

АО «СИГНАЛ-КОМ»

УТВЕРЖДЕНО
ШКНР.00051-01 34 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС
SIGNAL-COM CLOUD DSS
Версия 1.0

Руководство пользователя

ШКНР.00051-01 34 01
Листов 13

АННОТАЦИЯ

Настоящий документ содержит руководство пользователя 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 пользователя	7
3.3.1. Генерация ключей и запроса на создание сертификата	7
3.3.2. Выгрузка запроса на создание сертификата в файл	8
3.3.3. Загрузка сертификата из файла	8
3.3.4. Создание ЭП	8
3.3.5. Проверка ЭП	9
3.3.6. Обновление сертификата	10
3.3.7. Аннулирование сертификата	10
3.3.8. Удаление ключа ЭП	10
3.3.9. Смена пароля	10
3.3.10. Смена ПИН-кода	10
3.4. Завершение работы	11
4. Сообщения оператору	12
Литература	13

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

- генерация ключа электронной подписи и ключа проверки электронной подписи;
- формирование запроса на создание сертификата ключа проверки электронной подписи;
- отображение списка запросов на создание сертификатов ключей проверки электронной подписи и их статусов;
- отображение списка сертификатов ключей проверки электронной подписи и их статусов;
- формирование запроса в удостоверяющий центр на приостановление/аннулирование сертификата ключа проверки электронной подписи;
- выгрузка сформированного запроса на создание сертификата ключа проверки электронной подписи в файл;
- загрузка сертификата ключа проверки электронной подписи из файла;
- вывод на печать (по шаблону) запроса на создание сертификата ключа проверки электронной подписи.
- вывод на печать (по шаблону) сертификата ключа проверки электронной подписи.
- изменение параметров учётной записи пользователя;
- создание электронной подписи для документа;
- проверка электронной подписи для документа.

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 пользователя 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 пользователя ПАК Cloud DSS может выполняться в следующих операционных системах:

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

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

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Загрузка приложения

Для загрузки веб-приложения пользователя необходимо выполнить следующие действия:

- загрузить веб-браузер;
- в адресной строке задать адрес веб-приложения пользователя;
- после переадресации на веб-приложение идентификации, на странице аутентификации пользователя задать учетные данные пользователя (логин и пароль);
- если для пользователя 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 «Signal-COM HSM».

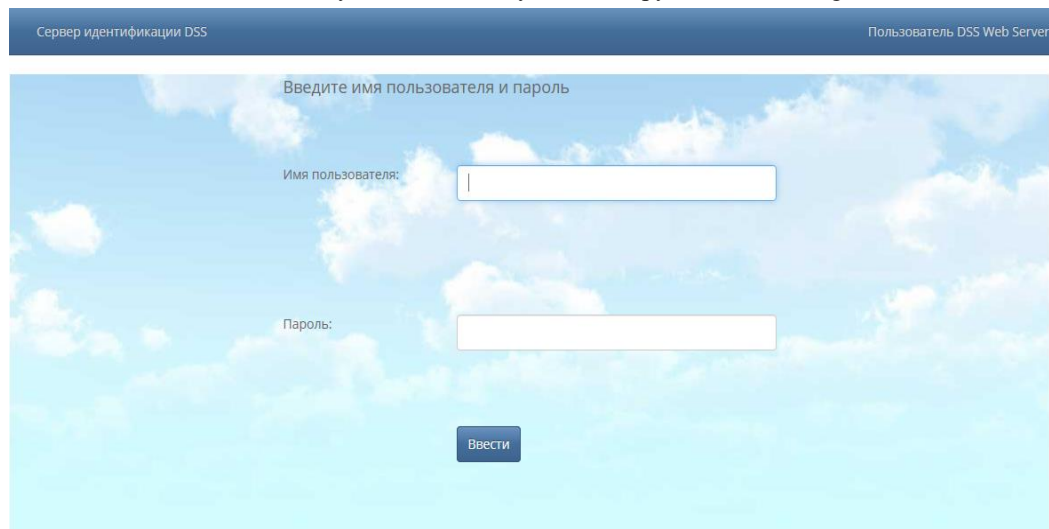


Рисунок 1

3.2. Основное меню

Основное меню веб-приложения пользователя 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 пользователя;
- «Сервисы» - меню для создания и проверки ЭП произвольных файлов.

3.3. Действия пользователя

3.3.1. Генерация ключей и запроса на создание сертификата

Для генерации ключей ЭП и запроса на создание сертификата ключа проверки ЭП 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;
- нажать кнопку «Сохранить» (см. Рисунок 3).

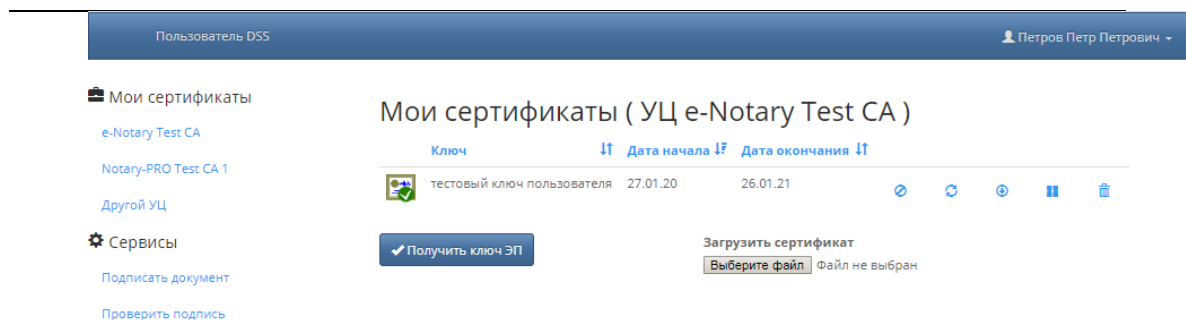


Рисунок 2

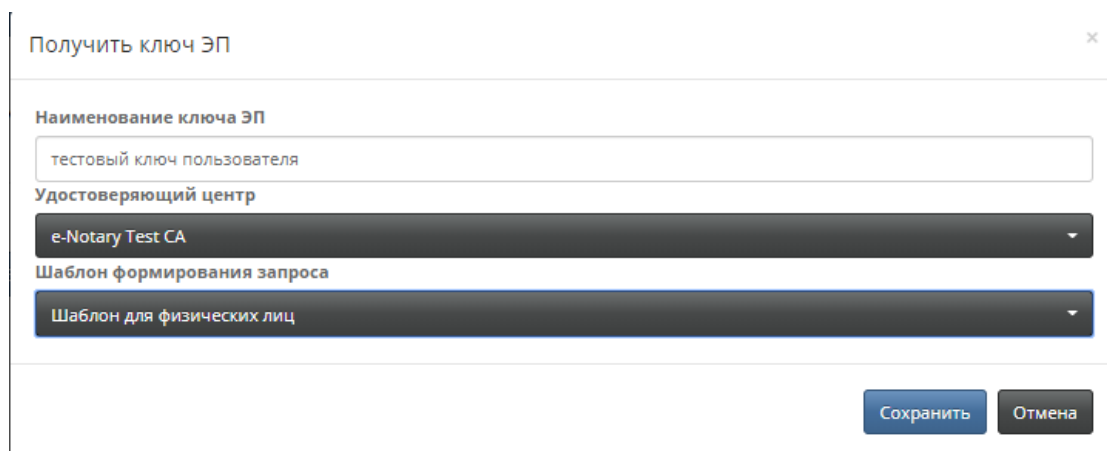


Рисунок 3

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. Создание ЭП

Для создания электронной подписи произвольного файла необходимо выполнить следующие действия:

- выбрать меню «Подписать документ»;
- задать сертификат ключа проверки ЭП в поле «Ключ ЭП»;
- задать название документа;
- выбрать файл, который необходимо подписать;
- нажать кнопку «Подписать» (см. Рисунок 4).

Пользователь DSS

Петров Петр Петрович

Мои сертификаты

- e-Notary Test CA
- Notary-PRO Test CA 1
- Другой УЦ

Сервисы

- Подписать документ
- Проверить подпись

Подписать документ

Ключ ЭП

тестовый ключ пользователя

Название документа

Тестовый документ

Загрузить файл для подписи

Выберите файл document

Подписать

Рисунок 4

После успешного завершения операции можно скачать файл электронной подписи, нажав на соответствующую ссылку (см. Рисунок 5).

Пользователь DSS

Петров Петр Петрович

Мои сертификаты

- e-Notary Test CA
- Notary-PRO Test CA 1
- Другой УЦ

Сервисы

- Подписать документ
- Проверить подпись

Подписать документ

Ключ ЭП

Выберите значение

Название документа

Загрузить файл для подписи

Выберите файл Файл не выбран

Подписать

Скачать файл подписи

Рисунок 5

3.3.5. Проверка ЭП

Для проверки электронной подписи произвольного файла необходимо выполнить следующие действия:

- выбрать меню «Проверить подпись»;
- выбрать файл проверяемого документа;
- выбрать файл электронной подписи документа;
- нажать кнопку «Проверить подпись» (см. Рисунок 6).

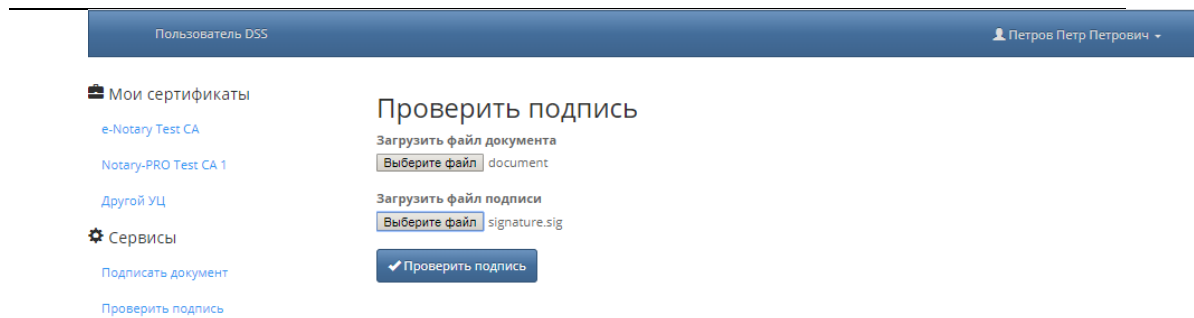


Рисунок 6

3.3.6. Обновление сертификата

Для обновления сертификата ключа проверки ЭП необходимо выполнить следующие действия:

- нажать отображаемое имя требуемого УЦ под пунктом «Мои сертификаты» главного меню;
- выбрать требуемый сертификат в списке и нажать значок обновления сертификата (см. Рисунок 2).

3.3.7. Аннулирование сертификата

Для аннулирования сертификата ключа проверки ЭП необходимо выполнить следующие действия:

- нажать отображаемое имя требуемого УЦ под пунктом «Мои сертификаты» главного меню;
- выбрать требуемый сертификат в списке и нажать значок аннулирования сертификата (см. Рисунок 2).

3.3.8. Удаление ключа ЭП

Для удаления ключа ЭП 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 (см. Рисунок 2);
- подтвердить удаление ключа ЭП.

3.3.9. Смена пароля

Для смены пароля пользователя необходимо выполнить следующие действия:

- нажать отображаемое имя пользователя 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».

3.3.10. Смена ПИН-кода

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

- нажать отображаемое имя пользователя 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 пользователя необходимо выполнить следующие действия:

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

4. СООБЩЕНИЯ ОПЕРАТОРУ

Сообщения программы оператору (пользователю) 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.