

KDH (Key Distribution Host)

Руководство пользователя

Версия 3.0.4

История изменений документа

Версия	Дата	Перечень изменений
1.0	22.11.2019	Первоначальная версия документа
1.1	17.02.2020	Добавлен пункт 4.4.4. Актуализирован пункт 4.4.1
1.2	14.07.2020	Изменение пункта 4.11.2

Содержание

1. Термины и определения	5
2. Введение	6
3. Краткое описание KDH	7
4. Работа с KDH через web-интерфейс.....	8
4.1. Описание web-интерфейс.....	8
4.2. Вход/ выход в (из) системы	8
4.3. Главная страница (KDH).....	9
4.4. Работа с пользователями (Users)	10
4.4.1. Добавление пользователя	11
4.4.2. Редактирование пользователя	12
4.4.3. Удаление пользователя	12
4.4.4. Первый вход пользователя	12
4.5. Роли пользователей (Users).....	13
4.5.1. Добавление роли.....	14
4.5.2. Редактирование роли	14
4.5.3. Удаление роли.....	15
4.6. Сертификаты (Certificates).....	16
4.6.1. Загрузка корневого сертификата «Root certificate»	17
4.6.2. Загрузка сертификата промежуточного УЦ «RKL certificate»	18
4.6.3. Сертификат KDH	19
4.6.4. Загрузка CRL листа «Certificates Revocation List»	21
4.7. Операции с ZMK (ZMK)	23
4.7.1. Статусы	24
4.7.2. Добавление ZMK.....	25
4.7.3. Формирование отчета	26
4.8. Операции с TMK (TMK)	27
4.8.1. Статусы	28
4.8.2. Загрузка списка мастер ключей (TMK)	29
4.8.3. Загрузка списка измененных статусов TMK.....	30
4.8.4. Формирование отчета	30
4.8.5. TWO и E-mail уведомления	31
4.9. Устройства (Devices)	33
4.9.1. Статусы	34
4.9.2. Загрузка списка S/N устройств (POS-терминалов).....	35
4.9.3. Загрузка файла с конфигурацией ключей.....	36
4.9.4. Формирование отчета	37
4.10. Хосты/ банки (References).....	38
4.10.1. Операции с хостами	38
4.10.2. Операции с банками	40
4.11. Настройки (Settings).....	42
4.11.1. Настройка остатка свободных ключей.....	42
4.11.2. Конфигурация TWO	43
4.11.3. Настройка срока действия ключей.....	44

4.11.4. Настройка HSM	45
4.12. Просмотр истории (History)	46
5. Порядок настройки стенда для работы с RKL.....	48
5.1. Подготовка компонент к работе с RKL.....	48
5.1.1. Подготовка UCM	48
5.1.2. Подготовка POS-терминала	48
5.1.3. Генерация ZMK	48
5.1.4. Подготовка KDH	49
5.2. Подготовка и загрузка конфигурации.....	49
5.2.1. Подготовка конфигурации в UCM	49
5.2.2. Загрузка конфигурации в POS-терминал	49
5.2.3. Загрузка конфигурации в KDH	49
5.3. Загрузка ТМК.....	49
5.3.1. Загрузка ключей в POS-терминал.....	49
6. Приложения	50

1. Термины и определения

УЦ	Удостоверяющий центр.
CRL	(Certificate Revocation List) – список отозванных сертификатов, заверенный цифровой подписью УЦ, выпускающего данные сертификаты.
FIID	Уникальный идентификатор Банка внутри МК. Используется для привязки POS-терминалов.
Host	Уникальный идентификатор хоста внутри МК. Используется для привязки ТМК.
HSM	Аппаратный модуль безопасности, который генерирует наборы секретных криптографических ключей для последующей загрузки в целевое устройство.
KDH	(Keys Distribution Host) – сервер загрузки ключей.
LMK	(Local Master Keys) - локальный мастер-ключ, который представляет собой ключ верхнего уровня, вводится в HSM и хранится в устройстве.
POS-терминал	электронное программно-техническое устройство, используемое для авторизации и проведения платежей по банковской карте.
Stunnel	SSL сервер
Single Merchant	Мерчант, у которого для каждого POS используется отдельный Terminal ID.
Multi Merchant	Мерчант, у которого для одного POS используется несколько Terminal ID.
ТМК	(Terminal Master Key) - мастер-ключ терминала, под которым проводится обмен рабочими ключами.
TWO	Хост МК (вендору Compass+)
ZMK	(Zone Master Key) - ключ TDES, которым шифруются все ключи данных, используемые для обмена информацией между двумя субъектами. ZMK используется для передачи ТМК на KDH.
UCM	Система параметризации POS-терминалов Unipos Config Manager.

2. Введение

Данный документ описывает web-интерфейс сервера удаленной загрузки ключей KDH и порядок работы с ним.

Данный документ предназначен для прочтения пользователем, осуществляющим работу с KDH через web-интерфейс.

Данный документ не содержит информацию по установке, настройке и запуску сервера KDH, а также требований к аппаратному и программному обеспечению, эти данные представлены в руководстве по установке KDH (KDH_Setup_Guide.pdf).

3. Краткое описание KDH

KDH является программным продуктом, представляющим из себя сервер удаленной загрузки симметричных ключей в POS – терминалы.

Основные функции системы KDH:

- Безопасное хранение криптограмм ТМК ключей для дальнейшей передачи POS-терминалу по запросу;
- Прием и обработка запросов от POS-терминалов на загрузку ТМК ключей;
- Безопасная передача ТМК ключей зарегистрированным в системе POS-терминалам;
- Отслеживание достаточного количества ТМК ключей в БД, в случае недостаточного количества формирование заявки на выпуск ключей и отправка уведомления по email;
- Отслеживание срока действия ключей.

Взаимодействие пользователя с KDH осуществляется через web-интерфейс данного сервера.

4. Работа с KDH через web-интерфейс

4.1. Описание web-интерфейс

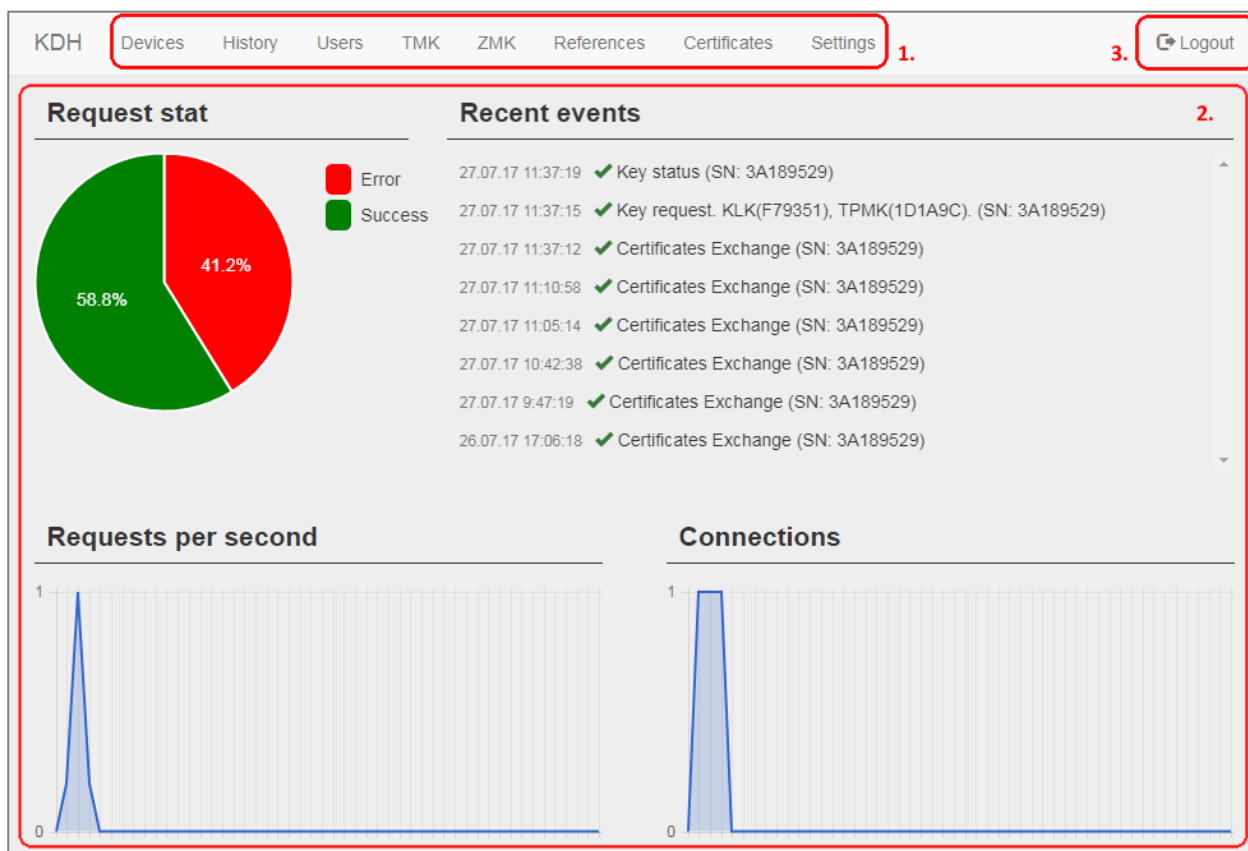


Рисунок 1. Главная страница системы KDH

Web-интерфейс системы KDH представляет собой страницу, содержащую следующие элементы:

1. Главное меню, состоит из следующих разделов: «**Devices**», «**History**», «**Users**», «**TMK**», «**ZMK**», «**References**», «**Certificates**», «**Settings**»;
2. Основное содержание раздела;
3. Кнопка выхода из личного кабинета пользователя.

4.2. Вход/ выход в (из) системы

Вход в систему выполняется после авторизации пользователя путем ввода логина/пароля на странице авторизации пользователя (Рисунок 2. Страница авторизации пользователя).

The screenshot shows a login form titled 'Please sign in'. It contains two input fields: the first for the username, which has 'admin' entered, and the second for the password, which has masked characters '.....'. Below these fields is a blue 'Sign in' button.

Рисунок 2. Страница авторизации пользователя

При первом запуске сервера авторизация может быть выполнена под пользователем с правами роли «**Administrator**», созданным системой по умолчанию со следующими данными:

- **Login** (логин): **admin**;
- **Password** (пароль): **admin**.

При успешной авторизации, открывается доступ к web-интерфейсу сервера KDH.

Доступность пунктов главного меню, выполняемых операций и отображаемых данных, описанных в данном разделе, определяется ролью пользователя, под которым была выполнена авторизация.

Выход пользователя осуществляется по нажатию кнопки .

4.3. Главная страница (KDH)

Данный раздел содержит информацию по взаимодействию сервера KDH с POS-терминалами (Рисунок 1. Главная страница системы KDH). Информация динамически обновляется по мере обращений POS-терминалов на KDH.

Переход в раздел осуществляется автоматически после авторизации пользователя или по нажатию на KDH в верхнем левом углу страницы.

Информация разбита по 4 секциям:

Request stat

Содержит информацию о результатах запросов POS-терминалов на сервер KDH, представленную в графическом виде (Рисунок 3. Request stat).

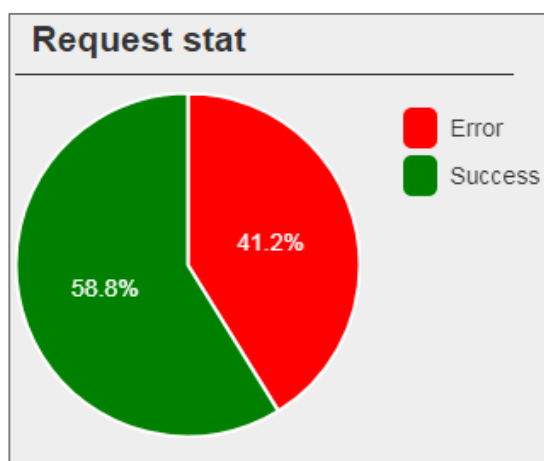


Рисунок 3. Request stat

Recent events

Содержит информацию о последних событиях в системе KDH (Рисунок 4. Recent events).

Recent events	
27.07.17 11:37:19	✓ Key status (SN: 3A189529)
27.07.17 11:37:15	✓ Key request. KLK(F79351), TPMK(1D1A9C). (SN: 3A189529)
27.07.17 11:37:12	✓ Certificates Exchange (SN: 3A189529)
27.07.17 11:10:58	✓ Certificates Exchange (SN: 3A189529)
27.07.17 11:05:14	✓ Certificates Exchange (SN: 3A189529)
27.07.17 10:42:38	✓ Certificates Exchange (SN: 3A189529)
27.07.17 9:47:19	✓ Certificates Exchange (SN: 3A189529)
26.07.17 17:06:18	✓ Certificates Exchange (SN: 3A189529)

Рисунок 4. Recent events

Requests per second

Содержит информацию о количестве запросов от POS-терминалов на сервер KDH в секунду, представленную в графическом виде (Рисунок 5. Requests per second).

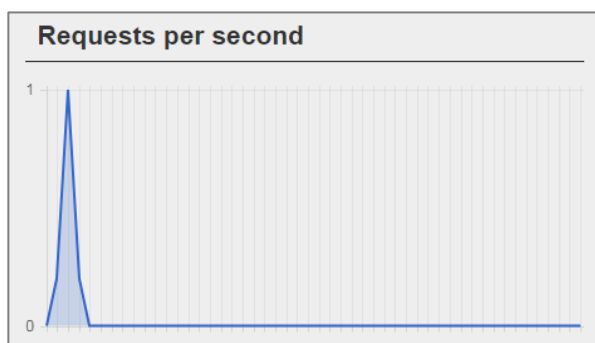


Рисунок 5. Requests per second

Connections

Содержит информацию о количестве соединений с POS-терминалами в секунду, представленную в графическом виде (Рисунок 6. Connection).

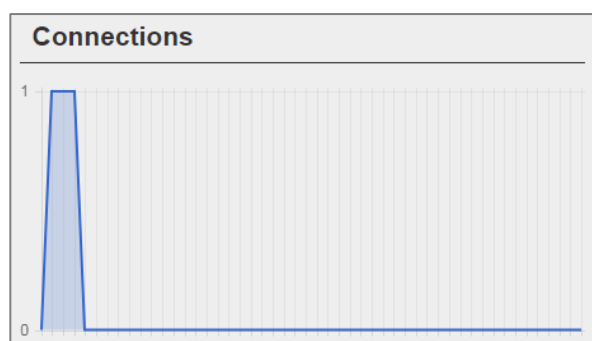


Рисунок 6. Connection

4.4. Работа с пользователями (Users)

Данный раздел содержит информацию и инструменты для работы с пользователями (Рисунок 7. Раздел "Users").

Переход в раздел осуществляется по выбору пункта «**Users**» в главном меню.

The screenshot shows the 'Users' management interface. At the top, there is a navigation bar with 'KDH', 'Users', 'References', 'Certificates', and 'Settings'. A 'Logout' button is in the top right. Below the navigation bar, there are tabs for 'Users' and 'Roles'. The 'Users' tab is active, showing a table with one user: 'Admin Admin [Administrator]'. To the right of the table is a form for creating a new user with fields for Login, Email, Name, Surname, Password, and Role. A 'Create' button is at the bottom left of the form area. A note at the bottom of the form states: 'Fields marked with an asterisk (*) are required.'

Рисунок 7. Раздел "Users"

Данный раздел представлен двумя вкладками:

- **Users** - данная вкладка содержит информацию и инструменты для работы с пользователями.
- **Roles** - данная вкладка содержит информацию и инструменты для работы с ролями пользователей.

4.4.1. Добавление пользователя

Для добавления нового пользователя необходимо выполнить следующие шаги (Рисунок 8. Раздел "Users", вкладка "Users"):

1. В разделе «Users» на вкладке «Users» нажать на кнопку «Create». Система создаст нового пользователя с пустыми полями.
2. Выполнить ввод данных в следующие поля:
 - **Login** – логин для авторизации пользователя.
 - **Email** – адрес электронной почты пользователя.
 - **Name** – имя пользователя.
 - **Surname** – фамилия пользователя.
 - **Password** – пароль для авторизации пользователя. Обязательные условия при создании пароля:
 - минимальная длина пароля – 8 символов;
 - пароль должен содержать буквы, цифры и специальные символы;
 - запрет создания пароля, который (-ые) был установлен для пользователя, в течении года (12 месяцев) до этого.
 - **Role** – роль пользователя. Выбирается из раскрывающегося списка.
3. Нажать кнопку «Save» для добавления нового пользователя или «Cancel» для отмены.

Рисунок 8. Раздел "Users", вкладка "Users"

Максимальный срок действия паролей пользователей и администраторов – 90 дней.

После пяти не успешных попыток входа в систему учетная запись пользователя – блокируется.

При нажатии кнопки «**Save**», система выдаст сообщение о результате «**Changes saved successfully**» – в случае успеха (Рисунок 9. Сообщение об успешном результате) или сообщение с описанием ошибки – в случае ошибки (Рисунок 10. Сообщение об ошибке).

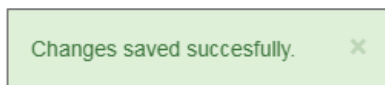


Рисунок 9. Сообщение об успешном результате

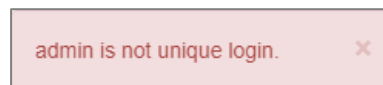


Рисунок 10. Сообщение об ошибке

4.4.2. Редактирование пользователя

Для редактирования пользователя необходимо выполнить следующие шаги:

1. В разделе «**Users**» на вкладке «**Users**» нажать на имени пользователя;
2. Внести необходимые изменения. После внесения изменений станут доступны кнопки «**Save**» и «**Cancel**».
3. Нажать кнопку «**Save**» для сохранения внесенных изменений или «**Cancel**» для отмены сделанных изменений. Нажать кнопку «**Save**» для добавления нового пользователя или «**Cancel**» для отмены.
4. При нажатии кнопки «**Save**», система выдаст сообщение о результате «**Changes saved successfully**» – в случае успеха (Рисунок 9. Сообщение об успешном результате) или сообщение с описанием ошибки – в случае ошибки (Рисунок 10. Сообщение об ошибке).

4.4.3. Удаление пользователя

Для удаления пользователя необходимо выполнить следующие шаги:

1. В разделе «**Users**» на вкладке «**Users**» нажать на иконку  рядом с именем, пользователя которого необходимо удалить.
2. Система запросит подтверждение на удаление (Рисунок 11. Запрос подтверждения на удаление пользователя).

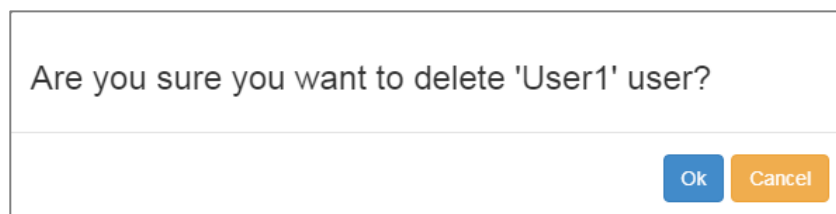


Рисунок 11. Запрос подтверждения на удаление пользователя

3. Нажать кнопку «**Ok**» для подтверждения удаления или «**Cancel**» для отмены.

4.4.4. Первый вход пользователя

При первом входе пользователя, после регистрации администратором, система «**KDH**» запросит сменить пароль, установленный администратором, на новый.

В отобразившемся окне «**Change user password**» нужно заполнить следующие поля и нажать кнопку «**Save**» (Рисунок 12. Окно изменения пароля при первом входе пользователя):

- **Current login:** - в данном поле указан логин изменяемого пользователя. Поле не доступно для редактирования;
- **Current password:** - в данное поле вводится текущий пароль пользователя (заданный администратором при создании пользователя);
- **New password:** - в данное поле вводится новый пароль. Обязательные условия при создании пароля:
 - минимальная длина пароля – 8 символов;
 - пароль должен содержать буквы, цифры и специальные символы;
 - запрет создания пароля, который (-ые) был установлен для пользователя, в течении года (12 месяцев) до этого.

- **Confirm password:** - в данное поле вводится идентичный пароль, введенному в поле «**New password:**», для подтверждения корректности ввода пароля.

После сохранения изменений система отобразит информационное сообщение «**New password saved successfully.**» и перейдет к странице авторизации (Рисунок 2. Страница авторизации пользователя).

Рисунок 12. Окно изменения пароля при первом входе пользователя

4.5. Роли пользователей (Users)

По умолчанию, на вкладке «**Roles**» представлены 3 роли пользователей с разными правами доступа:

- **Administrator** - имеет полномочия управления ролями и учетными записями пользователей;
- **TNM operator** - имеет полномочия, характерные при управлении терминальной сетью;
- **RCM operator** - имеет полномочия, характерные при управлении рисками, связанными с безопасностью.

KDH позволяет создавать/удалять/редактировать учетные записи пользователей, привязывая пользователя к той или иной роли.

В таблице ниже представлены операции, доступные для каждой роли пользователей по умолчанию.

Операции \ Роль	Administrator	TNM operator	RCM operator
Can load TMK	-	V	-
Can load ZMK	-	V	-
Can set TMK expire date	-	-	V
Can set ZMK expire date	-	-	V
Can load serial numbers	-	V	-
Can set "Compromised" TMK status	-	V	V
Can set "Compromised" ZMK status	-	V	V
Can set "DELETE", "NEW" as serial numbers status	-	V	-
Can load "DELETE" serial numbers	-	V	-
Can load compromised TMK	-	V	V
Can view keys	-	V	V
Can view devices page	-	V	V
Can generate serial numbers reports	-	V	V
Can generate TMK reports	-	V	V

Операции \ Роль	Administrator	TNM operator	RCM operator
Can edit users	V	-	-
Can edit roles	V	-	-

(-) операция недоступна для данной роли пользователя.

(V) операция доступна для данной роли пользователя.

4.5.1. Добавление роли

Для добавления новой роли пользователя необходимо выполнить следующие шаги (Рисунок 13.

Раздел "Users", вкладка "Roles"):

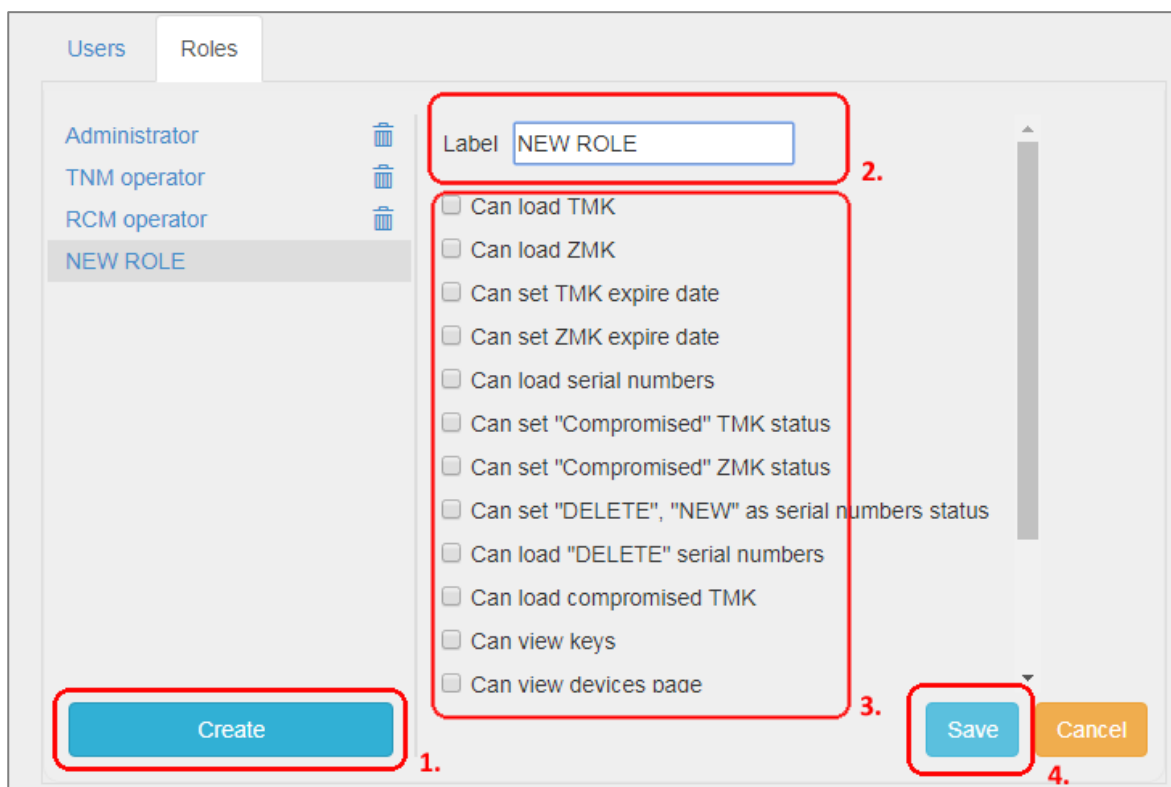


Рисунок 13. Раздел "Users", вкладка "Roles"

1. В разделе «**Users**» на вкладке «**Roles**» нажать на кнопку «**Create**». Система создаст новую роль на вкладке «**Roles**».
2. В поле «**Label**» ввести наименование роли.
3. Отметить флажком доступные операции для данной роли пользователей.
4. Нажать кнопку «**Save**» для сохранения новой роли пользователей с внесенными изменениями или «**Cancel**» для отмены создания. При нажатии кнопки «**Save**», система выдаст сообщение о результате «**Changes saved successfully**» – в случае успеха (Рисунок 9. Сообщение об успешном результате) или сообщение с описанием ошибки – в случае ошибки (Рисунок 10. Сообщение об ошибке).

4.5.2. Редактирование роли

Для редактирования роли пользователя необходимо выполнить следующие шаги:

1. В разделе «**Users**» на вкладке «**Roles**» нажать на наименование роли для внесения изменений;
2. Внести необходимые изменения:
 - a. изменить наименование роли «**Label**»;
 - b. отредактировать перечень доступных операций.

- После внесения изменений станут доступны кнопки «**Save**» и «**Cancel**». Нажать кнопку «**Save**» для сохранения внесенных изменений или «**Cancel**» для отмены сделанных изменений. При нажатии кнопки «**Save**», система выдаст сообщение о результате: «**Changes saved successfully**» – в случае успеха (Рисунок 9. Сообщение об успешном результате) или сообщение с описанием ошибки – в случае ошибки (Рисунок 10. Сообщение об ошибке).

4.5.3. Удаление роли

Для удаления роли пользователя необходимо выполнить следующие шаги:

- В разделе «**Users**» на вкладке «**Roles**» нажать на иконку  рядом с наименованием роли которую необходимо удалить.
- Система запросит подтверждение на удаление (Рисунок 14. Запрос подтверждения на удаление роли пользователя).

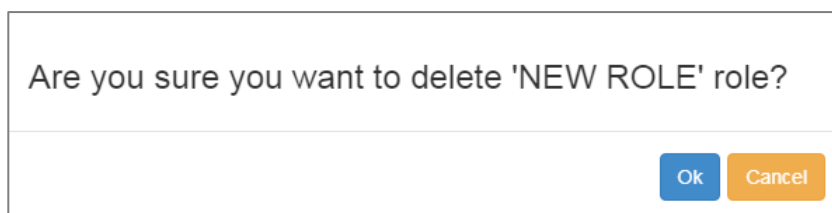


Рисунок 14. Запрос подтверждения на удаление роли пользователя

- Нажать кнопку «**Ok**» для подтверждения удаления или «**Cancel**» для отмены.

4.6. Сертификаты (Certificates)

Данный раздел содержит информацию и инструменты для работы с сертификатами (Рисунок 15. Раздел "Certificates"). За выпуском данных сертификатов необходимо обратиться в «**Удостоверяющий Центр ИНПАС**», предварительно выполнив генерацию запроса на сертификат KDH (см. п. [4.6.3.1 Генерация запроса на сертификат KDH](#)).

Переход в раздел осуществляется по выбору пункта «**Certificates**» в главном меню.

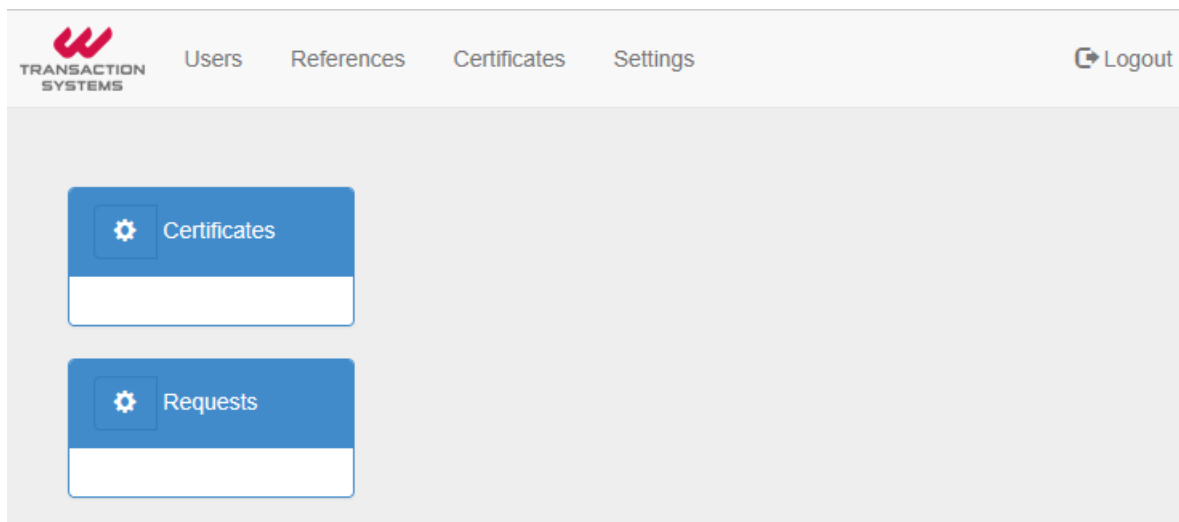


Рисунок 15. Раздел "Certificates"

Информация по сертификатам разбита на 2 секции:

- **Certificate** - в данной секции предоставлена возможность воспользоваться следующими инструментами:
 - **Import Certificate** – позволяет импортировать сертификат корневого УЦ, сертификат RLK (промежуточный УЦ, являющийся издателем сертификата KDH, сертификат RKL заверен корневым УЦ) и сертификат KDH;
 - **Export Certificate** – позволяет экспортировать сертификат корневого УЦ, сертификат RLK (промежуточный УЦ, являющийся издателем сертификата KDH, сертификат RKL заверен корневым УЦ) и сертификат KDH;
 - **Import CRL** - позволяет импортировать CRL-листы, издаваемым корневым УЦ;
 - **Export CRL** - позволяет экспортировать CRL-листы, издаваемым корневым УЦ;
 - **Delete Certificate** – позволяет удалить сертификат корневого УЦ, сертификат RLK (промежуточный УЦ, являющийся издателем сертификата KDH, сертификат RKL заверен корневым УЦ) и сертификат KDH.
- **Request** - в данной секции представлена возможность воспользоваться следующими инструментами:
 - **Regenerate RSA key pair** – выполняется повторная генерация ключевой пары;
 - **Generate** – выполняется генерация запроса на получение сертификата KDH;
 - **Export** – выполняется экспорт запроса на получение сертификата KDH;
 - **Delete** – выполняется удаление запроса на получение сертификата KDH.

Внимание: необходимо соблюдать следующую последовательность загрузки сертификатов:

1. **Root certificate** (корневой сертификат);
2. **Certificates Revocation List** (список отозванных сертификатов);
3. **RKL certificate** (сертификат промежуточного УЦ);
4. **KDH certificate** (сертификат KDH).

При загрузке сертификатов KDH выполняет проверку сертификата, в случае нарушения данной последовательности загрузки, сертификат может не пройти проверку, тогда система выдаст сообщение об ошибке «**KDH certificate doesn't correspond to existing CA certificate**».

4.6.1. Загрузка корневого сертификата «Root certificate»

Сертификат должен быть стандарта «X.509» и представлен в формате «PEM». Для загрузки корневого сертификата необходимо выполнить следующие шаги:

1. Нажать на  в секции «Certificate» и выбрать пункт «Import Certificate».
2. В открывшемся окне «Load» вставить данные сертификата, полученные от УЦ ИНПАС, в текстовую область (Рисунок 16. Окно загрузки корневого сертификата).

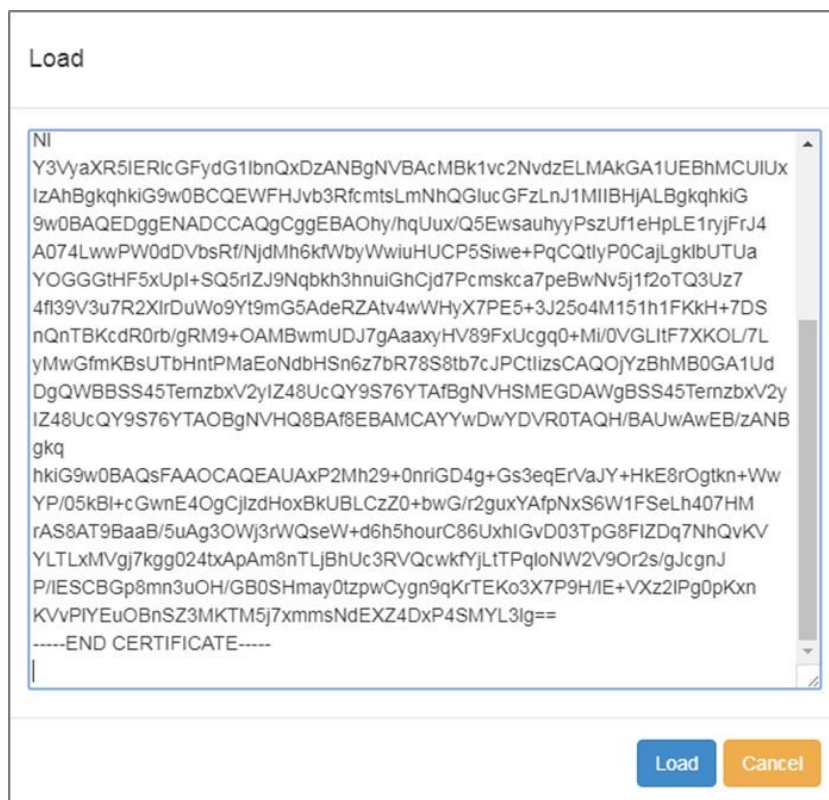


Рисунок 16. Окно загрузки корневого сертификата

3. Нажать кнопку «Load» для загрузки корневого сертификата.

После нажатия кнопки «Load» будет выполнена загрузка сертификата. В секции «Certificate» будет отображаться загруженный сертификат (Рисунок 17. Раздел "Certificates" секция "Certificate"). Для отображения информации о сертификате нужно кликнуть по нему левой кнопкой мыши.

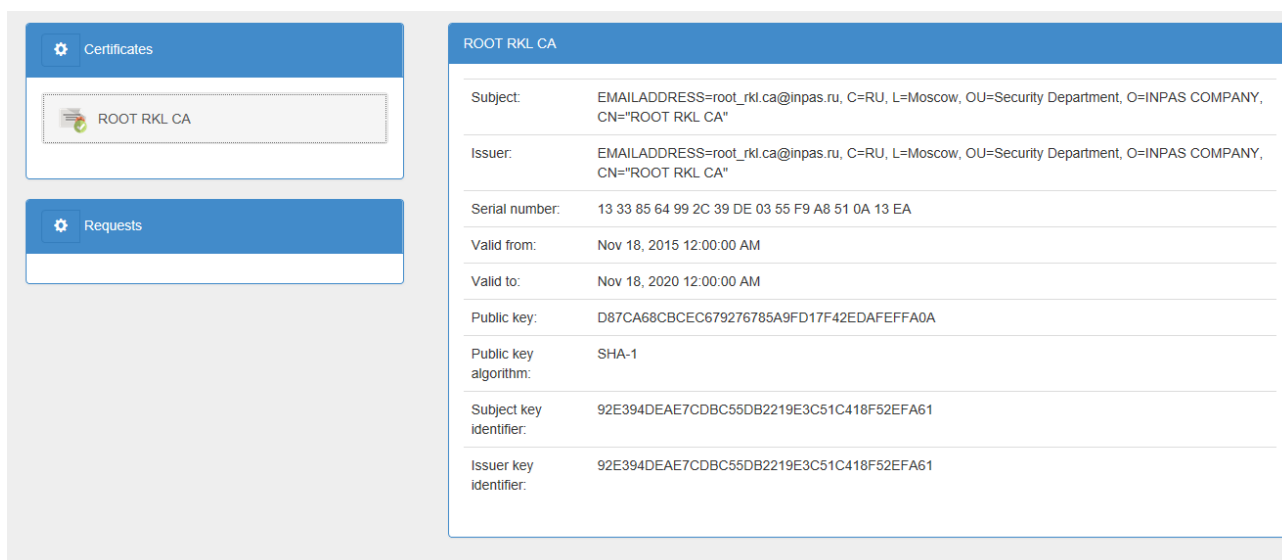


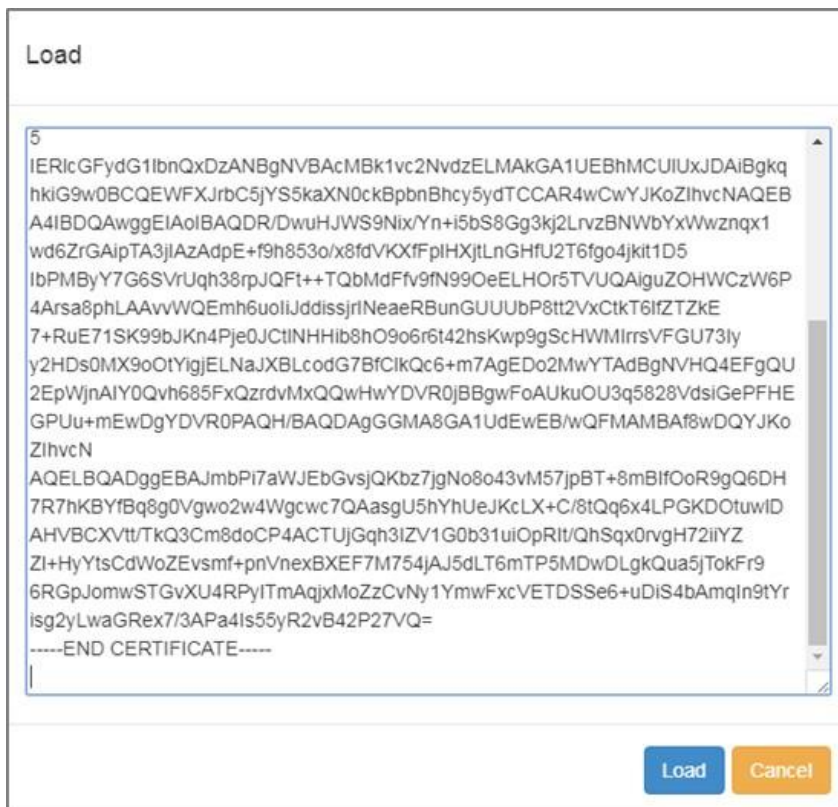
Рисунок 17. Раздел "Certificates" секция "Certificate"

4.6.2. Загрузка сертификата промежуточного УЦ «RKL certificate»

Сертификат должен быть стандарта «X.509» и представлен в формате «PEM».

Для загрузки сертификата промежуточного УЦ RKL необходимо выполнить следующие шаги:

1. Нажать на  в секции «Certificate» и выбрать пункт «Import Certificate».
2. В открывшемся окне «Load» вставить данные сертификата, полученные от УЦ ИНПАС, в текстовую область (Рисунок 18. Окно загрузки промежуточного сертификата RKL).



Load

```

5
IERlcGFydG1lbnQxZDZANBgNVBACMBk1vc2NvdzELMAKGA1UEBhMCUUIxJDAiBgkq
hkiG9w0BCQEWFXJrbC5jYS5kaXN0ckBpbmBhcy5ydTCCAR4wCwYJKoZIhvcNAQEB
A4IBDQAwggEIAoIBAQRD/DwuHJWS9Nix/Yn+i5bS8Gg3kj2LrvzBNWbYxWwznqx1
wd6ZrGAipTA3jIAzAdpE+f9h853o/x8fdVKXfFpIHxJtLnGHfU2T6fgo4jkit1D5
IbPMBYy7G6SVrUqh38rpJQFt++TQbMdFfv9fN99OeELHOr5TVUQAiguZOHWCzW6P
4Arsa8phLAavvWQEmh6uoljddissjrlNeaeRBunGUUUbP8tt2VxCtkT6fZTZKE
7+RuE71SK99bJKn4Pje0JCTlNHhIB8hO9o6r6t42hsKwp9gScHWMlrrsVFGU73Iy
y2HDS0MX9oOYigjELNaJXBLcodG7BfCikQc6+m7AgEDo2MwYTAdbgNVHQ4EFgQU
2EpWjnAIY0Qvh685FvQzrdvMxQQwHwYDVR0JBBgwFoAUkuOU3q5828VdsiGePFHE
GPUu+mEwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wDQYJKo
ZIhvcN
AQELBQADggEBAJmbPI7aWJEbGvsjQKbz7jgNo8o43vM57jpBT+8mBlfOoR9gQ6DH
7R7hKBYfBq8g0Vgwo2w4Wgcwc7QAasgU5hYhUeJKcLX+C/8tQq6x4LPGKDOTuWiD
AHVBCXVt/TkQ3Cm8doCP4ACTUjGqh3iZV1G0b31uiOpRlt/QhSqx0rvgh72iiYZ
Zi+HyYtsCdWoZEvsfmf+pnVnxBXEF7M754JAj5dLT6mTP5MDwDLgkQua5jTokFr9
6RGpJomwSTGvXU4RPYITmAjxMoZzCvNy1YmwFxcVETDSSe6+uDiS4bAmqIn9tYr
isg2yLwaGRex7/3APa4Is55yR2vB42P27VQ=
-----END CERTIFICATE-----

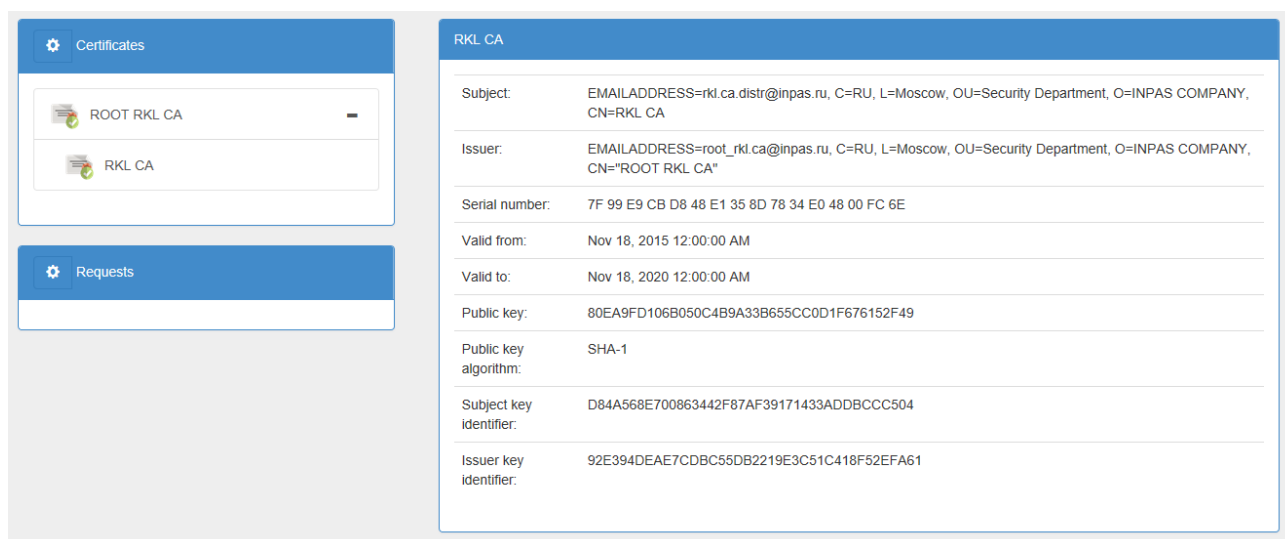
```

Load Cancel

Рисунок 18. Окно загрузки промежуточного сертификата RKL

3. Нажать кнопку «Load» для загрузки сертификата промежуточного УЦ RKL.

После нажатия кнопки «Load» будет выполнена загрузка сертификата. В секции «Certificate» будет отображаться загруженный сертификат (Рисунок 19. Раздел "Certificates" секция "Certificate"). Для отображения информации о сертификате нужно кликнуть по нему левой кнопкой мыши.



Certificates

- ROOT RKL CA
- RKL CA

Requests

RKL CA

Subject:	EMAILADDRESS=rkl.ca.distr@inpas.ru, C=RU, L=Moscow, OU=Security Department, O=INPAS COMPANY, CN=RKL CA
Issuer:	EMAILADDRESS=root_rkl.ca@inpas.ru, C=RU, L=Moscow, OU=Security Department, O=INPAS COMPANY, CN="ROOT RKL CA"
Serial number:	7F 99 E9 CB D8 48 E1 35 8D 78 34 E0 48 00 FC 6E
Valid from:	Nov 18, 2015 12:00:00 AM
Valid to:	Nov 18, 2020 12:00:00 AM
Public key:	80EA9FD106B050C4B9A33B655CC0D1F676152F49
Public key algorithm:	SHA-1
Subject key identifier:	D84A568E700863442F87AF39171433ADDBCC504
Issuer key identifier:	92E394DEAE7CDBC55DB2219E3C51C418F52EFA61

Рисунок 19. Раздел "Certificates" секция "Certificate"

4.6.3. Сертификат KDH

4.6.3.1. Генерация запроса на сертификат KDH

Для генерации запроса на сертификат KDH необходимо выполнить следующие шаги:

1. Нажать на  в секции «Requests» и выбрать пункт «Generate».
2. В открывшемся окне в текстовой области будет представлен сгенерированный запрос на сертификат KDH (Рисунок 20. Генерация запроса на сертификат KDH).



Рисунок 20. Генерация запроса на сертификат KDH

3. Сохранить данный запрос, выполнив копирование и сохранение в файл. Обратится в УЦ ИНПАС за выпуском сертификатов, приложив данный запрос.
4. Для закрытия окна нажать кнопку «Close».
5. В секции «Requests» отобразится созданный запрос на сертификат KDH (Рисунок 21. Секция "Request". Запросы сертификата KDH).

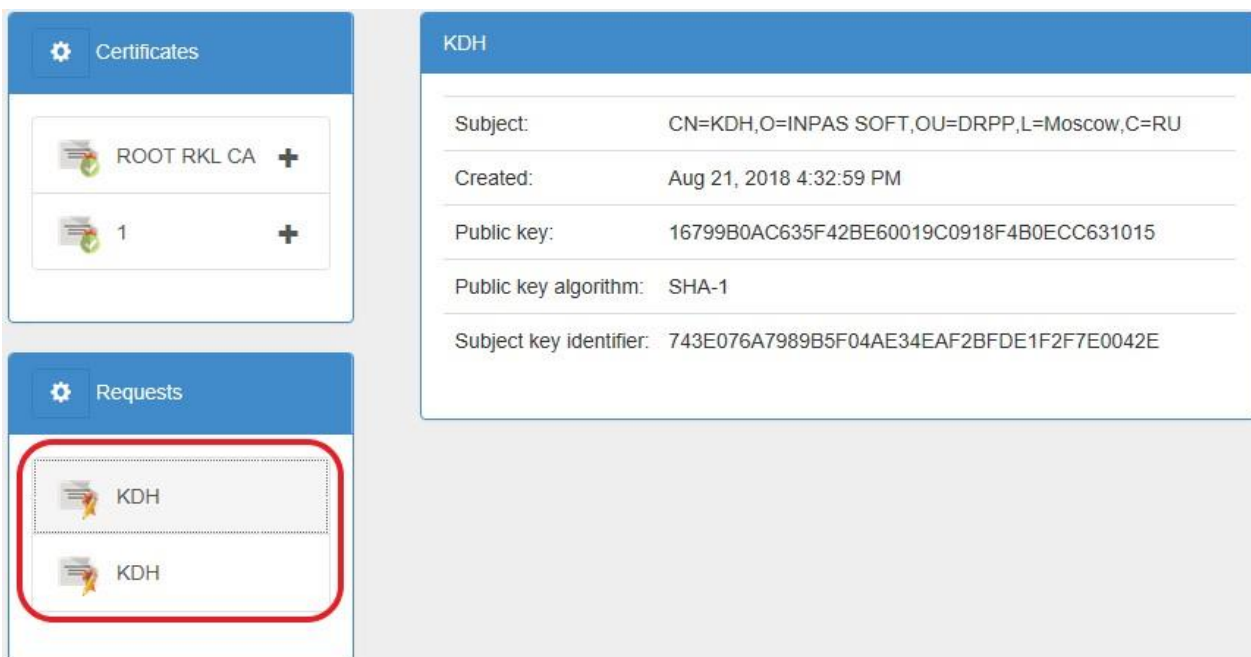


Рисунок 21. Секция "Request". Запросы сертификата KDH

4.6.3.1.1. Повторная генерация ключевой пары

Если ключевая пара была сгенерирована на одном HSM, а подпись запроса происходит на другом HSM, у которого совсем другой LMK, то он не сможет расшифровать криптограмму ключа и выдаст ошибку. Для того, чтобы избежать данной проблемы, перед тем, как генерировать запрос на сертификат KDH, нужно выполнить повторную генерацию ключей пары.

1. Нажать на  в секции «Requests» и выбрать пункт «Regenerate RSA key pair» (Рисунок 22. Секция "Request". Повторная генерация ключевой пары).

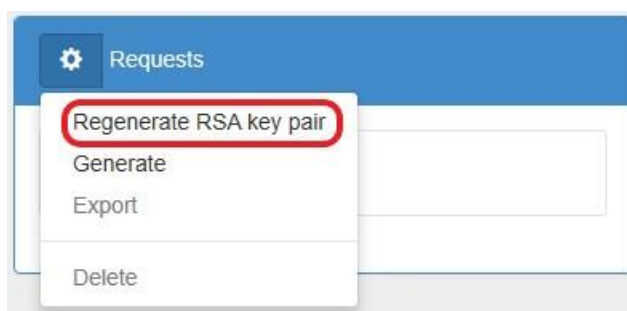


Рисунок 22. Секция "Request". Повторная генерация ключевой пары

2. Отобразится окно успешного выполнения повторной генерации ключевой пары с сообщением «RSA key pair is successfully regenerated».

Примечание: RSA-ключ, используемый KDH для организации безопасного обмена с терминалами, автоматически конвертируется в формат 'Keyblock' при первом использовании RSA-ключа.

4.6.3.2. Загрузка сертификата KDH

Сертификат должен быть стандарта «X.509» и представлен в формате «PEM». Для загрузки сертификата KDH необходимо выполнить следующие шаги:

1. Нажать на  в секции «Certificate» и выбрать пункт «Import Certificate».
2. В открывшемся окне «Load» вставить данные сертификата KDH, полученные от УЦ ИНПАС, в текстовую область (Рисунок 23. Окно загрузки сертификата KDH).

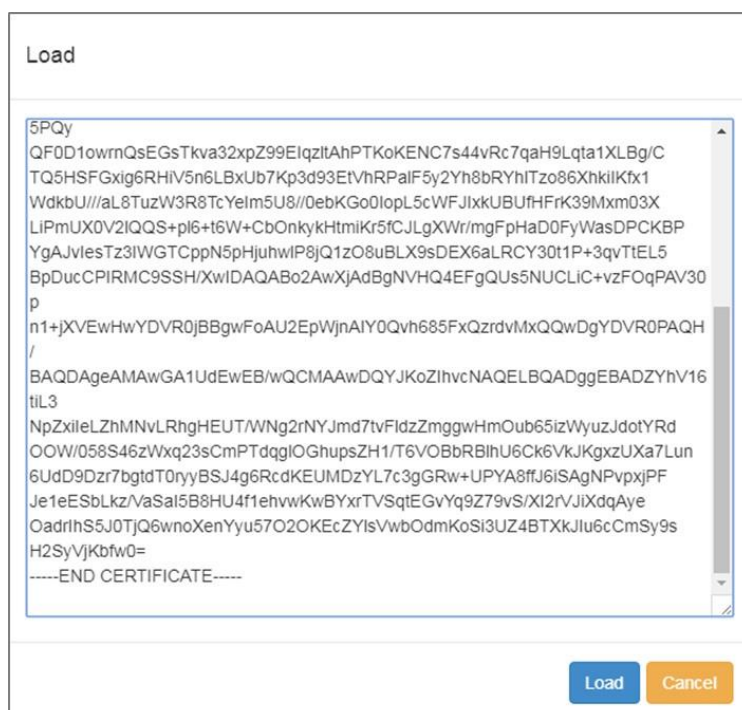


Рисунок 23. Окно загрузки сертификата KDH

3. Нажать кнопку «Load» для загрузки сертификата KDH.

После нажатия кнопки «Load» будет выполнена загрузка сертификата KDH. В секции «Certificate» будет отображаться загруженный сертификат (Рисунок 24. Раздел "Certificates" секция "Certificate"). Для отображения информации о сертификате нужно кликнуть по нему левой кнопкой мыши.

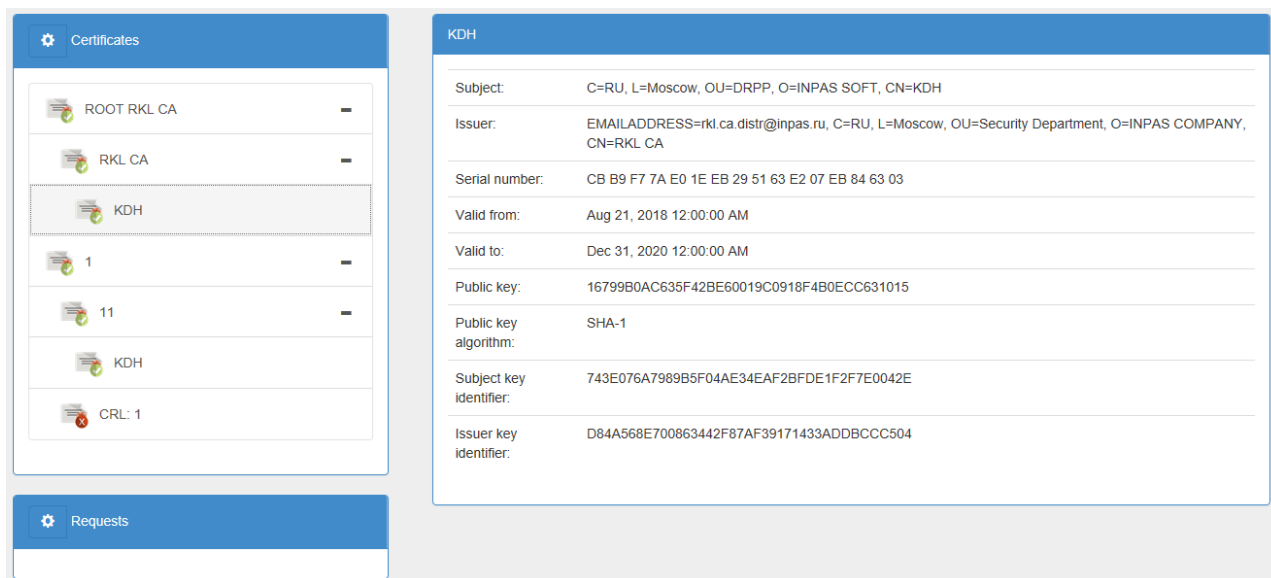


Рисунок 24. Раздел "Certificates" секция "Certificate"

4.6.4. Загрузка CRL листа «Certificates Revocation List»

CRL должен быть стандарта «X.509» и представлен в формате «PEM».

Для загрузки CRL листа необходимо выполнить следующие шаги:

Нажать на  в секции «Certificate» и выбрать пункт «Import CRL».

В открывшемся окне «Load» вставить данные CRL, полученного от УЦ ИНПАС, в текстовую область (Рисунок 25. Окно загрузки CRL листа).

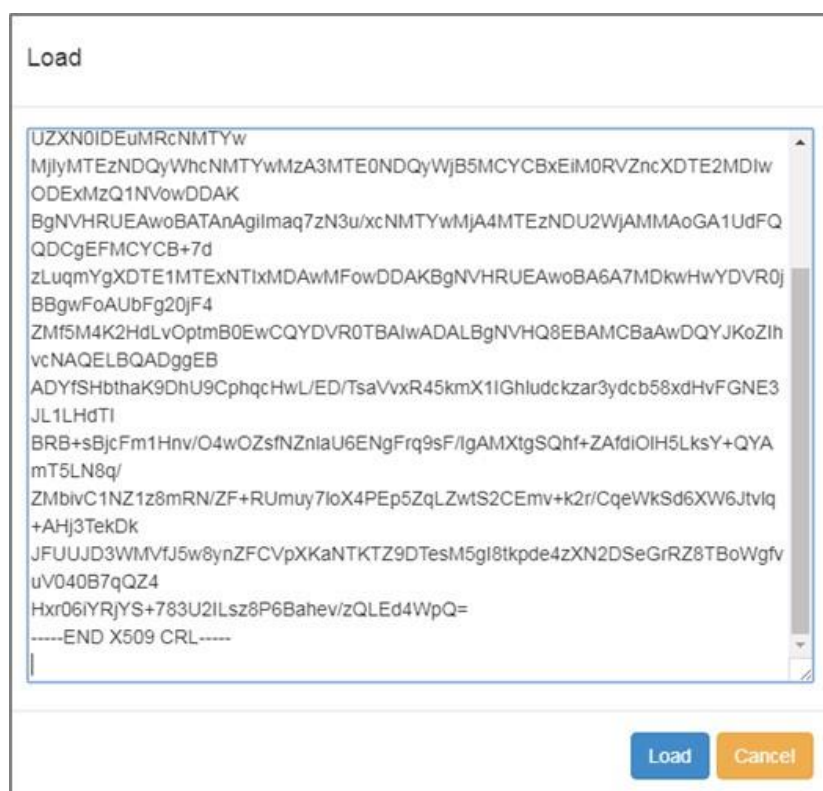


Рисунок 25. Окно загрузки CRL листа

Нажать кнопку «Load» для загрузки CRL листа.

После нажатия кнопки «Load» будет выполнена загрузка. В секции «Certificates» будут представлены данные загруженного CRL (Рисунок 26. Раздел "Certificates" секция "Certificates"). Для отображения информации о сертификате нужно кликнуть по нему левой кнопкой мыши.

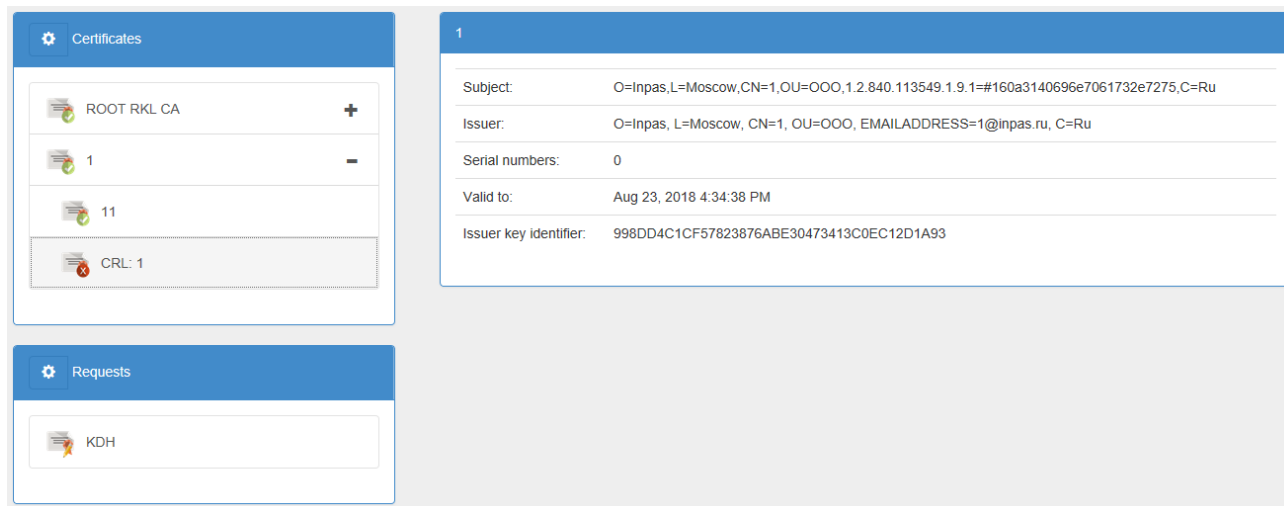


Рисунок 26. Раздел "Certificates" секция "Certificates"

Внимание: Начиная с версии 1.4.10 (от 01.08.2018) в KDH возможно загружать несколько (2 и более) цепочек сертификатов (сертификат корневого УЦ, сертификат RKL и сертификат KDH) (Рисунок 27. Раздел "Certificates". Две цепочки сертификатов).

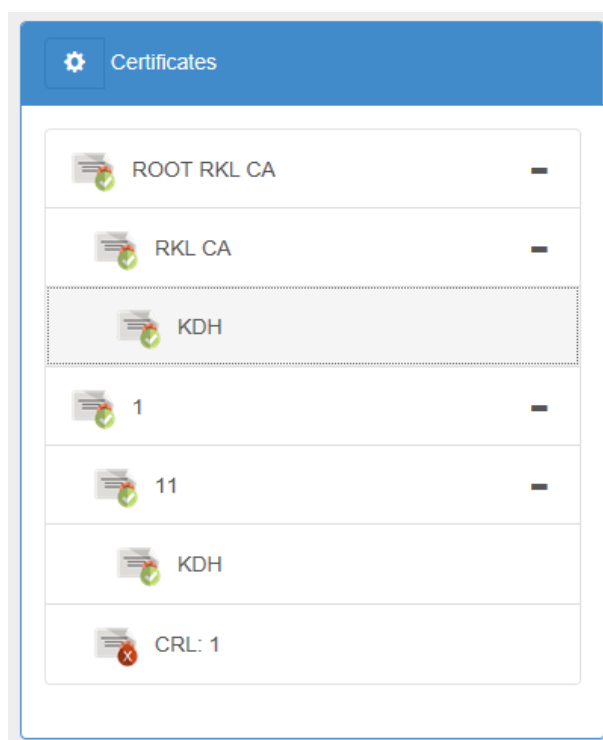


Рисунок 27. Раздел "Certificates". Две цепочки сертификатов

4.7. Операции с ZMK (ZMK)

Данный раздел содержит информацию по зарегистрированным в системе ZMK и инструменты для работы с ними, позволяющие пользователю:

- загрузить ZMK для хоста/банка;
- просмотреть информацию по загруженным ZMK;
- сформировать отчет по нужным данным.

Переход в раздел осуществляется по выбору пункта ZMK в главном меню.

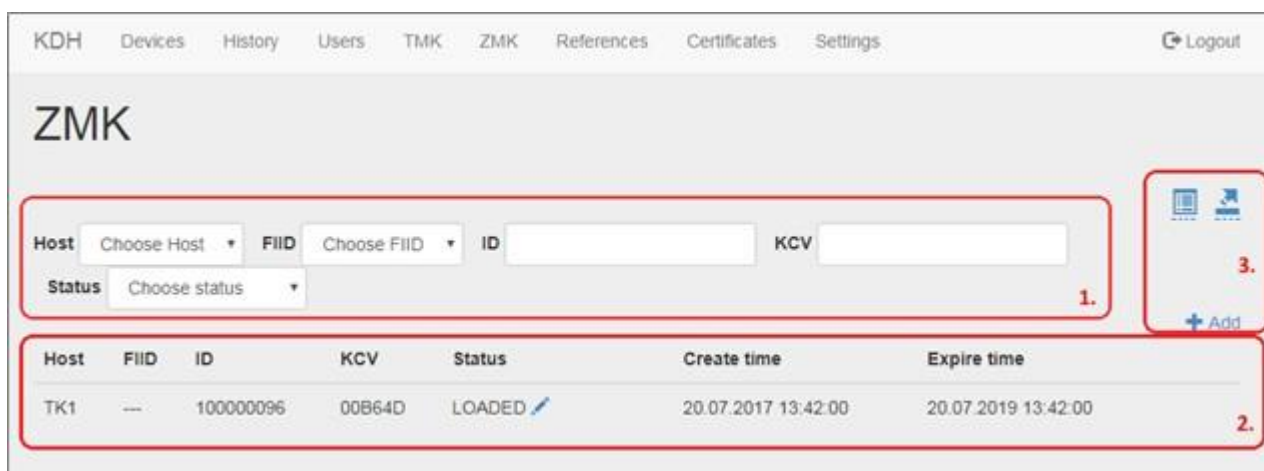


Рисунок 28. Раздел "ZMK"

Данный раздел содержит:

- Фильтр (область 1. на Рисунок 28. Раздел "ZMK");
- Информацию по ZMK (область 2. на Рисунок 28. Раздел "ZMK");
- Инструменты по работе с данными (область 3. на Рисунок 28. Раздел "ZMK").

Фильтр

Фильтр (область 1. на Рисунок 28. Раздел "ZMK") позволяет осуществлять поиск нужной информации, используя следующие поля для фильтрации данных (описание полей приводится ниже в описании атрибутов ZMK):

- **Host;**
- **FIID;**
- **ID;**
- **KCV;**
- **Status.**

Информация по ZMK

Информация по ZMK имеет табличное представление (область 2. на Рисунок 28. Раздел "ZMK"). Данные разбиты по следующим столбцам (атрибутам ZMK):

- **Host** - идентификатор хоста, к которому привязан данный ZMK;
- **FIID** - идентификатор Банка, к которому привязан ZMK, если ZMK был зарегистрирован в системе с привязкой к конкретному Банку;
- **ID** - идентификатор ZMK;
- **KCV** - контрольная сумма;
- **Status** - текущий статус. Статус может иметь следующие значения: «**LOADED**», «**COMPROMISED**», «**EXPIRED**», «**CANCELLED**». Для более подробной информации смотри пункт [4.7.1 Статусы](#);
- **Create time** - дата и время создания ZMK;
- **Expire time** - дата и время, до которого действителен ZMK.

Инструменты по работе с данными

Для работы с данными доступны следующие инструменты (наличие и доступность инструментов определяется правами для данной роли пользователя):



- позволяет настроить столбцы для отображения данных в табличном представлении;



- позволяет выполнить экспорт данных в файл;



- позволяет добавить ZMK.

4.7.1. Статусы

ZMK может иметь следующие статусы:

- **LOADED** - ZMK может быть использован для импорта TMK.
- **COMPROMISED** - ZMK скомпрометирован. При данном статусе все TMK со статусом «**READY**» под данным ZMK меняют свой статус на «**COMPROMISED**».
- **EXPIRED** - срок действия ZMK истек. При данном статусе ключа все TMK со статусом «**READY**» под данным ZMK меняют свой статус на «**EXPIRED**». Криптограмма ZMK и соответствующих ему TMK в БД очищается.
- **CANCELLED** - ZMK выведен из обращения. При данном статусе все TMK со статусом «**READY**» под данным ZMK меняют свой статус на «**CANCELLED**».

4.7.1.1. Изменение статуса

Статус ZMK может быть изменен:

- Автоматически системой KDH;
- Вручную пользователем с соответствующими правами.

Автоматическое изменение статуса

Система KDH автоматически меняет статус ZMK в следующих ситуациях:

- При истечении срока действия изменяет статус ZMK на «**EXPIRED**».

Ручное изменение статуса.

Доступность данного функционала определяется правами для данной роли пользователя.

Для изменения статуса ZMK вручную необходимо выполнить следующие шаги:

1. В разделе «**ZMK**» в строке со статусом ZMK нажать на иконку инструмента  (редактирование). Поле статуса станет доступно для редактирования;
2. В раскрывающемся списке выбрать нужный статус;
3. Нажать иконку рядом с полем статуса:  - для сохранения внесенных изменений или  - для отмены сделанных изменений.

При нажатии иконки  система выдаст сообщение о результате «**Status successfully changed**» – в случае успеха или сообщение с описанием ошибки – в случае ошибки.

4.7.1.2. Просмотр истории изменения статуса

Для просмотра истории изменения статуса конкретного ZMK и экспорта отчета по данной информации в формате «**Excel**» необходимо выполнить следующие шаги:

1. В разделе «**ZMK**» нажать на строке с ZMK, историю изменения статуса которого необходимо просмотреть.

Status log (id: 10)			
Old status	New status	Change time	Changed by
LOADED	EXPIRED	06.10.2016 16:03:00	---
			Export Close

Рисунок 29. Раздел "ZMK". История изменения статуса ZMK

В открывшемся окне (Рисунок 29. Раздел "ZMK". История изменения статуса ZMK) будет представлена история изменения статуса для данного ТМК, содержащая следующие данные:

- **Old status** - предыдущий статус;
- **New status** - новый статус;
- **Change time** - дата и время смены статуса;
- **Changed by** - пользователь, инициировавший смену статуса (при изменении статуса вручную пользователем).

2. Нажать на кнопку: Export для экспорта данных в отчет в формате «Excel» или Close для закрытия окна.

При нажатии кнопки «Export» KDH выполнит экспорт данных в отчет формата «Excel» и сохранит его по указанному пути.

4.7.2. Добавление ZMK

Для добавления ZMK необходимо выполнить следующие шаги:

1. В разделе «ZMK» нажать на +Add.
2. В открывшемся окне (Рисунок 30. Окно добавления ZMK) выполнить ввод данных в следующие поля:

ID

ID

Cryptogramm

Cryptogramm

KCV

KCV

Generation time

24.07.2017 12:04

☐ Set manual expiration time

Expiration time

24.07.2017 12:04

Link with

☒ Host
 TK1

☐ FIID
 VBEX

Add
Cancel

Рисунок 30. Окно добавления ZMK

- **ID** – идентификатор ZMK;
- **Cryptogramm** – криптограмма ZMK ключа под LMK;
- **KCV** – контрольная сумма;
- **Generation time** – дата и время генерации ключа;
- **Set manual expiration time** – установленный флаг в чек бокс позволяет редактировать поле «**Expiration time**»;
- **Expiration time** – дата/время, до которого ключ действителен;
- **Link with** – привязка ZMK к хосту либо к банку;
 - **Host** – идентификатор хоста, к которому привязан данный ZMK. Если ZMK выпущен только для Host, то действие ZMK распространяется на все FIID в рамках данного Host;
 - **FIID** – идентификатор банка к которому привязан данный ZMK. Если ZMK выпущен только для FIID в рамках Host, то действие ZMK распространяется только на данный FIID в рамках данного Host.

3. Нажать кнопку «**Add**» для добавления нового ZMK или «**Cancel**» для отмены.

При нажатии кнопки «**Add**», система выдаст сообщение о результате «**ZMK successfully added**» – в случае успеха или сообщение об ошибке – в случае ошибки.

4.7.3. Формирование отчета

Доступность данного функционала определяется правами для данной роли пользователя. Для формирования отчета в формате Excel необходимо выполнить следующие шаги:

1. В разделе «**ZMK**» нажать на иконку инструмента  (экспорт);
2. В открывшемся списке нажать на один из предложенных пунктов:
 - a. **All fields** – для формирования отчета по всем полям (столбцам);
 - b. **Only visible fields** – для формирования отчета только по видимым полям (столбцам).
3. Указать путь для сохранения сформированного отчета;
4. KDH выполнит экспорт данных в отчет формата «**Excel**» и сохранит его по указанному пути.

Примечание: При использовании фильтра, отчет формируется только по отфильтрованным данным, т.е. только по тем строкам, которые отображаются в таблице с информацией по ZMK (область 2. на Рисунок 28. Раздел "ZMK").

4.8. Операции с ТМК (ТМК)

Данный раздел содержит информацию по зарегистрированным в системе ТМК и инструменты для работы с ними, позволяющие пользователю:

- загрузить ТМК для хоста;
- просмотреть информацию по загруженным ТМК;
- сформировать отчет по нужным данным.

Переход в раздел осуществляется по выбору пункта «ТМК» в главном меню.

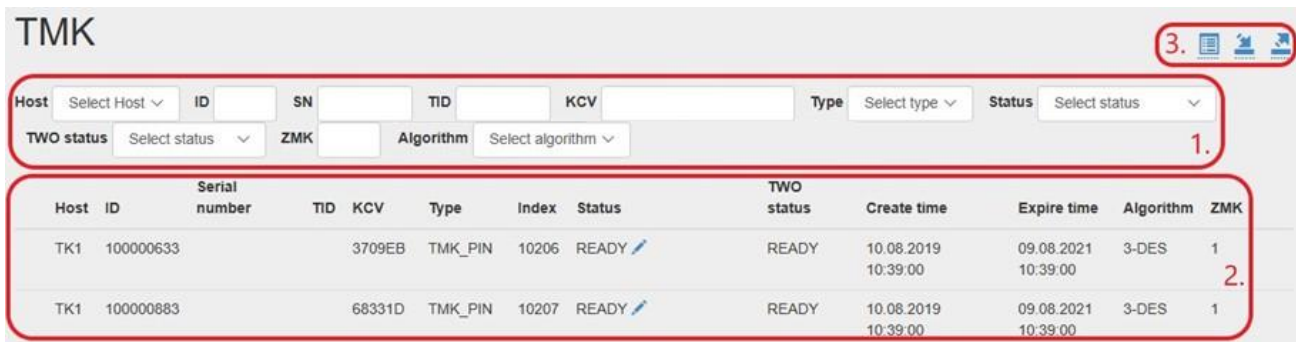


Рисунок 31. Раздел "ТМК"

Данный раздел содержит:

- Фильтр (область 1. на Рисунок 31. Раздел "ТМК");
- Информацию по ТМК (область 2. на Рисунок 31. Раздел "ТМК");
- Инструменты по работе с данными (область 3. на Рисунок 31. Раздел "ТМК").

Фильтр

Фильтр (область 1. на Рисунок 31. Раздел "ТМК") позволяет осуществлять поиск нужной информации используя следующие поля для фильтрации данных (описание полей приводится ниже в описании атрибутов ТМК):

- Host;
- ID;
- SN;
- TID;
- KCV;
- Type;
- Status;
- TWO status;
- ZMK;
- Algorithm.

Информация по ТМК

Информация по ТМК имеет табличное представление (область 2. на Рисунок 31. Раздел "ТМК"). Данные разбиты по следующим столбцам (атрибутам ТМК):

- **Host** - идентификатор хоста, к которому привязан данный ТМК.
- **ID** - идентификатор ТМК, единый для KDH и Авторизационного хоста;
- **Serial number** - серийный номер POS-терминала, на который загружен данный ТМК;
- **TID** - идентификационный номер POS-терминала на который загружен данный ТМК;
- **KCV** - контрольная сумма ТМК;
- **Type** - тип ключа: «MAC», «PIN»;
- **Index** - индекс ключа в БД;
- **Status** - текущий статус. Статус может иметь следующие значения: «READY», «COMPROMISED», «EXPIRED», «CANCELLED». Для более подробной информации смотри [4.8.1 Статусы](#);

- **TWO status** - статус уведомления TWO о привязке ключа к POS-терминалу;
- **Create time** - дата и время создания ТМК;
- **Expire time** - дата и время истечения срока действия ключа;
- **Algorithm** – алгоритм шифрования ключа;
- **ZMK** - идентификатор ZMK, на котором зашифрован данный ТМК.

Инструменты по работе с данными

Для работы с данными доступны следующие инструменты (наличие и доступность инструментов определяется правами для данной роли пользователя):



- позволяет настроить столбцы для отображения данных в табличном представлении;



- позволяет выполнить импорт данных из файла (загрузка файла со списком новых ТМК, загрузка файла со списком измененных статусов ТМК);



- позволяет выполнить экспорт данных в файл.

4.8.1. Статусы

ТМК может иметь следующие статусы:

- **READY** - ТМК загружен на KDH и может быть загружен в терминал по запросу последнего;
- **LOADED_IN_POS** - ТМК загружен в терминал;
- **LOADED_IN_TWO** - TWO уведомлен о привязке ТМК к TID;
- **COMPROMISED** - ТМК скомпрометирован;
- **EXPIRED** - Срок действия ТМК истек. Криптограмма ТМК в БД KDH очищается;
- **CANCELLED** - ТМК выведен из обращения.

4.8.1.1. Изменение статуса

После изменения статусов ТМК KDH уведомляет TWO о смене статуса ТМК.

Статус ТМК может быть изменен:

- Автоматически системой KDH;
- Вручную пользователем с соответствующими правами.

Автоматическое изменение статуса

Система KDH автоматически меняет статус ТМК в следующих ситуациях:

- Если ТМК имел статус «**LOADED_IN_POS**» или «**LOADED_IN_TWO**» (был ранее загружен в POS-терминал), и POS-терминал был переведен из статуса «**USED**» в статус «**READY**» или «**NEW**», то KDH изменяет статус ТМК на «**CANCELLED**».
- При загрузке ТМК на POS-терминал меняет статус на «**LOADED_IN_POS**».
- Если ТМК имеет статус «**LOADED_IN_POS**», то после успешного уведомления TWO о загрузке ТМК в POS-терминал, KDH меняет статус ТМК на «**LOADED_IN_TWO**».
- При истечении срока действия изменяет статус на «**EXPIRED**».
- Если ТМК имеет статус «**READY**», то в случае изменения статуса ZMK, на котором зашифрован данный ТМК, KDH меняет статус на аналогичный ZMK («**EXPIRED**», «**COMPROMISED**», «**CANCELLED**»).

Ручное изменение статуса

Доступность данного функционала определяется правами для данной роли пользователя.

Для изменения статуса ТМК вручную необходимо выполнить следующие шаги:

1. В разделе «**ТМК**» в строке со статусом ТМК нажать на иконку инструмента  (редактирование). Поле статуса станет доступно для редактирования;
2. В раскрывающемся списке выбрать нужный статус;

3. Нажать иконку рядом с полем статуса:  для сохранения внесенных изменений или  для отмены сделанных изменений.

При нажатии иконки  система выдаст сообщение о результате «**Status successfully changed**» – в случае успеха или сообщение с описанием ошибки – в случае ошибки.

4.8.1.2. Просмотр истории изменения статуса

Для просмотра истории изменения статуса конкретного ТМК и экспорта отчета по данной информации в формате «**Excel**» необходимо выполнить следующие шаги:

1. В разделе «**ТМК**» нажать на строке с ТМК, историю изменения статуса которого необходимо просмотреть.

Status log (Key id: 100000003)			
Old status	New status	Change time	Changed by
READY	LOADED_IN_POS	27.07.2017 11:37:19	---
		Export	Close

Рисунок 32. Раздел "ТМК". История изменения статуса ТМК

В открывшемся окне (Рисунок 32. Раздел "ТМК". История изменения статуса ТМК) будет представлена история изменения статуса для данного ТМК, содержащая следующие данные:

- **Old status** - предыдущий статус;
- **New status** - новый статус;
- **Change time** - дата и время смены статуса;
- **Changed by** - пользователь, инициировавший смену статуса (при изменении статуса вручную пользователем).

2. Нажать на кнопку [Export](#) для экспорта данных в отчет в формате «**Excel**» или [Close](#) для закрытия окна.

При нажатии кнопки «**Export**» KDH выполнит экспорт данных в отчет формата «**Excel**» и сохранит его по указанному пути.

4.8.2. Загрузка списка мастер ключей (ТМК)

Список мастер ключей (ТМК) представляет из себя файл в формате «**XML**». Формирование файла выполняется банком. Информацию о формате и структуре файла возможно посмотреть в пункте [6 Приложения](#).

Загрузка списка новых ТМК в KDH может быть выполнена следующими способами:

- Добавление файла со списком ТМК ключей в указанную при установке KDH папку;
- Через web-интерфейс системы KDH.

Для загрузки мастер ключей (ТМК) в KDH через web-интерфейс необходимо выполнить следующие шаги:

1. В разделе «**ТМК**» нажать на инструмент .
2. В открывшемся списке выбрать пункт «**Load TMK**».
3. В открывшемся окне выбрать файл для загрузки и нажать кнопку «**Открыть**». Система выполнит загрузку указанного файла и выведет результат в отдельном окне (Рисунок 33. Сообщение о результате загрузки файла с ТМК).

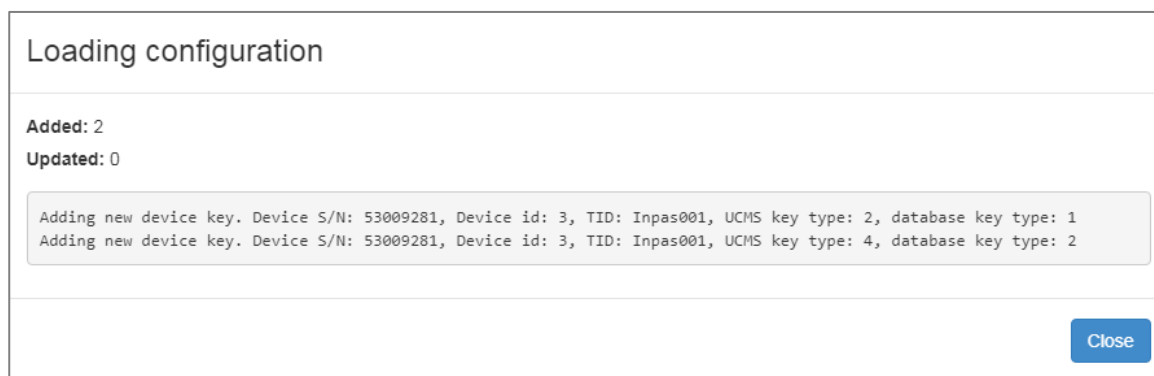


Рисунок 33. Сообщение о результате загрузки файла с ТМК

4. Нажать кнопку **«Close»** для закрытия окна и возврата к странице раздела **«ТМК»**. Данные из загруженного файла будут добавлены в таблицу с информацией по ТМК.

4.8.3. Загрузка списка измененных статусов ТМК

Список измененных статусов ТМК представляет из себя файл в формате **«ТХТ»**. Формирование файла выполняется банком. Информацию о формате и структуре файла возможно посмотреть в пункте 6 Приложения.

Загрузка списка измененных статусов ТМК в KDH может быть выполнена следующими способами:

- Добавление файла со списком измененных статусов ТМК ключей в указанную при установке KDH папку.
- Через web-интерфейс системы KDH.

Для загрузки списка измененных статусов мастер ключей (ТМК) в KDH через web-интерфейс необходимо выполнить следующие шаги:

1. В разделе **«ТМК»** нажать на инструмент .
2. В открывшемся списке выбрать пункт **«Load TMK status changes»**.
3. В открывшемся окне выбрать файл для загрузки и нажать кнопку **«Открыть»**. Система выполнит загрузку указанного файла и выведет результат в отдельном окне (Рисунок 34. Сообщение о результате загрузки файла с измененными статусами ТМК).

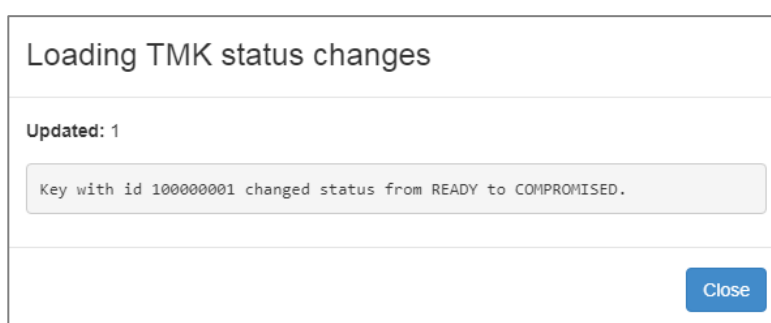


Рисунок 34. Сообщение о результате загрузки файла с измененными статусами ТМК

4. Нажать кнопку **«Close»** для закрытия окна и возврата к странице раздела **«ТМК»**. Данные из загруженного файла будут добавлены в таблицу с информацией по ТМК с обновлением статусов.

4.8.4. Формирование отчета

Доступность данного функционала определяется правами для данной роли пользователя. Для формирования отчета в формате **«Excel»** необходимо выполнить следующие шаги:

1. В разделе **«ТМК»** нажать на иконку инструмента  (экспорт);
2. В открывшемся списке нажать на один из предложенных пунктов:

- a. **All fields** – для формирования отчета по всем полям (столбцам);
- b. **Only visible fields** – для формирования отчета только по видимым полям (столбцам).
3. Указать путь для сохранения сформированного отчета;
4. KDH выполнит экспорт данных в отчет формата «Excel» и сохранит его по указанному пути.

Примечание: При использовании фильтра, отчет формируется только по отфильтрованным данным, т.е. только по тем строкам, которые отображаются в таблице с информацией по ТМК (область 2. на Рисунок 31. Раздел "ТМК").

4.8.5. TWO и E-mail уведомления

В разделе «ТМК» для каждого ключа ТМК есть значки (кнопки), позволяющие управлять «TWO-уведомлениями» и «E-mail уведомлениями»:

-  - означает, что выполняется автоповтор TWO уведомлений для данного ТМК;
-  - означает, что для данного ТМК не выполняется автоповтор TWO уведомлений;
-  - означает, что выполняется отправка e-mail уведомлений для данного ТМК;
-  - означает, что отправка e-mail уведомлений для данного ТМК не выполняется.

Для управления повторной отправкой «TWO и E-mail уведомлений» должны выполняться одновременно 2 условия:

- TWO статус ТМК перешел в «LOAD_ERROR»;
- Ошибка, в результате которой произошел переход в «LOAD_ERROR», НЕ является I/O Exception.

Ограничение.

В случае I/O Exception отправка уведомлений происходит безусловно, управление повторной отправкой уведомлений через настройки недоступно.

В зависимости от выставленного значения в параметре «Повтор уведомлений» (4.11.2 Конфигурация TWO) для каждого ТМК отображается определенный значок (кнопка).

Условия	«Повтор уведомлений» = «Да»	«Повтор уведомлений» = «Нет»
Новый ТМК, по которым возникла ошибка отправки, получают по умолчанию значок отправки TWO-уведомлений	Отображается значок  .	Отображается значок  .
Переключение между кнопками для TWO-уведомлений	Доступно.	По нажатию на кнопку  выполняется однократная попытка повторного отправления уведомления. Переключение на автоповтор отправки уведомлений не происходит.
Новый ТМК, по которым возникла ошибка отправки, получают по умолчанию значок отправки E-mail уведомления	Ни каких значков (кнопок) не отображается. Отправка e-mail уведомлений не выполняется.	Отображается значок  .

Переключение между кнопками для E-mail уведомлений	Недоступно.	Доступно переключение с ☒ на ☐ и обратно.
--	-------------	--

При нажатии на кнопку ☐ изменится значок на  и прекратится выполнение автоповторов TWO уведомлений для данного ТМК. Если нажать на кнопку , то значок изменится на ☐ и будет выполняться автоповтор TWO уведомлений для данного ТМК.

При нажатии на кнопку ☒ изменится значок на ☐ и прекратится отправка e-mail уведомлений для данного ТМК. Если нажать на кнопку ☐, то значок изменится на ☒ и будут отправляться e-mail уведомления для данного ТМК.

4.9. Устройства (Devices)

Данный раздел содержит информацию по зарегистрированным в системе POS-терминалам и инструменты для работы с этими данными, позволяющие пользователю:

- загрузить данные (серийные номера устройств, конфигурацию мастер-ключей) по POS-терминалам, для которых требуется загрузка ключей;
- просмотреть информацию по данным устройствам с возможностью фильтрации;
- сформировать отчет по нужным данным.

Переход в раздел осуществляется по выбору пункта «**Devices**» в главном меню.

Devices

3. [Icons]

1. [Search filters: S/N, Status, Added from, Added to, Vendor, Model]

Serial number	Status	Keys	Time added	Last request	Vendor	Model	Certificate
3A307423	READY	TMMK TPMK	27.10.2017 13:34:28				
280122610	READY	TMMK TPMK	20.12.2017 16:42:44	20.12.2017 17:05:39	Verifone	VX520	view
324300847	NEW		16.07.2019 17:10:12	25.07.2019 17:03:07	Verifone	VX680	view
68000259	READY	TMMK TPMK	08.08.2019 12:42:04				
261689767	READY	TMMK TPMK	08.08.2019 16:22:28	09.08.2019 10:24:44	Verifone	VX520	view

2. [Table]

Filtered: 5. Total: 5.

Рисунок 35. Раздел "Devices"

Данный раздел содержит:

- **Фильтр** (область 1. на Рисунок 35. Раздел "Devices");
- **Информацию по устройствам** (область 2. на Рисунок 35. Раздел "Devices");
- **Инструменты по работе с данными** (область 3. на Рисунок 35. Раздел "Devices").

Фильтр

Фильтр (область 1. на Рисунок 35. Раздел "Devices") позволяет осуществлять поиск нужной информации используя следующие поля для фильтрации данных (описание полей приводится ниже в описании атрибутов устройств):

- **S/N**;
- **Status**;
- **Added from**;
- **Added to**;
- **Vendor**;
- **Model**.

Информация по устройствам

Информация по POS-терминалам имеет табличное представление (область 2. на Рисунок 35. Раздел "Devices"). Данные разбиты по следующим столбцам (атрибутам устройств):

- **Serial number** - серийный номер POS-терминала;
- **Status** - текущий статус. Статус может иметь следующие значения: «**NEW**», «**READY**», «**USED**». Для более подробной информации смотри [4.9.1 Статусы](#);
- **Keys** - информация о ключах, которые загружены или будут загружены в POS-терминал;
- **Time added** - дата и время добавление POS-терминала в систему KDH;

- **Last request** - дата и время последнего обращения POS-терминала на KDH;
- **Vendor** – вендор;
- **Model** – модель;
- **Certificate** - содержит ссылку на информацию из сертификата публичного ключа POS-терминала: субъект (содержит S/N POS-терминала), издатель, серийный номер сертификата, время начала и окончания срока действия сертификата, отпечаток публичного ключа, алгоритм публичного ключа.

Инструменты по работе с данными

Для работы с данными доступны следующие инструменты (наличие и доступность инструментов определяется правами для данной роли пользователя):



- позволяет настроить столбцы для отображения данных в табличном представлении;



позволяет выполнить импорт данных из файла (загрузка файла со списком новых POS-терминалов, загрузка файла с конфигурацией ключей POS-терминала;



- позволяет выполнить экспорт данных в файл.

4.9.1. Статусы

POS-терминал может иметь следующие статусы:

- **NEW** - POS-терминал зарегистрирован на KDH;
- **READY** - в KDH загружена конфигурация ключей для данного POS-терминала. POS-терминал готов к загрузке ключей;
- **USED** - в KDH к данному S/N привязаны ТМК. В POS-терминал с данным S/N выполнена загрузка ТМК.

4.9.1.1. Изменение статуса

Статус POS-терминала может быть изменен:

- Автоматически системой KDH;
- Вручную пользователем с соответствующими правами.

Автоматическое изменение статуса

Система KDH автоматически меняет статус устройства в следующих ситуациях:

- При изменении статуса на «**NEW**», KDH автоматически удаляет загруженную конфигурацию ключей для данного устройства;
- При изменении статуса на «**READY**» KDH автоматически отвязывает ТМК ключи от данного устройства, меняя их статус на «**CANCELLED**»;
- При изменении статуса на «**NEW**» KDH автоматически отвязывает ТМК ключи от данного устройства, меняя их статус на «**CANCELLED**», а также автоматически удаляет загруженную конфигурацию ключей для данного устройства;
- При загрузке конфигурации ключей для данного S/N устройства KDH меняет статус с «**NEW**» на «**READY**»;
- При успешной загрузке ТМК в POS-терминал KDH меняет статус с «**READY**» на «**USED**».

Ручное изменение статуса

Доступность данного функционала определяется правами для данной роли пользователя.

Для изменения статуса устройства вручную необходимо выполнить следующие шаги:

1. В разделе «**Devices**» в строке со статусом POS-терминала нажать на иконку инструмента  (редактирование). Поле статуса станет доступно для редактирования.
2. В раскрывающемся списке выбрать нужный статус.

3. Нажать иконку рядом с полем статуса:  для сохранения внесенных изменений или  для отмены сделанных изменений.

При нажатии иконки система выдаст сообщение о результате «**Status successfully changed**» – в случае успеха или сообщение с описанием ошибки – в случае ошибки.

4.9.1.2. Просмотра истории изменения статуса POS-терминала

Для просмотра истории изменения статуса конкретного S/N устройства и экспорта отчета по данной информации в формате «**Excel**» необходимо выполнить следующие шаги:

1. В разделе «**Devices**» нажать на строке с S/N устройства, историю изменения статуса которого необходимо просмотреть;

Status log (S/N:3A189529)			
Old status	New status	Change time	Changed by
READY	USED	27.07.2017 11:37:19	---
NEW	READY	27.07.2017 11:10:41	User1
		<button>Export</button>	<button>Close</button>

Рисунок 36. Раздел "Devices". История изменения статуса устройства

В открывшемся окне (Рисунок 36. Раздел "Devices". История изменения статуса устройства) будет представлена история изменения статуса для данного S/N устройства содержащая следующие данные:

- **Old status** - предыдущий статус;
- **New status** - новый статус;
- **Change time** - дата и время смены статуса
- **Changed by** - пользователь, инициировавший смену статуса (при изменении статуса вручную пользователем).

2. Нажать на кнопку  для экспорта данных в отчет в формате «**Excel**» или  для закрытия окна.

При нажатии кнопки «**Export**» KDH выполнит экспорт данных в отчет формата «**Excel**» и сохранит его по указанному пути.

4.9.2. Загрузка списка S/N устройств (POS-терминалов)

Список серийных номеров представляет из себя файл в формате «**ТХТ**». Информацию о формате и структуре файла возможно посмотреть в пункте 6 Приложения.

Загрузка списка серийных номеров POS-терминалов KDH может быть выполнена следующими способами:

- Добавление файла со списком S/N устройств в указанную при инсталляции KDH папку.
- Через web-интерфейс системы KDH.

Для загрузки списка серийных номеров POS-терминалов, в которые требуется загрузить ТМК ключи, необходимо выполнить следующие шаги:

1. В разделе «**Devices**» нажать на ;
2. В открывшемся списке выбрать пункт «**Load S/N list**»;
3. В открывшемся окне выбрать файл для загрузки и нажать кнопку «**Открыть**». Система выполнит загрузку указанного файла и выведет результат в отдельном окне (Рисунок 37. Сообщение о результате загрузки файла с S/N устройств);

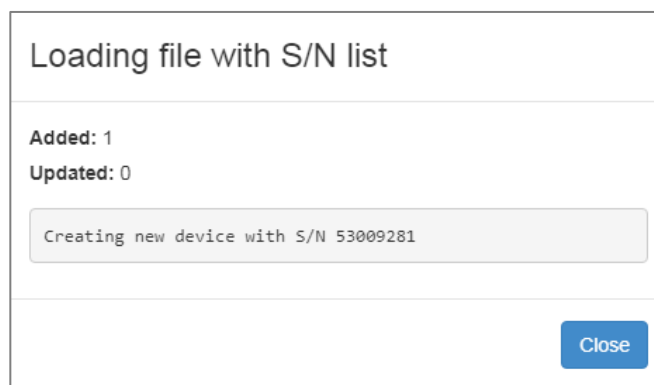


Рисунок 37. Сообщение о результате загрузки файла с S/N устройств

4. Нажать кнопку **«Close»** для закрытия окна и возврата к странице раздела **«Devices»**. Данные из загруженного файла будут добавлены в таблицу с информацией по POS-терминалам.

4.9.3. Загрузка файла с конфигурацией ключей

Файл с конфигурацией ключей представляет из себя файл в формате **«XML»**. Формирование файла выполняется системой параметризации UCMS (плагином RKL) (см. п. [5.1 Подготовка компонент к работе с RKL](#)).

Система KDH поддерживает работу с конфигурациями, содержащими одну **«Single-merchant»** или более **«Multi-merchant»** организаций.

Примечание: в случае конфигурации **«Multi-merchant»** для всех **«TID»** состав ключевой информации (типы ключей и номера ячеек) должны быть идентичны.

Загрузка конфигураций ключей в KDH может быть выполнена следующими способами:

- Добавление файла с конфигурацией ТМК ключей в указанную при инсталляции KDH папку;
- Через web-интерфейс системы KDH.

Для загрузки конфигурации ключей для POS-терминалов через web-интерфейс необходимо выполнить следующие шаги:

1. В разделе **«Devices»** нажать на ;
2. В открывшемся списке выбрать пункт **«Load configuration»**;
3. В открывшемся окне выбрать файл для загрузки и нажать кнопку **«Открыть»**. Система выполнит загрузку указанного файла и выведет результат в отдельном окне (Рисунок 38. Сообщение о результате загрузки файла с конфигурацией ключей);

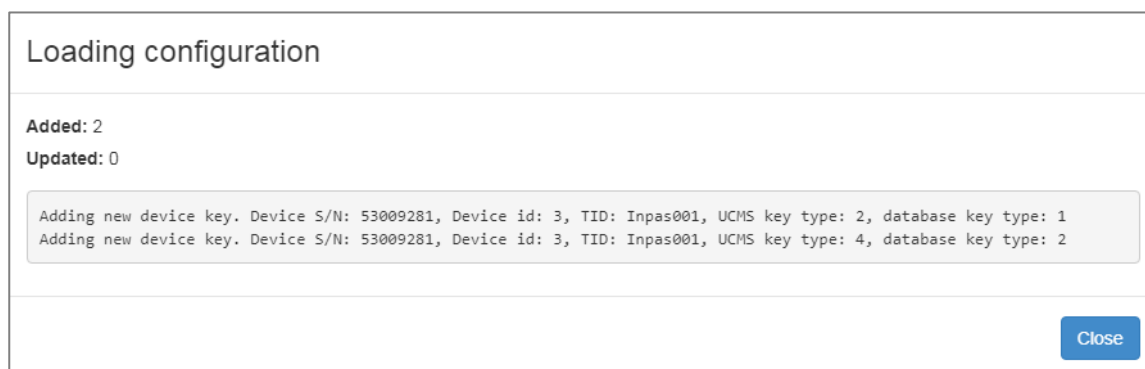


Рисунок 38. Сообщение о результате загрузки файла с конфигурацией ключей

4. Нажать кнопку **«Close»** для закрытия окна и возврата к странице раздела **«Devices»**. Данные о конфигурации ключей из загруженного файла будут добавлены в таблицу с информацией по POS-терминалам в столбец **«Keys»**.

4.9.4. Формирование отчета

Доступность данного функционала определяется правами для данной роли пользователя.

Для формирования отчета по зарегистрированным в системе POS-терминалам в формате «**Excel**» необходимо выполнить следующие шаги:

1. В разделе «**Devices**» нажать на иконку инструмента  (экспорт);
2. В открывшемся списке нажать на один из предложенных пунктов:
 - а. **All fields** – для формирования отчета по всем полям (столбцам);
 - б. **Only visible fields** – для формирования отчета только по видимым полям (столбцам).
3. Указать путь для сохранения сформированного отчета;
4. KDH выполнит экспорт данных в отчет в формате «**Excel**» и сохранит его по указанному пути.

Примечание: При использовании фильтра, отчет формируется только по отфильтрованным данным, т.е. только по тем строкам, которые отображаются в таблице с информацией по устройствам (область 2. на Рисунок 35. Раздел "Devices").

4.10. Хосты/ банки (References)

Данный раздел содержит информацию и инструменты для работы с банками и их хостами (Рисунок 39. Раздел "References").

Переход в раздел осуществляется по выбору пункта «**References**» в главном меню.

KDH	Users	References	Certificates	Settings	Logout
Hosts					+Add
ID	Name	URL	Clerk	Password	
192837465	Host1	http://10.35.90.151:7065	admin	*****	
3265987841	Host2	http://10.35.90.90:7777	admin	*****	
FIID					+Add
Name		Host			
Bank1		Host1			
Bank2		Host2			

Рисунок 39. Раздел "References"

Информация разбита на 2 секции:

- **Hosts** - в данной секции представлена информация и инструменты для работы с хостами.
- **FIID** - в данной секции представлена информация и инструменты для работы с банками.

4.10.1. Операции с хостами

4.10.1.1. Добавление хоста

Для добавления хоста необходимо выполнить следующие шаги:

1. В разделе «**References**» в секции «**Hosts**» нажать на . В открывшемся окне (Рисунок 40. Окно добавления хоста) выполнить ввод данных в следующие поля:

ID

Host id

Host name

Name

URL

URL

Clerk

admin

Password

.....

Add

Cancel

Рисунок 40. Окно добавления хоста

- **ID** – идентификатор хоста;
- **Host name** – наименование хоста.

Параметры соединения с TWO для отправки уведомлений:

- **URL** – URL-адрес хоста;
- **Clerk** – логин пользователя;
- **Password** – пароль пользователя.

2. Нажать кнопку **«Add»** для добавления нового хоста или **«Cancel»** для отмены. При нажатии кнопки **«Add»**, система выдаст сообщение о результате **«Host successfully added»** – в случае успеха (Рисунок 41. Сообщение об успешном результате) или сообщение с описанием ошибки – в случае ошибки (Рисунок 42. Сообщение об ошибке).

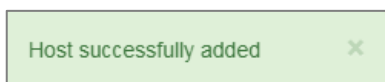


Рисунок 41. Сообщение об успешном результате

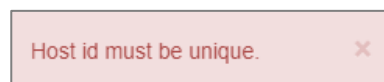


Рисунок 42. Сообщение об ошибке

4.10.1.2. Редактирование хоста

Для редактирования хоста необходимо выполнить следующие шаги:

1. В разделе **«References»** в секции **«Hosts»** навести курсор мыши на строку с данными хоста которые необходимо отредактировать. В конце строки появятся инструменты (Рисунок 43. Раздел "References" секция "Hosts");

Hosts					+Add
ID	Name	URL	Clerk	Password	
789456123	Host1	http://10.35.90.151:7064	admin	*****	 

Рисунок 43. Раздел "References" секция "Hosts"

2. Нажать на иконку инструмента  (редактирование). Поля строки с данными хоста станут доступны для редактирования (Рисунок 44. Раздел "References" секция "Hosts". Редактирование);

Hosts					+Add
ID	Name	URL	Clerk	Password	
789456123	Host1	http://10.35.90.151:7064	admin	*****	 

Рисунок 44. Раздел "References" секция "Hosts". Редактирование

3. Внести необходимые изменения;
4. Нажать иконку в конце строки  для сохранения внесенных изменений или  для отмены сделанных изменений.

При нажатии иконки  система выдаст сообщение о результате **«Changes successfully saved»** – в случае успеха или сообщение с описанием ошибки – в случае ошибки.

4.10.1.3. Удаление хоста

Для удаления хоста необходимо выполнить следующие шаги:

1. В разделе **«References»** в секции **«Hosts»** навести курсор мыши на строку с данными хоста, который необходимо удалить. В конце строки появятся инструменты (Рисунок 43. Раздел "References" секция "Hosts");
2. Нажать на иконку инструмента  (удаление). Система запросит подтверждение на удаление (Рисунок 45. Запрос подтверждения на удаление хоста);

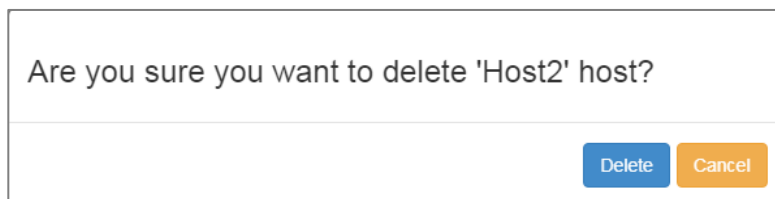


Рисунок 45. Запрос подтверждения на удаление хоста

3. Нажать кнопку «**Delete**» для подтверждения удаления или «**Cancel**» для отмены.

4.10.2. Операции с банками

4.10.2.1. Добавление банка

Для добавления банка необходимо выполнить следующие шаги:

1. В разделе «**References**» в секции «**FIID**» нажать на . В открывшемся окне (Рисунок 46. Окно добавления банка) выполнить ввод данных в следующие поля:

Рисунок 46. Окно добавления банка

- **FIID name** – наименование банка;
 - **Host** – наименование хоста. Выбирается из раскрывающегося списка созданных хостов.
2. Нажать кнопку «**Add**» для добавления нового хоста или «**Cancel**» для отмены. При нажатии кнопки «**Add**», система выдаст сообщение о результате «**FIID successfully added**» – в случае успеха или сообщение с описанием ошибки – в случае ошибки.

4.10.2.2. Редактирование банка

Для редактирования банка необходимо выполнить следующие шаги:

1. В разделе «**References**» в секции «**FIID**» навести курсор мыши на строку с данными банка которые необходимо отредактировать. В конце строки появятся инструменты (Рисунок 47. Раздел "References" секция "FIID");

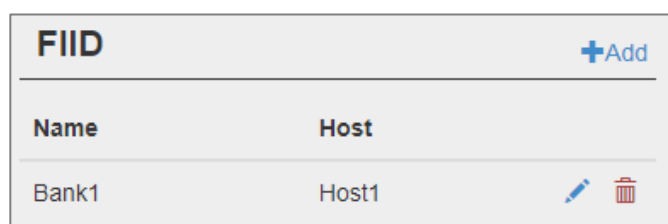


Рисунок 47. Раздел "References" секция "FIID"

2. Нажать на иконку инструмента  (редактирование). Поля строки с данными банка станут доступны для редактирования (Рисунок 48. Раздел "References" секция "FIID". Редактирование);

FIID		+Add
Name	Host	
Bank1	Host1	✓ ✗

Рисунок 48. Раздел "References" секция "FIID". Редактирование

3. Внести необходимые изменения;

4. Нажать иконку в конце строки  для сохранения внесенных изменений или  для отмены сделанных изменений.

При нажатии иконки  система выдаст сообщение о результате «**Changes successfully saved**» – в случае успеха или сообщение с описанием ошибки – в случае ошибки.

4.10.2.3. Удаление банка

Для удаления банка необходимо выполнить следующие шаги:

1. В разделе «**References**» в секции «**FIID**» навести курсор мыши на строку с данными банка, который необходимо удалить. В конце строки появятся инструменты (Рисунок 47. Раздел "References" секция "FIID");
2. Нажать на иконку инструмента  (удаление). Система запросит подтверждение на удаление (Рисунок 49. Запрос подтверждения на удаление банка);

Are you sure you want to delete 'Bank2' FIID?

[Delete](#) [Cancel](#)

Рисунок 49. Запрос подтверждения на удаление банка

3. Нажать кнопку «**Delete**» для подтверждения удаления или «**Cancel**» для отмены.

4.11. Настройки (Settings)

Данный раздел содержит настройки параметров работы KDH (Рисунок 50. Раздел "Settings"). Переход в раздел осуществляется по выбору пункта **«Settings»** в главном меню.

Рисунок 50. Раздел "Settings"

Параметры разбиты по следующим блокам:

- Остаток свободных ключей;
- Конфигурация TWO;
- Настройки срока действия ключей;
- Настройки HSM.

4.11.1. Настройка остатка свободных ключей

Данный блок параметров используется для настройки периодической проверки наличия достаточного количества ТМК заданного типа для каждого Хоста. Для каждого хоста KDH рассчитывает количество записей S/N (Host_ID(n)) и количество записей Key_ID (Host_ID(n)) и производит сравнение значений. Если количество Key_ID(Host_ID(n)) превышает количество S/N (Host_ID(n)) на число, меньшее значения неснижаемого остатка, KDH направляет заявку на генерацию ключей для Host_ID в размере разницы между числом записей (S/N (Host_ID(n)) и числом записей (Key_ID(Host_ID(n)) + заданное число дополнительных ключей. Заявка формируется в виде файла (путь указывается в настройках KDH) и, опционально, в виде e-mail по заданному в настройках KDH адресу.

Для настройки остатка свободных ключей необходимо выполнить следующие шаги:

1. В меню раздела **«Settings»** выбрать пункт **«Остаток свободных ключей»**;

Рисунок 51. Раздел "Settings". Остаток свободных ключей

2. В блоке параметров «**Остаток свободных ключей**» (Рисунок 51. Раздел "Settings". Остаток свободных ключей) задать следующие параметры:
 - **Неснижаемый остаток по хосту** - задает неснижаемый остаток ТМК ключей, по достижению которого KDH сформирует заявку на генерацию ключей, а также отправит уведомление пользователю на указанный Email;
 - **Число дополнительных ключей** - задает количество дополнительных ТМК ключей;
 - **Email для уведомлений** - Email для уведомления пользователя о формировании заявки на генерацию ТМК ключей;
 - **Периодичность проверки** - интервал выполнения проверки в часах;
 - **Проверяемые ключи (разделенные запятой)** - тип ключа(ей) ТМК для проверки. Например, PIN, MAC. (Рисунок 51. Раздел "Settings". Остаток свободных ключей).
3. Нажать кнопку «**Save**» для сохранения изменений.

4.11.2. Конфигурация TWO

Данный блок параметров используется для управления «**TWO-уведомлениями**» о смене статуса ключа и привязке ключа к терминалу и «**E-mail уведомлениями**» о неуспешной отправке «**TWO-уведомлений**».

Для включения (отключения) «**TWO-уведомлений**» и указания адреса электронной почты для «**E-mail уведомлений**» необходимо выполнить следующие шаги:

1. В меню раздела «**Settings**» выбрать пункт «**Конфигурация TWO**»;

Рисунок 52. Раздел "Settings". Управление TWO и E-mail уведомлениями

2. В блоке параметров «**Конфигурация TWO**» (Рисунок 52. Раздел "Settings". Управление TWO и E-mail уведомлениями) задать следующие параметры:
 - **Повтор уведомлений** – включает/ отключает автоматическую повторную отправку «**TWO-уведомлений**»;
 - **Период повтора** –указывается период повтора отправки «**TWO-уведомлений**» в секундах. Используется, если в параметре «**Повтор уведомлений**» установлено значение «**Да**»;
 - **Email для уведомлений** – указывается адрес электронной почты для отправки уведомлений. Возможно указать несколько адресов электронной почты с помощью разделителя «;». Используется совместно с параметрами «**Повтор уведомлений**» (если установлено значение «**Нет**»), «**Отправлять уведомление на почту при уведомлении хоста**» (если установлено значение «**Да**»);

- **Период повтора уведомлений по e-mail** – указывается интервал повторной отправки e-mail уведомлений. Используется, если в параметре «**Повтор уведомлений**» установлено значение «**Да**»;
- **Отправлять уведомление на почту при уведомлении хоста** – включает отправку Email уведомлений на электронную почту при получении терминалом ключей. Уведомление отправляется после успешного подтверждения терминалом получения ключей и изменения статуса ключа на «**Loaded_in_POS**».

3. Нажать кнопку «**Save**» для сохранения изменений.

При переключении параметра «**Повтор уведомлений**» в разделе «**ТМК**» (4.8 Операции с ТМК (ТМК)) меняются значки (кнопки):

Отображение значка	Изменения значения параметра « Повтор уведомлений » с « Да » на « Нет »	Изменения значения параметра « Повтор уведомлений » с « Нет » на « Да »
	Значок (кнопка) прекращает отображаться для ТМК, отправка TWO-уведомлений прекращается	Значок (кнопка) появляется для ТМК, выполняется отправка TWO-уведомлений
	Значок (кнопка) отображается, но меняется поведение при нажатии. Выполняется однократная повторная отправка TWO-уведомления	Значок (кнопка) отображается, но меняется поведение при нажатии. Выполняется повторная отправка TWO-уведомления, пока процесс не закончится успехом
	Значок (кнопка) появляется для ТМК	Значок (кнопка) прекращает отображаться
	Значок (кнопка) появляется для ТМК, выполняется отправка e-mail уведомлений	Значок (кнопка) прекращает отображаться для ТМК, отправка e-mail уведомлений не выполняется

4.11.3. Настройка срока действия ключей

Данный блок параметров используется для настройки периодической проверки срока действия ключей ZMK и ТМК. При истечении срока действия ключей KDH изменяет статус на «**EXPIRED**», очищает в БД криптограмму, уведомляет TWO о смене статуса ТМК.

Для настройки срока действия ключей необходимо выполнить следующие шаги:

1. В меню раздела «**Settings**» выбрать пункт «**Настройка срока действия ключей**»;

Рисунок 53. Раздел "Settings". Настройка срока действия ключей

2. В блоке параметров «**Настройка срока действия ключей**» (Рисунок 53. Раздел "Settings". Настройка срока действия ключей) задать следующие параметры:

- **Периодичность проверки** - интервал выполнения проверки в минутах;
 - **Срок действия ZMK** - срок действия ZMK ключей в днях с момента создания;
 - **Срок действия TMK** - срок действия TMK ключей в днях с момента создания.
3. Нажать кнопку **«Save»** для сохранения изменений.

4.11.4. Настройка HSM

Данный блок содержит перечень HSM и параметры взаимодействия с ними.

4.11.4.1. Общие настройки HSM

Для настройки параметров взаимодействия с HSM необходимо выполнить следующие шаги:

1. В меню раздела **«Settings»** выбрать пункт **«Настройка HSM»**;

Рисунок 54. Раздел "Settings". Настройка HSM

2. В блоке параметров **«Настройка HSM»** в секции **«Общие настройки HSM»** (Рисунок 54. Раздел "Settings". Настройка HSM) задать следующие параметры:
 - **Таймаут соединения** - таймаут установления соединения в секундах;
 - **Таймаут ответа** - таймаут получения ответа в секундах;
 - **Время неактивности соединения** - время удержания соединения в отсутствие обмена в секундах;
3. Нажать кнопку **«Save»** для сохранения изменений.

Чтобы изменения вступили в силу необходимо перезапустить сервер KDH (см. [KDH Setup Guide.pdf](#)).

4.11.4.2. Список HSM

Данная секция содержит список HSM и инструменты для работы (добавление/удаление) с ним.

Добавление HSM

Для добавления HSM необходимо выполнить следующие шаги:

1. Нажать на кнопку  в разделе **«Settings»** в блоке параметров **«Настройки HSM»** в секции **«Список HSM»** (Рисунок 54. Раздел "Settings". Настройка HSM);

2. Задать следующие параметры в добавленной строке:
 - IP адрес или название хоста HSM;
 - TCP/IP порт HSM;
 - Размер пула соединений - количество одновременных соединений.

3. Нажать кнопку «Save» для сохранения изменений.

Чтобы изменения вступили в силу необходимо перезапустить сервер KDH (см. [KDH Setup Guide.pdf](#)).

Удаление HSM

Для Удаления HSM необходимо выполнить следующие шаги:

1. В разделе «Settings» в блоке параметров «Настройки HSM» в секции «Список HSM»

(Рисунок 54. Раздел "Settings". Настройка HSM) нажать на кнопку  в конце строки, которую необходимо удалить. Выбранная строка будет удалена из списка HSM.

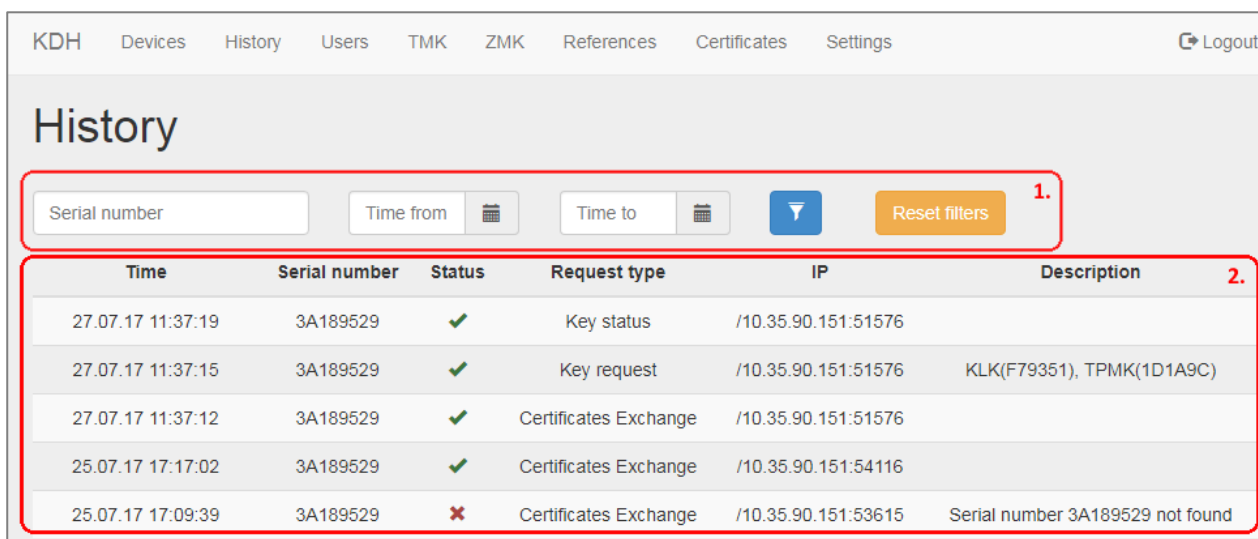
2. Нажать кнопку «Save» для сохранения изменений.

Чтобы изменения вступили в силу необходимо перезапустить сервер KDH (см. [KDH Setup Guide.pdf](#)).

4.12. Просмотр истории (History)

Данный раздел содержит историю запросов от POS-терминалов на KDH.

Переход в раздел осуществляется по выбору пункта «History» в главном меню.



Time	Serial number	Status	Request type	IP	Description
27.07.17 11:37:19	3A189529	✓	Key status	/10.35.90.151:51576	
27.07.17 11:37:15	3A189529	✓	Key request	/10.35.90.151:51576	KLK(F79351), TPKK(1D1A9C)
27.07.17 11:37:12	3A189529	✓	Certificates Exchange	/10.35.90.151:51576	
25.07.17 17:17:02	3A189529	✓	Certificates Exchange	/10.35.90.151:54116	
25.07.17 17:09:39	3A189529	✗	Certificates Exchange	/10.35.90.151:53615	Serial number 3A189529 not found

Рисунок 55. Раздел "History"

Данный раздел содержит:

- Фильтр (область 1. на Рисунок 55. Раздел "History");
- Информацию по запросам от POS-терминалов на KDH (область 2. на Рисунок 55. Раздел "History").

Фильтр

Фильтр (область 1. на Рисунок 55. Раздел "History") позволяет осуществить поиск нужной информации используя следующие поля для фильтрации данных:

- Serial number - серийный номер POS-терминала;
- Time from – время от;
- Time to – время до.

Для применения фильтра к данным необходимо нажать кнопку .

Для сброса установленных значений фильтра необходимо нажать кнопку .

Информация по запросам от POS-терминалов на KDH

Информация имеет табличное представление (область 2. на Рисунок 55. Раздел "History"). Данные разбиты по следующим столбцам:

- **Time** - дата и время события;
- **Serial number** - серийный номер POS-терминала;
- **Status** - результат обращения: успех или ошибка;
- **Request type** - тип запроса. (**Certificates Exchange** – обмен сертификатами, **Key request** – запрос ТМК ключей, **Key status** – изменение статуса ключей);
- **IP** - IP-адрес, с которого был выполнен запрос;
- **Description** - дополнительное описание.

5. Порядок настройки стенда для работы с RKL

Данный раздел содержит последовательность действий, необходимых для подготовки различных компонент решения для взаимодействия при работе с RKL, а также ссылки на соответствующие разделы и документы с подробным описанием их выполнения.

В данном разделе описывается подготовка следующих компонент: «UCM», «POS-терминал», «KDH».

5.1. Подготовка компонент к работе с RKL

5.1.1. Подготовка UCM

1. Настроить работу плагина RKL:
 - а. Положить файл плагина «**RKLPlugin.dll**» в папку Download Server: «...**Download server**\Scripts**RKLPlugin.dll**».
 - б. В «UCM» в окне «**Настройки Download Server**» в блоке «**Доп. настройка сервера RKL**» установить следующие значения (Рисунок 56. Доп. настройки сервера RKL):

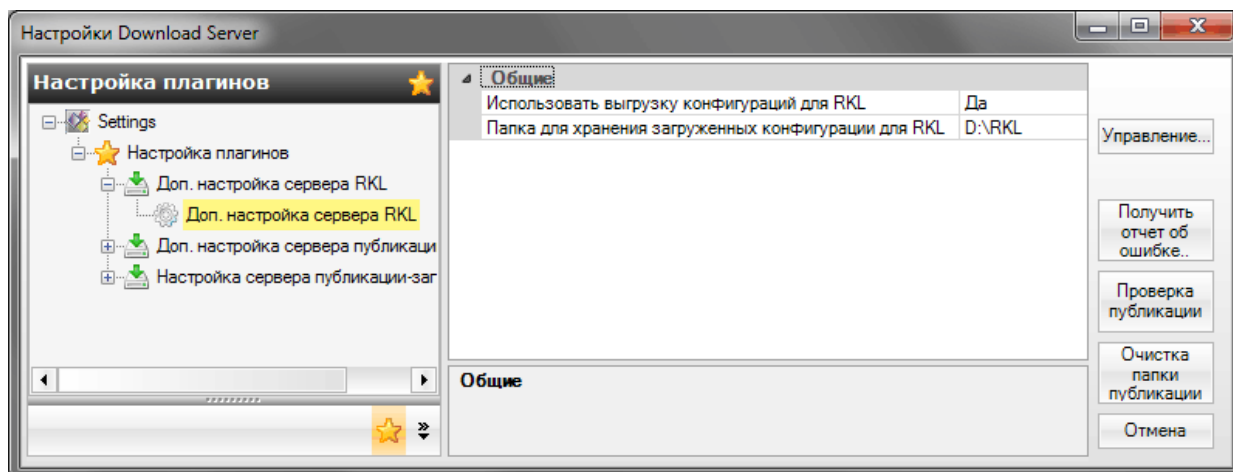


Рисунок 56. Доп. настройки сервера RKL

- **Использовать выгрузку конфигураций RKL** – Да.
- **Папка для хранения загруженных конфигураций для RKL** – задать путь сохранения файла конфигурации ключей.

5.1.2. Подготовка POS-терминала

1. Данный пункт выполняется сотрудниками ИНПАС.

Выполнить инициализацию POS-терминала (загрузка ПО Unipos, RSA-ключей и сертификатов).

Процесс инициализации подробно описан в документах:

- Инициализация PAX Monitor для RKL.pdf;
- Инициализация PAX Prolin для RKL.pdf;
- Инициализация Verifone для RKL.pdf.

5.1.3. Генерация ZMK

На HSM Банка выполняется генерация ZMK под LMK. Затем выполняется печать трех PIN-конвертов, содержащих компоненты сгенерированного ZMK-ключа, один конверт = одна компонента ZMK-ключа, всего 3 конверта/компоненты. Далее необходимо ввести данный ZMK под LMK в HSM, который подключен к KDH. Для этого офицеры безопасности, используя консоль HSM, подключенного к KDH, покомпонентно вводят ZMK-ключ. HSM собирает ZMK ключ из компонент и шифрует на своем LMK. В KDH вводится криптограмма ZMK под LMK того HSM, который подключен к KDH.

5.1.4. Подготовка KDH

1. Загрузить сертификаты:
 - a. Выполнить генерацию запроса на сертификат KDH (см. п. [4.6.3.1 Генерация запроса на сертификат KDH](#)) и обратиться в УЦ ИНПАС за выпуском сертификатов;
 - b. Выполнить загрузку полученных от ИНПАС сертификатов, соблюдая следующую последовательность:
 - i. Корневой сертификат (см. п. [4.6.1 Загрузка корневого сертификата «Root certificate»](#));
 - ii. CRL лист (см. п. [4.6.4 Загрузка CRL листа «Certificates Revocation List»](#));
 - iii. Промежуточный сертификат (см. п. [4.6.2 Загрузка сертификата промежуточного УЦ «RKL certificate»](#));
 - iv. Сертификат KDH (см. п. [4.6.3.2 Загрузка сертификата KDH](#)).
2. Добавить банки (см. п. [4.10.2.1 Добавление банка](#)) и хосты (см. п. [4.10.1.1 Добавление хоста](#));
3. Добавить ZMK для заведенного на предыдущем шаге хоста/банка (см. п. [4.7.2 Добавление ZMK](#));
4. Загрузить ТМК ключи для хоста, добавленного на шаге 4 (см. п. [4.8.2 Загрузка списка мастер ключей \(ТМК\)](#));
5. Загрузить список S/N POS-терминалов (см. п. [4.9.2 Загрузка списка S/N устройств \(POS-терминалов\)](#)).

5.2. Подготовка и загрузка конфигурации

5.2.1. Подготовка конфигурации в UCM

1. Подготовить конфигурацию для загрузки в POS-терминал:
 - a. В справочнике «**Терминалы**» в блоке параметров «**Общие**» задать следующие значения параметров:
 - **Идентификатор терминала** – S/N устройства POS-терминала;
 - **Серийный номер** - S/N устройства POS-терминала;
 - **Идентификатор хоста** – ID хоста для RKL (уникальный идентификатор хоста (Host) на KDH).
 - b. В справочнике «**Профили ключей**» настроить конфигурацию мастер ключей с указанием типа ключей и номеров ячеек и привязать ее к POS-терминалу.

5.2.2. Загрузка конфигурации в POS-терминал

1. Выполнить загрузку параметров из Config Manager. «**Config Manager**» выполнит генерацию файла с конфигурацией ключей и сохранит по указанному на шаге 1.2 пути.

5.2.3. Загрузка конфигурации в KDH

1. Загрузить файл(ы) с конфигурацией(ями) ключей (см. п. [4.9.3 Загрузка файла с конфигурацией ключей](#)).

5.3. Загрузка ТМК

5.3.1. Загрузка ключей в POS-терминал

1. В «**KeyInstaller**» настроить соединение с сервером KDH «**Параметры**» / «**Редактирование**» / «**Сервер KDH**».

Примечание: Если на POS-терминале используется версия ПО, которая работает только по SSL, то, так как KDH не поддерживает работу по SSL, необходимо настроить соединение POS-терминала с KDH через Stunnel (SSL сервер), предварительно загрузив файл с доверенным сертификатом SSL-сервера в POS-терминал.

2. Инициировать загрузку ключей с KDH «**Загрузка ключей**» / «**С сервера KDH**».

6. Приложения

Форматы файлов обмена KDH возможно посмотреть в следующих файлах:

- KDH для OW Схема взаимодействия;
- KDH для PSP Схема взаимодействия;
- Описание форматов файлов обмена для GazPromBank;
- Описание форматов файлов обмена для Тинькофф.