

АО «СИГНАЛ-КОМ»

УТВЕРЖДЕНО  
ШКНР.00051-01 34 02-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС  
SIGNAL-COM CLOUD DSS  
Версия 1.0

Руководство оператора

ШКНР.00051-01 34 02  
Листов 19

## **АННОТАЦИЯ**

Настоящий документ содержит руководство оператора программно-аппаратного комплекса Signal-COM Cloud DSS, предназначенного для централизованного хранения и дистанционного применения ключей электронной подписи.

---

## СОДЕРЖАНИЕ

Аннотация .....	2
Содержание .....	3
1. Назначение программы .....	4
1.1. Список сокращений .....	4
1.2. Термины и определения .....	4
2. Условия выполнения программы .....	6
2.1. Требования к аппаратным средствам .....	6
2.2. Требования к программным средствам .....	6
3. Выполнение программы .....	7
3.1. Загрузка приложения .....	7
3.2. Основное меню .....	7
3.3. Действия оператора .....	7
3.3.1. Генерация ключей и запроса на создание сертификата .....	7
3.3.2. Выгрузка запроса на создание сертификата в файл .....	9
3.3.3. Загрузка сертификата из файла .....	9
3.3.4. Работа с группами пользователей .....	10
3.3.5. Работа со списком пользователей .....	10
3.3.6. Регистрация учётной записи пользователя .....	10
3.3.7. Ввод атрибутов различительного имени пользователя .....	11
3.3.8. Получение разделяемого секрета .....	12
3.3.9. Подтверждение номера телефона .....	13
3.3.10. Подтверждение адреса электронной почты .....	14
3.3.11. Изменение параметров учётной записи пользователя .....	15
3.3.12. Блокировка/разблокировка учётной записи пользователя .....	15
3.3.13. Удаление учётной записи пользователя .....	16
3.3.14. Подписание запросов на создание сертификатов пользователей .....	16
3.3.15. Аннулирование сертификата .....	16
3.3.16. Удаление ключа ЭП .....	17
3.3.17. Смена пароля .....	17
3.3.18. Смена ПИН-кода .....	17
3.4. Завершение работы .....	17
4. Сообщения оператору .....	18
Литература .....	19

## 1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программно-аппаратный комплекс Signal-COM Cloud DSS (далее Cloud DSS) предназначен для централизованного хранения и дистанционного применения ключей электронной подписи.

Веб-приложение оператора является программным компонентом программно-аппаратного комплекса Cloud DSS, предназначенным для выполнения следующих функций:

- регистрация новой учётной записи пользователя;
- отображение списка зарегистрированных учётных данных пользователей;
- перенос учётной записи пользователя из одной группы в другую;
- изменение параметров учётной записи пользователя;
- удаление/блокировка учётной записи пользователя;
- изменение параметров учётной записи оператора;
- генерация ключа электронной подписи и ключа проверки электронной подписи (для оператора и пользователей);
- формирование запроса на создание сертификата ключа проверки электронной подписи (для оператора и пользователей);
- выгрузка сформированного запроса на создание сертификата ключа проверки электронной подписи в файл;
- автоматическая передача запроса на создание сертификата ключа проверки электронной подписи в удостоверяющий центр.
- отображение списка сертификатов ключей проверки электронной подписи и их статусов (для оператора и пользователей);
- загрузка сертификата ключа проверки электронной подписи из файла;
- формирование запроса в удостоверяющий центр на приостановление/аннулирование сертификата ключа проверки электронной подписи;
- вывод на печать (по шаблону) запроса на создание сертификата ключа проверки электронной подписи;
- вывод на печать (по шаблону) сертификата ключа проверки электронной подписи.

### 1.1. Список сокращений

В настоящем руководстве используются следующие сокращения:

- ПАК – программно-аппаратный комплекс;
- ПАКМ – программно-аппаратный криптографический модуль;
- ПИН – персональный идентификационный номер;
- ПЭВМ – персональная электронно-вычислительная машина;
- УЦ – удостоверяющий центр;
- ЭП – электронная подпись;
- CMC - Certificate Management over CMS;
- CMS – Cryptographic Message Syntax;
- CRL – Certificate Revocation List;
- HOTP - HMAC-Based One-Time Password Algorithm.
- ITU-T – International Telecommunication Union - Telecommunication sector;
- OTP - One-Time Password;
- PIN – Personal Identification Number;
- RFC – Request for Comments;
- SMS - Short Message Service;
- TOTP - Time-Based One-Time Password Algorithm;
- XML – eXtensible Markup Language;

### 1.2. Термины и определения

В настоящем руководстве используются следующие термины:

- веб-сервис – реализация интерфейса взаимодействия между различными приложениями по протоколам REST и SOAP;
- ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;

- удостоверяющий центр – юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей;
- сертификат ключа проверки электронной подписи – документ в электронном виде или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;
- электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

## **2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ**

### **2.1. Требования к аппаратным средствам**

Веб-приложение оператора ПАК Cloud DSS может выполняться на следующих типах устройств:

- персональная ЭВМ;
- планшет;
- смартфон.

Минимальная аппаратная конфигурация для ПЭВМ:

- процессор Intel x86;
- оперативная память 2 Гб;
- жёсткий диск 500 Мб;
- сетевой адаптер;
- клавиатура;
- манипулятор «мышь».

### **2.2. Требования к программным средствам**

Веб-приложение оператора ПАК Cloud DSS может выполняться в следующих операционных системах:

- Windows;
- Linux;
- macOS;
- Android;
- iOS;
- iPadOS.

Для работы веб-приложения оператора ПАК Cloud DSS требуется веб-браузер, поддерживающий протокол HTML 4.0.

### 3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

#### 3.1. Загрузка приложения

Для загрузки веб-приложения оператора необходимо выполнить следующие действия:

- загрузить веб-браузер;
- в адресной строке задать адрес веб-приложения оператора;
- после переадресации на веб-приложение идентификации, на странице аутентификации пользователя задать учетные данные оператора (логин и пароль);
- если для оператора требуется вторичная аутентификация (определяется настройками ПАК Cloud DSS), необходимо ввести одноразовый пароль, полученный в сообщении (например, в SMS) или сформированный специальной программой на мобильном устройстве (по протоколу HOTP [3] или TOTP [2]);
- ввести ПИН-код для доступа к ключевому контейнеру на ПАКМ «Сигнал-КОМ HSM».

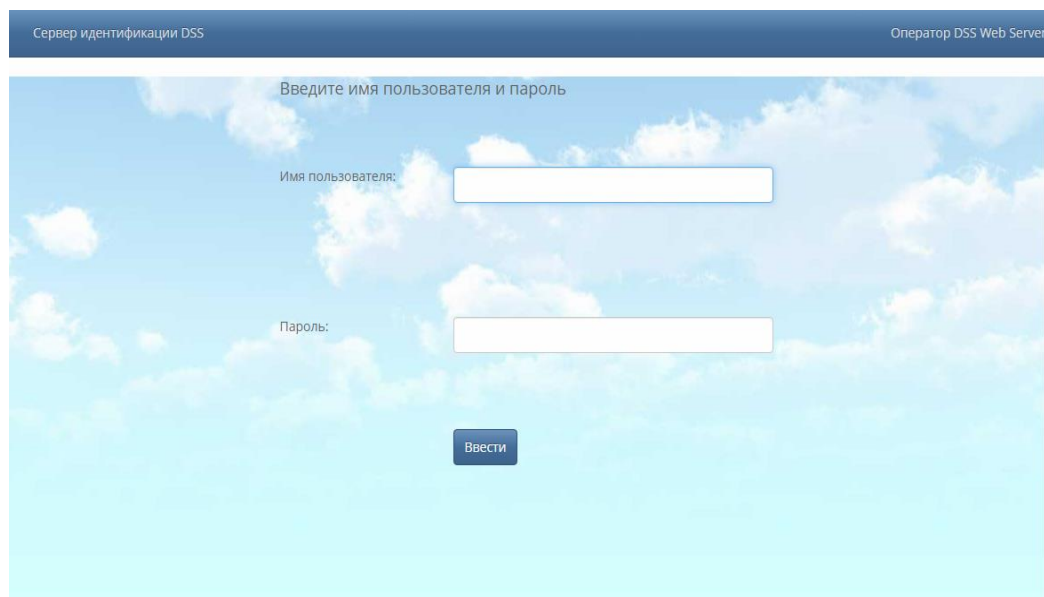


Рисунок 1

#### 3.2. Основное меню

Основное меню веб-приложения оператора располагается в левой части веб-страницы и содержит следующие пункты:

- «Мои сертификаты» - меню для работы с запросами на создание сертификатов ключей проверки ЭП и сертификатами ключей проверки ЭП оператора;
- «Пользователи» - меню для работы со списками пользователей;
- «Запросы на сертификат» - меню для работы с запросами на создание сертификатов ключей проверки ЭП пользователей;
- «Сертификаты пользователей» - меню для работы с сертификатами ключей проверки ЭП пользователей.

#### 3.3. Действия оператора

##### 3.3.1. Генерация ключей и запроса на создание сертификата

Для генерации ключей ЭП и запроса на создание сертификата ключа проверки ЭП оператора необходимо выполнить следующие действия:

- нажать отображаемое имя требуемого УЦ под пунктом «Мои сертификаты» главного меню;
- нажать кнопку «Получить ключ ЭП» (см. Рисунок 2);
- задать наименование ключа ЭП;
- выбрать УЦ;
- выбрать шаблон формирования запроса на создание сертификата ключа проверки ЭП;

- задать атрибуты различительного имени в запросе на сертификат ключа проверки ЭП;
- нажать кнопку «Сохранить» (см. Рисунок 3).

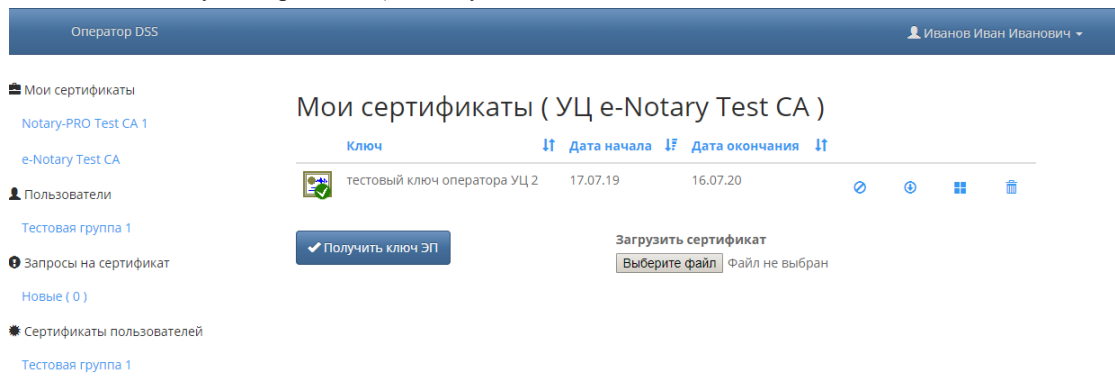


Рисунок 2



Получить ключ ЭП

Наименование ключа ЭП

тестовый ключ оператора УЦ

Удостоверяющий центр

e-Notary Test CA

Шаблон формирования запроса

Шаблон оператора

Персональные данные пользователя

\*Ф.И.О. (CommonName)

Иванов Иван Иванович

\*Адрес электронной почты (E-Mail)

iii@example.com

\*Организация (OrganizationName)

\*Подразделение (OrganizationUnitName)

\*Должность (Title)

оператор DSS

\*Город (LocalityName)

Москва

\*Область (StateOrProvinceName)

\*Страна (CountryName)

RU

Серийный номер (SerialNumber)

Почтовый адрес (PostalAddress)

Псевдоним (Pseudonym)

Неструктурированное имя (UnstructuredName)

\*ИНН (INN)

РНС ФСС (RNS FSS)

КП ФСС (KP FSS)

\*Фамилия (SurName)

\*Имя, Отчество (GivenName)

Название улицы, номер дома (StreetAddress)

ОГРН (OGRN)

ОГРН ИП (OGRNIP)

\*СНИЛС (SNILS)

Сохранить

Отмена

Рисунок 3

### 3.3.2. Выгрузка запроса на создание сертификата в файл

Для выгрузки запроса на создание сертификата ключа проверки ЭП в файл необходимо выполнить следующие действия:

- нажать отображаемое имя требуемого УЦ под пунктом «Мои сертификаты» главного меню;
- выбрать требуемый ключ и нажать значок загрузки файла (см. Рисунок 2).

### 3.3.3. Загрузка сертификата из файла

Для загрузки сертификата ключа проверки ЭП из файла необходимо выполнить следующие действия:

- нажать отображаемое имя требуемого УЦ под пунктом «Мои сертификаты» главного меню;

- нажать кнопку «Выберите файл» (см. Рисунок 2).

### 3.3.4. Работа с группами пользователей

Для выбора группы пользователей необходимо нажать отображаемое имя группы под пунктом «Пользователи» основного меню веб-приложения оператора (см. п. 3.2).

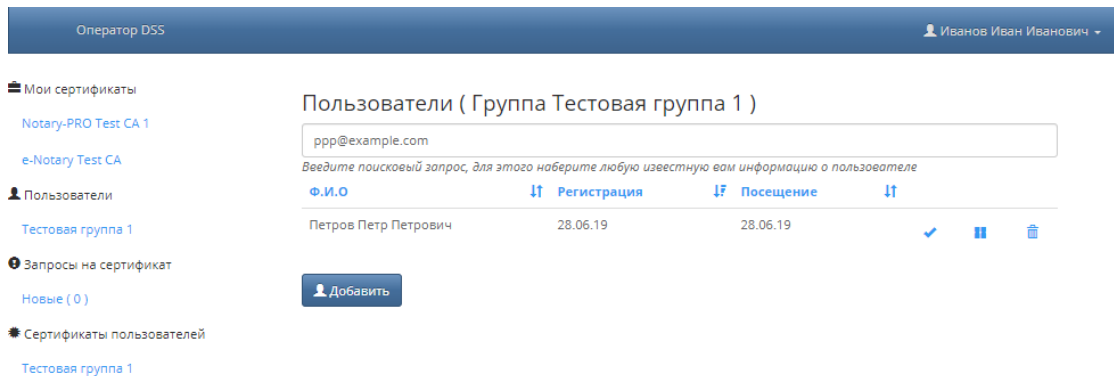


Рисунок 4

### 3.3.5. Работа со списком пользователей

После выбора группы пользователей (см. п. 3.3.4), в правой части веб-приложения будет отображаться список пользователей данной группы (см. Рисунок 4).

### 3.3.6. Регистрация учётной записи пользователя

Для создания новой учётной записи пользователя необходимо выполнить следующие действия:

- на странице со списком пользователей (см. п. 3.3.5) нажать кнопку «Добавить»;
- на странице профиля пользователя ввести фамилию, имя, отчество пользователя;
- ввести адрес электронной почты;
- ввести номер мобильного телефона;
- выбрать группу, в которую будет включен пользователь;
- выбрать метод вторичной аутентификации;
- выбрать параметры ОТР, если был задан метод вторичной аутентификации TOTP [2] или HOTP [3];
- сформировать список операций, требующих подтверждения пользователя;
- сформировать список транспортных служб для оповещения пользователя;
- нажать кнопку «Сохранить» (см. Рисунок 5);
- сообщить учетные данные (логин и пароль) пользователю.

Если требуется отменить добавление учётной записи, нажмите кнопку «Вернуться».

После создания учетная запись пользователя будет заблокирована. Чтобы разблокировать учетную запись см. п. 3.3.12.

Оператор DSS Иванов Иван Иванович

**Мои сертификаты**  
e-Notary Test CA  
Notary-PRO Test CA 1

**Пользователи**  
Тестовая группа 1

**Запросы на сертификат**  
Новые ( 0 )

**Сертификаты пользователей**  
Тестовая группа 1

### Профиль пользователя ( Группа Тестовая группа 1 )

Профиль

Ф.И.О. (CommonName)  
Петров Петр Петрович

Адрес электронной почты (E-Mail)  
ppp@example.com

Номер мобильного телефона  
|

Группа  
Тестовая группа 1

Метод аутентификации  
TOTP

Параметры OTP  
TOTP

Операции требующие подтверждения

Available	Selected
Вход в систему	Подпись
Смена пароля	
Генерация ключей и формирование запроса	
Смена пина	
Обновление сертификата	
Отзыв сертификата	
Удаление ключа	

Транспорт оповещения

Available	Selected
Email	
SMS	

[Сохранить](#) [Вернуться](#)

Рисунок 5

### 3.3.7. Ввод атрибутов различительного имени пользователя

Атрибуты различительного имени в профиле пользователя используются для формирования запроса на создание сертификата ключа проверки ЭП пользователя. Процедура занесения указанной информации (идентификация личности заявителя, рассмотрение документов и т.д.) выполняется оператором Cloud DSS в соответствии с Регламентом Удостоверяющего центра.

Ввод данной информации возможен после завершения процедуры создания учетной записи пользователя (см. п. 3.3.6).

Для задания атрибутов различительного имени в запросе на сертификат ключа проверки ЭП пользователя необходимо выполнить следующие действия:

- на странице со списком пользователей (см. п. 3.3.5) найти закладку с требуемой учетной записью;
- нажать значок параметров требуемой учетной записи;
- выбрать вкладку «Атрибуты имени X509»;
- задать проверенные атрибуты пользователя;
- нажать кнопку «Сохранить» (см. Рисунок 6).

Оператор DSS

Иванов Иван Иванович

Мои сертификаты

e-Notary Test CA

Notary-PRO Test CA 1

Пользователи

Тестовая группа 1

Запросы на сертификат

Новые ( 0 )

Сертификаты пользователей

Тестовая группа 1

Профиль пользователя: Петров Петр Петрович ( Группа Тестовая группа 1 )

Профиль

Атрибуты имени X509

Сертификаты

Второй фактор аутентификации

Ф.И.О. (CommonName)

Петров Петр Петрович

Адрес электронной почты (E-Mail)

ppp@example.com

Организация (OrganizationName)

Подразделение (OrganizationUnitName)

Должность (Title)

Город (LocalityName)

Область (StateOrProvinceName)

Страна (CountryName)

Серийный номер (SerialNumber)

Почтовый адрес (PostalAddress)

Псевдоним (Pseudonym)

Неструктурированное имя (UnstructuredName)

ИНН (INN)

РНС ФСС (RNS FSS)

КП ФСС (KP FSS)

Фамилия (SurName)

Имя, Отчество (GivenName)

Название улицы, номер дома (StreetAddress)

ОГРН (OGRN)

ОГРН ИП (OGRNIP)

СНИЛС (SNILS)

Сохранить

Рисунок 6

### 3.3.8. Получение разделяемого секрета

Разделяемый секрет используется в протоколах TOTP [2] и HOTP [3] для вторичной аутентификации пользователей. Разделяемый секрет является конфиденциальной информацией и должен передаваться пользователю при личной встрече (например, при регистрации учетной записи). Способы передачи разделяемого секрета могут быть следующими:

- сканирование QR-кода пользователем непосредственно с экрана монитора оператора с помощью мобильного приложения OTP-клиента (например, Google Authenticator);
- передача QR-кода пользователю на бумажном носителе для последующего сканирования с помощью мобильного приложения OTP-клиента.

Данный функционал доступен оператору, если в профиле пользователя задан метод вторичной аутентификации TOTP или HOTP (см. п. 3.3.6).

Получение данной информации возможно после завершения процедуры создания учетной записи пользователя (см. п. 3.3.6).

Для получения разделяемого секрета пользователя в виде QR-кода необходимо выполнить следующие действия:

- на странице со списком пользователей (см. п. 3.3.5) найти закладку с требуемой учетной записью;
- нажать значок параметров требуемой учетной записи;
- выбрать вкладку «Второй фактор аутентификации»;
- нажать кнопку справа от поля «Разделяемый секрет для TOTP и HOTP методов» (см. Рисунок 7).

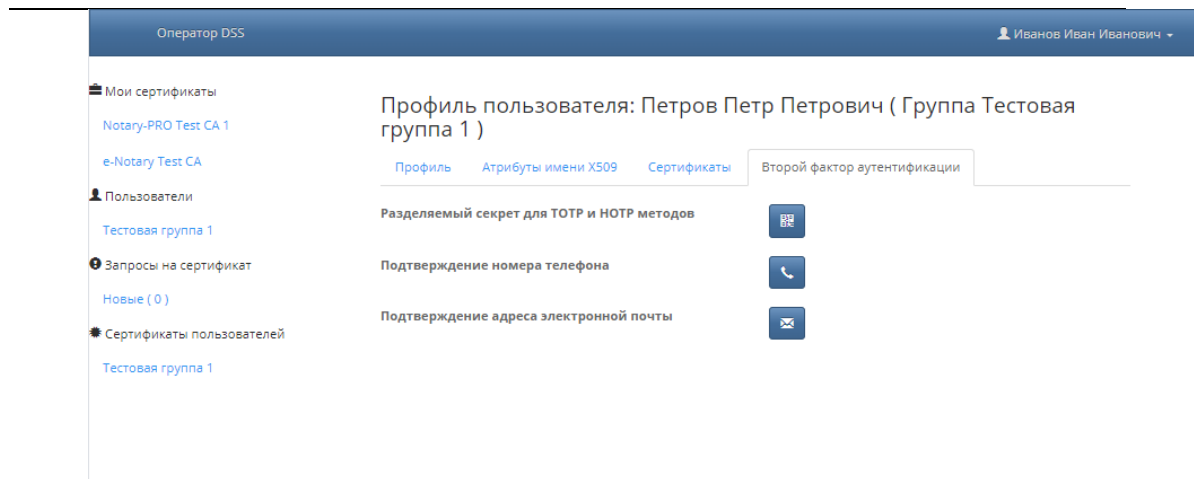


Рисунок 7

В случае успешного выполнения операции на текущей странице будет отображаться QR-код разделяемого секрета пользователя (см. Рисунок 8).



Рисунок 8

### 3.3.9. Подтверждение номера телефона

Для отправки SMS пользователю (например, если в профиле пользователя задан метод вторичной аутентификации «OTP через SMS» и/или транспорт оповещения «SMS») необходимо подтверждение номера телефона пользователя. Подтверждение номера телефона пользователя осуществляется при личной встрече (например, при регистрации учетной записи) и при наличии у пользователя соответствующего устройства для приема SMS.

Перед выполнением данной операции номер телефона пользователя должен быть предварительно сохранен в профиле пользователя (см. п. 3.3.6).

Для подтверждения номера телефона пользователя необходимо выполнить следующие действия:

- на странице со списком пользователей (см. п. 3.3.5) найти закладку с требуемой учетной записью;

- нажать значок параметров требуемой учетной записи;
- выбрать вкладку «Второй фактор аутентификации»;
- нажать кнопку справа от поля «Подтверждение номера телефона» (см. Рисунок 7);
- оператор будет перенаправлен на страницу сервера идентификации (см. Рисунок 9), а пользователю будет отправлено SMS с одноразовым паролем, который он должен сообщить оператору;
- на странице сервера идентификации оператор должен задать сообщенный пользователем одноразовый пароль и нажать кнопку «Ввести»;
- после успешного завершения операции оператор будет перенаправлен обратно на страницу профиля пользователя (в заголовке номера мобильного телефона будет отображаться статус «телефон подтвержден»).

The screenshot shows a web interface for confirming a phone number. At the top, it says 'Введите код подтверждения' (Enter confirmation code). Below that, a transaction ID is displayed: 'Транзакция 94603970. Подтверждение номера телефона. Введите код из СМС.' (Transaction 94603970. Confirmation of phone number. Enter code from SMS). A yellow box indicates the remaining time for confirmation: 'Оставшееся время для подтверждения' (Remaining time for confirmation) with a timer showing '00:16:31'. Below this is a label 'Код подтверждения:' (Confirmation code:) followed by a text input field. At the bottom, there are three buttons: 'Ввести' (Enter) in blue, 'Отправить новый код подтверждения' (Send new confirmation code) in blue, and 'Вернуться в приложение' (Return to app) in red.

Рисунок 9

### 3.3.10. Подтверждение адреса электронной почты

Для отправки электронной почты пользователю (например, если в профиле пользователя задан метод вторичной аутентификации «ОТР через eMail» и/или транспорт оповещения «Email») необходимо подтверждение адреса электронной почты пользователя. Подтверждение адреса электронной почты пользователя осуществляется при личной встрече (например, при регистрации учетной записи) и при возможности пользователя получать и просматривать сообщения своей электронной почты.

Перед выполнением данной операции адрес электронной почты пользователя должен быть предварительно сохранен в профиле пользователя (см. п. 3.3.6).

Для подтверждения адреса электронной почты пользователя необходимо выполнить следующие действия:

- на странице со списком пользователей (см. п. 3.3.5) найти закладку с требуемой учетной записью;
- нажать значок параметров требуемой учетной записи;
- выбрать вкладку «Второй фактор аутентификации»;

- нажать кнопку справа от поля «Подтверждение адреса электронной почты» (см. Рисунок 7);
- оператор будет перенаправлен на страницу сервера идентификации (см. Рисунок 10), а пользователю будет отправлено сообщение электронной почты с одноразовым паролем, который он должен сообщить оператору;
- на странице сервера идентификации оператор должен задать сообщенный пользователем одноразовый пароль и нажать кнопку «Ввести»;
- после успешного завершения операции оператор будет перенаправлен обратно на страницу профиля пользователя (в заголовке адреса электронной почты будет отображаться статус «адрес электронной почты подтвержден»).

Рисунок 10

### 3.3.11. Изменение параметров учётной записи пользователя

Для изменения параметров учетной записи пользователя необходимо выполнить следующие действия:

- на странице со списком пользователей (см. п. 3.3.5) найти закладку с требуемой учетной записью;
- нажать значок параметров требуемой учетной записи;
- изменить требуемые параметры;
- нажать кнопку «Сохранить» (см. Рисунок 5).

Если требуется отменить внесенные изменения, нажмите кнопку «Вернуться».

### 3.3.12. Блокировка/разблокировка учётной записи пользователя

Для блокировки/разблокировки учетной записи пользователя необходимо выполнить следующие действия:

- на странице со списком пользователей (см. п. 3.3.5) найти закладку с требуемой учетной записью;

- нажать значок статуса требуемой учетной записи;
- подтвердить изменение статуса учетной записи.

### 3.3.13. Удаление учётной записи пользователя

Для удаления учетной записи пользователя необходимо выполнить следующие действия:

- на странице со списком пользователей (см. п. 3.3.5) найти закладку с требуемой учетной записью;
- нажать значок удаления требуемой учетной записи;
- подтвердить удаление учетной записи.

Логин удаленной учетной записи не может в дальнейшем использоваться при регистрации/редактировании других учетных записей.

### 3.3.14. Подписание запросов на создание сертификатов пользователей

Для выполнения данной операции оператор должен сгенерировать ключи и получить в УЦ сертификат ключа проверки ЭП оператора УЦ (см. п. 3.3.1, п. 3.3.2 и п. 3.3.3).

Для подписания и отправки в УЦ запросов на создание сертификатов ключей проверки ЭП пользователей необходимо выполнить следующие действия:

- выбрать в меню «Запросы на сертификат» пункт «Новые»;
- выбрать требуемый запрос на создание сертификата;
- нажать значок сертификации;
- подтвердить сертификацию запроса на создание сертификата.

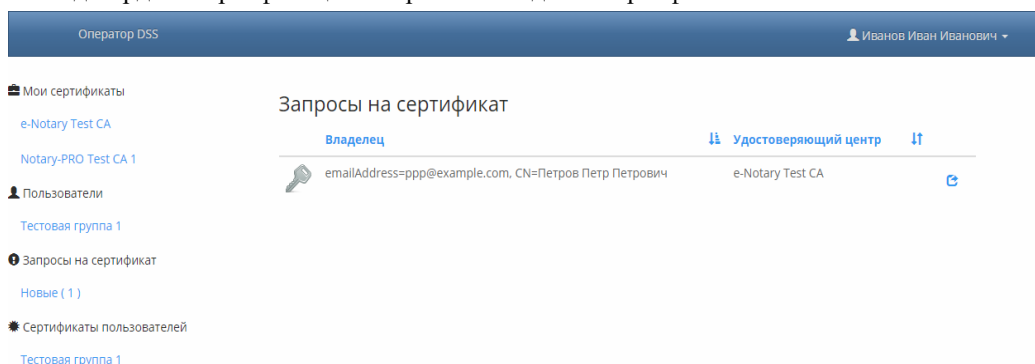


Рисунок 11

### 3.3.15. Аннулирование сертификата

Для аннулирования сертификата ключа проверки ЭП оператора необходимо выполнить следующие действия:

- нажать отображаемое имя требуемого УЦ под пунктом «Мои сертификаты» главного меню;
- выбрать вкладку «Сертификаты»;
- выбрать требуемый сертификат в списке и нажать значок свойств сертификата;
- на странице свойств сертификата нажать кнопку «Отозвать сертификат» (см. Рисунок 12).

Для аннулирования сертификата ключа проверки ЭП пользователя необходимо выполнить следующие действия:

- нажать отображаемое имя требуемой группы пользователей под пунктом «Сертификаты пользователей» главного меню;
- выбрать требуемый сертификат в списке и нажать значок свойств сертификата;
- на странице свойств сертификата нажать кнопку «Отозвать сертификат» (см. Рисунок 12).



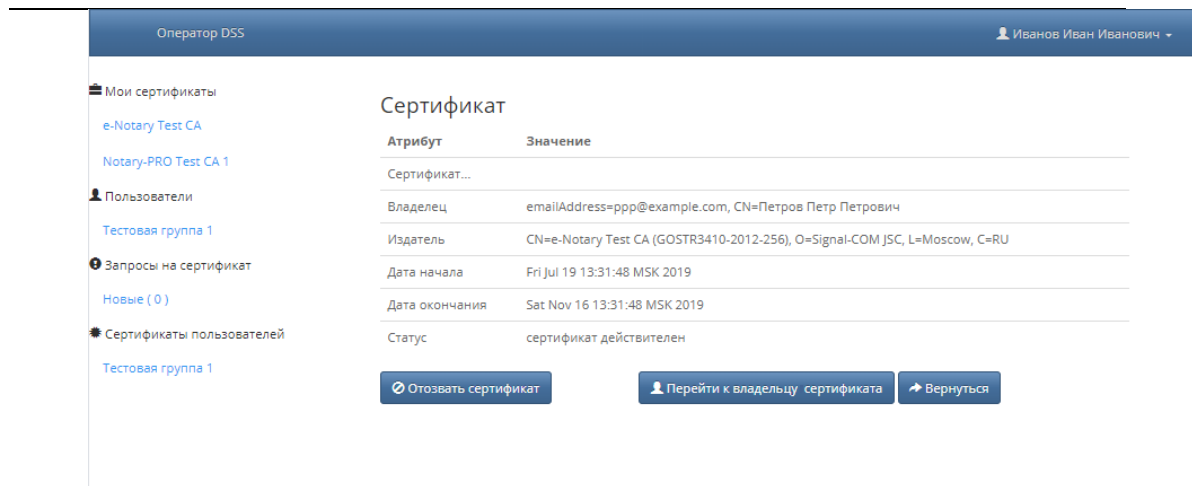


Рисунок 12

### 3.3.16. Удаление ключа ЭП

Для удаления ключа ЭП оператора необходимо выполнить следующие действия:

- нажать отображаемое имя требуемого УЦ под пунктом «Мои сертификаты» главного меню;
- выбрать требуемый ключ ЭП в списке и нажать значок удаления;
- подтвердить удаление ключа ЭП.

### 3.3.17. Смена пароля

Для смены пароля оператора необходимо выполнить следующие действия:

- нажать отображаемое имя оператора в правом верхнем углу веб-приложения;
- выбрать пункт меню «Сменить пароль»;
- после переадресации на веб-приложение идентификации, на странице смены пароля ввести старый пароль и новый пароль (дважды для подтверждения);
- нажать кнопку «Установить».

### 3.3.18. Смена ПИН-кода

Для смены ПИН-кода для доступа к ключевому контейнеру оператора необходимо выполнить следующие действия:

- нажать отображаемое имя оператора в правом верхнем углу веб-приложения;
- выбрать пункт меню «Сменить ПИН-код»;
- после переадресации на веб-приложение идентификации, на странице смены ПИН-кода ввести старый ПИН-код и новый ПИН-код (дважды для подтверждения);
- нажать кнопку «Установить».

## 3.4. Завершение работы

Для завершения работы в веб-приложении оператора необходимо выполнить следующие действия:

- нажать отображаемое имя оператора в правом верхнем углу веб-приложения;
- выбрать пункт меню «Выход».

#### **4. СООБЩЕНИЯ ОПЕРАТОРУ**

Сообщения программы оператору реализованы в виде модальных диалогов или в виде надписей и подсказок, отображаемых на текущей веб-странице.

### **ЛИТЕРАТУРА**

1. Signal-COM Cloud DSS. Описание применения. ШКНР.00051-01 31 01. АО «СИГНАЛ-КОМ», 2021.
2. D. M'Raihi, S. Machani, M. Pei, J. Rydell, TOTP: Time-Based One-Time Password Algorithm, RFC 6238, May 2011.
3. D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen, HOTP: An HMAC-Based One-Time Password Algorithm, RFC 4226, December 2005.