SKY TECHNOLOGIES

ООО «СКАЙ ТЕХНОЛОДЖИС»
196006, г. Санкт-Петербург,
ул. Заставская д.22 к.2, Лит.А,
этаж 6, помещение № 454
Телефон: +7 (812) 779-20-79
Email: ask@sky-technologies.ru

REMOTE KEY MANAGEMENT

innovative payments

Руководство пользователя

Версия 1.00

SKY TECHNOLOGIES

Оглавление

Глоссарий

Термин	Расшифровка
API	Application Program Interface, описание способов (набор классов, процедур, функций, структур или констант), которыми RKM может взаимодействовать с другими клиентскими сервисами.
CPU	Central Processing Unit, центральный процессор
CSR	Certificate Sign Request – запрос на подпись сертификата
FW	Firmware, версия прошивки конечного клиентского устройства.
HDD	Твёрдотельный накопитель, жесткий диск ПЗУ
HSM	Hardware Security Module, программно-аппаратный криптографичес-кий модуль
KCV	Key Check Value, контрольная сумма ключа
KLK	Key Loader Key, специальный ключ, которым зашифровывается мастер ключ для последующей его передачи на целевой терминал
KM	Собственный мастер-ключ HSM
PCI DSS	Payment Card Industry Data Security Standard, стандарт безопасности данных индустрии платежных карт
POS	Терминал, предназначенный для приёма банковских карт для осуществления безналичных платежей
RKI	Remote Key Injector транспортный сервис передачи криптографических мастерключей
TID	Terminal ID, уникальный идентификатор терминала в системе
WSL	Windows Subsystem for Linux, подсистема Windows для совместимости с Linux
ZMK	Специальный криптографический ключ 3DES, которым шифруются все ключи данных, используемые для обмена информацией между двумя субъектами. ZMK используется для передачи TMK на RKI
ОЗУ	Память с произвольным доступом или оперативное запоминающее устро́йство
ПЦ Way4	Процессинговый центр Банка, работающий на протоколе OpenWay Way4, отвечающий за обработку транзакций, генерацию рабочих ключей и т.п.
СУБД	Система управления базами данных (БД)
УЗК	Удалённый загрузчик ключей или RKL - Remote Key Loader

Введение

Данный документ разработан ООО "Скай Технолоджис" и содержит описание процесса работы с системой SkyRKM – программно-аппаратным комплексом, при помощи которого выполняется безопасная автоматическая удаленная загрузка комплекта начальных криптографических мастер-ключей в платежные терминалы, предназначенные для установки в торгово-сервисные предприятия и банки.

Документ предназначается для владельцев и директоров организаций, операторов банковской инфраструктуры и банковским офицерам безопасности, ответственным ITинженерам финансовых организаций.

Допускается незначительные несоответствия данной документации и программного обеспечения, связанные с постоянным развитием программных продуктов.

Не допускается использование текстов и изображений, входящих в данный документ, без согласования с ООО «Скай Технолоджис»

1. Общее описание SkyRKM

SkyRKM – это программно-аппаратный комплекс, при помощи которого выполняется процесс безопасной автоматической удаленной загрузки комплекта начальных криптографических мастер-ключей в платежные терминалы, предназначенные для установки в торгово-сервисные предприятия и банки.

В состав SkyRKM входит:

- сервис SkyCA - Система подписи сертификатов (Сервер Загрузки Сертификатов, СЗС);
- сервис SkyRKI - Централизованная система управления сервисами загрузки криптографических ключей (Сервер Загрузки Ключей, СЗК);
- HSM – устройство, которое генерирует ключи, для последующей загрузки в целевые терминалы (ключи передаются в зашифрованном виде); работа с сервисами выполняется через web-интерфейс.

Основное назначение системы SkyRKM – реализация загрузки мастер-ключей в целевые платежные терминалы (устройства) в полном соответствии с требованиями PCI DSS, PTS и VISA PIN Attestation of Compliance.

Компоненты системы SkyRKM устанавливается в виде сервиса на специализированный сервер, установленный в PCI среде.

В процессе загрузки ключей выполняется аутентификация устройств по «белому» списку внутри локальной контролируемой сетевой среды, сама процедура загрузки ключей удовлетворяет всем требованиям безопасности PCI.

Для ограничения загрузки ключей в компрометированные целевые устройства используется «черный» список для, посредством которого выполняется контроль попыток подключения таких устройств.

Система SkyRKM является многопользовательской, пользователь с соответствующей ролью выполняет определенные функции.

Web-интерфейс SkyRKM позволяет:

- управлять белыми и черными списками;
- контролировать запросы и отчеты в системе;
- просматривать статусы загрузки ключей (успешная / неуспешная);
- управлять возможностью повторной загрузки ключей;
- выполнять администрирование системы;
- обеспечивать доступ к файлам логирования системы.

Доступные функции зависят от уровня доступа пользователей.

Передача ключей на клиентский терминал осуществляется по каналу связи, защищённому TLS 1.2.

Модульная структура SkyRKM позволяет безболезненно интегрировать систему удаленной загрузки ключей в текущую инфраструктуру банка или организации, осуществляющую продажу терминалов конечным клиентам.

2. Работа с сервисом SkyRKM

Данный раздел содержит описание основного функционала программного решения SkyRKM и работы с ним.

2.1. Вход в систему

Работа с SkyRKM выполняется через web-интерфейс - запустите интернет обозреватель и введите в адресную строку адрес http://localhost:9220/web/rkl/ – на экране отобразится экран входа в систему SkyRKM.

	*ВАЖНО:* *В данном документе описан объединенный функционал сервисов CA и RKI, при необходимости сервисы можно установить отдельно.* *В таком случае для входа в сервисы необходимо ввести адреса http://localhost:9220/web/ca/ и http://localhost:9220/web/rki/ соответственно.*

	*ПРИМЕЧАНИЕ:* *Пара логин/пароль задаётся пользователем при переходе по ссылке из письма приглашения.* *Пароль может быть изменён пользователем.*

Введите Логин и Пароль для входа в систему и нажмите кнопку «Войти».

Если Логин и Пароль введены верно, откроется интерфейс системы.
Если Логин и Пароль введены неверно, отобразится соответствующее сообщение об ошибке.

	ПРИМЕЧАНИЕ: *При необходимости выберите язык интерфейса системы из выпадающего списка, расположенного в правом верхнем углу экрана (English/Russian) .* *Рядом с выпадающим списком отображается знак вопроса, нажав на который отображаются контакты технической поддержки.*

2.1.1. Восстановление пароля

Если пользователь забыл пароль в SkyRKM предусмотрен функционал восстановления пароля. Для того, чтобы восстановить пароль, нажмите кнопку «Забыли пароль», расположенную на странице авторизации пользователя. Введите Логин, использующийся для входа в систему.

На привязанный к учетной записи адрес электронной почты будет отправлено письмо с описанием порядка восстановления пароля и ссылка на форму ввода нового пароля

2.1.2. Выход из системы

Для того, чтобы выйти из системы нажмите кнопку «Выход», расположенную в правом верхнем углу экрана.

2.2. Роли пользователей

Доступ к системе является многопользовательским, доступный функционал SkyRKM зависит от роли пользователя, вошедшего в систему:

- Офицер безопасности – пользователь с этой ролью может просматривать и генерировать сертификаты для приложений, работать с ключами, изменять настройки системы;
- Оператор RKM – пользователь с этой ролью может создавать записи в белых списках целевых устройств для их последующей авторизации в системе и загрузки в них ключей, а так же просматривать историю подключений целевых устройств к SkyRKM и результат выполнения авторизации или загрузки ключей;
- Администратор – пользователь с этой ролью управляет пользователями в системе и задает определенные настройки системы.

2.3. Главное меню SkyRKM

Экран системы SkyRKM разделен на две части: в левой части экрана расположено Главное меню, в правой части экрана расположена рабочая область системы.

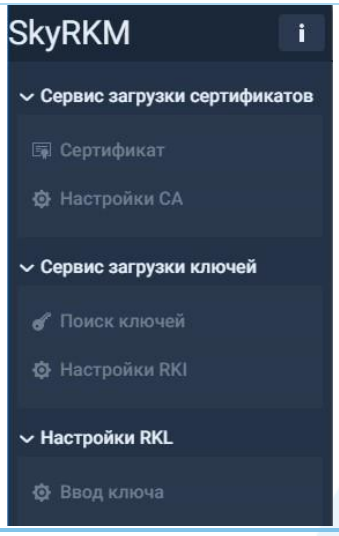
Через главное меню SkyRKM осуществляется доступ к основным функциональным разделам системы.

Для каждой роли пользователя реализован доступ к различным функциям соответствующих разделов:

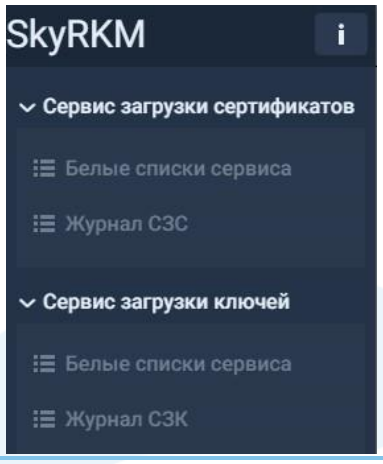
- Сервис загрузки сертификатов – раздел предназначен для управления и контроля процесса подписания сертификата целевых терминалов – функционал данного раздела доступен пользователям с ролью Офицер Безопасности и Оператор RKM (для каждой роли пользователя реализован доступ к различным функциям);
- Сервис загрузки ключей – раздел предназначен для управления и контроля процесса загрузки ключей в целевые терминалы – функционал данного раздела доступен пользователям с ролью Офицер Безопасности и Оператор RKM;
- Настройки RKL – раздел предназначен для выполнения настроек процесса удаленной загрузки ключей – функционал данного раздела доступен пользователям с ролью Офицер Безопасности и Администратор;
- Доступ – раздел предназначен для управления пользователями системы и выполнения аудита работы системы – функционал данного раздела доступен только пользователю с ролью Администратор.

ВАЖНО:

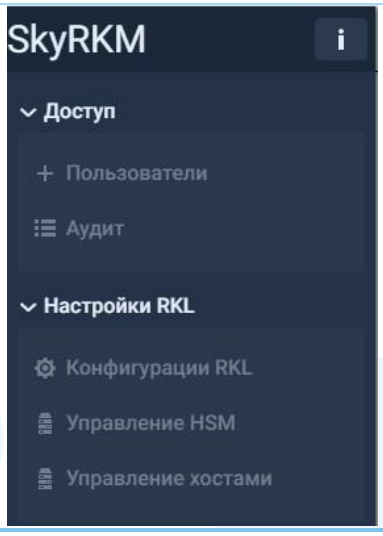
Если CA и RKI установлены на разных серверах в Главном меню разделы Сервис загрузки сертификатов и Сервис загрузки ключей будут отображаться по отдельности.



Главное меню пользователя с ролью Офицер безопасности



Главное меню пользователя с ролью Оператор



Главное меню пользователя с ролью Администратор

2.3.1. Версия приложения

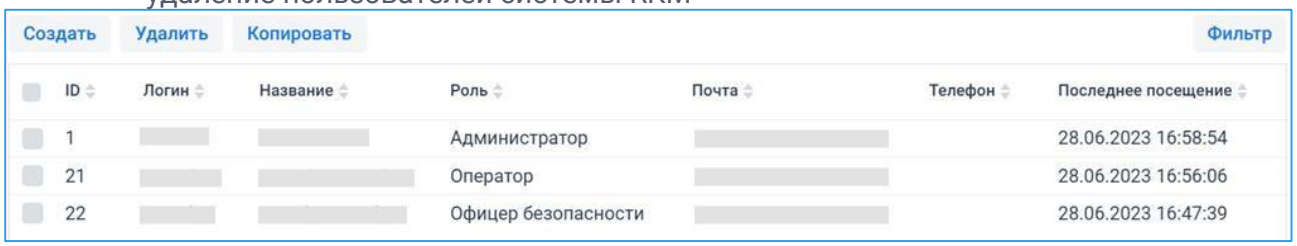
Для того, чтобы узнать текущую версию SkyRKM нажмите кнопку i, расположенную слева от названия Главного меню. На экране отобразится следующая информация:

- номер текущей версии приложения;
- список обновленного функционала, вошедшего в текущую версию приложения, а также всю историю изменений приложения – номер версии и подробное описание нового функционала.

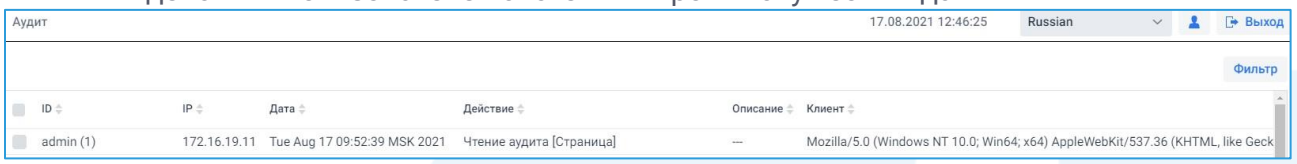
2.4. Функционал Администратора

Для пользователя с ролью Администратор доступен следующий функционал разделов Главного меню:

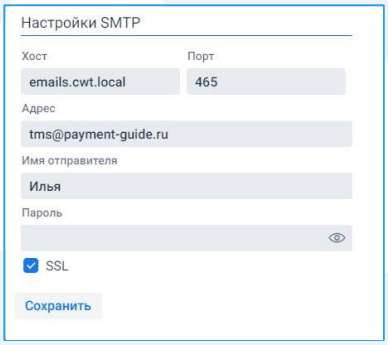
- Доступ:
  - > Пользователи – просмотр списка пользователей, управление доступом, создание и удаление пользователей системы RKM



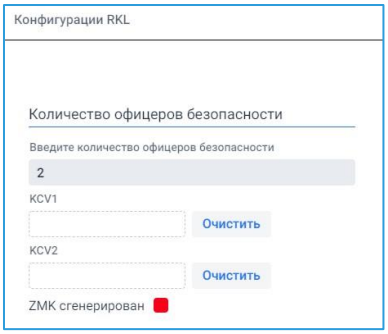
  - > Аудит – аудит действий пользователей системы RKM – просмотр событий и действий пользователей системы и прочих служебных данных.



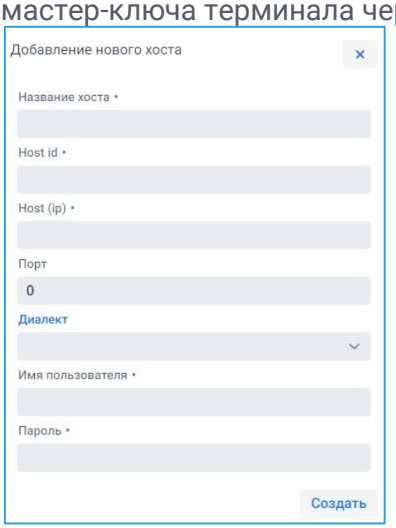
- Настройки RKI
  - > Конфигурация RKI – настройка параметров сервера исходящей почты RKI:
    - Хост;
    - Порт;
    - Адрес;
    - Имя отправителя;
    - Пароль;
    - SSL.



- Конфигурация RKL – настройка параметров удаленного загрузчика ключей:
  - Количество офицеров безопасности – задается количество пользователей с ролью Офицер безопасности, в присутствии которых необходимо выполнять ввод ключа в базу данных SkyRKM для последующей загрузки в терминалы;
  - KCV1;
  - KCV2;
  - ZMK сгенерирован;



- Управление хостами – добавление нового хоста процессинга, в который следует передать криптограмму мастер-ключа терминала через REST API.



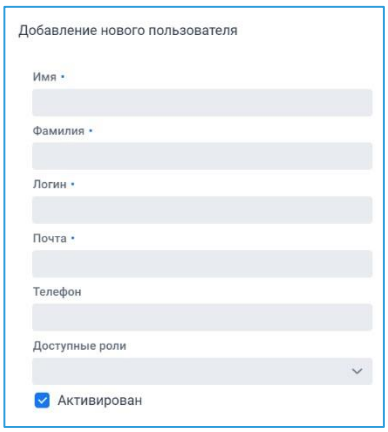
2.4.1. Создание нового пользователя

Для того, чтобы создать нового пользователя нажмите кнопку «Создать», расположенную в верхней части экрана над списком пользователей – откроется окно ввода данных нового пользователя со следующими полями:

- Имя – имя нового пользователя;
- Фамилия – фамилия нового пользователя;
- Логин – логин нового пользователя – длина логина должна быть более 3 символов;
- Почта – адрес электронной почты – на этот адрес будут отправляться письма, например, для восстановления пароля;
- Телефон – номер телефона пользователя;
- Доступные роли – выберите роль пользователя из выпадающего списка:

- RKL integrational API (GET) – специализированная роль пользователя для работы по API;
- RKL integrational API (POST) – специализированная роль пользователя для работы по API;
- Администратор;
- Офицер безопасности;
- Оператор;

- Активирован – если флаг установлен, пользователь может авторизоваться в системе (данное поле используется в том случае, если пользователь ввел неправильный пароль и его аккаунт заблокировался).



2.4.2. Копирование пользователя

Для того, чтобы создать копию пользователя системы, выделите нужного пользователя, установив галочку, и нажмите кнопку «Копировать», расположенную в верхней части экрана над списком пользователей – откроется окно ввода данных пользователя, заполненное теми же значениями, что и исходный пользователь – измените логин для пользователя и, при необходимости, другие данные.

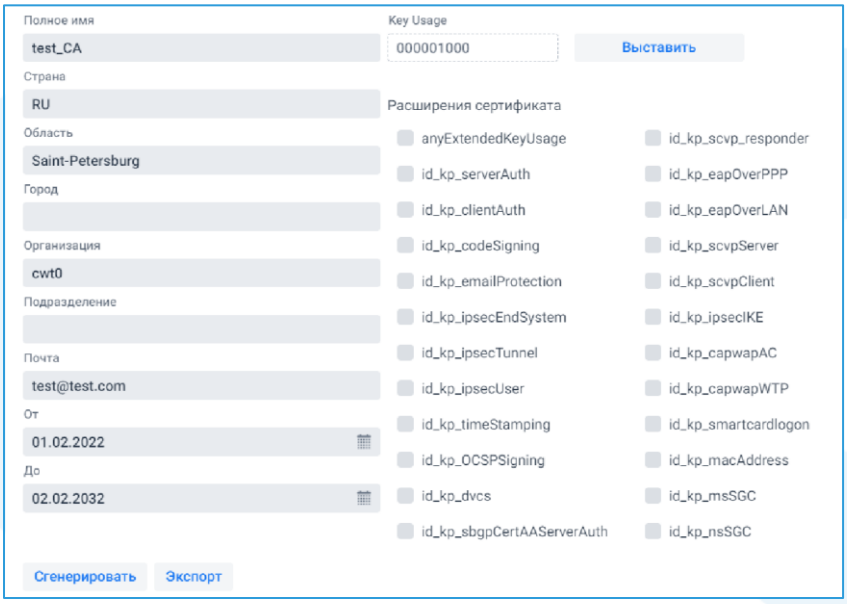
2.4.3. Удаление пользователя

Для того, чтобы удалить пользователя из системы, выделите нужного пользователя, установив галочку, и нажмите кнопку «Удалить», расположенную в верхней части экрана над списком пользователей и подтвердите удаление записей.

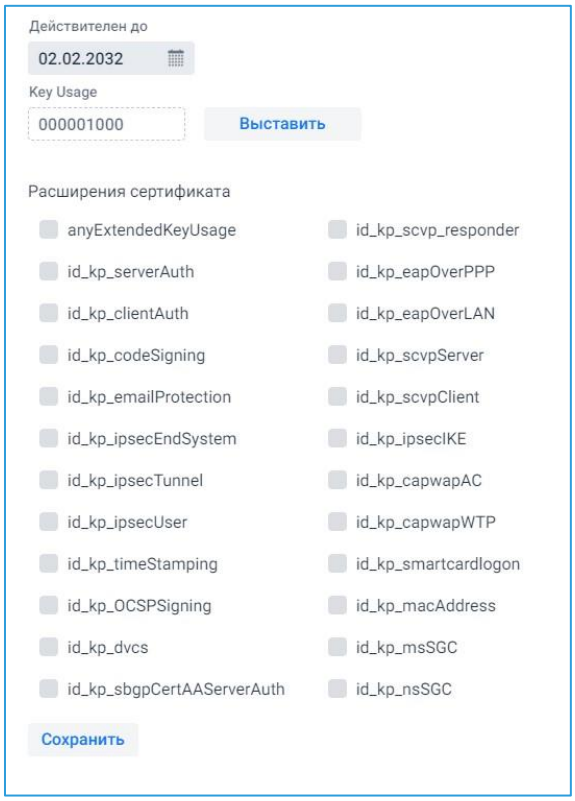
2.5. Функционал пользователя с ролью Офицер безопасности

Для пользователя с ролью Оператор доступен следующий функционал разделов Главного меню:

- Сервис загрузки сертификатов:
  - Сертификат – генерация и экспорт в Сервис Загрузки Ключей сертификата обмена данными – задаются следующие параметры сертификатов:
    - Страна;

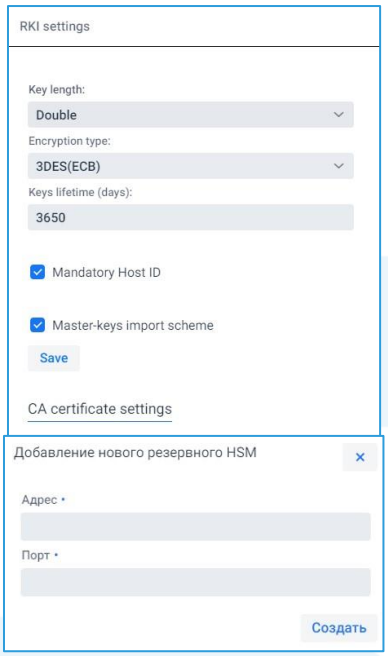


- Область;
- Город;
- Организация;
- Подразделение;
- Почта;
- От – срок начала действия сертификата;
- До – завершение действия сертификата;
- Расширение сертификата – отметьте расширения для сертификата.



> Настройка CA – сохранение сертификата CA – параметры сертификата CA:
> Действителен до – срок действия сертификата CA;
> Key Usage – для чего будет использоваться данный сертификат (Выставить);
> Расширения сертификата - отметьте необходимые расширения для сертификата. После ввода параметров нажмите кнопку «Сохранить» - внесенные параметры Сертификата CA будут сохранены.

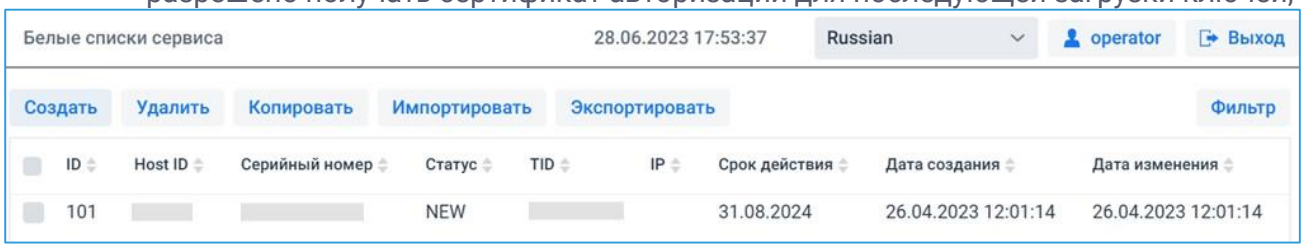
- Сервис загрузки ключей:
  > Поиск ключей – функционал позволяет выполнить поиск ключей по TID и Серийному номер;
  > Импорт ключей – загрузка XML файлов с криптограммами TAMK и TPMK, предварительно созданных для последующей передачи на терминалы;
  > Настройки RKI – В данном разделе настраивается срок жизни добавляемых ключей, управляется жесткая проверка Host ID и импортируется сертификат, ранее созданный в CA.
- Настройки RKL:
  > Ввод ключа – ручной ввод компоненты ключа ZMK.
  > Управление HSM – в данном разделе отображается список HSM;
  > Адрес;
  > Порт;
  > > Управление хостами – добавление хостов, параметров соединения с FIMI, отображение мастер-ключей для Host ID



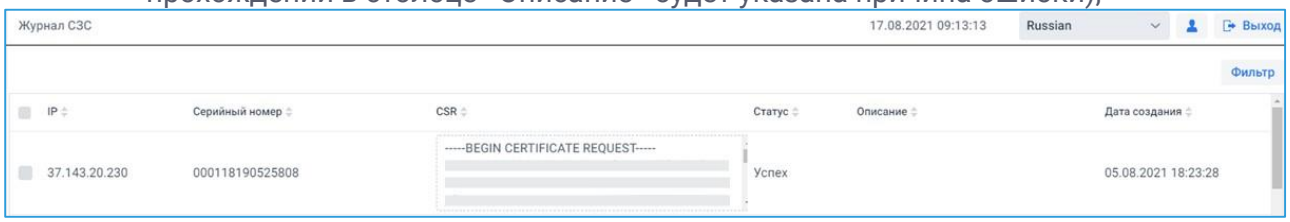
2.6. Функционал пользователя с ролью Оператор

Для пользователя с ролью Оператор доступен следующий функционал разделов Главного меню:

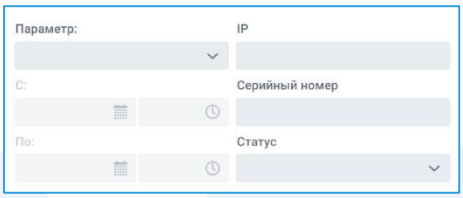
- Сервис загрузки сертификатов:
  - > Белые списки сервиса – список терминалов (целевых устройств), которым разрешено получать сертификат авторизации для последующей загрузки ключей;



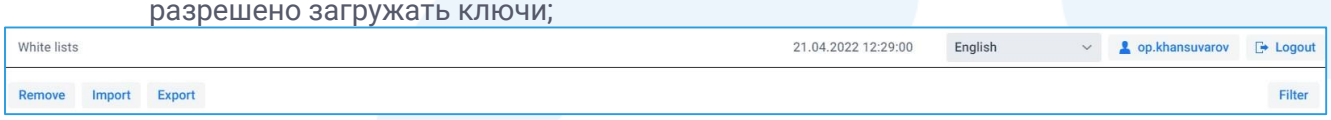
  - > Журнал СЗС – просмотр истории подключений к сервису авторизации и анализ результатов прохождения процедуры СА по финальному статусу (при неуспешном прохождении в столбце «Описание» будет указана причина ошибки);



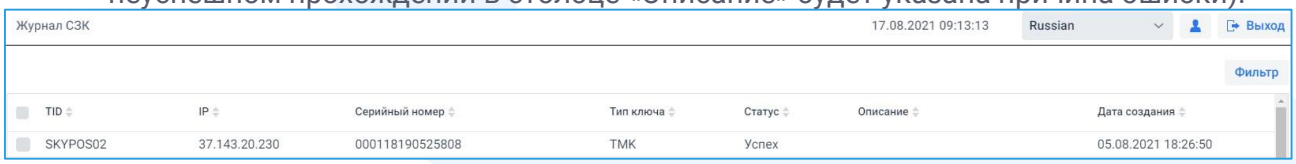
При необходимости данные в таблице можно отфильтровать в соответсвии с заданными параметрами, нажав кнопку «Фильтр»: ○ Параметр: ○ С; ○ По; ○ IP; ○ Серийный номер; ○ Статус.



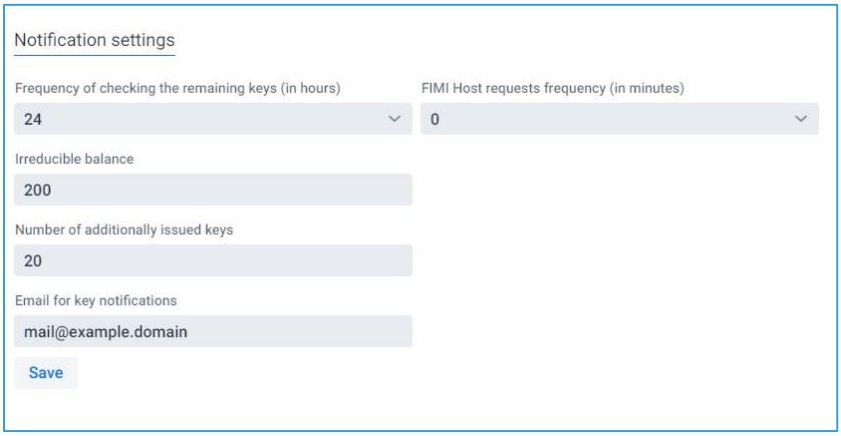
- Сервис загрузки ключей:
  - > Белые списки сервиса – управление белым списком целевых устройств – в устройства, которые находятся в белом списке и подключились к Сервису Загрузки Ключей, разрешено загружать ключи;



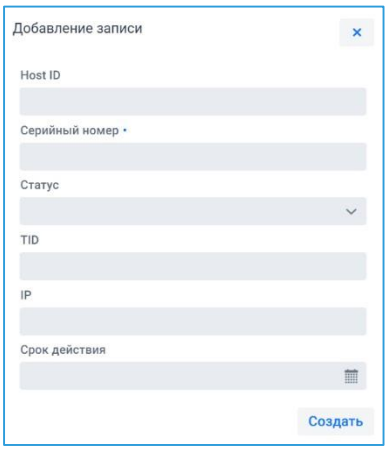
  - > Журнал СЗК – просмотр подключений к сервису загрузки ключей и анализ результатов прохождения процедуры загрузки ключей по финальному статусу (при неуспешном прохождении в столбце «Описание» будет указана причина ошибки).



  - > Настройки RKI – функционал позволяет настроить параметры уведомлений при определении остатков ключей и частоту опроса банковского хоста.



2.6.1. Добавление терминала в белый список



Для того, чтобы добавить терминал в Белый список, нажмите кнопку «Создать», расположенную в верхней части экрана над списком терминалов – откроется окно ввода данных со следующими полями:

- Host ID – идентификатор хоста;
- серийный номер – серийный номер терминала;
- статус – выберите значение из выпадающего списка:
  - NEW – новый терминал;
  - USED – терминал уже приходил за сертификатом;
  - CANCELLED – терминалу нельзя приходить за сертификатом;
- TID;
- IP;
- срок действия.

Введите параметры целевого терминала, который необхоидмо добавтиь в белый список, и нажмите кнопку «Создать» - терминал появится в списке терминалов.

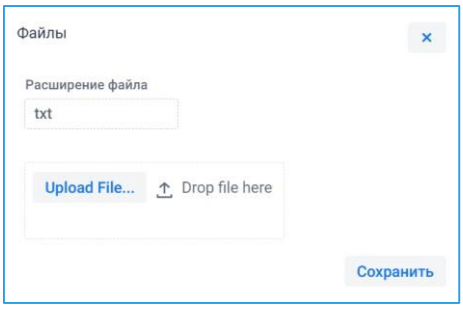
2.6.2. Копирование терминала для добавления в белый список

Для того, чтобы создать копию терминала из списка, выделите нужный терминал, установив галочку, и нажмите кнопку «Копировать», расположенную в верхней части экрана над списком терминалов – откроется окно ввода данных терминала, заполненное теми же значениями, что и исходный терминал из белого списка – измените серийный номер и TID, при необходимости, другие данные.

2.6.3. Удаление терминала из белого списка

Для того, чтобы удалить терминал из белого списка, выделите нужный терминал, установив галочку, и нажмите кнопку «Удалить», расположенную в верхней части экрана над списком записей.

2.6.4. Импорт файла с белым списком терминалов



Для удобства работы с системой реализован функционал загрузки терминалов в белый список при помощи зашифрованных файлов.

Формат содержимого файла:

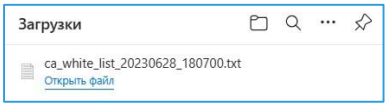
HostID|SN|статус

Где:

- HostID – идентификатор хоста терминала; SN – серийный номер терминала; Статус – может принимать значение:
  - > NEW – новая запись RKI;
  - > CANCELLED - новый статус, отменён/запрещён для загрузки;

Если при обработке файла в строке офранцужена ошибка, RKI загрузит все строки, кроме строки с ошибкой, в аудит при этом сохранится уведомление об ошибке и номер строки файла.

2.6.5. Экспорт белого списка



При необходимости можно выполнить экспорт белого списка – для этого нажмите кнопку «Экспорт», расположенную над таблицей.

2.6.6. Фильтр белого списка

При необходимости данные терминалов, отображающиеся в Белом списке, можно отфильтровать.