СОМЕРС
ПОС

Remote Key Management

Руководство по установке и настройке

Версия: 3.00

ОГЛАВЛЕНИЕ

ИСТОРИЯ ИЗМЕНЕНИЙ

Версия документа	Дата изменения	Автор	Описание
3.00	05/04/2025	Шмидт В.В.	Ребрендинг документа на основе документа версии 2.00.

ГЛОССАРИЙ

Термин	Расшифровка
SomersRKM	Программно-аппаратный комплекс для управления удалённой загрузкой ключей (Remote Key Manager).
POS	Терминал, предназначенный для приёма банковских карт для осуществления безналичных платежей.
CA	Certificate Authentification, процедура аутентификации сертификата.
SomersCA	Сервис CA – составная часть SomersRKM, осуществляет процедуру CA, далее – Сервис Загрузки Сертификатов, СЗС.
RKI	Remote Key Injection, процедура удаленной загрузки ключей.
SomersRKI	Сервис RKI – составная часть SomersRKM, осуществляет процедуру передачи криптографических мастер-ключей, далее – Сервис Загрузки Ключей, СЗК.
HSM	Hardware Security Module, программно-аппаратный криптографический модуль.
SomersHSM	Программно-аппаратный комплекс, состоящий из POS-терминала и специализи-рованного ПО, выполняющий функции HSM, в текущей схеме работает в режиме SomersHSM CA Mode (используемый для авторизации целевого терминала.
PCI DSS	Payment Card Industry Data Security Standard, стандарт безопасности данных индустрии платежных карт.
PCI PIN Security	Payment Card Industry PIN Security Requirements, требования безопасности индустрии платежных карт по управлению, обработке и передаче данных ПИН-кода держателя карты и дистрибуции криптографических ключей.
TMS	Terminal Management System, система параметризации POS терминалов.
TID	Terminal ID, уникальный идентификатор терминала в системе.
ZMK	Zone Master Key, специальный криптографический ключ 3DES, которым шифруются все ключи данных, используемые для обмена информацией между двумя субъектами. ZMK используется для передачи TMK в SomersRKM.
TMK	Terminal Master Key, специальный криптографический ключ, который используется для шифрования / дешифрования сессионных (рабочих) ключей шифрования данных (TPK или TAK) для передачи их с хоста на POS-терминал.
KCV	Key Check Value, контрольная сумма ключа.
ПЦ TPTP	Процессинговый центр Банка, работающий на протоколе TPTP, отвечающий за обработку транзакций, генерацию рабочих ключей и т.п.

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 установки компонент системы SomersRKM – программно-аппаратного комплекса, 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 безопасная автоматическая удаленная загрузка комплекта начальных криптографических мастер-ключей в платежные терминалы, предназначенные для установки в торгово-сервисные предприятия и банки.
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);
- веб-интерфейс – многопользовательский доступ к функционалу СЗК и СЗС с возможностью распределения функционала.
- HSM – устройство, которое генерирует ключи, для последующей загрузки в целевые терминалы (ключи передаются в зашифрованном виде).

2. УСТАНОВКА SOMERSRKM

В этом разделе содержится описание процесса установки программного продукта SomersRKM в инфраструктуре банка.

Убедитесь, что Вы зарегистрированы на сервисах Сомерс и у Вас есть учетная запись для обращения к облачным хранилищам RKM.
Для получения учетной записи (Логин и Пароль) напишите письмо на адрес технической поддержки support@sky-technologies.ru, в ответ Вам будет отправлен Логин и Пароль.

2.1. Комплект поставки

Система SomersRKM поставляется в виде трех docker контейнеров и двух .zip архивов следующего содержания:

- Архив CA – архив для установки Сервиса Загрузки Сертификатов:
  - папка rkl-ca – папка с файлами для работы Сервиса Загрузки Сертификатов;
  - папка rkl-sec – папка с файлами для работы системы SomersRKM (offline) в целом.
  - файл .env – параметры приложения;
  - файл docker-compose.yml – скрипт для работы с docker контейнером (пример содержания файл см. ПРИЛОЖЕНИЕ 1. ПРИМЕРЫ ФАЙЛОВ DOCKER);
- Архив RKI – архив для установки Сервиса Загрузки Ключей:
  - папка rkl-keys – папка с файлами для работы Сервиса Загрузки Ключей;
  - папка rkl-sec – папка с файлами для работы системы SomersRKM (offline) в целом.
  - файл .env – параметры приложения;
  - файл docker-compose.yml – скрипт для работы с docker контейнером (пример содержания файл см. ПРИЛОЖЕНИЕ 1. ПРИМЕРЫ ФАЙЛОВ DOCKER);

Для SomersRKL (offline) с функционалом автоматических отчетов о загруженных ключах в комплект поставки включена дополнительная папка reports – изначально эта папка пустая, в дальнейшем в нее будут выгружаться файлы отчетов.

Во всех папках реализована следующая вложенная структура:

- Папка conf – содержит файлы конфигурации компонент системы:
  - ptconfig.properties – основной конфигурационный файл;
  - log4j2.xml – файл с настройками логирования;
  - logging.properties – файлы для настройки журналов работы системы.
  - log4j.properties – параметры логирования;
- Папка logs – содержит файлы логирования:
  - access.txt;
  - platform.txt.

2.2. Системные требования

Сервер, на котором будет установлены компоненты SomersRKM должен соответствовать следующим системным требованиям:

- **Операционная система**: Linux family: Oracle Linux; Red Hat Enterprise Linux; CentOS; Ubuntu Server.
- **ОЗУ:** 8 Гб и более.

- Свободное место на HDD: 100 Гб и более
- **Частота CPU**: 2.67GHz (например Intel(R) Xeon(R) X5650) и выше.
- **СУБД**: Oracle 18c / MariaDB 10.
- **Система виртуализации**: дополнительные требования отсутствуют.

Производительность системы при соблюдении данных Системных требований - 600 операций шифрования-расшифрования в секунду. Добиться большего числа операций возможно увеличением производительности инфраструктуры.

2.3. Установка с использованием Docker

2.3.1. Установка и обновление Docker

Для работы с продуктами Сомерс необходимо использовать Docker.
Выполните его установку перед установкой системы.
Для установки на ОС Linux используется пакетный менеджер, например, **yum install docker** или **apt install docker**.
Для серверов с ОС Windows: установите Docker.

Одним из требований Docker для Windows является наличие компоненты WSL. Инструкция по установке доступна по ссылке: https://docs.microsoft.com/ru-ru/windows/wsl/install-win10.

Убедитесь, что для Docker установлены все обновления, чтобы их установка не помешала установке SomersRKM (online).

2.3.2. Получение образов решения из репозитория registry.skypos.ru

Убедитесь, что аппаратные средства соответствуют минимальным требованиям и существует доступ к серверам Сомерс с репозитариями компонент SomersRKM (offline) - проверьте доступ командой ping registry.skypos.ru.

Для скачивания образов решения и запуска используется технология docker-compose.
1. Распакуйте содержимое .zip архивов в корневую папку сервера.

Убедитесь, что для Docker установлены все обновления, чтобы их установка не помешала установке компонент SomersRKM.

2. Перейдите в консоль и запустите команду docker login registry.skypos.ru.
3. Введите Логин и Пароль.

Если при вводе пароля отобразилась ошибка 401 Unauthorized Логин и Пароль недействительны, обратитесь в техническую поддержку Сомерс для уточнения данных учетной записи.

2.3.3. Распаковка образов решения без репозитория registry.skypos.ru

Компоненты SomersRKM поставляются через любой доступный канал связи.
Загрузите образы компонент SomersRKM (online) в Docker на компьютере:
1. Распакуйте zip-архив images.zip в корневую папку диска.
2. Загрузите файлы RKM в Docker двумя последовательными командами из C:\images:
   - docker load -i rkm.tar;
   - docker load -i oracle.tar.

3. Создайте в каталоге C:\images папку для базы данных RKM:
   - для Сервиса Загрузки Сертификатов: *C:\images\ca-db-oracle*;
   - для Сервиса Загрузки C:\images\rki-db-oracle.
4. Распакуйте zip-архив в корневую папку диска:
   - /rkm/ca для Сервиса Загрузки Сертификатов;
   - /rkm/rki для Сервиса Загрузки Ключей.
5. В файле .env в переменной ORACLE_DATA определите директорию для файлов базы данных (например, C:\images\rki-db-oracle, примеры содержания файлов см. ПРИЛОЖЕНИЕ 2. ПРИМЕРЫ ФАЙЛОВ .ENV).

2.3.4. Установка образов решений

1. Запустите установку RKM из папки в Docker:

```
docker-compose up –d.
```

2. Для контроля процесса установки можно использовать логгер:

```
docker-compose logs –f.
```

После завершения установки и запуска компонент SomersRKM может потребоваться до 20 минут для построения таблиц базы данных Oracle.
После завершения на экране отобразится сообщение DATABASE READY.
Приступайте к работе с системой не раньше этого времени.

3. Запустите интернет-обозреватель и введите адрес:
   - SomersRKM (online): http://localhost:9220/web/rkl;
   - SomersRKM (offline):
     - для Сервиса Загрузки Сертификатов: http://localhost:9220/web/ca;
     - для Сервиса Загрузки Ключей http://localhost:9220/web/rki.
4. На экране отобразится страница входа в соответствующую компоненту SomersRKM.

Для первоначальной авторизации используйте логин admin и пароль admin1.
Системный администратор может назначить произвольную URL для веб-интерфейса RKM, развёрнутого на сервере.

3. НАСТРОЙКА МОДУЛЕЙ

Основные настройки SomersRKM задаются в файлах ptconfig.properties, которые расположены в соответствующих папках комплекта поставки.

3.1. Общие параметры SomersRKM

Основные настройки SomersRKM задаются в файле ptconfig.properties, расположенный в папке \rkl_online\rkl-sec\conf. Этот файл содержит следующие параметры:

- logging.level.root – уровень логирования, необходим для формирования лог файлов при возникновении технических проблем и при тестировании;

Не рекомендуется раскомментировать параметр при использовании SomersRKM в реальной среде.

- db.user – логин для подключения к базе данных;
- db.pass – пароль для подключения к базе данных;
- db.url – ссылка для подключения к базе данных;
- ha.members – IP адреса модулей rkl-ca, rkl-keys и rkl-sec внутри docker-сети (параметр hazelcast необходим для корректоной работы микросервисной архитектуры;
- ha.port – порт по которому передаются данные внутри hazelcast сети;
- ha.name – наименование модуля (rkl-sec) внутри hazelcast сети;
- server.address.link – полный адрес, на котором развернут rkl-sec модуль, необходим для формирования корректной ссылки на восстановление пароля;
- server.port – порт веб-модуля (пользовательского интерфейса);
- rki.server.port – номер порта, на который должен приходить запрос от Целевых терминалов (например, номер порта, заданного в server.port +1);
- node – служебное поле, необходимое для настройки связи между модулями, не рекомендуется менять предустановленное значение данного параметра;
- vaadin.urlMapping – базовый путь по которому открывается WEB интерфейс;
- ovaadin.productionMode – служебный параметр, определяющий режим работы, не рекомендуется изменять значение параметра;
- spring.profiles.active – профили приложения, доступные значения:
  - oracle – при использовании БД oracle;
  - mysql – при использовании БД mariaDB или mysql;

При использовании mariaDB добавьте строчку sql.scripts=mysql/default-data-mysql.sql сразу после параметра db.url.

  - и др. – список доступных параметров зависит от предоставляемого функционала и предоставляется Сомерс;
- keysearch.table – режим отображения страницы Key search, служебное поле, менять не рекомендуется;
- log_off_time – время до разлогинивания при бездействии (в миллисекундах).
- restore.password.link.lifetime – время жизни ссылки на восстановление пароля (в секундах).
- caHsm – HSM, с которым будет взаимодействовать СЗС (значение параметра зависит от типа HSM, запросите значение в Сомерс);
- rkiHsm – HSM, с которым будет взаимодействовать СЗК (значение параметра зависит от типа HSM, запросите значение в Сомерс);

- safeNet.slot – слот HSM – применимо только при использовании HSM SafeNet;
- safeNet.pin – ПИН HSM – применимо только при использовании HSM SafeNet;
- hsm.safenet.host – адрес HSM – применимо только при использовании HSM SafeNet;
- hsm.safenet.port – порт HSM – применимо только при использовании HSM SafeNet;
- hsm.thales.host – адрес доступа к основному HSM (Thales);
- hsm.thales.port – порт доступа к основному HSM (Thales);
- hsm.thales.cell - ячейка в которой лежит Thales key block LMK;
- hsm.readTimeOut – таймаут чтения данных с HSM;
- hsm.connectTimeOut – таймаут подключения к HSM.

Пример файла SomersRKM_ptconfig.properties

```
# Database settings
db.user=login
db.pass=password
db.url=url

ha.members=172.18.0.11,172.18.0.12,172.18.0.13
ha.port=5701
ha.name=hazelcastRKL
node=RKL-SEC

hsm.readTimeOut=5
hsm.connectTimeOut=5
hsm.thales.cell=01
hsm.thales.host=1.1.1.1
hsm.thales.port=1500

server.address.link=http://app-rkipos01.open.ru:9220
server.port=9220
rki.server.port=9221

vaadin.urlMapping=/web/rkl/*
vaadin.productionMode=true

spring.profiles.active=hsm.thales,inputPageTF, oracle

keysearch.table=on
restore.password.link.lifetime=86400
```

3.2. Параметры Сервиса загрузки сертификатов (rkl-ca)

3.2.1. Файл web-ca\rkl-ca\conf\ptconfig.properties

Параметры:

- db.user – логин для подключения к базе данных СЗС;
- db.pass – пароль для подключения к базе данных СЗС;
- db.url – ссылка для подключения к базе данных СЗС;
- spring.profiles.active – профили приложения;

- ha.members – IP адреса модулей rkl-ca, rkl-keys и rkl-sec внутри docker-сети (параметр
- ha.port – порт по которому передаются данные внутри hazelcast сети;
- ha.name – наименование модуля (rkl-sec) внутри hazelcast сети;
- node – служебное поле, необходимое для настройки связи между модулями, не рекомендуется менять предустановленное значение данного параметра;
- ca.server.port – номер порта, на который должен приходить запрос от Целевых терминалов.

Пример файла web-ca\rkl-ca\conf\ptconfig.properties

```
 # Database settings
db.user=user
db.pass=password
db.url=jdbc:oracle:thin:@172.16.18.10:1521/XEPDB1
spring.profiles.active=oracle
ha.members=172.18.0.11,172.18.0.12
ha.port=5701
ha.name=hazelcastRKL
node=RKL-CA
ca.server.port=9227
```

3.2.2. Файл rkl-sec\conf\ptconfig.properties

Параметры:

db.user – логин для подключения к базе данных;
db.pass – пароль для подключения к базе данных;
db.url – ссылка для подключения к базе данных;
spring.profiles.active – профили приложения, доступные значения:
oracle – при использовании БД oracle;
mysql – при использовании БД mariaDB или mysql;

При использовании mariaDB добавьте строчку sql.scripts=mysql/default-data-mysql.sql сразу после параметра db.url.

и др. – список доступных параметров зависит от предоставляемого функционала и предоставляется Сомерс;
ha.members – IP адреса модулей rkl-ca, rkl-keys и rkl-sec внутри docker-сети (параметр hazelcast необходим для корректоной работы микросервисной архитектуры;
ha.port – порт по которому передаются данные внутри hazelcast сети;
ha.name – наименование модуля (rkl-sec) внутри hazelcast сети;
node – служебное поле, необходимое для настройки связи между модулями, не рекомендуется менять предустановленное значение данного параметра;
server.address.link – полный адрес, на котором развернут rkl-sec модуль, необходим для формирования корректной ссылки на востановление пароля;
server.port – порт веб-модуля;
rki.server.port – номер порта, на который должен приходить запрос от Целевых терминалов;
vaadin.urlMapping – базовый путь по которому открывается WEB интерфейс;
ovaadin.productionMode – служебный параметр, определяющий режим работы, не рекомендуется изменять значение параметра;
keysearch.table – режим отображения страницы Key search, служебное поле, менять не рекомендуется;

safeNet.slot – слот HSM – применимо только при использовании HSM SafeNet, значение определяется Администратором HSM.
safeNet.pin – ПИН HSM – применимо только при использовании HSM SafeNet, значение определяется Администратором HSM.
log_off_time – время до разлогинивания при бездействии (в миллисекундах).

Пример файла web-ca\rkl-sec\conf\ptconfig.properties

```
# Database settings
db.user=user
db.pass=password
db.url=jdbc:oracle:thin:@172.16.18.10:1521/XEPDB1
# Network settings
ha.members=172.18.0.11,172.18.0.12
ha.port=5701
ha.name=hazelcastRKL
server.address.link=rkl2.skypos.ru
server.port=9222
rki.server.port=9223
node=RKL-SEC
vaadin.urlMapping=/web/rkl/*
ovaadin.productionMode=true
spring.profiles.active=wl.ca.page,log.ca.page,setting.ca.page,crt.conf.page,oracle
log_off_time=600000
keysearch.table=on
```

3.3. Настройка Сервиса Загрузки Ключей (rkl-keys)

3.3.1. Файл web-rki\rkl-keys\conf\ptconfig.properties

Параметры:

- db.user – логин для подключения к базе данных СЗК;
- db.pass – пароль для подключения к базе данных СЗК;
- db.url – ссылка для подключения к базе данных СЗК;
- ha.members – IP адреса модулей rkl-ca, rkl-keys и rkl-sec внутри docker-сети (параметр hazelcast необходим для корректоной работы микросервисной архитектуры;
- ha.port – порт по которому передаются данные внутри hazelcast сети;
- ha.name – наименование модуля (rkl-sec) внутри hazelcast сети;
- node – служебное поле, необходимое для настройки связи между модулями, не рекомендуется менять предустановленное значение данного параметра;
- rki.server.port – номер порта, на который должен приходить запрос от Целевых терминалов.

Пример файла web-rki\rkl-keys\conf\ptconfig.properties

```
# Database settings
db.user=user                                    // логин в используемую базу записей СЗК
db.pass=password                                // пароль в используемую базу записей СЗК
db.url=jdbc:oracle:thin:@172.16.18.10:1521/XEPDB1 // адрес используемой базы СЗК
```

```
# Network settings
ha.members=172.18.1.11,172.18.1.13
ha.port=5701
ha.name=hazelcastRKL
node=RKL-KEYS
rki.server.port=9228
```

3.3.2. Файл web-rki\rkl-sec\conf\ptconfig.properties

Параметры:

- db.user – логин для подключения к базе данных;
- db.pass – пароль для подключения к базе данных;
- db.url – ссылка для подключения к базе данных;
- spring.profiles.active – профили приложения, доступные значения:
  - oracle – при использовании БД oracle;
  - mysql – при использовании БД mariaDB или mysql;

> *При использовании mariaDB добавьте строчку sql.scripts=mysql/default-data-mysql.sql сразу после параметра db.url.*

  - и др. – список доступных параметров зависит от предоставляемого функционала и предоставляется Сомерс;
- ha.members – IP адреса модулей rkl-ca, rkl-keys и rkl-sec внутри docker-сети (параметр hazelcast необходим для корректоной работы микросервисной архитектуры;
- ha.port – порт по которому передаются данные внутри hazelcast сети;
- ha.name – наименование модуля (rkl-sec) внутри hazelcast сети;
- node – служебное поле, необходимое для настройки связи между модулями, не рекомендуется менять предустановленное значение данного параметра;
- server.address.link – полный адрес, на котором развернут rkl-sec модуль, необходим для формирования корректной ссылки на востановление пароля;
- server.port – порт веб-модуля;
- rki.server.port – номер порта, на который должен приходить запрос от Целевых терминалов;
- vaadin.urlMapping – базовый путь по которому открывается WEB интерфейс;
- ovaadin.productionMode – служебный параметр, определяющий режим работы, не рекомендуется изменять значение параметра;
- vaadin.closeIdleSessions;
- keysearch.table – режим отображения страницы Key search, служебное поле, менять не рекомендуется;
- log_off_time – время до разлогинивания при бездействии (в миллисекундах).

Пример файла web-rki\rkl-sec\conf\ptconfig.properties

```
# Database settings
db.user=user  // логин в используемую базу записей веб-интерефейс
db.pass=password                                    // логин в используемую базу записей веб-интерефейса
db.url=jdbc:oracle:thin:@172.16.18.10:1521/XEPDB1 // адрес используемой базы записей веб-интерфейса
```

```
# Network settings
ha.members=172.18.1.11,172.18.1.13
ha.port=5701
ha.name=hazelcastRKL
server.address.link=rkl.skypos.ru
server.port=9222
rki.server.port=9223
node=RKL-SEC
vaadin.urlMapping=/web/rkl/*
ovaadin.productionMode=true
vaadin.closeIdleSessions=true
spring.profiles.active=wl.rki.page,log.rki.page,key.search.tab.page,key.import.tab.page,setting.rki.p
age,input.page.table,host.man.page,oracle
log_off_time=600000
keysearch.table=on
```

4. НАСТРОЙКИ SOMERSMDM

4.1. Настройка хостов

Для того, чтобы целевые терминалы смогли подключиться к компонентам SomersRKM в SomersMDM необходимо:

- настроить Хосты для подключения к сервису CA и RKI, диалект - TLV;
- объединить созданные профили в Профиль хостов или добавить их к существующему Профилю хостов;
- привязать созданный Профиль хостов к конфигурации целевого терминала, если он не привязан.

4.2. Настройка параметров ключей

Если в SomersRKM в разделе Настройки RKI при настройке параметров ключей активирован параметр «Строгая проверка Host_ID» в конфигурации терминала в параметрах Банковского терминала необходимо задать значение параметра Host ID. Это значение должно совпадать с названием хоста, указанном в

4.3. Настройка пользователя API

Для того, чтобы SomersMDM и SomersRKL могли взаимодействовать по API необходимо задать пользователя в разделе Настройки MDM – Конфигурации MDM – Настройки внешнего УЗК.

5. УПРАВЛЕНИЕ СЕРВИСАМИ SOMERSRKM

Для того, чтобы управлять компонентами сервиса SomersRKM:
1. перейдите в корневую директорию компонент SomersRKM;
2. выполните команду:

```
docker login registry.skypos.ru
```

3. последовательно введите Логин и Пароль.

Если Логин и Пароль недействительны, на экране отобразится ошибка:
401 Unauthorized
Обратитесь в Сомерс за уточнением данных учетной записи.

Используйте следующие команды для управления:

- docker-compose stop - остановки сервиса;
- docker-compose up –d – запуск сервиса;
- docker-compose down – удаление всех образов сервисов.

При удалении всех образов сервисов файлы логирования и конфигурационные файлы не удаляются.

5.1. Обновление

Для того, чтобы обновить SomersRKM:
1. остановите SomersRKM;
2. замените файл docker-compose.yml на новый (передается в рамках технической поддержки);
3. перезапустите SomersRKM.

5.2. Контроль версий SomersRKM

На данный момент спецификация версии SomersRKM собирается следующим образом:

```
SomersRKM-X.Y.Z-SomersHSM
```

Где:

- X = 1;
- Y – увеличивается при внесении значительных изменений, например, функционала, расширяющего возможности веб-интерфейса SomersRKM;
- Z – увеличивается при внесении незначительных изменений, например, при исправлении бага предыдущего релиза, влиявшего на работоспособность;
- SomersHSM указывает на работу с ПО SomersHSM.

ПРИЛОЖЕНИЕ 1.
ПРИМЕРЫ ФАЙЛОВ DOCKER

Файл web-ca\docker-compose.yml

```
version: '2.1'
services:
    rkl-sec:
        container_name: rkl-sec
        image: ${IMAGE_rklsec}
        restart: always
        volumes:
        - /opt/rkl/web-ca/rkl-sec/logs:/logs
        - /opt/rkl/web-ca/rkl-sec/conf:/conf
        cap_add:
        - SYS_PTRACE
        ports:
        - ${PORT_sec}:9222
        environment:
        - ET_HSM_NETCLIENT_SERVERLIST=172.16.18.10     //Адрес HSM safenet
    - ET_HSM_NETCLIENT_HEARTBEAT=ON
        networks:
            default:
            ipv4_address: 172.18.0.11                  //внутренний адрес в подсети докер.
    rkl-ca:
        container_name: rkl-ca
            image: ${IMAGE_rklca}
            restart: always
            volumes:
            - /opt/rkl/web-ca/rkl-ca/logs:/logs
            - /opt/rkl/web-ca/rkl-ca/conf:/conf
            ports:
            - ${PORT_ca}:9227
    networks:
        default:
            ipv4_address: 172.18.0.12                  //внутренний адрес в подсети докер.
            networks:                                  //настройки подсети докер, необходимы для
                                                       //правильного взаимодействия модулей
        default:
            driver: bridge
            ipam:
            driver: default
            config:
            - subnet: 172.18.0.0/24
            gateway: 172.18.0.1                        // порт для эндпойнта подписи сертификатов
                                                       // клиентских пос-терминалов
```

Файл web-rki\docker-compose.yml

```
version: '2.1'
services:
rkl-sec:
container_name: web-rki-sec
        image: ${IMAGE_rklsec}
        restart: always
        volumes:
        - ./rkl-sec/logs:/logs
        - ./rkl-sec/conf:/conf
        cap_add:
        - SYS_PTRACE
        ports:
        - ${PORT_sec}:9222
        networks:
            default:
            ipv4_address: 172.18.1.11

    rkl-keys:
        container_name: rkl-keys
        image: ${IMAGE_rklkeys}
        restart: always
        volumes:
        - ./rkl-keys/logs:/logs
        - ./rkl-keys/conf:/conf
        ports:
        - ${PORT_keys}:9228
        networks:
            default:
            ipv4_address: 172.18.1.13

    networks:
        default:
        driver: bridge
        ipam:
            driver: default
            config:
                - subnet: 172.18.1.0/24
                gateway: 172.18.1.1
```

ПРИЛОЖЕНИЕ 2.
ПРИМЕРЫ ФАЙЛОВ .ENV

Пример файла web-ca\.env

```
IMAGE_rklsec=registry.skypos.ru/rklsec:v1.1.0      // версия интерфейса офицера безопасности
IMAGE_rklca=registry.skypos.ru/rklca:v1.1.0        // версия сервиса СЗС
LOG_DIR=./rkl_sec/conf
CONF_DIR=./rkl/rkl_sec/conf
PORT_sec=9222                                      // порт для веб-интерфейса офицера
                                                   // безопасности, админа и оператора
PORT_ca=9227
```

Пример файла web-rki\.env

```
IMAGE_rklsec=registry.skypos.ru/rklsec:v1.1.0      // версия интерфейса офицера безопасности
IMAGE_rklca=registry.skypos.ru/rklca:v1.1.0        // версия сервиса СЗС
LOG_DIR=./rkl_sec/conf
CONF_DIR=./rkl/rkl_sec/conf
PORT_sec=9222                                      // порт для веб-интерфейса офицера
                                                   // безопасности, админа и оператора
PORT_ca=9227                                       // порт для эндпойнта подписи сертификатов
                                                   // клиентских POS-терминалов
```

ПРИЛОЖЕНИЕ 3.
СРОК ЖИЗНИ ПАРОЛЯ БД ORACLE

Если для сервисов SomersRKM используется база данных Oracle, может потребоваться выполнить отключение срока жизни пароля, чтобы не возникло непредвиденных сбоев в работе SomersRKM. По умолчанию срок жизни пароля ***для*** подключения к базе данных Oracle составляет 180 дней.

Для того, чтобы снять ограничение на срок жизни пароля выполните следующие действия:

1. Зайдите в Linux под пользователем oracle, а затем авторизуйтесь в БД Oracle под пользователем sys.

```
sqlplus sys/iMC123@orcl as sysdba
```

где

- **sys** – имя пользователя базы данных;
- **iMC123** – пароль пользователя;
- **orcl** – название сетевого сервиса;
- **sysdba** – привилегии администратора, которые позволяют выполнять базовые задачи администрирования.

2. Выполните запрос для отображения срока действия паролей:

```
SQL> select * from dba_profiles s where s.profile='DEFAULT'
and resource_name='PASSWORD_LIFE_TIME';
```

в результате отобразится жизненный срок пароля:

```
PROFILE      RESOURCE_NAME        RESOURCE          LIMIT
-------------------------------------------------------------
DEFAULT    PASSWORD_LIFE_TIME     PASSWORD          180dys
```

т.е. срок жизни пароля для всех пользователей (в Oracle все пользователи имеют общий профиль DEFAULT) составляет 180 дней.

3. Для того, чтобы установить неограниченный жизненный срок паролей пользователей выполните следующую команду:

```
SQL> ALTER PROFILE DEFAULT LIMIT PASSWORD_LIFE_TIME UNLIMITED;
```

4. Обновите пароль пользователя, для которого истек срок действия пароля:

```
SQL> ALTER USER [username] IDENTIFIED BY [new_password];
```

После выполнения этих действий пароли пользователей в БД Oracle будут не ограничены.