



Remote Key Management

Руководство пользователя

Версия: 2.00

ОГЛАВЛЕНИЕ

История изменений	3
Глоссарий	4
Условные обозначения	5
Введение	6
1. Общее описание SomersRKM	7
1.1. Пользователи	7
1.2. Порядок работы с комплексом SomersRKM	8
1.2.1. Предварительная подготовка компонент комплекса	8
1.2.2. Загрузка ключей	8
1.3. Модели HSM	10
2. Работа с SomersRKM	11
2.1. Вход в систему	11
2.2. Выбор языка интерфейса	11
2.3. Восстановление пароля	11
2.4. Выход из системы	12
2.5. Интерфейс SomersRKM	12
2.6. Версия приложения	12
3. Функционал Администратора	13
3.1. Управление пользователями	13
3.1.1. Создание нового пользователя	13
3.1.2. Копирование пользователя	14
3.1.3. Редактирование пользователя	14
3.1.4. Удаление пользователя	15
3.1.5. Аудит действий пользователя	15
3.2. Настройки RKL	15
3.2.1. Количество офицеров безопасности	15
3.2.2. Настройка SMTP для отправки сообщений	15
3.2.3. Дополнительные схемы загрузки ключей	16
3.3. Настройка резервных HSM	16
3.4. Настройка параметров хоста	16
4. Функционал Офицера безопасности	18
4.1. Генерация сертификата	18
4.2. Настройки СА	19
4.3. Информация о загруженных ключах	21
4.3.1. Поиск ключей	21
4.3.2. Передача информации о ключах на хост	21
4.4. Настройка параметров ключей	22
4.5. Ввод ZMK (опционально)	23
4.5.1. Ручной ввод ключа ZMK	23
4.5.2. Загрузка ZMK при помощи файла	23
5. Функционал Оператора	25
5.1. Управление белым списком терминалов СЗС / СЗК	25
5.1.1. Импорт файла с белым списком терминалов	25
5.1.2. Редактирование Белого списка	26
5.1.3. Фильтр белого списка	27
5.2. Экспорт белого списка СЗС	27
5.3. Статусная модель	27
5.4. История подключений к СЗС	28
5.5. История подключений к СЗК	28

ИСТОРИЯ ИЗМЕНЕНИЙ

Версия документа	Дата изменения	Автор	Описание
3.00	05/06/2025	Шмидт В.В.	Ребрендинг документа на основе документа версии 2.00

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 криптографический 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 ТМК на RKI
ОЗУ	Память с произвольным доступом или оперативное запоминающее устройство
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

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ



ВНИМАНИЕ!
Очень важная информация!



ПРИМЕЧАНИЕ:
Полезная информация

RFU – Reserved for Future Use – функционал с такой пометкой не реализован на момент написания документации, но в интерфейсе зарезервирован.

ВВЕДЕНИЕ

Данный документ разработан Сомерс (ООО "Скайтех") и содержит описание процесса работы с системой SomersRKM – 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 IT инженерам 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 Сомерс.

1. ОБЩЕЕ ОПИСАНИЕ SOMERSRKM

SomersRKM – 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. Основное назначение системы SomersRKM – 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 SomersRKM устанавливаются в виде сервиса на специализированный сервер, установленный в PCI среде.

В состав SomersRKM входит:

- сервис SomersCA - Система подписи сертификатов (Сервер Загрузки Сертификатов, СЗС);
- сервис SomersRKI - 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) – поддерживается интеграция с несколькими моделями HSM, подробнее см. п. 1.3. Модели HSM;

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, посредством которого выполняется контроль попыток подключения таких устройств.

Работа с сервисами выполняется через web-интерфейс, который 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.

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

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

1.1. Пользователи

SomersRKM является многопользовательской системой, в которой реализовано несколько ролей пользователей с различным функционалом:

- **Администратор системы (admin)** – пользователь с данной ролью имеет доступ к функционалу управления SomersRKM, может задавать параметры для подключения к банковским хостам и резервным HSM, создавать пользователей, но администратор системы не имеет доступа к функционалу, который касается непосредственно криптографических ключей и их криптограмм;
- **Офицер безопасности (security officer)** – пользователь с данной ролью имеет доступ к просмотру, экспорту, импорту криптограмм криптографических ключей ТМК и ЗМК;
- **Оператор (operator)** – пользователь с данной ролью имеет доступ к функционалу ведения «белых» и «черных» списков серийных номеров целевых терминалов,

управляющих загрузкой ключей на конечные целевые устройства, а также имеет доступ к отчетам SomersRKM.

1.2. Порядок работы с комплексом SomersRKM



Различные этапы работы комплекса выполняются пользователями с соответствующим функционалом.

1.2.1. Предварительная подготовка компонент комплекса

Администратор системы:

1. Настройка количества офицеров безопасности в соответствии с требованиями безопасности (подробнее см. п. 3.2.1. Количество офицеров безопасности);
2. Ввод параметров SMTP для отправки сообщений для авторизации пользователей (подробнее см. п. 3.2.2. Настройка SMTP для отправки сообщений);
3. Создание пользователей с ролями Офицер безопасности и Оператор (подробнее см. п. 3.1.1. Создание нового пользователя);



При создании нового пользователя на указанный при регистрации адрес электронной почты отправляется ссылка для доступа и установки пароля. Эта ссылка действует 15 минут, после чего пользователь должен запросить повторную ссылку.

4. Добавление хоста банка (подробнее см. п. 3.4. Настройка параметров хоста);
5. Управление параметрами резервных HSM (опционально).

Офицер безопасности:

6. Генерация сертификата, которым будет выполняться подпись при авторизации терминалов (подробнее см. п. 4.1. Генерация сертификата); Настройка параметров ключей и схемы работы комплекса (подробнее см. п. 4.3.2. Настройки параметров ключей);



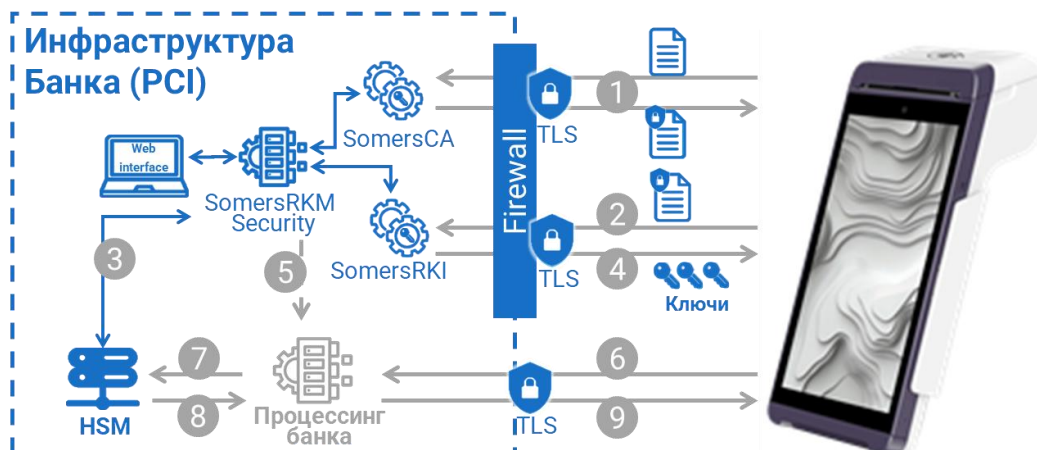
Для продукта SomersRKM_LK_01 на подготовительном этапе выполняется загрузка ZMK, подробнее см. п. 4.4. Настройки RKL, в настройках параметров ключей и хостов должны быть активированы необходимые настройки.

Оператор:

1. Загрузка на СЗС и СЗК белого списка терминалов – этот процесс может быть выполнен вручную, или при помощи файла (подробнее см. п. 5.1. Управление Белым списком СЗС / СЗК).

1.2.2. Загрузка ключей

После выполнения предварительных настроек SomersRKM, а так же после установки ПО и загрузки конфигурации на терминал в платёжном ПО выполняется операция Активации терминала – начинается взаимодействие POS-терминала с компонентами комплекса.



- (1) Инициализация POS терминала:
 - POS-терминал обращается к Сервису Загрузки Сертификатов (СЗС, SomersCA) по защищенному каналу связи и передает ему свой сертификат и серийный номер;
Для того, чтобы терминал смог инициализироваться на СЗС, он должен находиться в Белом списке терминалов и иметь соответствующий статус – Если серийный номер целевого терминала отсутствует в Белом списке, процедура прерывается с фиксацией в журнале УЗК обращения «неразрешённого» устройства.
 - СЗС проверяет наличие серийного номера в Белом списке и возвращает терминалу его сертификат, подписанный публичным ключом. Статус терминала в Белом списке обновляется.
- (2) Запрос ключей POS-терминалом: POS-терминал обращается к Сервису Загрузки Ключей (СЗК, SomersRKI), по защищенному каналу связи и передает сертификат, подписанный публичным ключом (полученный при процедуре инициализации), серийный номер и TID.
Для того, чтобы терминал смог запросить ключи на СЗК, он должен находиться в Белом списке терминалов и иметь соответствующий статус. Если серийный номер целевого терминала отсутствует в Белом списке, процедура прерывается с фиксацией в журнале УЗК обращения «неразрешённого» устройства.
- (3) Запрос ключей KLK на HSM: СЗК обращается к HSM и запрашивает криптограмму KLK целевого устройства под публичным ключом для TID, полученного в запросе.
- (4) Передача ключа KLK на Целевой терминал: СЗК возвращает криптограмму KLK под публичным ключом целевого устройства на целевой терминал.
- (5) Передача ключа KLK на хост: Набор данных из Криптограммы KLK, контрольной суммы KLK и TID целевого терминала передаются на процессинг банка – этот процесс может быть выполнен вручную (при помощи файла), или по API.
- (6) Запрос рабочих ключей с хоста: загрузка рабочих ключей с хоста выполняется в процессе активации целевого терминала или при выполнении команды «Загрузка ключей» - терминал обращается на банковский хост за рабочими ключами, в соответствии со спецификацией.
- (7,8) Получение рабочих ключей: процессинг банка находит криптограмму ключа и обращается к HSM с криптограммой KLK под ZMK для генерации рабочих ключей для целевого устройства.
- (9) Передача рабочих ключей с хоста: процессинг передаёт криптограммы рабочих ключей под KLK на целевое устройство, которое сохраняет рабочие ключи в безопасную память.

1.3. Модели HSM

SomersRKM может быть интегрирован со следующими моделями HSM:

- SomersHSM – проприетарный HSM на основе терминального оборудования, разработанный Сомерс – поддерживаются следующие команды API SomersHSM:
 - Генерация RSA ключа;
 - Подпись RSA ключа;
 - Шифрование RSA ключа;
 - 3DES шифрование;
 - Генерация 3DES ключей;
- Thales Luna EFT 2.0.0 Payment HSM;
- Thales PayShield;



SomersRKM может работать как с вариантными ключами, так и с ключами в формате Key Block, если HSM поддерживает такой формат.

- КриптоПРО версия 2.0.

Возможно настроить индивидуальные алгоритмы шифрования для различных моделей клиентских устройств, при условии их поддержки HSM.



SomersHSM (СЗК) должен иметь одинаковый локальный ключ LKM с используемым в процессинге HSM для гарантированной расшифровки ТМК.

2. РАБОТА С SOMERSRKM

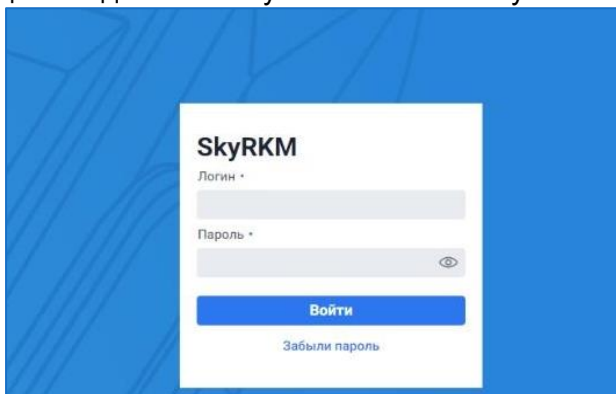
2.1. Вход в систему

Работа с SomersRKM 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 SomersRKM.



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.

2.2. Выбор языка интерфейса

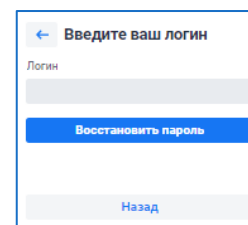
Интерфейс сервисов SomersRKM реализован на двух языках – русском и английском. Переключение языка интерфейса можно выполнить на странице ввода пароля и после авторизации в SomersRKM.



При переключении языка интерфейса из рабочей области убедитесь, что все внесенные изменения сохранены, т.к. несохраненные данные пропадут.

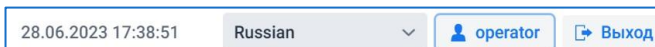
2.3. Восстановление пароля

Если пользователь забыл пароль в SomersRKM 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.



2.4. Выход из системы

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




2.5. Интерфейс SomersRKM

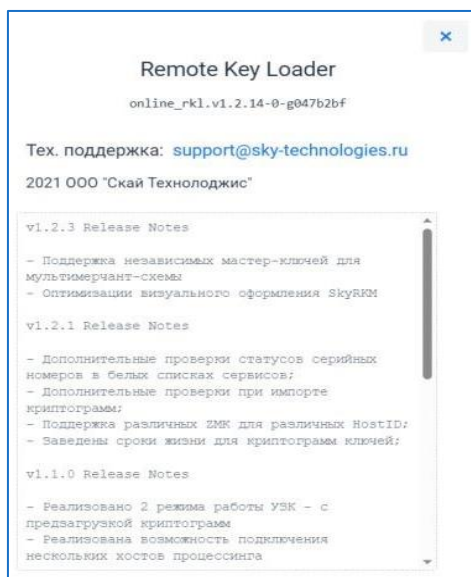
Экран сервисов системы SomersRKM разделен на две части:

- в левой части экрана расположено Главное меню, в котором отображаются функциональные разделы, доступные пользователю, работающему с сервисом:
 - Сервис загрузки сертификатов – раздел предназначен для управления и контроля процесса подписания сертификата целевых терминалов;
 - Сервис загрузки ключей – раздел предназначен для управления и контроля процесса загрузки ключей в целевые терминалы;
 - Настройки RKL – раздел предназначен для выполнения настроек процесса удаленной загрузки ключей;
 - Доступ – раздел предназначен для управления пользователями системы и выполнения аудита работы системы.
- в правой части экрана расположена рабочая область системы, состав которой зависит от выбранного функционала.

2.6. Версия приложения

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

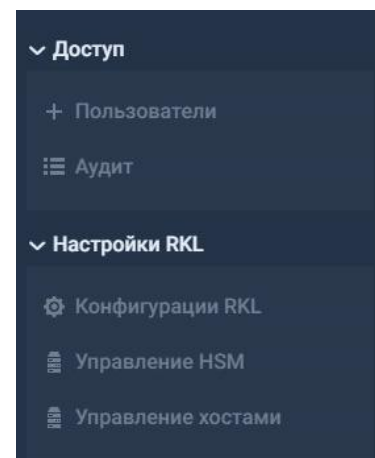
- номер текущей версии приложения;
- список обновленного функционала, вошедшего в текущую версию приложения, а также всю историю изменений приложения – номер версии и подробное описание нового функционала.



3. ФУНКЦИОНАЛ АДМИНИСТРАТОРА

При авторизации пользователя с ролью Администратор в Главном меню web интерфейса отображаются следующие функциональные разделы:

- Доступ – раздел позволяет управлять пользователями:
 - Пользователи – создание, удаление и редактирование, блокировка и разблокировка пользователей с различными ролями;
 - Аудит – журнал действий пользователей.
- Настройки RKL – раздел позволяет задать параметры для работы с RKL:
 - Конфигурация RKL – настройка параметров Удаленного загрузчика ключей;
 - Управление HSM – параметры резервных HSM;
 - Управление хостами – настройка Банковского хоста.



3.1. Управление пользователями

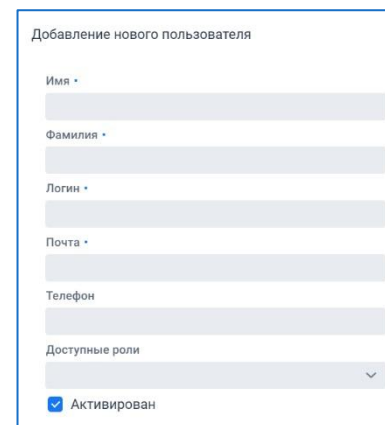
Управление пользователями выполняется из раздела «Доступ» - «Пользователи» – в разделе отображается список всех пользователей, зарегистрированных в системе RKM.

Создать	Удалить	Копировать				Фильтр
ID	Логин	Название	Роль	Почта	Телефон	Последнее посещение
1			Администратор			28.06.2023 16:58:54
21			Оператор			28.06.2023 16:56:06
22			Офицер безопасности			28.06.2023 16:47:39

3.1.1. 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 4 символов;
- Почта – адрес электронной почты – на этот адрес будет отправлено письмо для установки пароля пользователя, а так же письма 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 (RFU);
 - RKL integrational API (POST) – специализированная роль пользователя для работы по API;





Присвоение логина и пароля выполняется стандартным образом, затем параметры пользователя необходимо настроить в SomersMDM (в разделе Настройки MDM - Конфигурации MDM – Настройки внешнего УЗК).

- Администратор;
- Офицер безопасности;



Количество пользователей с ролью «Офицер безопасности» задается в разделе «Настройки RKL».

- Оператор;
- Активирован – если флаг установлен, пользователь может авторизоваться в системе.

После ввода всех параметров нажмите кнопку «Создать».

На указанный при создании пользователя адрес электронной почты будет отправлено письмо со ссылкой для установки пароля и подключения к SomersRKL.

Пользователь должен перейти по соответствующей ссылке «Сменить Пароль На RKL» - откроется страница входа в RKL, на которой необходимо ввести пароль и подтвердить его.



По умолчанию срок действия ссылки на установку пароля – 15 минут, после завершения этого периода необходимо запросить новую ссылку.

Введите новый пароль

Пароль

Подтвердите пароль

Восстановить пароль

3.1.2. 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.

3.1.3. Редактирование пользователя

Для того, чтобы отредактировать параметры пользователя нажмите дважды на пользователя – откроется окно редактирования данных пользователя.

Измените необходимые параметры:

- чтобы разблокировать пользователя, который ввел неправильный пароль, установите флаг «Активирован»;
- для принудительного изменения пароля пользователя введите Старый пароль пользователя, Новый пароль и подтвердите ввод нового пароля.

После внесения всех необходимых изменений нажмите кнопку «Сохранить».

NewUser NewUser (NewUser) ✕

<p>Имя <input style="width: 90%;" type="text" value="NewUser"/></p> <p>Фамилия <input style="width: 90%;" type="text" value="NewUser"/></p> <p>Логин <input style="width: 90%;" type="text" value="NewUser"/></p> <p>Почта <input style="width: 90%;" type="text" value="newuser@mail.ru"/></p> <p>Телефон <input style="width: 90%;" type="text" value=""/></p> <p>Доступные роли <input style="width: 90%;" type="text" value="Оператор"/></p> <p><input checked="" type="checkbox"/> Активирован</p>	<p>Старый пароль <input style="width: 90%;" type="password" value=""/></p> <p>Новый пароль <input style="width: 90%;" type="password" value=""/></p> <p>Подтвердите пароль <input style="width: 90%;" type="password" value=""/></p>
---	--

Сохранить

3.1.4. 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.

3.1.5. Аудит действий пользователя

Для того, чтобы просмотреть события и действия пользователей системы и прочие служебные данные, перейдите в раздел «Доступ» - «Аудит».

Аудит						17.08.2021 12:46:25	Russian		Выход
<div>Фильтр</div>									
	ID	IP	Дата	Действие	Описание	Клиент			
	admin (1)	172.16.19.11	Tue Aug 17 09:52:39 MSK 2021	Чтение аудита [Страница]	—	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)			

В разделе отображается:

- ID пользователя, выполнившего действие;
- IP, с которого пользователь подключился к системе;
- Дата события;
- Действие пользователя;
- Описание;
- Интернет-обозреватель, с которого выполнен вход пользователя.

3.2. Настройки RKL

3.2.1. Количество офицеров безопасности

При создании пользователей количество пользователей с ролью «Офицер безопасности», зарегистрированных в SomersRKM, ограничено значением, заданным в соответствующем параметре в разделе «Настройки RKL» - «Конфигурации RKL».

Количество офицеров безопасности
Введите количество офицеров безопасности
2

3.2.2. Настройка SMTP для отправки сообщений

Для того, чтобы задать параметры сервера исходящей почты RKL перейдите в раздел «Настройки RKL» - «Конфигурации RKL»:

- Хост;
- Порт;
- Адрес;
- Имя отправителя;
- Пароль;
- SSL.

Настройки SMTP	
Хост	Порт
emails.cwt.local	25
Адрес	
tms@payment-guide.ru	
Имя отправителя	
RKL-System	
Пароль	

<input type="checkbox"/> SSL	

3.2.3. Дополнительные схемы загрузки ключей

В SomersRKM реализованы дополнительные параметры работы:

- Использовать схему Variant LMK – активация использования HSM Thales в формате Variant LMK, т.е. с «голыми» ключами (по умолчанию SomersRKM работает с ключами в формате Key Block);
- Использовать схему привязки к tid – при активации данного функционала SomersRKM, получая от SomersMDM связку SN+TID, сохраняет TID в белый список терминалов (при работе с SomersPOS_OW_2).

Дополнительные настройки

☒ Использовать схему Variant LMK
 ☐ Использовать схему привязки к tid

3.3. Настройка резервных HSM

Раздел «Управление HSM» предназначен для создания резервных HSM.



Параметры основного HSM задаются в соответствующем параметре файла `ptconfig.properties`.

HSM	Адрес	Порт	
HSM1	127.0.0.1	1500	Обновить - x +
HSM2	172.16.21.182	8080	Обновить - x +
HSM3	123.123.123.123	1234	Обновить - x +

Чтобы задать параметры нового резервного HSM:

- Нажмите кнопку «+», расположенную в конце строки;
- Введите параметры HSM:
 - Адрес – адрес резервного HSM;
 - Порт – порт резервного HSM.
- Нажмите кнопку «Сохранить».

Для того, чтобы изменить параметры существующего HSM дважды кликните на его название.

Чтобы удалить или копировать существующий HSM используйте соответствующие кнопки, расположенные над таблицей.

При необходимости используйте фильтр.

Добавление нового резервного HSM

Адрес *

Порт *

Создать

3.4. Настройка параметров хоста

Раздел «Управление хостами» позволяет создавать, редактировать и удалять хост процессинга, в который следует передать криптограмму мастер-ключа терминала через REST API.

08.04.2025 12:55:53 Russian admin Выход									
Настройка хостов									
Host	Название хоста	Host ID	Host (ip)	Порт	Диалект	Имя пользова...	Пароль	ZMK сгенерир...	
Host1	Host1	Host1	127.0.0.2	1505	OpenWay Wa...				Обновить
Host2	tmp1	tmp1	123.123.123...	1234	OpenWay Wa...				Обновить

Нажмите кнопку «+», расположенную в конце любой строки.

В открывшемся окне задайте параметры хоста:

- Название хоста – произвольное название записи;
- Host ID – идентификатор хоста, который будет задаваться во всех параметрах;
- Диалект – выберите из выпадающего списка диалект хоста:

— SmartVista *;



При выборе значения SmartVista-AGPB становится доступен параметр «Адрес привязки ключа» - адрес API для привязки ключа, остальные параметры становятся недоступными.

— Compass+ *;

— Tieto;

— T-SYS;

— Cortex;

— TLV;

— CWT-PGW;

— UIC RSA TLV;

— OpenWay Way4;



При выборе значения OpenWay Way4 вместо параметра «пароль» становятся доступны параметры:

- Передавать под ZMK – активация функционала передачи криптограмм мастер-ключей, зашифрованных ключом ZMK (если флаг не установлен, криптограмма ключа передается под LMK);
- Передавать без длины ключа – при передаче ключа SomersRKL не передает первый символ - его длину.

Остальные параметры становятся недоступными.

- Host (ip) – IP адрес хоста, куда будет передаваться информация о загруженных в Целевые терминалы ключах (например, Way4);
- Порт – порт для подключения к хосту;
- Имя пользователя – введите имя пользователя для подключения к хосту;
- Пароль – введите пароль для подключения к хосту;

Для изменения параметров хоста нажмите кнопку «Обновить», расположенную в конце строки хоста, который необходимо изменить.

Для удаления хоста нажмите кнопку «X», расположенную в конце строки хоста, который необходимо удалить.

Добавление нового хоста

Название хоста *

Host ID *

Диалект *

Адрес привязки ключа *

Host (ip) *

Порт

Имя пользователя *

Пароль *

☐ Передавать под ZMK

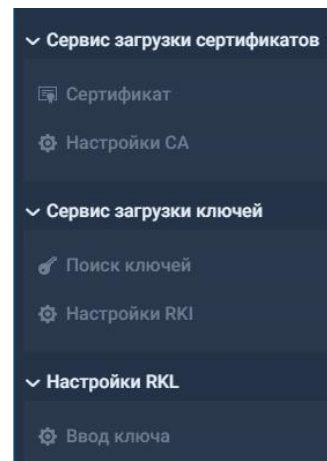
☐ Передавать без длины ключа

Создать

4. ФУНКЦИОНАЛ ОФИЦЕРА БЕЗОПАСНОСТИ

При авторизации пользователя с ролью Офицер безопасности в Главном меню web интерфейса отображаются следующие функциональные разделы:

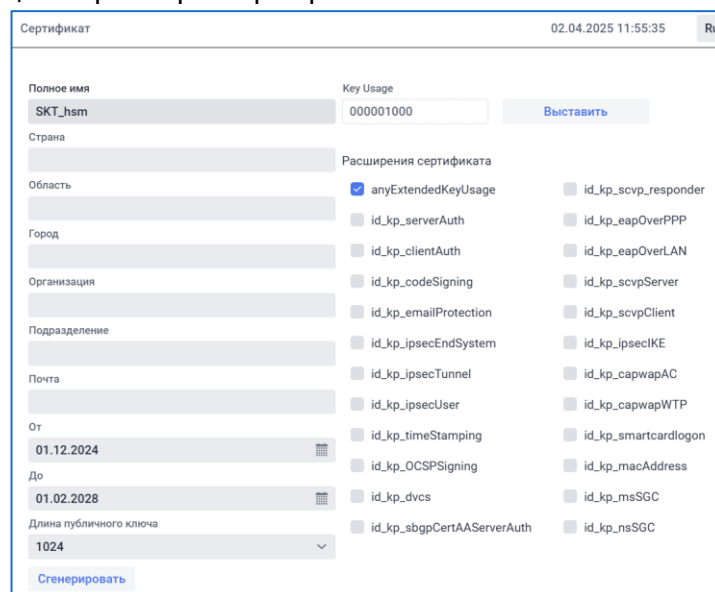
- Сервис загрузки сертификатов – раздел для работы с функционалом Сервиса загрузки сертификатов:
 - Сертификат – генерация сертификата, которым будут подписываться сертификаты Целевых терминалов, пришедших для авторизации
 - Настройки СА – ввод параметров сертификата СА;
- Сервис загрузки ключей – раздел для работы с функционалом Сервиса загрузки ключей:
 - Поиск ключей – функционал позволяет выполнить поиск ключей по TID и Серийному номер, остановить или перезапустить передачу информации о загруженных ключах на хост;
 - Импорт ключей – раздел для импорта ключей при активированной настройке «Предварительная генерация ТМК» (RFU);
 - Настройки RKL – в данном разделе задается срок жизни добавляемых ключей, настраивается проверка Host ID и передача данных о загруженных ключах на банковский хост;
- Настройки RKL – раздел для настройки RKL:
 - Ввод ключа – в данном разделе задается ZMK ключ (при работе с SomersRKM_LK_01).



4.1. Генерация сертификата

Процесс генерации сертификата для обмена данными с Целевым терминалом задается в разделе «Сертификат». Задайте следующие параметры сертификатов:

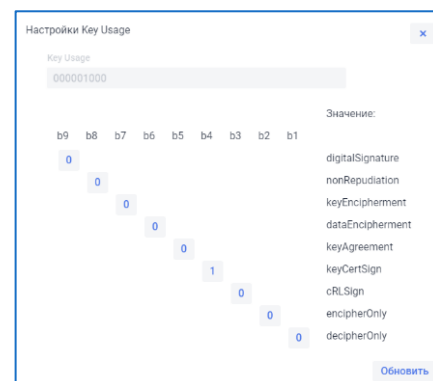
- Полное имя;
- Страна;
- Область;
- Город;
- Организация;
- Подразделение;
- Почта;
- От – срок начала действия сертификата;
- До – завершение действия сертификата;
- Длина публичного ключа – 1024 / 2048
- Key Usage – использование ключа – нажмите кнопку «Выставить значение» и в открывшемся окне установите «1» в соответствующих признаках и нажмите кнопку «Обновить»:



- digitalSignature;
- nonrepudiation;
- keyEncipherment;
- dataEncipherment;
- keyAgreement;
- keyCertSign;
- cRLSign;
- encipherOnly;
- decipherOnly.



Если сертификат будет использоваться для подписи, выберите значение keyCertSign.



- Расширения сертификата – отметьте расширения для сертификата.



Генерацию сертификата рекомендуется выполнить только один раз, чтобы все терминалы, которые будут выполнять авторизацию, а затем, загрузку ключей, использовали один и тот же сертификат! При возникновении такой ситуации, при попытке загрузки ключей, в журнале СЗК отобразится ошибка «Invalid certificate».

После заполнения параметров сертификата нажмите кнопку «Сгенерировать» - SomersRKM сгенерирует сертификат для авторизации терминалов.



При генерации сертификата убедитесь в доступности HSM, т.к сертификат генерируется с его использованием!

4.2. Настройки СА

Раздел «Настройка СА» позволяет внести дополнительные параметры сертификатов, необходимые для генерации сертификата СА.

Задайте параметры сертификата СА:



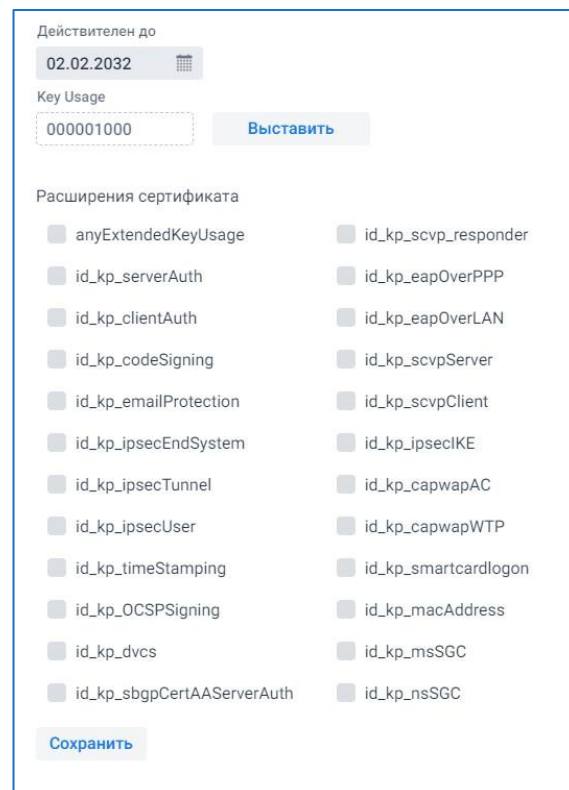
Как правило, в данном разделе рекомендуется указать параметры, аналогичные с параметрами, заданными в разделе «Сертификат».

- Действителен до – срок действия сертификата СА;
- Key Usage – для чего будет использоваться данный сертификат (Выставить);
- Расширения сертификата - отметьте необходимые расширения для сертификата:



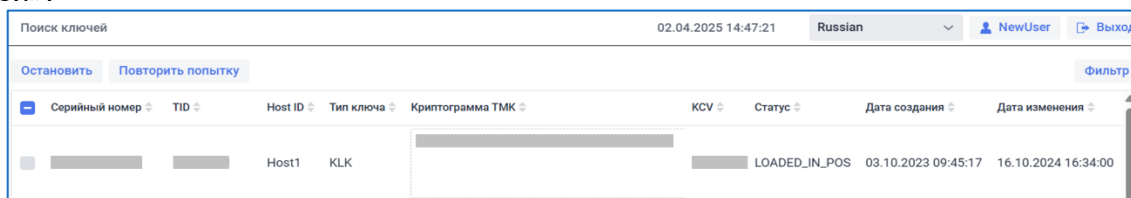
Как правило, в данном разделе рекомендуется указать расширения, аналогичные расширениям, заданным в разделе «Сертификат».

После ввода параметров нажмите кнопку «Сохранить» - внесенные параметры Сертификата СА будут сохранены.



4.3. Информация о загруженных ключах

Информация о загруженных в целевые терминалы ключах отображается в разделе «Поиск ключей».



Серийный номер	TID	Host ID	Тип ключа	Криптограмма ТМК	KCV	Статус	Дата создания	Дата изменения
		Host1	KLK			LOADED_IN_POS	03.10.2023 09:45:17	16.10.2024 16:34:00

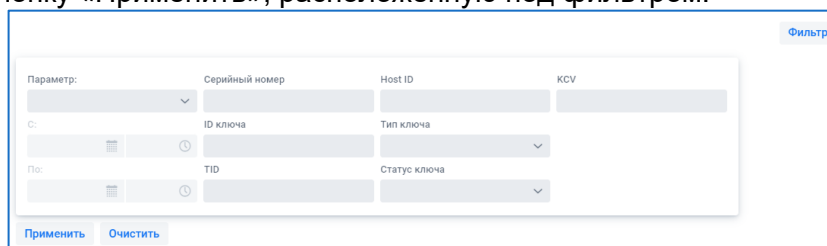
В таблице отображаются следующие параметры:

- Серийный номер – серийный номер терминала, в который загружен данный ключ;
- TID – идентификатор терминала на хосте;
- Host ID – идентификатор хоста;
- Тип ключа – тип загруженного ключа;
- Криптограмма ТМК – криптограмма загруженного ключа;
- KCV – контрольная сумма загруженного ключа;
- Статус – может принимать следующие значения:
 - LOADED_IN_POS – ключ загружен в целевой терминал;
 - LOADED_IN_TWO – информация о загруженном на целевой терминал ключе успешно отправлена на хост;
- Дата создания – дата создания записи в СЗК;
- Дата изменения – дата изменения записи в СЗК.

4.3.1. Поиск ключей

При необходимости выполните поиск ключей в списке, для этого используйте фильтр:

- нажмите кнопку «Фильтр», расположенную над таблицей слева;
- введите параметры для поиска терминала в белом списке;
- нажмите кнопку «Применить», расположенную под фильтром.



Для того, чтобы отменить фильтрацию данных в таблице, нажмите кнопку «Очистить». Чтобы свернуть отображение параметров нажмите кнопку «фильтр» еще раз.

4.3.2. Передача информации о ключах на хост

После того, как ключ загружается в Целевой терминал, он отображается в списке «Поиск ключей», его статус устанавливается в значение «Loaded in POS». Информация о загруженном ключе передается на хост для последующей авторизации терминалов.

В случае невозможности передачи этой информации попытки повторяются в фоновом режиме.



Периодичность отправки задается в соответствующем параметре в параметре Частота повторных уведомлений хоста (в минутах) в разделе «Настройки RKI».

В некоторых случаях может возникнуть необходимость прекратить передачу этой информации на хост, или запустить процесс. Для этого выделите ключ, передачу информации о котором необходимо остановить, и нажмите соответствующую функциональную кнопку, расположенную над таблицей:

- Остановить - остановить попытки передачи на хост информации о ключе;
- Повторить попытку – повторная попытка передачи информации о ключе на хост, если попытки передачи информации о загруженном ключе были остановлены вручную (кнопка «Остановить»).



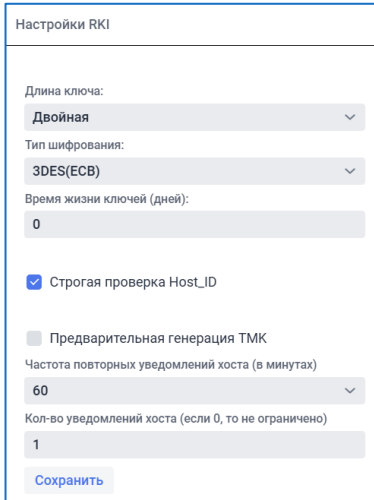
Как только информация о ключе успешно передана на хост, эти кнопки становятся недоступными.

4.4. Настройка параметров ключей

Для того, чтобы задать параметры ключей, загружаемых в целевые терминалы, перейдите в раздел «Настройки RKI».

В разделе задаются следующие параметры ключей:

- Длина ключа – выберите значение из выпадающего списка (значение должно соответствовать рекомендациям безопасности, используемому в Банке):
 - Двойная;
 - Тройная;
- Тип шифрования – выберите значение из выпадающего списка (значение должно соответствовать рекомендациям безопасности, используемому в Банке):
 - 3DES(ECB);
 - 3DES(CBC);
 - AES;
- Время жизни ключей (дней) – введите произвольное значение;
- Строгая проверка Host_ID – активация проверки наличия Host_ID в данных терминала, полученных от SomersMDM, а также передача информации о загруженных ключах на заданный банковский хост – если у терминала не указан HostID, отображается сообщение «host_id поле должно быть заполнено»;




Значение задается в соответствующем параметре Банковского терминала и должно совпадать с названием хоста, указанном в настройках параметров хостов .

- Предварительная генерация ТМК – активация схемы работы, в которой криптограммы ключей загружаются из файла (RFU);



Если флаг Предварительная генерация ТМК не установлен применяется алгоритм работы SomersRKL, при котором генерация ключа выполняется, когда терминал приходит за ключом на HSM.

- Частота повторных уведомлений хоста (в минутах) – периодичность отправки на хост информации о ключах, загруженных в целевые терминалы (в статусе Loaded in POS) – выберите значение из выпадающего списка (1/2/5/10/20/30/60);

- Кол-во уведомлений хоста (если 0, то не ограничено) – количество попыток отправки на хост информации о ключах, загруженных в целевые терминалы.



Процесс передачи SomersRKM на хост информации о ключах, загруженных в целевые терминалы, может занимать длительное время, или в процессе передачи могут возникнуть перебои со связью. В результате, может возникнуть необходимость приостановить процесс передачи этой информации на хост. Для этого в SomersRKM реализован соответствующий функционал, подробнее см. п. 4.3.1. Поиск ключей.

Нажмите кнопку «Сохранить» после изменения параметров.

4.5. Ввод ZMK (опционально)

Раздел предназначен для ввода криптограммы ключа ZMK (только для продукта SomersRKL_LK_01).

Ввод ZMK ключа может выполнить двумя способами:

- Вручную – ввод параметров ключа через интерфейс SomersRKM;
- При помощи файла – загрузка ключа в SomersRKM при помощи файла, сгенерированного Банком, подробнее см. п. 4.5.2. Загрузка ZMK при помощи файла.

4.5.1. Ручной ввод ключа ZMK

При работе с процессингом Way4 в SomersRKM необходимо выполнить ввод ZMK. Для этого перейдите в раздел «Настройки RKL» - «Ввод ключа».

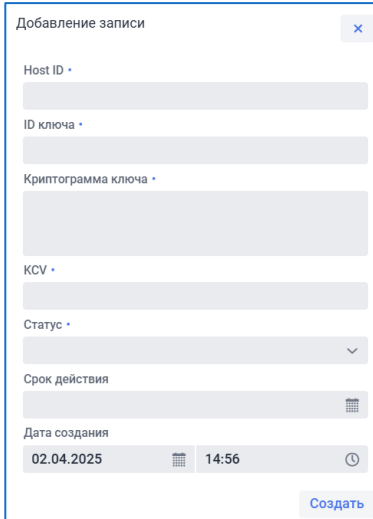
- – для этого нажмите кнопку «Создать» и задайте параметры ключа:



- Host ID - идентификатор хоста, уникальное значение в строковом формате, необходимо для аутентификации хоста

Значение должно совпадать с названием как минимум одного хоста, заведенного на странице "Управление хостами".

- ID ключа – идентификатор ключа;
- Криптограмма ключа – криптограмма ключа ZMK под LMK;
- KCV – контрольная сумма криптограммы;
- Статус – статус ключа, может принимать значения:
 - READY – ключ можно загружать в терминал;
 - COMPROMISED – ключ скомпрометирован;
- Срок действия – срок действия ключа;
- Дата создания – дата создания ключа.



4.5.2. Загрузка ZMK при помощи файла

В SomersRKM реализована поддержка загрузки ZMK при помощи xml файла.

Формат файла:

```
<KeySet xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Row>
  <HostId>YYY</HostId>
  <Id>100000003</Id>
```

```
<UnderLMK>U389C78C5F6D5A361A4A1A9E831B1401E</UnderLMK>  
<KeyCheck>2198B6</KeyCheck>  
<Date>20250115</Date>  
<Time>1347</Time>  
</Row>  
</KeySet>
```

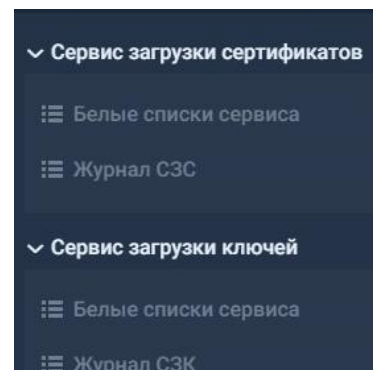
Где:

- HostId - наименование хоста, уникальное значение в строковом формате, необходимо для аутентификации хоста (должно совпадать с каким либо Хостом заведенным на странице "Управление хостами");
- Id - идентификатор ключа, числовое значение не длиннее Long;
- UnderLMK - криптограмма ZMK (под LMK);
- KeyCheck - KCV (key check value);
- Date - дата создания ключа;
- Time - время создания ключа.

5. ФУНКЦИОНАЛ ОПЕРАТОРА

При авторизации пользователя с ролью Оператора в Главном меню web интерфейса отображаются следующие функциональные разделы:

- Сервис загрузки сертификатов – раздел для работы с функционалом Сервиса загрузки сертификатов:
 - Белые списки сервиса – формирование белых / черных списков терминалов, которым разрешено / запрещено подключаться к СЗС для авторизации;
 - Журнал СЗС – контроль событий СЗС;
- Сервис загрузки ключей – раздел для работы с функционалом Сервиса загрузки ключей:
 - Белые списки сервиса – формирование белых / черных списков терминалов, в которые разрешено / запрещено загружать ключи;
 - Журнал СЗС – контроль событий СЗК.



5.1. Управление белым списком терминалов СЗС / СЗК

Интерфейс разделов «Белые списки сервиса» СЗС и СЗК идентичен, и отличается только отсутствием кнопки «Экспортировать» в СЗК.



По умолчанию в таблице разделов «Белые списки сервиса» СЗС и СЗК отображаются только серийные номера терминалов со статусом «NEW». Для того, чтобы просмотреть список полностью или отобразить какой-то определенный статус, воспользуйтесь фильтром.

Принцип работы с Белыми списками заключается в следующем:

1. Так как терминалы сначала выполняют авторизацию в СЗС они должны сначала быть внесены в белый список СЗС. Для массового внесения терминалов в белый список СЗС реализована возможность импорта списка терминалов из файла. При необходимости этот список можно отредактировать – внести в него новый терминал, удалить внесенный терминал, копировать запись или отредактировать ее.
2. После того, как терминалы, находящиеся в белом списке СЗС, выполнили авторизацию, выполняется экспорт белого списка терминалов СЗС для последующей загрузки в СЗК – формируется файл соответствующего формата.
3. После импорта на СЗК файла, полученного от СЗС, терминалы, находящиеся в белом списке СЗК могут прийти для загрузки ключей.

Управление белым списком терминалов выполняется в разделе «Сервис загрузки сертификатов» - «Белые списки сервиса» при помощи функциональных кнопок, расположенных над таблицей.

Белые списки сервиса				28.06.2023 17:53:37	Russian	operator	Выход
Создать				Удалить	Копировать	Импортировать	Экспортировать
				Фильтр			
ID	Host ID	Серийный номер	Статус	TID	IP	Срок действия	Дата создания
101			NEW			31.08.2024	26.04.2023 12:01:14

5.1.1. Импорт файла с белым списком терминалов

Для того, чтобы импортировать список терминалов нажмите кнопку «Импортировать» и загрузите файл белого списка необходимого формата:

- Файл белого списка для загрузки в СЗС представляет собой *.txt файл, содержащий произвольное количество строк следующего вида:

SN;HostID;TID

Где:

- SN – серийный номер терминала;
- HostID – идентификатор хоста;
- TID – идентификатор терминала.

Статус всех записей, импортированных из файла, устанавливается в значение «NEW».



Статус терминала автоматически изменится на «USED», после того, как терминал придет на СЗС и выполнит авторизацию.

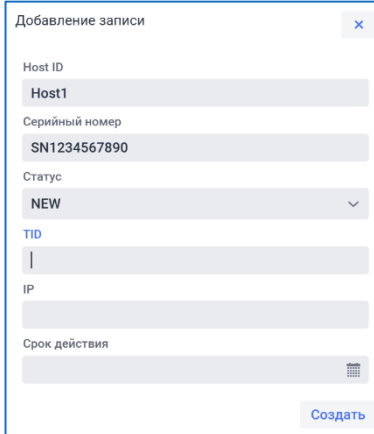
- Файл для загрузки в СЗК – это файл, экспортированный из СЗС, подробнее см. п. 5.2. Экспорт белого списка СЗС.

5.1.2. Редактирование Белого списка

Добавить терминал в список

Для того, чтобы добавить терминал в список терминалов, нажмите кнопку «Создать» – 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 (терминал находится в черном списке);
- TID – TMS ID терминала, заданный на SomersMDM;
- IP – адрес терминала;
- Срок действия – временной период, на протяжении которого терминалу можно обратиться за авторизацией.



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

Редактировать терминал

При необходимости, выберите терминал, заданный в списке, и измените его параметры – окно редактирования содержит те же параметры, что и окно создания новой записи.

Редактирование терминала может потребоваться, например, для того, чтобы выполнить повторную авторизацию / загрузку ключа – для этого переключите статус в «NEW».

Удалить терминал из 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.

Копировать терминал

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, измените другие данные терминала, и нажмите кнопку «Сохранить».

5.1.3. Фильтр белого списка

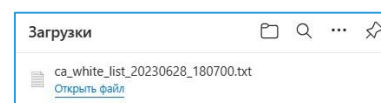
При необходимости данные терминалов, отображающиеся в Белом списке, можно отфильтровать по любому из доступных параметров.

5.2. Экспорт белого списка СЗС

После того, как Целевые терминалы авторизовались на СЗС, необходимо выполнить экспорт Белого списка терминалов, для последующей передачи этого списка в СЗК для загрузки ключей.

Для того, чтобы выполнить экспорт белого списка, нажмите кнопку «Экспорт», расположенную над таблицей.

Выполнится экспорт файла белого списка, в котором выгружаются строки следующего формата:



```
[SN];[Host];[TID];[Timestamp];[IP];
```

где:

- [SN] – серийный номер терминала;
- [Host] – идентификатор хоста;
- [TID] – идентификатор терминала на SomersMDM;
- [Timestamp] – дата создания записи (опциональный параметр);
- [IP] – IP адрес терминала (опциональный параметр).

Например:

```
SN12345678901;Host1;1234;1745960400000;123;  
SN1234567890;Host1;123;1745960400000;123;
```

Этот файл можно сразу импортировать в СЗК.

5.3. Статусная модель

Статусы на СЗС (при выгрузке):

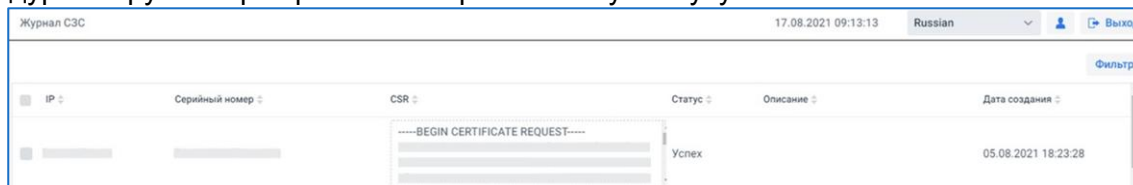
- NEW – выполнен импорт записи терминала (создана новая запись);
- USED – терминал обратился на СЗС и получил подпись сертификата;
- CANCELLED – терминал не может пройти процедуру авторизации (черный список).

Статусы на СЗК (при импорте):

- NEW – выполнен импорт записи терминала (создана новая запись);
- READY – SomersRKM получил от SomersMDM информацию о том, что на терминал загружена конфигурация и он готов к получению ключей - статус меняется автоматически по API;
- USED – терминал обратился на СЗК и получил ключ;
- CANCELLED – терминал не может пройти процедуру загрузки ключей (черный список).

5.4. История подключений к СЗС

История подключений к СЗС отображается в разделе «Журнал СЗС» – в таблице отображается список подключений к сервису авторизации и результат прохождения процедуры загрузки сертификатов по финальному статусу.



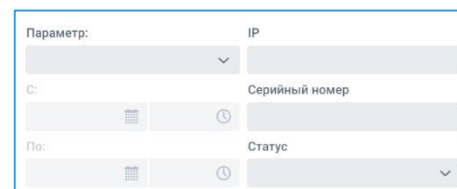
IP	Серийный номер	CSR	Статус	Описание	Дата создания
		-----BEGIN CERTIFICATE REQUEST-----	Успех		05.08.2021 18:23:28

В таблице отображаются следующие параметры:

- IP – адрес подключившегося терминала;
- Серийный номер – серийный номер подключившегося терминала;
- CRS – сертификат, загруженный в терминал;
- Статус – статус загрузки (успех / сбой);
- Описание – описание ошибки, в случае сбоя;
- Дата создания – дата и время добавления записи в таблицу (подключения терминала).

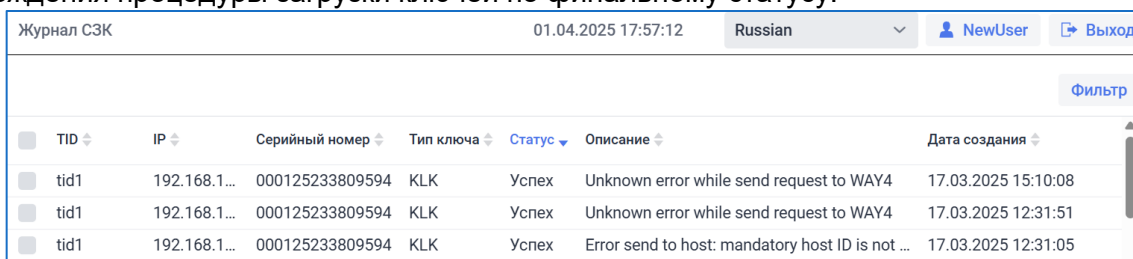
При необходимости данные в таблице можно отфильтровать в соответствии с заданными параметрами, нажав кнопку «Фильтр»:

- Параметр – выберите параметр из выпадающего списка и задайте его значение (дата создания);
- С – По – период создания записи;
- IP – адрес, с которого подключался целевой терминал;
- Серийный номер – серийный номер целевого терминала;
- Статус – статус загрузки сертификата.



5.5. История подключений к СЗК

История подключений к СЗК отображается в разделе «Журнал СЗС» – в разделе отображается список подключений к сервису загрузки ключей и анализ результатов прохождения процедуры загрузки ключей по финальному статусу.



TID	IP	Серийный номер	Тип ключа	Статус	Описание	Дата создания
tid1	192.168.1...	000125233809594	KLK	Успех	Unknown error while send request to WAY4	17.03.2025 15:10:08
tid1	192.168.1...	000125233809594	KLK	Успех	Unknown error while send request to WAY4	17.03.2025 12:31:51
tid1	192.168.1...	000125233809594	KLK	Успех	Error send to host: mandatory host ID is not ...	17.03.2025 12:31:05

В таблице отображаются следующие параметры:

- TID – идентификатор подключившегося терминала;
- IP – адрес подключившегося терминала;
- Серийный номер – серийный номер подключившегося терминала;
- Тип ключа – тип загруженного в подключившийся терминал ключа;
- Статус – статус загрузки (успех / сбой);
- Описание – описание ошибки;



В параметре «Описание» может отображаться сообщение об ошибке, даже если статус загрузки ключа «Успех» - такая ситуация может возникнуть, например, в том случае, если ключ был успешно загружен в терминал, но информация о ключе по каким-то причинам не была доставлена на хост.

Список сообщений в параметре «Описание» будет доступен в следующих версиях документа.

- Дата создания – дата и время добавления записи в таблицу (подключения терминала).