перейти к п. 4.

4. Настройка и использование приложения для аутентификации в СЭП

1. Получить от Оператора СЭП код активации в соответствии со способом, выбранном на шаге 5 (п. 2) (см. Рисунок 8):

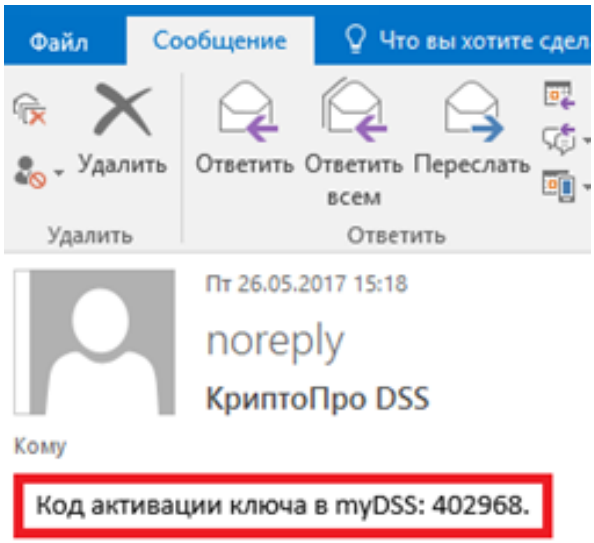


Рисунок 8. Код активации

2. На мобильном устройстве запустить приложение myDSS (см. Рисунок 9).

3. Если ранее ни один ключ авторизации зарегистрирован не был, автоматически запускается сканер QR-кода (см. Рисунок **9. Запуск приложения myDSS**):

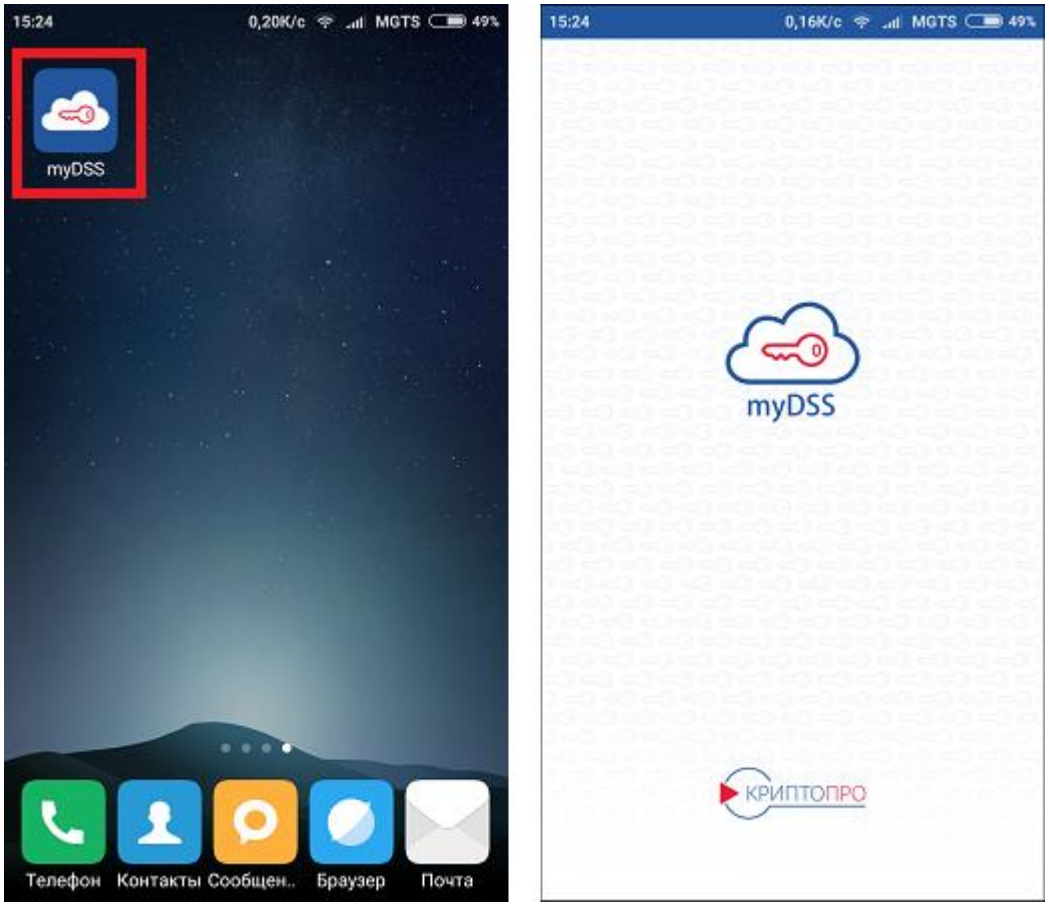


Рисунок 9. Запуск приложения myDSS

4. Камеру мобильного устройства навести на QR-код, который был получен на шаге 7 (см. Рисунок 10):

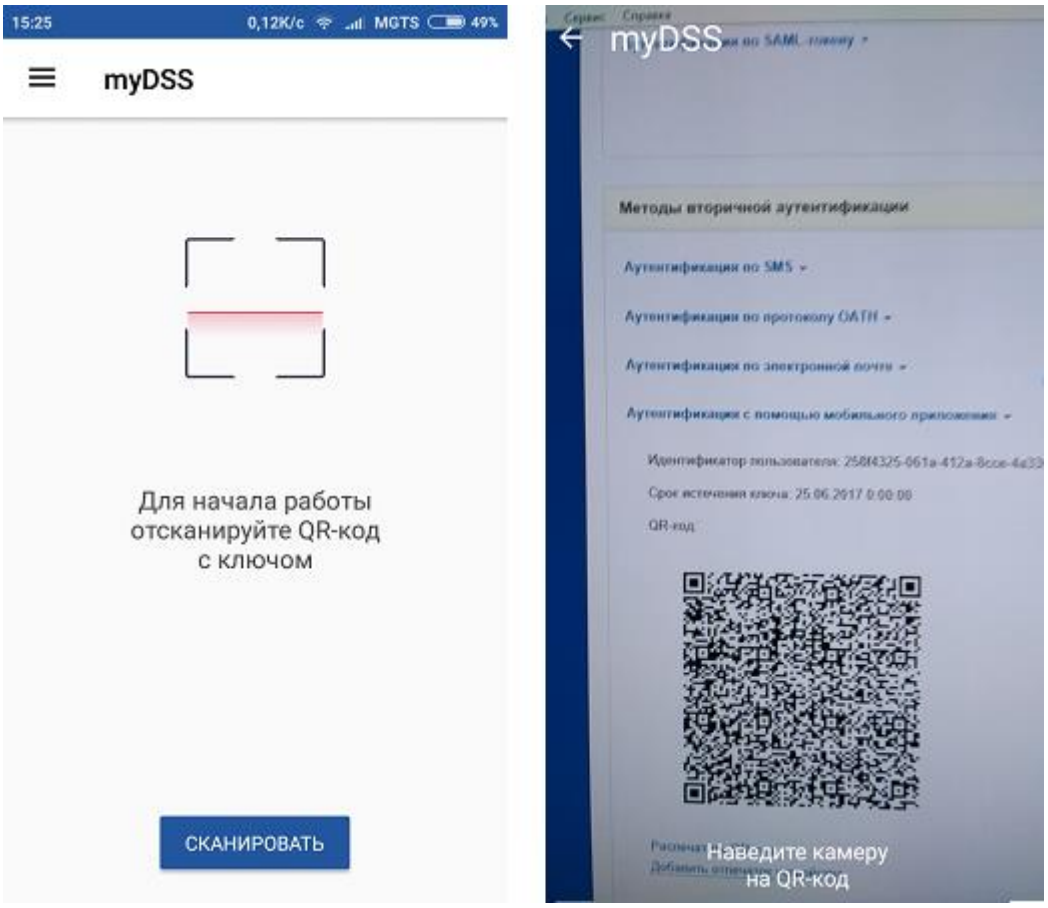


Рисунок 10. Сканирование QR-кода

5. Мобильное устройство распознает QR-код;
6. Ввести код активации, полученный на шаге 1;
7. Нажать кнопку «**Продолжить**»;
8. Задать имя ключу авторизации и пароль для доступа к ключу (см. Рисунок 11):

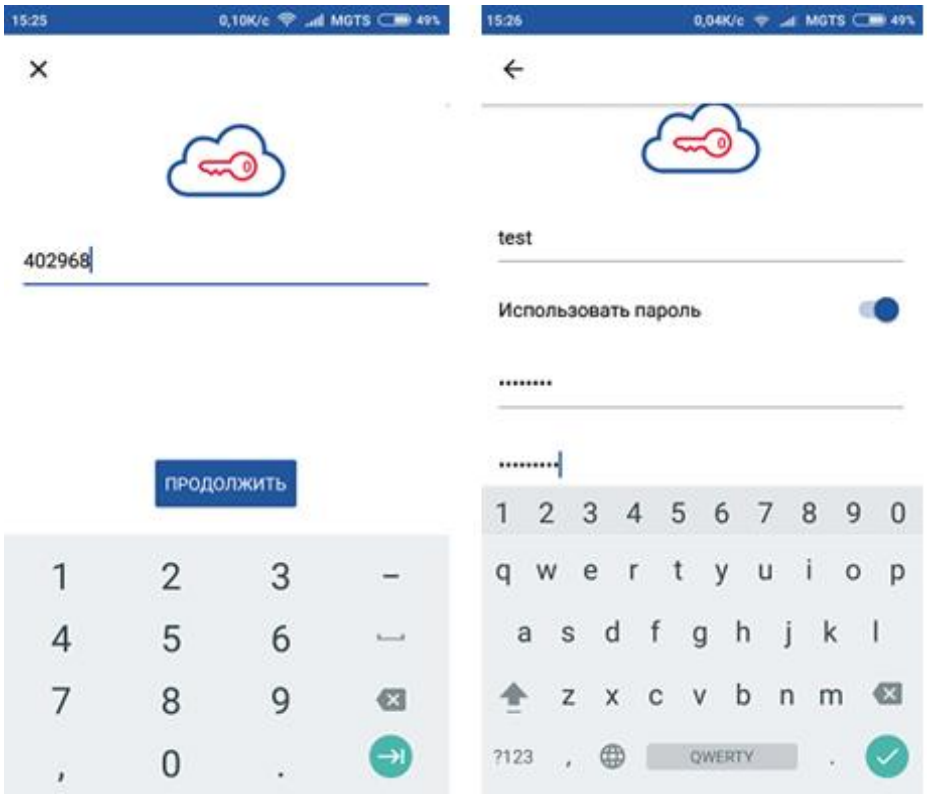


Рисунок 11. Ввод кода активации ключа myDSS

9. Ознакомиться с информацией об успешном сохранении ключа и нажать кнопку «**Закрыть**» (см. Рисунок 12):

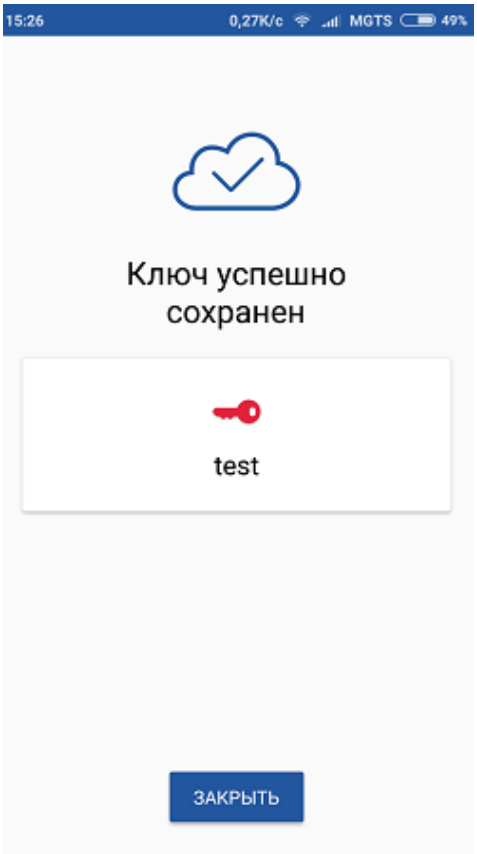


Рисунок 12. Окончание регистрации ключа

10. В приложении появится информация об созданном ключе авторизации (см. Рисунок 13):

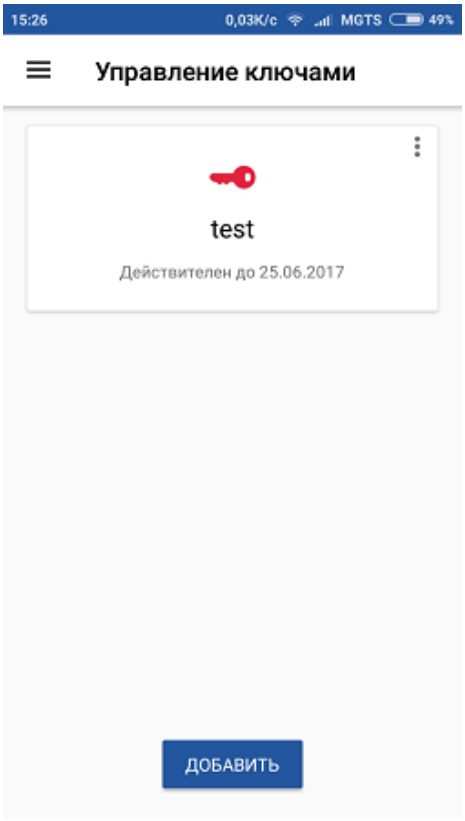


Рисунок 13. Отображение доступных ключей подтверждения операций

4.1. Использование приложения для аутентификации в СЭП

1. Подключиться к личному кабинету пользователя по адресу: https://stenddss.cryptopro.ru/Frontend/;
2. Ввести логин пользователя и пароль (см. Рисунок 14):

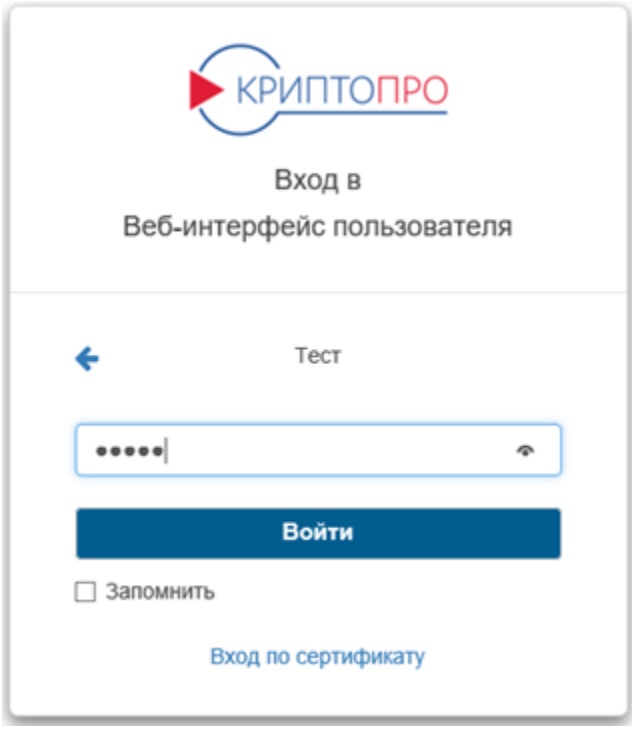


Рисунок 14. Вход в Вэб-интерфейс пользователя СЭП

3. Откроется страница вторичной аутентификации с просьбой подтвердить операцию входа и указан идентификатор запроса (см. Рисунок 15):

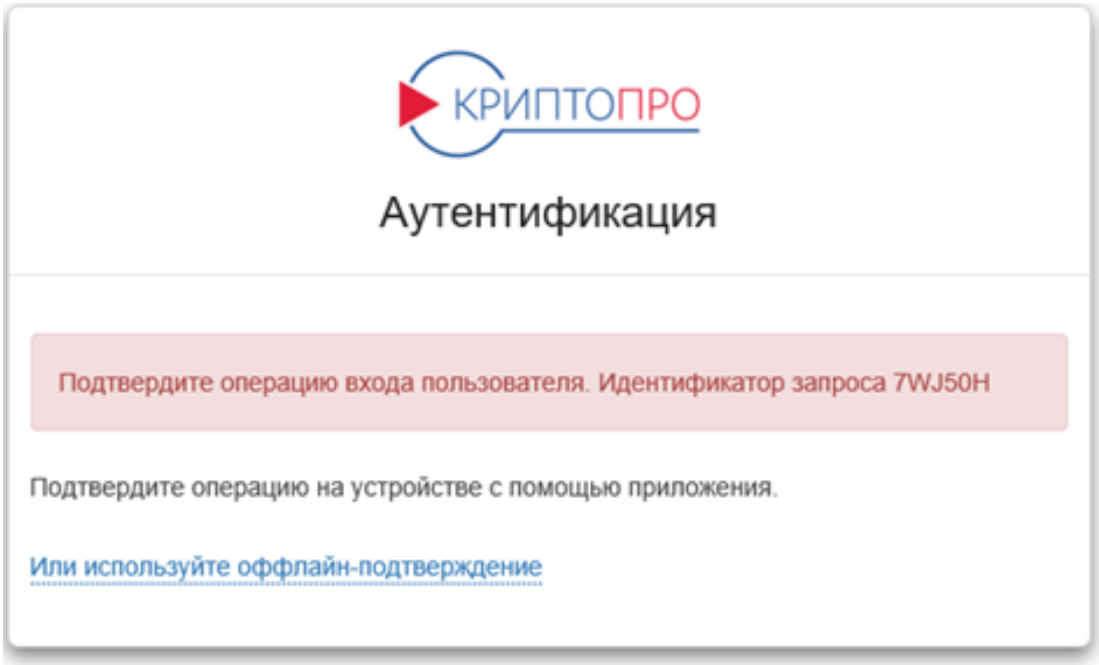


Рисунок 15. Подтверждение аутентификации

4.1.1. При наличии доступа в интернет с мобильного устройства (on-line)

1. Войти в меню и выбрать пункт «**Подтвердить операции**» (см. Рисунок 16):

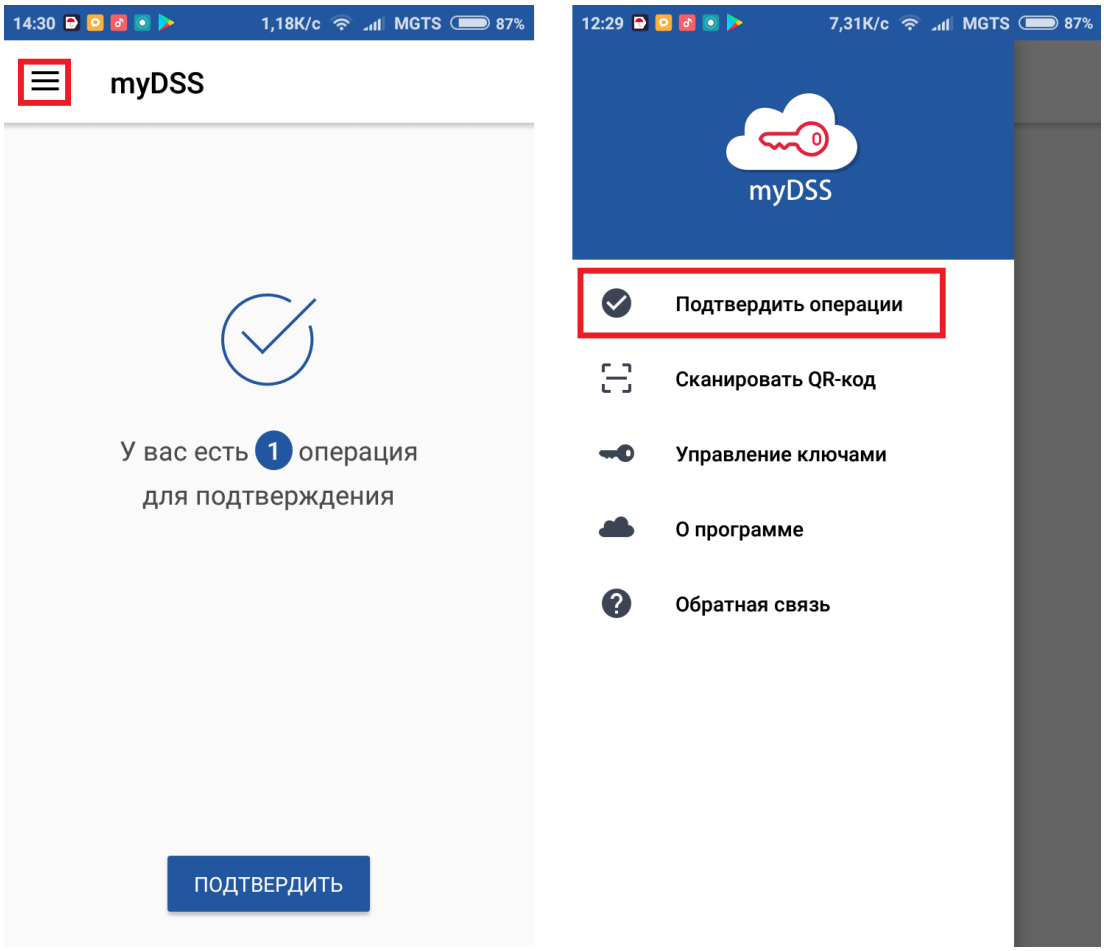


Рисунок 16. Подтверждение операции

2. Выбрать ключ авторизации, ввести пароль на ключ и нажать кнопку «**Продолжить**» (см. Рисунок 17):

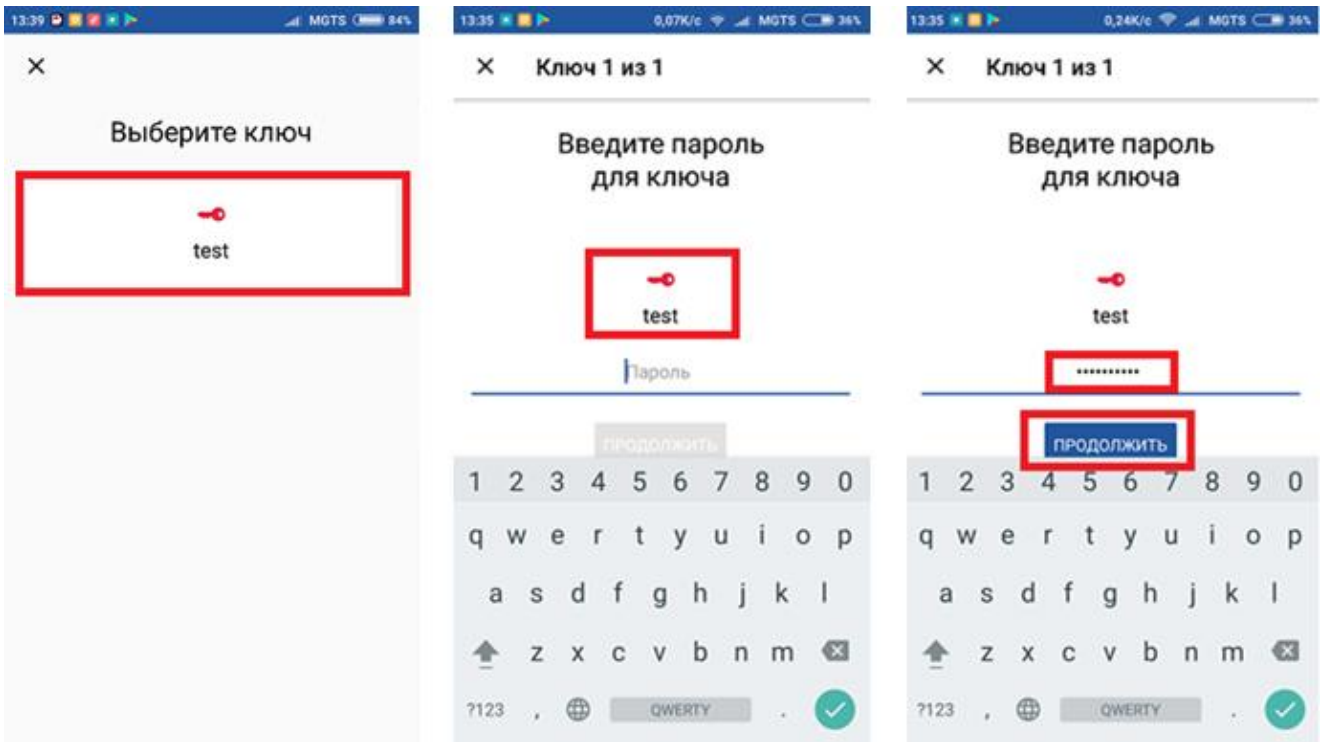


Рисунок 17. Использование ключа подтверждения операции

3. Отобразится идентификатор запроса (п. **3** с. 13) и предложение отказать или подтвердить операцию входа пользователя. Для подтверждения операции нажать кнопку «**Подтвердить**», при открытии следующего окна - «**Продолжить**» (см. Рисунок 18), после чего произойдёт переход к начальному экрану мобильного приложения:

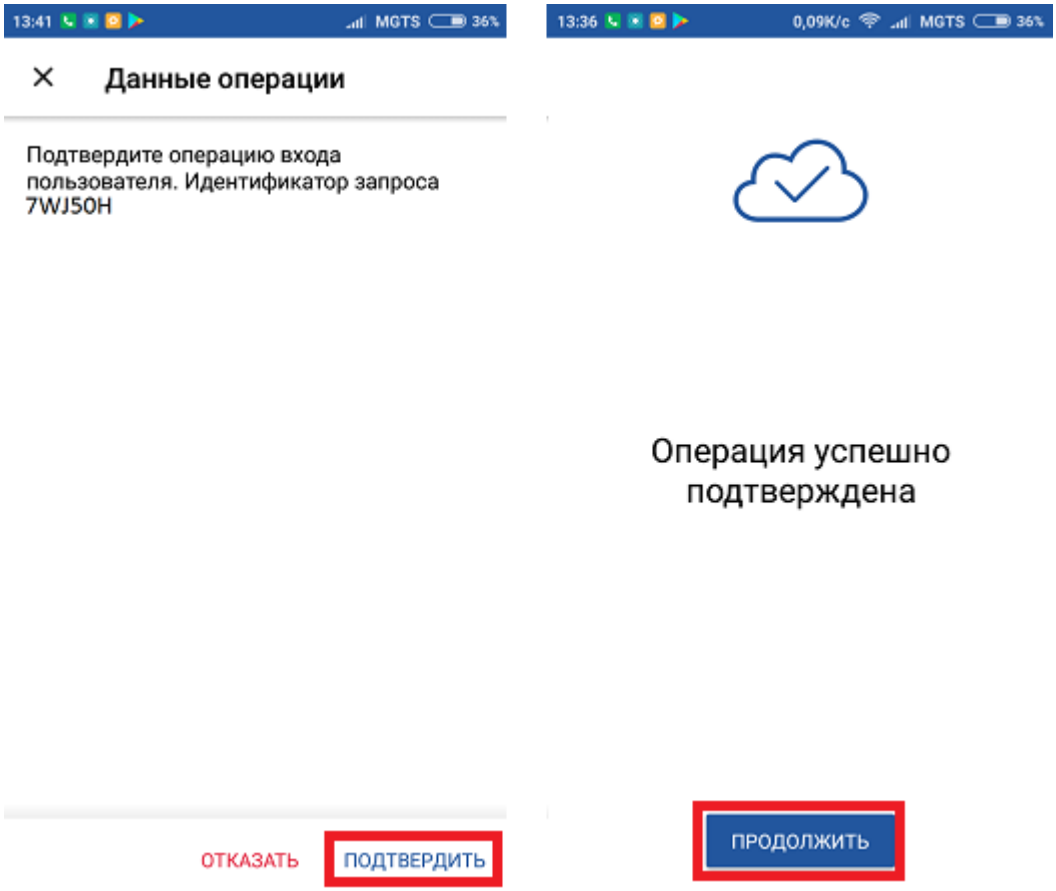


Рисунок 18. Подтверждение операции входа пользователя

4. Отобразиться информация, что операция подтверждена и на рабочем месте произойдёт автоматический вход Пользователя в СЭП (см. Рисунок 19):

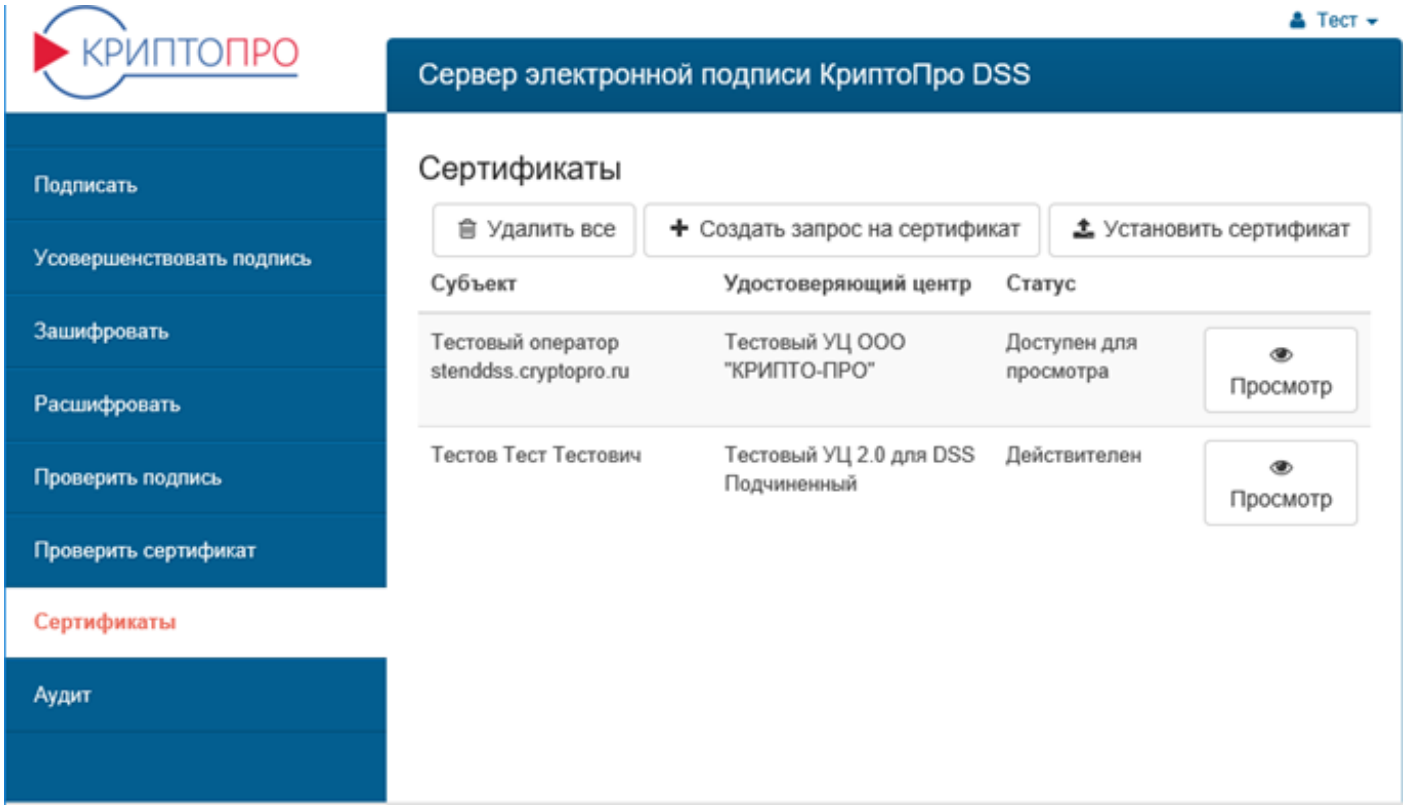


Рисунок 19. Личный кабинет пользователя в СЭП

4.1.2. При отсутствии доступа в интернет с мобильного устройства (off-line)

1. Нажать на «**оффлайн-подтверждение**» (см. Рисунок 20):

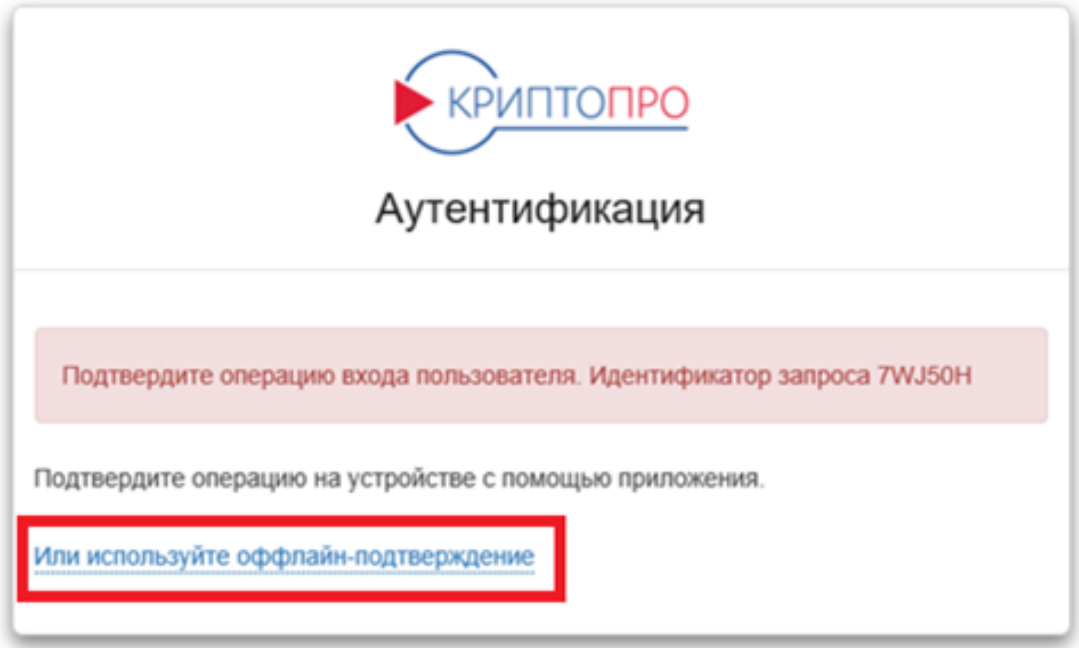


Рисунок 20. Использование оффлайн-подтверждения

2. Откроется изображение с QR-кодом и строка для ввода кода подтверждения (см. Рисунок 21):

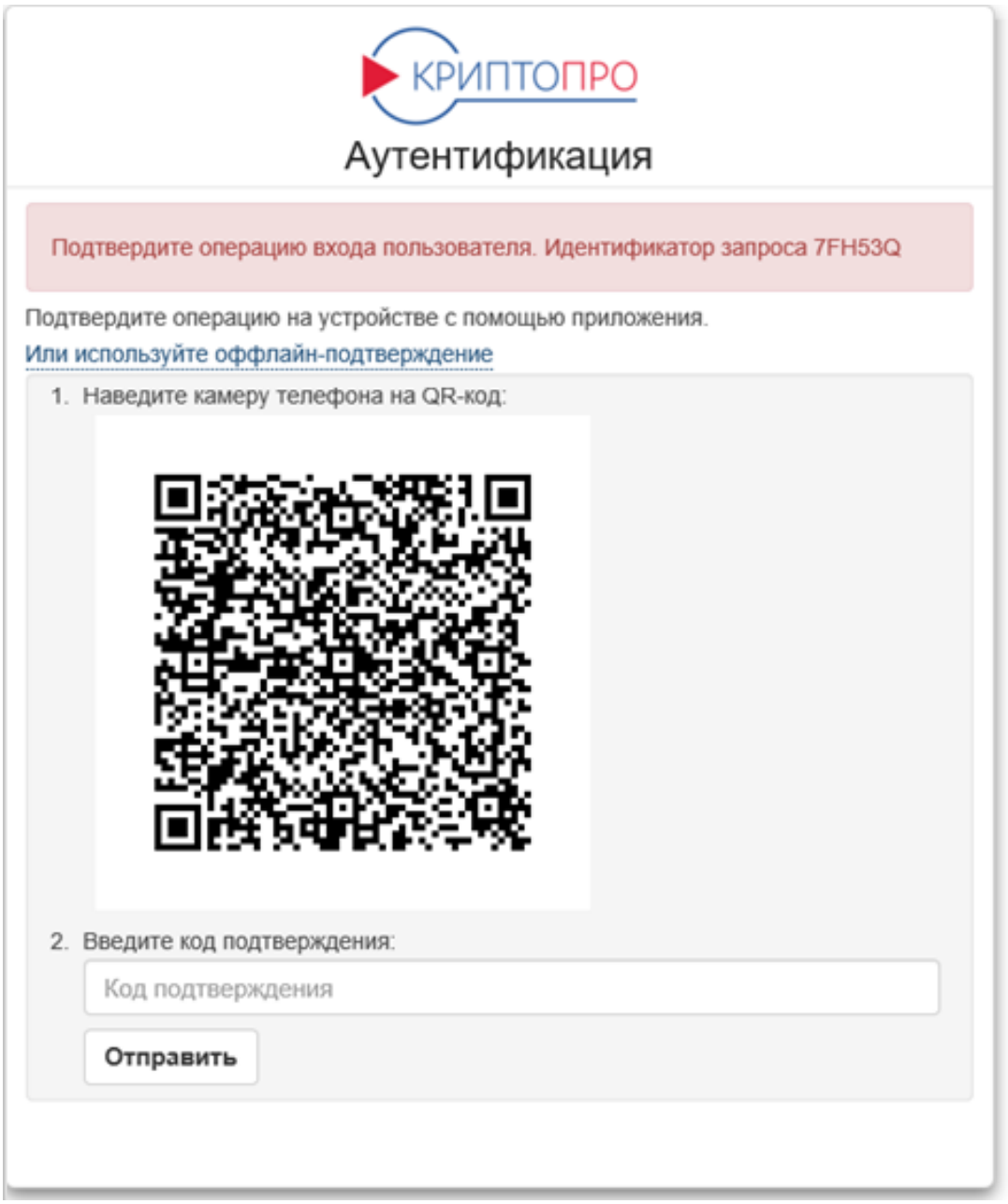


Рисунок 21. QR-код для поддтверждения операции входя пользователя

3. В мобильном приложении зайти в меню и нажать на «**Сканировать QR-код**», камеру мобильного устройства навести на отображаемый на экране QR-код (см. Рисунок 22):

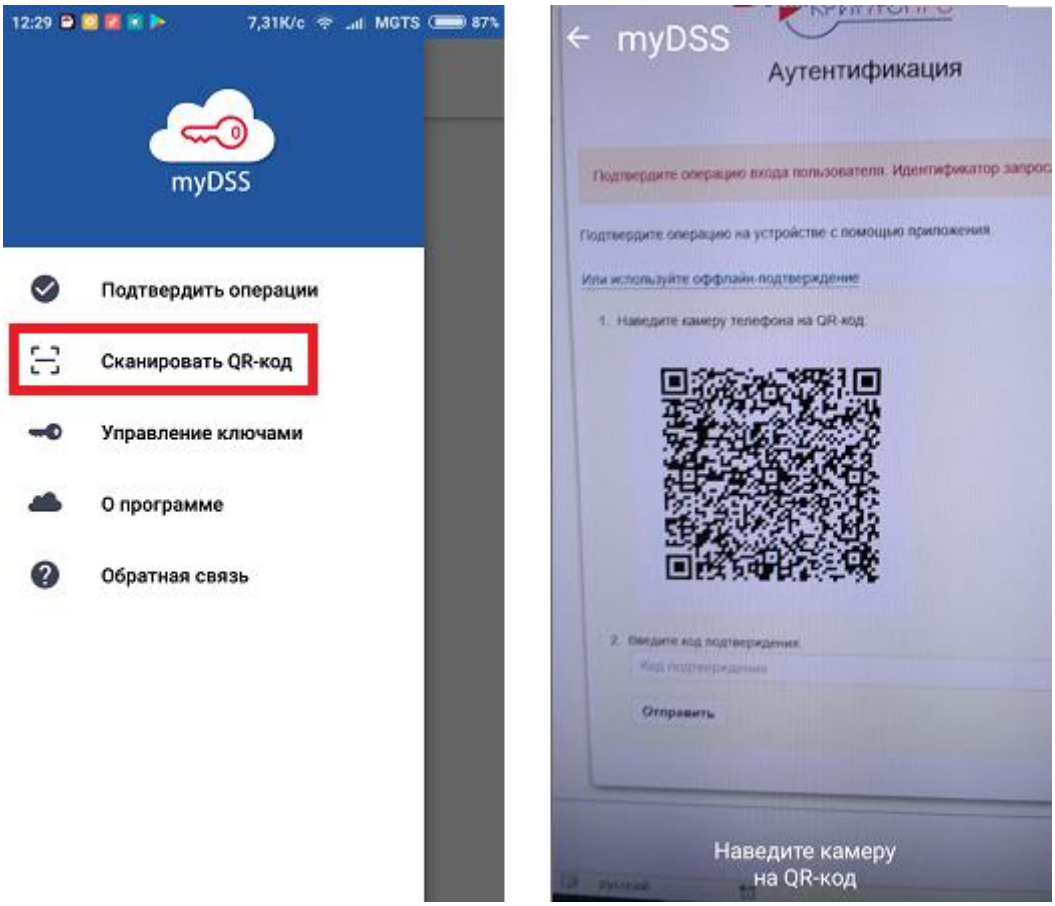


Рисунок 22. Сканирование QR-кода

4. Отобразится идентификатор запроса (п. 2 с. 17) и предложение отказать или подтвердить запрос. Для подтверждения запроса нажать кнопку «**Подтвердить»** (см. Рисунок 23):

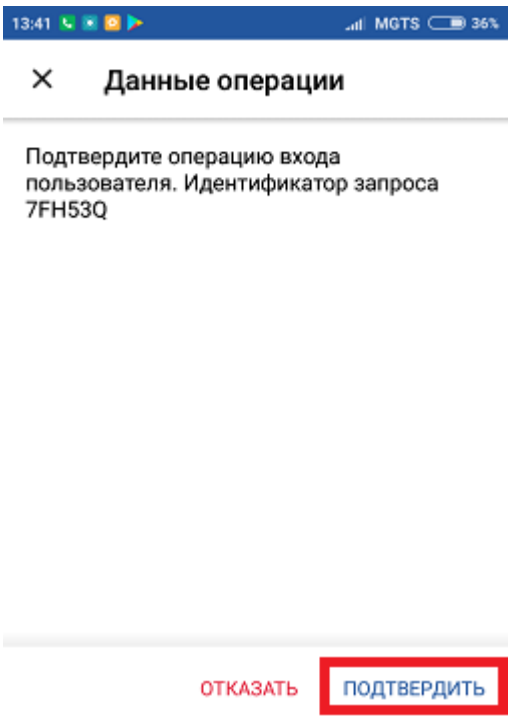


Рисунок 23. Подтверждение операции входа пользователя

5. Выбрать ключ авторизации, ввести пароль для доступа к ключу и нажать кнопку «**Продолжить**» (см. Рисунок 24):

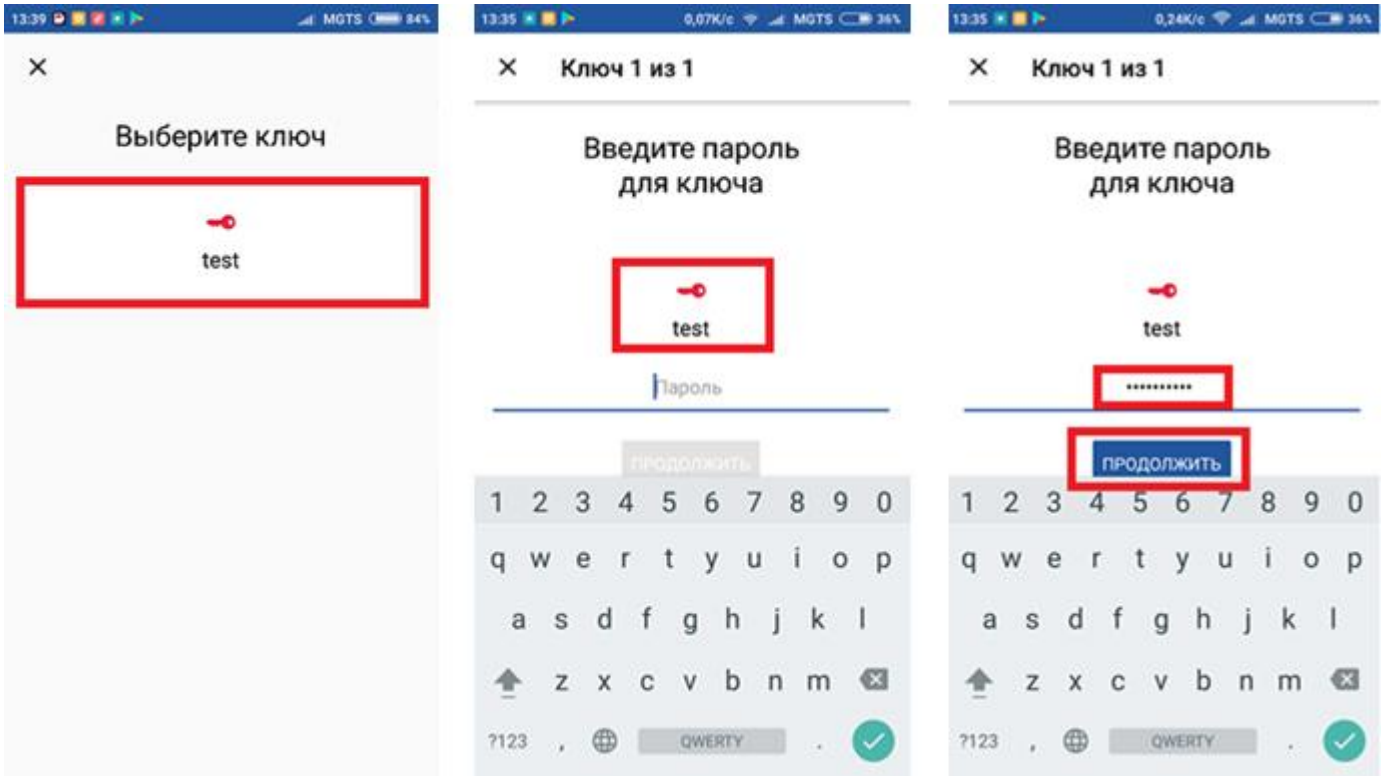


Рисунок 24. Использование ключа подтверждения операции

6. Отобразится код подтверждения который необходимо ввести на странице аутентификации (см. Рисунок 25, Рисунок 26):

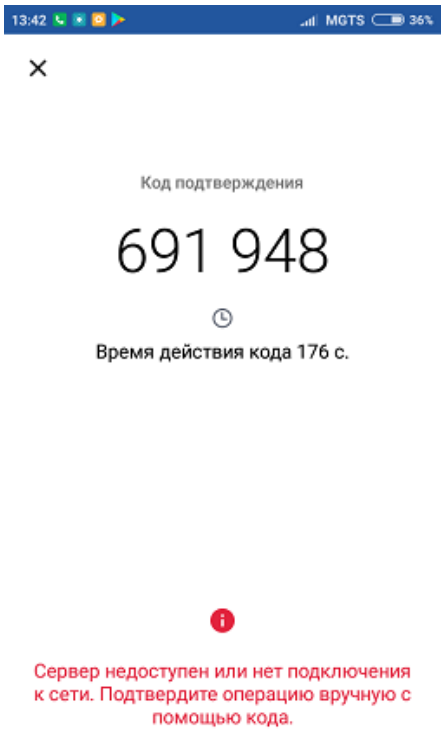


Рисунок 25. Код подтверждения операции

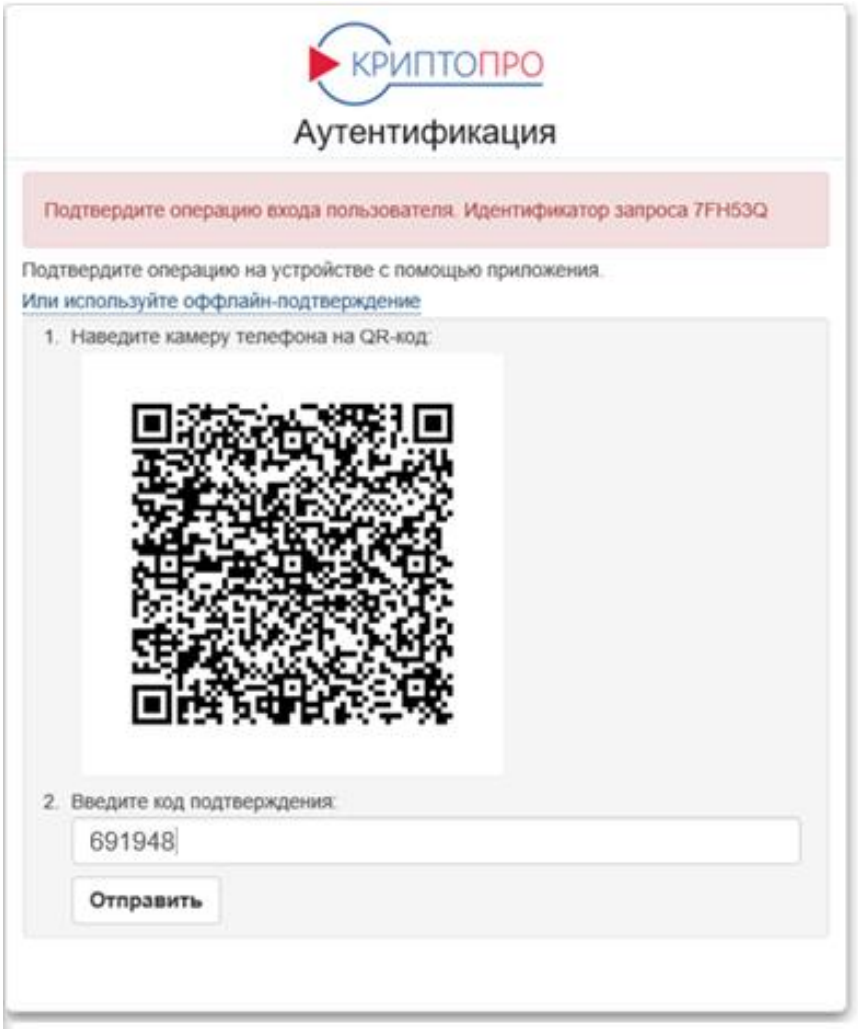


Рисунок 26. Ввод кода подтверждения операции на странице аутентификации

7. Произойдёт автоматический вход Пользователя в СЭП (см. Рисунок 27):

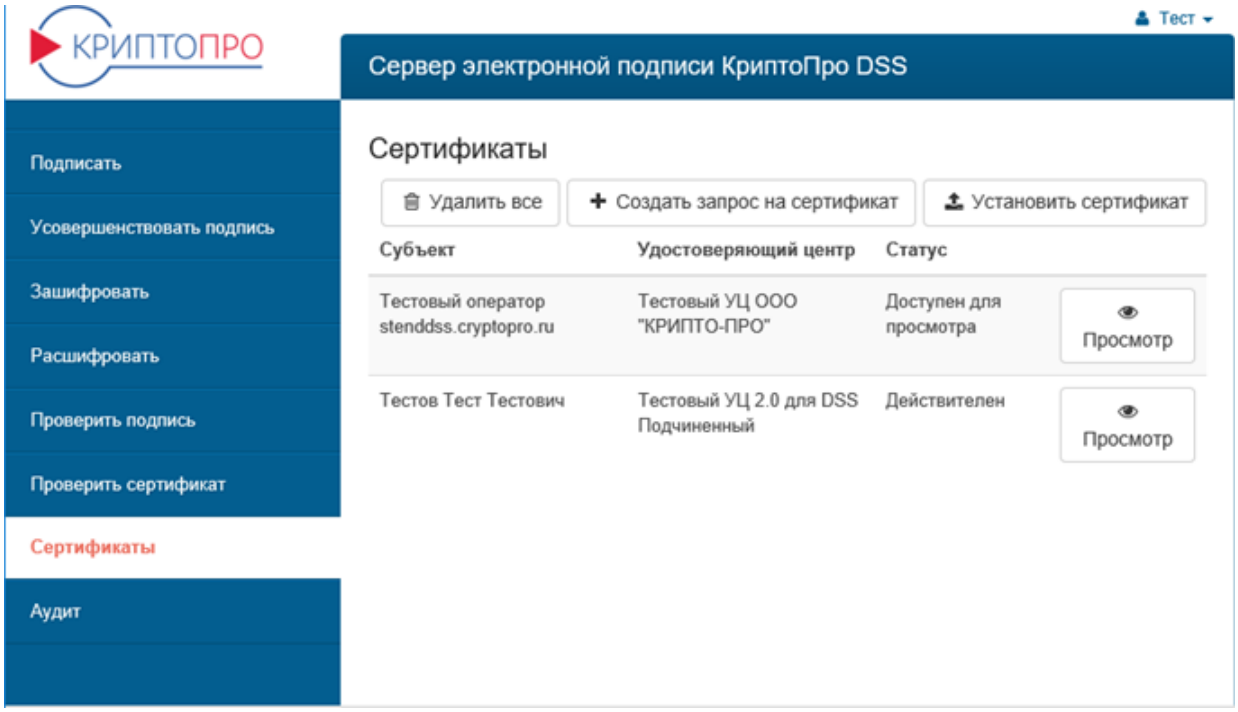


Рисунок 27. Вход пользователя в СЭП

4.2.Использование приложения для подтверждения действий в СЭП

Для подписания документа в СЭП, после выбора документа и установки всех необходимых параметров:

1. На странице «Создание подписи» нажать «**Подписать**» (см. Рисунок 28):

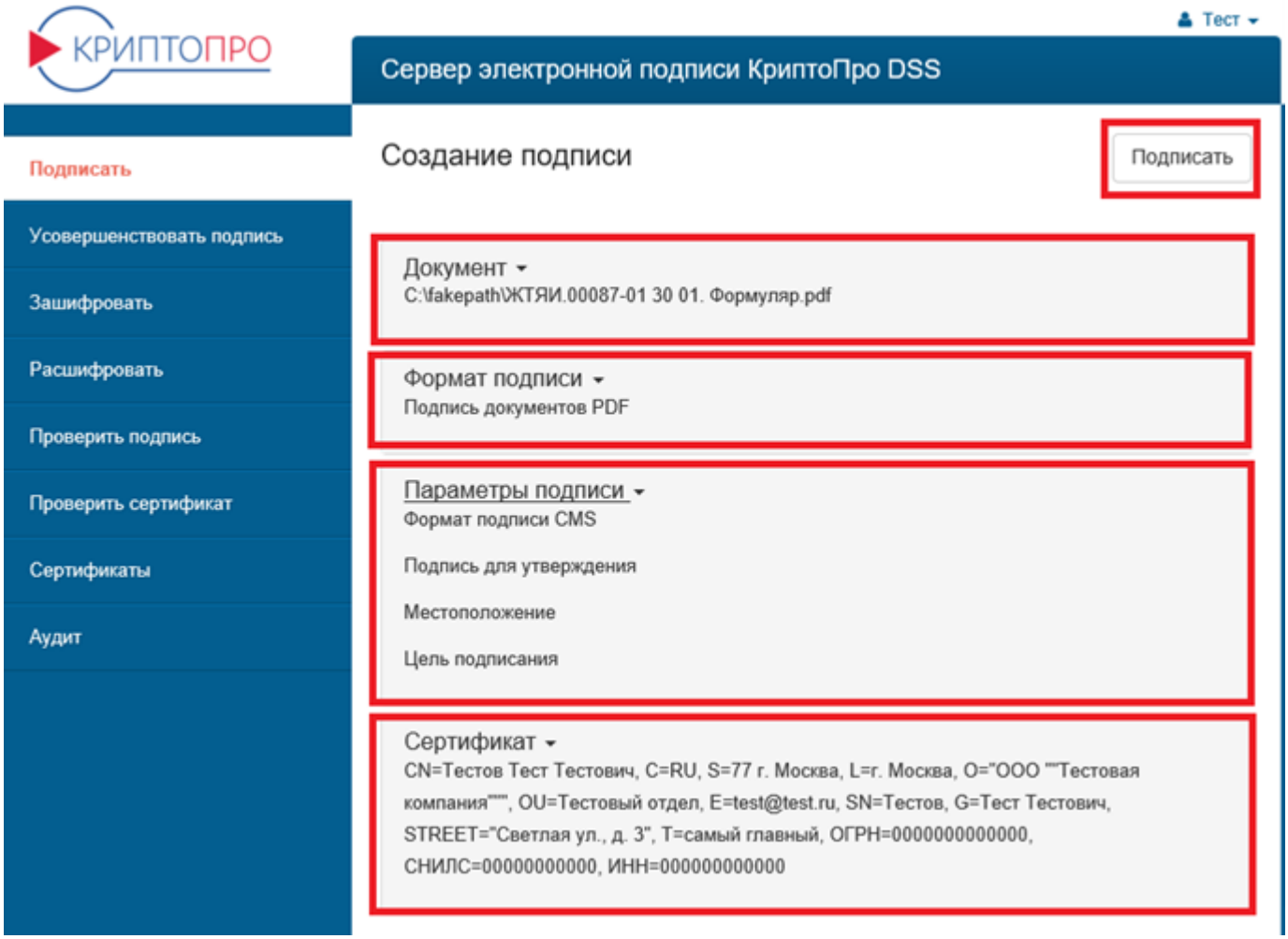


Рисунок 28. Выбор параметров для создания подписи документа

2. Отобразится диалоговое окно с предложением подтвердить операцию с использованием мобильного устройства (см. Рисунок 29):

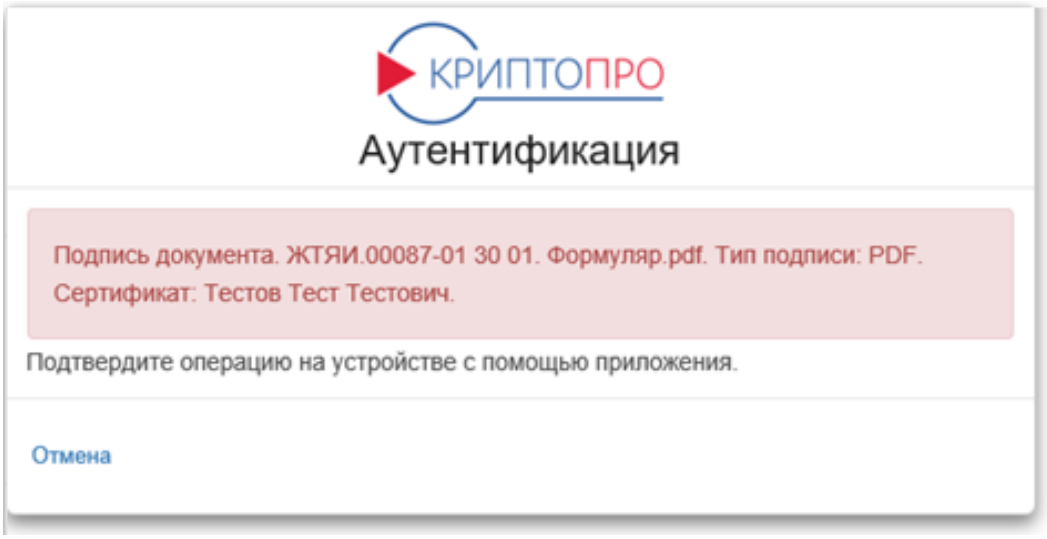


Рисунок 29. Запрос на подтверждение операции подписания документа

3. Ввести пин-кода на от контейнера ключа подписи (см. Рисунок 30):

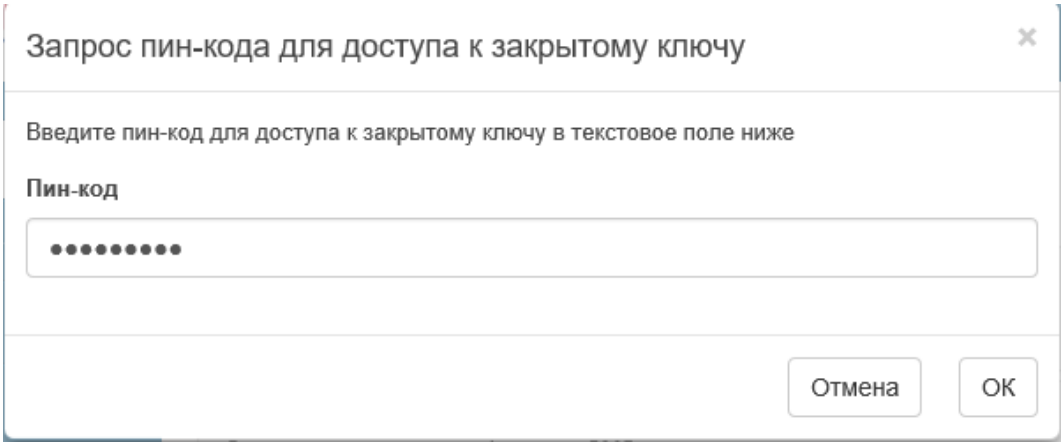


Рисунок 30. Запрос пин-кода к ключевому контейнеру

4. СЭП потребует подтверждение операции с использованием мобильного приложения (см. Рисунок 31):

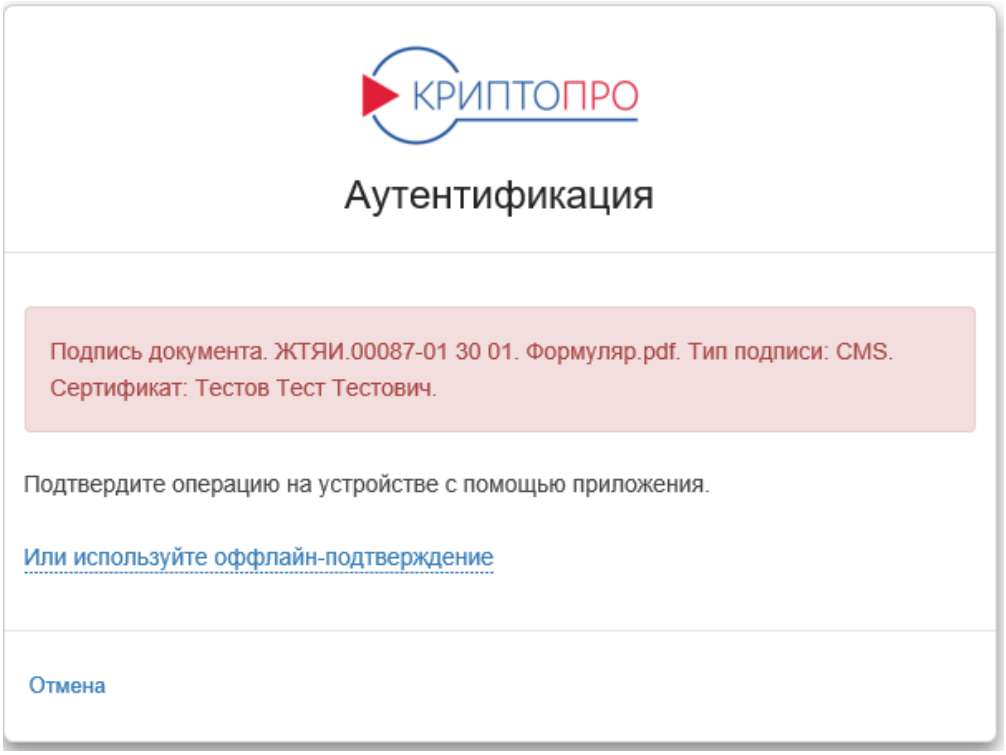


Рисунок 31. Подтверждение операции с использованием приложения

5. В приложении отобразится уведомление о том, что есть операции, требующие подтверждения.
6. Для начала подтверждения операции нажать кнопку «**Подтвердить**».
7. Выбрать нужный авторизации и ввести к нему пароль.
8. В приложении для ознакомления и подтверждения отобразиться информация о подписываемом документе (при условии использования совместимого формата документа).
9. Нажать кнопку «**Подтвердить**», появится уведомление об успешном подтверждении операции.
10. Для продолжения работы в приложении – нажать кнопку «**Продолжить**».

Выполнение пунктов с 5 по 10 отражено на Рисунок 32.

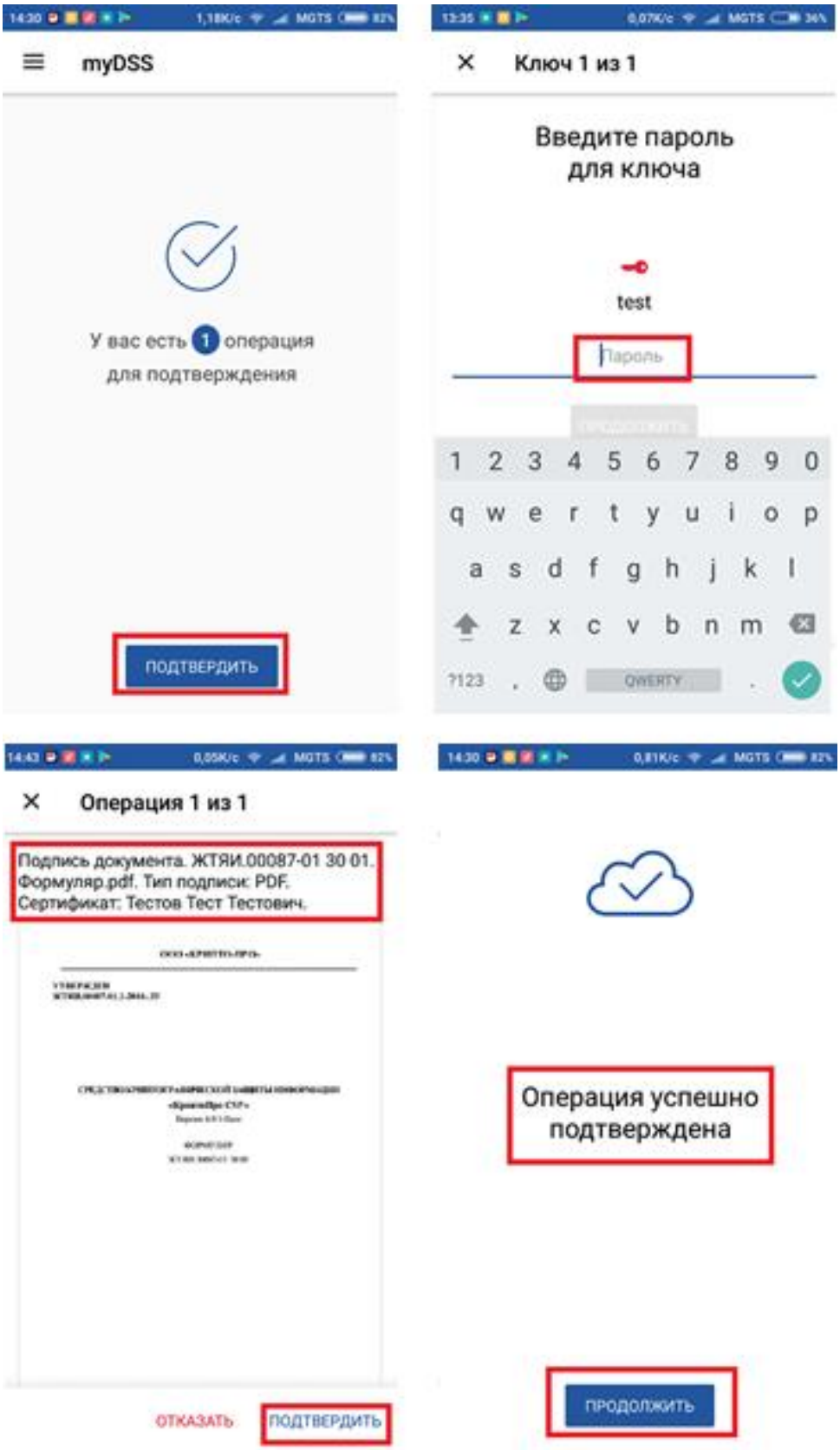


Рисунок 32. Подтверждение операции подписания документа в приложении

11. После успешного подтверждения операции в приложении, в личном кабинете СЭП пользователя появится сообщение об успешном заверении операции (см. Рисунок 33):

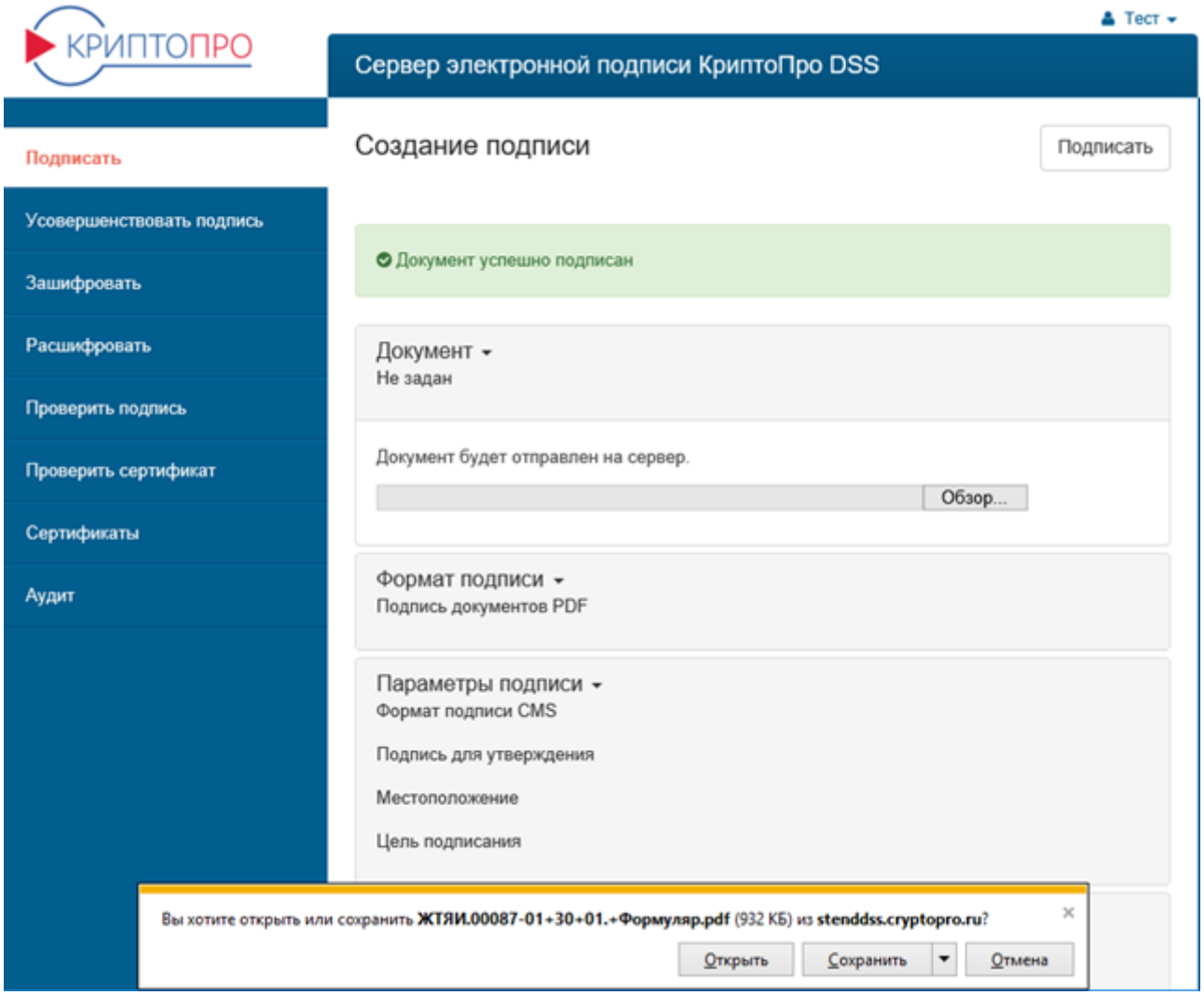


Рисунок 33. Успешное завершение операции Создания подписи

5. Раздел мобильного приложения «Управление ключами»

Данный раздел в мобильном приложении предназначен для совершения действий пользователя над зарегистрированными в мобильно приложении ключами авторизации.

Для управления ключами авторизации, зарегистрированными в мобильном приложении:

1. Зайти в меню и нажать «**Управление ключами**», откроется список зарегистрированных ключей;
2. Для добавления нового ключа необходимо добавить на кнопку «**Добавить**», процесс добавления нового ключа описан на в п. 4 с. 8.;
3. Для управления существующим ключом нажать на значок  ;

4. На значке существующего ключа, появится меню с возможностью переименования, изменения и удаления существующего ключа (см. Рисунок 34):

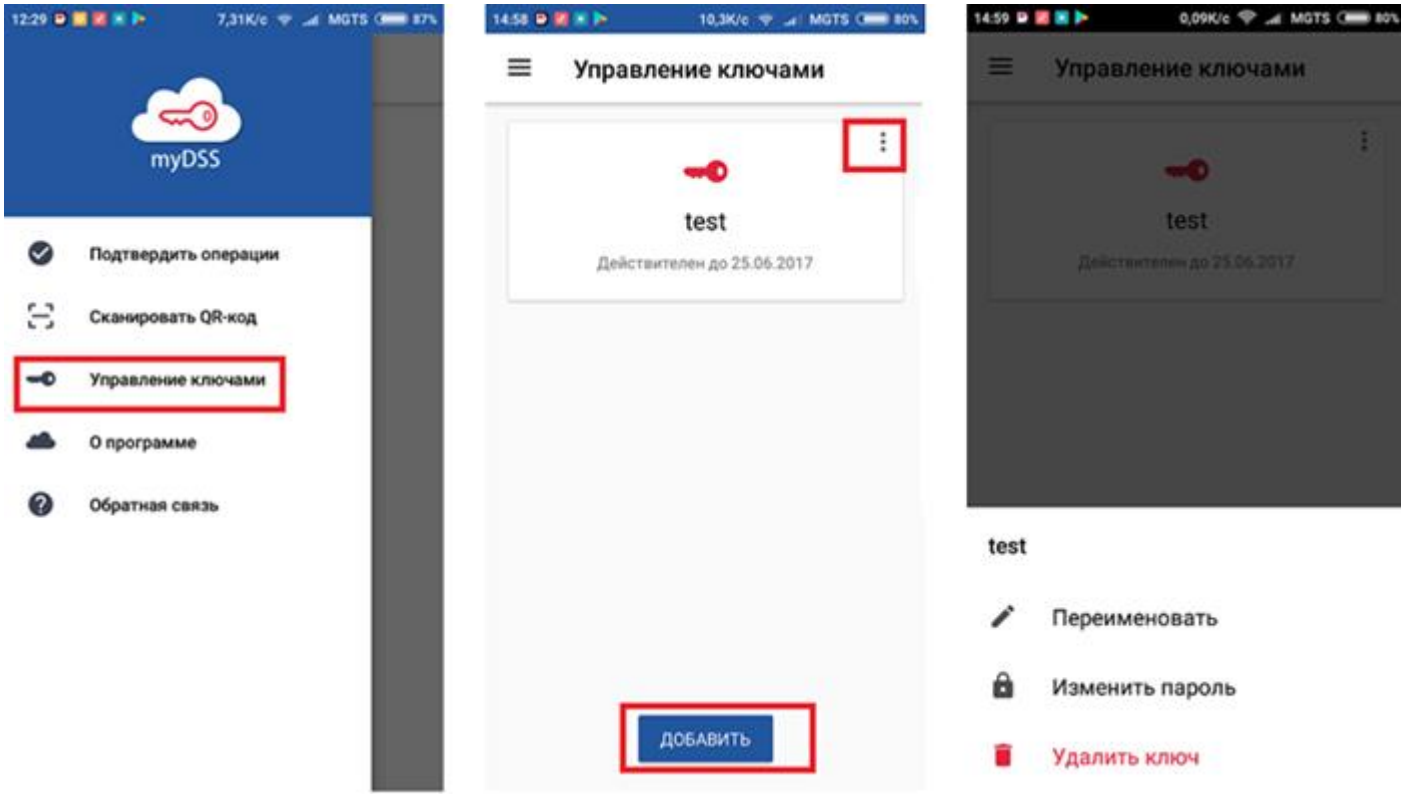


Рисунок 34. Меню управления ключом

5.1. Переименование ключей

При необходимости переименования ключа авторизации выполнить следующие операции:

1. Выбрать соответствующий пункт в меню управления ключами;
2. Ввести новое имя ключа;
3. Нажать «Сохранить», после этого имя ключа изменится (см. Рисунок 35):

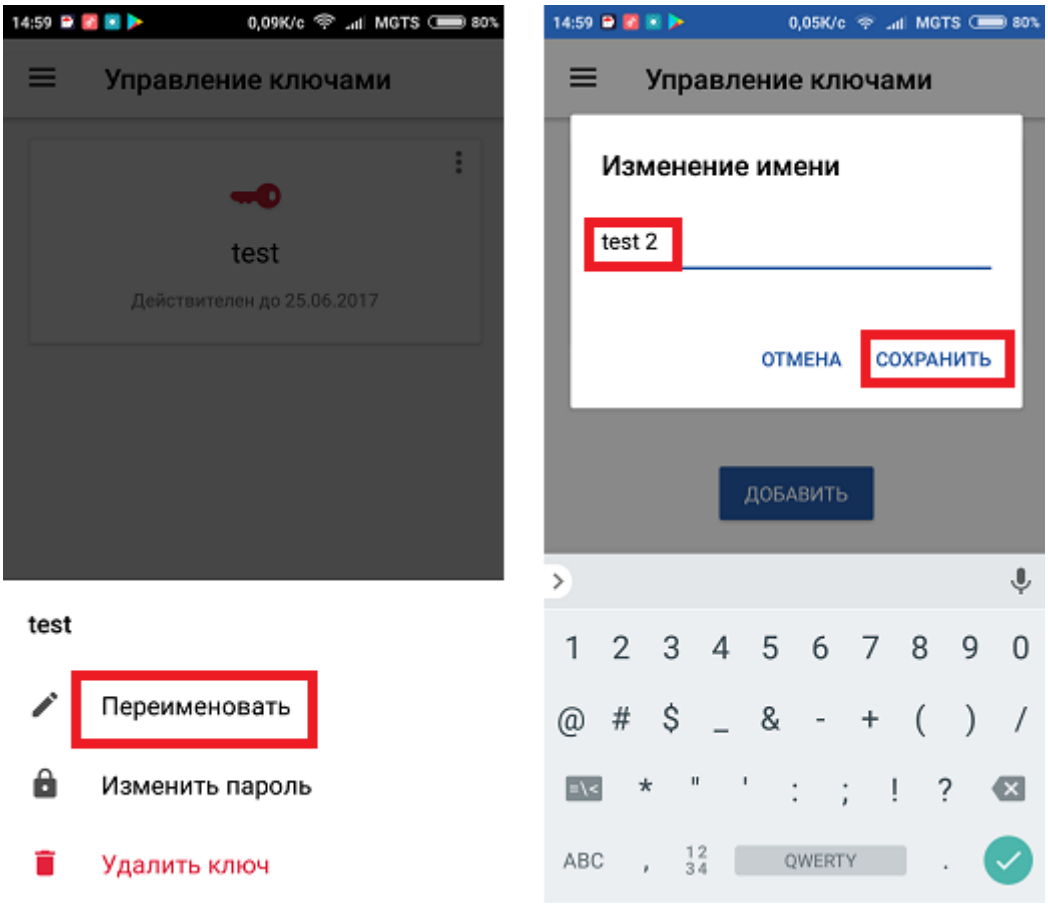


Рисунок 35. Переименование ключа

5.2. Изменение пароля для использования ключа авторизации

Для изменения пароля на ключ авторизации выполнить следующие операции:

1. Выбрать соответствующий пункт в меню управления ключами;
2. Ввести существующий пароль;
3. Нажать «**Далее**»;
4. Дважды ввести новый пароль;
5. Нажать «**Готово**» после этого пароль на ключ авторизации будет изменён (см. Рисунок 36):

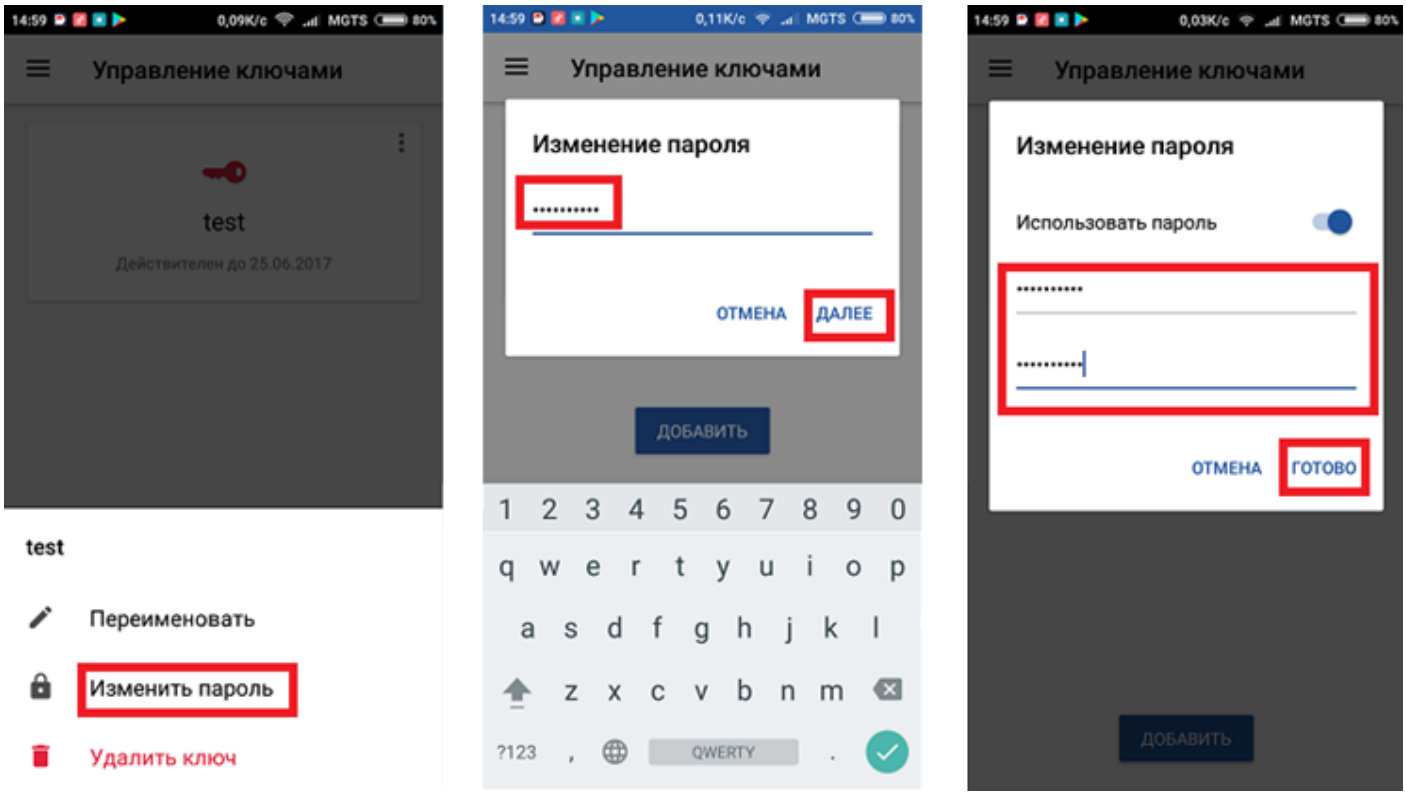


Рисунок 36. Изменение пароля ключа

5.3. Удаление ключа

Для удаления ключа авторизации выполнить следующие операции:

1. Выбрать соответствующий пункт в меню управления ключом;
2. На вопрос «Вы действительно хотите удалить ключ» нажать «**ДА**», после этого ключ будет удалён (см. Рисунок 37):

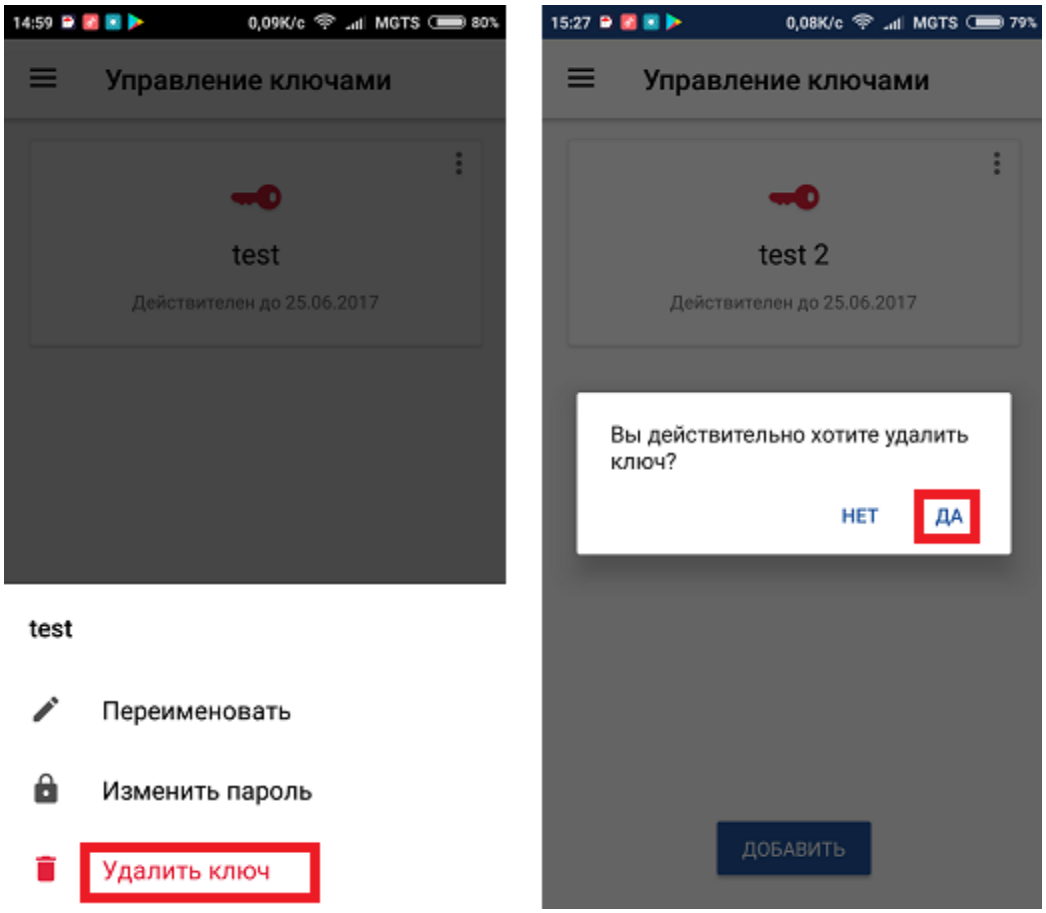


Рисунок 37. Удаление ключа

Перечень рисунков