

# **KDH (Key Distribution Host)**

## **Руководство по инсталляции**

Версия 3.0.4

### История изменений документа

| Версия | Дата       | Перечень изменений                                                            |
|--------|------------|-------------------------------------------------------------------------------|
| 1.0    | 17.10.2018 | Первоначальная версия документа                                               |
| 1.1    | 21.06.2019 | Обновлены скриншоты и описание установки                                      |
| 1.2    | 22.08.2019 | Обновлен пункт 3.1.11. Добавлен пункт 3.2.                                    |
| 1.3    | 01.11.2019 | Внесены изменения в пункты: «2», «3.1.12», «4.2».                             |
| 1.4    | 13.04.2020 | Обновлены скриншоты и описание установки. Добавлен пункт «3.3»                |
| 1.5    | 07.05.2020 | Добавлены пункты: «8.1», «8.2», «8.3», «8.4», «8.5», «8.6»                    |
| 1.6    | 01.10.2020 | Добавлен пункт «7». В пункт «3.1.13» добавлено «Важно». Добавлен пункт «8.7». |
|        |            |                                                                               |

# Содержание

|                                                       |           |
|-------------------------------------------------------|-----------|
| <b>1. Введение .....</b>                              | <b>4</b>  |
| <b>2. Подготовка к инсталляции .....</b>              | <b>5</b>  |
| <b>3. Инсталляция .....</b>                           | <b>6</b>  |
| 3.1. Инсталляция в обычном режиме .....               | 6         |
| 3.1.1. Запуск инсталлятора.....                       | 6         |
| 3.1.2. Принятие лицензии.....                         | 7         |
| 3.1.3. Выбор каталога для установки .....             | 7         |
| 3.1.4. Выбор каталога для хранения log-файлов.....    | 8         |
| 3.1.5. Копирование файлов.....                        | 8         |
| 3.1.6. Выбор виртуальной машины.....                  | 8         |
| 3.1.7. Выбор компонентов для установки .....          | 9         |
| 3.1.8. Выбор TCP/ IP портов .....                     | 10        |
| 3.1.9. Настройка доступа к web-интерфейсу .....       | 11        |
| 3.1.10. Настройка уведомлений .....                   | 12        |
| 3.1.11. Настройка связи с HSM.....                    | 12        |
| 3.1.12. Настройка папок обмена .....                  | 13        |
| 3.1.13. Настройка доступа к БД .....                  | 14        |
| 3.2. Инсталляция в «Silent-режиме» .....              | 16        |
| 3.2.1. Подготовка к установке.....                    | 16        |
| 3.2.2. Запуск командной строки .....                  | 16        |
| 3.2.3. Выполнение установки в «Silent-режиме» .....   | 16        |
| 3.3. Обновление в «Silent-режиме» .....               | 17        |
| <b>4. Запуск и остановка .....</b>                    | <b>18</b> |
| 4.1. Программа и управление сервером .....            | 18        |
| 4.2. Управление сервером вручную.....                 | 19        |
| <b>5. Диагностика проблем с запуском .....</b>        | <b>21</b> |
| <b>6. Изменение текущей инсталляции.....</b>          | <b>22</b> |
| 6.1. Повторна конфигурация «Reconfigure server» ..... | 22        |
| 6.2. Обновление компонент «Upgrade components» .....  | 22        |
| 6.3. Удаление «Uninstall server» .....                | 22        |
| <b>7. Настройка HTTPS.....</b>                        | <b>23</b> |
| <b>8. Приложение .....</b>                            | <b>25</b> |
| 8.1. kdh-db.properties.....                           | 25        |
| 8.2. kdh-mc-hsm.properties .....                      | 25        |
| 8.3. kdh-sinc.properties.....                         | 25        |
| 8.4. licence.properties.....                          | 25        |
| 8.5. notification.properties .....                    | 26        |
| 8.6. server.properties .....                          | 26        |
| 8.7. x509.properties .....                            | 26        |

## 1. Введение

Данный документ описывает процесс инсталляции сервера загрузки ключей (KDH). Данный документ предназначен для прочтения пользователем, осуществляющим процесс инсталляции KDH.

Требования к аппаратному обеспечению описаны в документациях на соответствующий продукт и зависят от планируемой загрузки системы.

## 2. Подготовка к установке

### MySQL

Необходимо установить «MySQL» версии 5.7.

Добавить в конфигурацию «MySQL» (my.cnf) настройки:

- lower\_case\_table\_names=1 - использование нижнего регистра в наименовании таблиц;
- sql\_mode=STRICT\_TRANS\_TABLES,NO\_ZERO\_IN\_DATE,NO\_ZERO\_DATE,ERROR\_FOR\_DIVISION\_BY\_ZERO,NO\_AUTO\_CREATE\_USER,NO\_ENGINE\_SUBSTITUTION – снимает ограничение на использование «ORDERED BY».

После добавления в конфигурацию «MySQL» (my.cnf) настроек, нужно перезапустить службу «MySQL» (перезагрузить базу данных).

### Java

Для установки на компьютере должна быть установлена Java версии 8. Для установки не имеет значения разрядность (32 или 64) виртуальной машины Java. Инструкции по установке Java: [https://www.java.com/en/download/help/download\\_options.xml](https://www.java.com/en/download/help/download_options.xml).

#### Операционные системы семейства Windows

Для установки на windows системы необходимы права администратора.

#### Операционные системы семейства Linux

Перед установкой необходимо установить программу sudo и bash.

Приложение устанавливается от пользователя «root», но запуск происходит от пользователя «etp-user», который создается в процессе установки, если его нет.

Пользователь, который производит установку, должен принадлежать sudoer'ам.

Операционная система должна иметь графическую подсистему (Gnome или KDE).  
Установленные виртуальные машины Java могут находиться в следующих каталогах:

/usr/lib/jvm, /usr/lib/java, /usr/java, /usr/jvm, /opt.

#### Операционные системы семейства Unix

Установить X-windows (X11) и убедиться, что пользователь с правами root имеет доступ к X-windows.

## 3. Инсталляция

### 3.1. Инсталляция в обычном режиме

#### 3.1.1. Запуск инсталлятора

Разархивируйте ZIP-файл инсталляции в какой-нибудь каталог.  
Запустите системную консоль под правами администратора.

Это можно сделать разными способами, ниже указаны способы для разных операционных систем:

##### Windows XP/2003 Server

Нажмите сочетание клавиш «**Windows+R**» или выберите меню «**Пуск**» пункт «**Выполнить программу**».

##### Windows 7

Нажмите сочетание клавиш «**Windows+R**» и в строку «**Open**» введите «**cmd.exe**», затем нажмите кнопку «**OK**».

Альтернативно, нажмите кнопку «**Start**», напечатайте в строке поиска «**cmd**», в результатах поиска в разделе «**Programs**» нажмите правой кнопкой мыши на найденную программу и выберите пункт «**Run as administrator**».

##### Windows 8.x

Создайте ярлык на рабочем столе и в качестве пути к программе укажите «**c:\windows\system32\cmd**». На закладке «**Security**» поставьте галочку «**Run as administrator**».  
Запустите консоль двойным кликом на созданный ярлык.

##### Windows 2008 Server/2012 Server

Запустите «**Power Shell**» (иконка находится на панели быстрого запуска, рядом с кнопкой Start).

##### Linux

Откройте консоль и выполните команду «**sudo su root**». При необходимости введите пароль.

Выполните команду «**cd c:\sap\_install**» или «**cd /opt/sap\_install**».

Выполните команду «**java -jar install.jar**».

Через некоторое время откроется окно.

### 3.1.2. Принятие лицензии

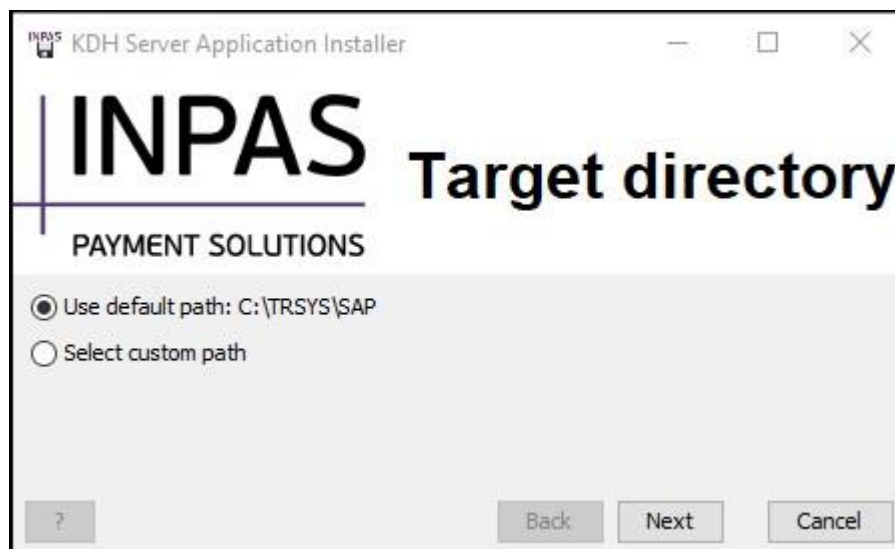
В окне «**License accept**» поставьте галочку «**I accept license**» и нажмите кнопку «**Next**».



### 3.1.3. Выбор каталога для установки

В окне «**Target directory**» выберите каталог для установки:

- **Use default path: C:\TRSYS\SAP** – для выполнения установки в каталог по умолчанию.
- **Select custom path** – для выбора каталога установки.

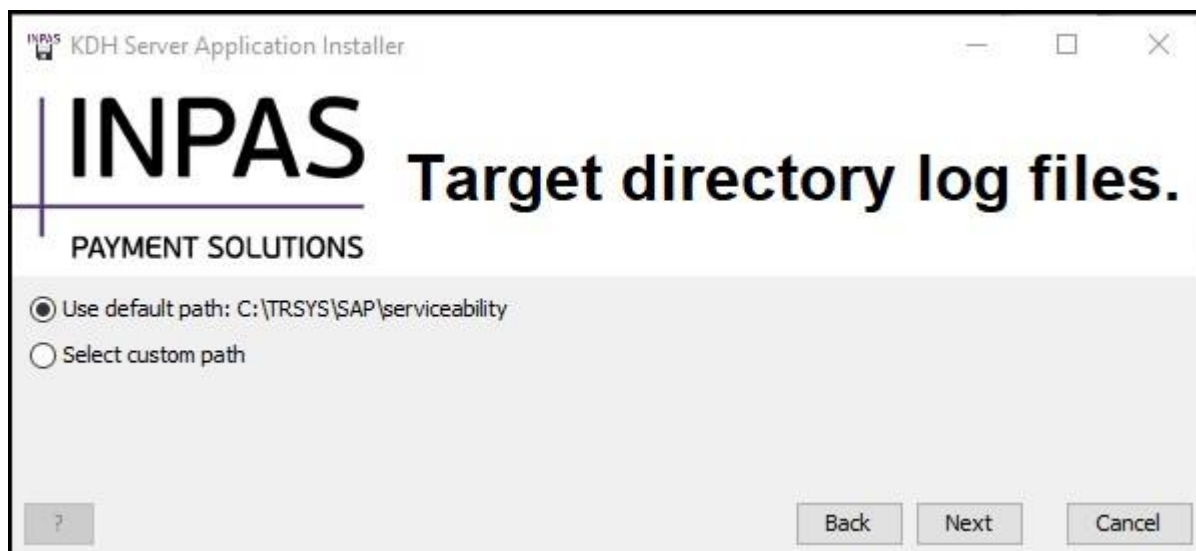


Нажмите кнопку «**Next**». Если заданный каталог не существует, будет предложено создать его.

### 3.1.4. Выбор каталога для хранения log-файлов

В окне «Target directory log files» выберите каталог куда будут сохраняться log-файлы:

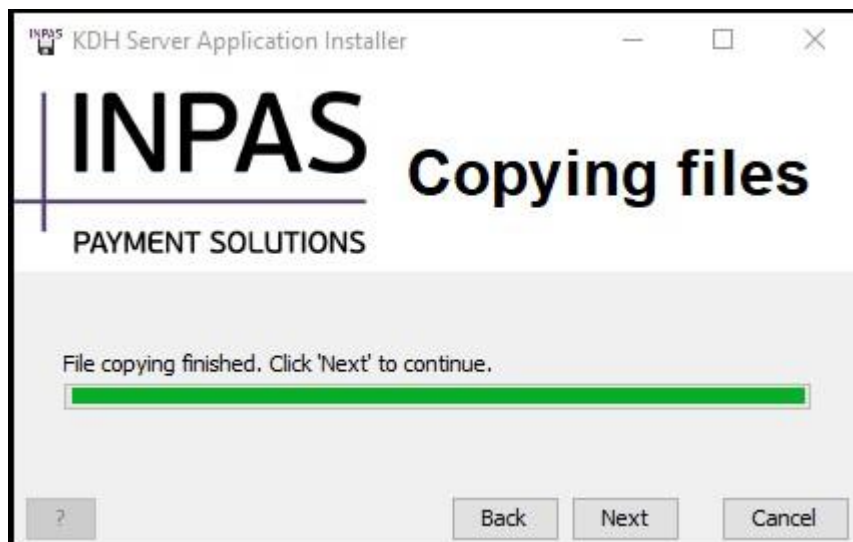
- **Use default path: C:\TRSYS\SAP\serviceability** – для выполнения сохранения в каталог по умолчанию.
- **Select custom path** – для выбора каталога установки.



Нажмите кнопку «**Next**». Если заданный каталог не существует, будет предложено создать его.

### 3.1.5. Копирование файлов

Инсталлятор выполнит копирование файлов серверной платформы.



После завершения копирования нажмите кнопку «**Next**».

### 3.1.6. Выбор виртуальной машины

В окне «Java Runtime Enviroment» выберите виртуальную машину Java.

Для ручного выбора виртуальной машины из списка установленных нужно сначала кликнуть на «**Manual selection**».

Для выбора виртуальной машины, под которой работает инсталлятор, нужно кликнуть на «**Use system JAVA\_PATH variable**»

**Примечание:** в случае, если список пуст (такое возможно на Linux), это означает, что инсталлятор не нашел ни одной виртуальной машины в известных каталогах для поиска (см. *Подготовка к установке*). Завершите выполнение установки, нажав кнопку «**Cancel**», установите виртуальную машину Java и запустите инсталлятор заново.

В параметре «**Maximum java permanent generation size (-XX:MaxPermSize)**» укажите количество резервируемой оперативной памяти для JVM такой, в которой хранятся постоянные сущности системы, например, описание классов.

В параметре «**Maximum java heap size, MB (-Xmx)**» укажите максимальное количество оперативной памяти, которое используется виртуальная машина для внутренней загрузки файлов. Этот параметр имеет значение по умолчанию – 256 Мбайт. Рекомендуемое значение – 1024 Мбайт.

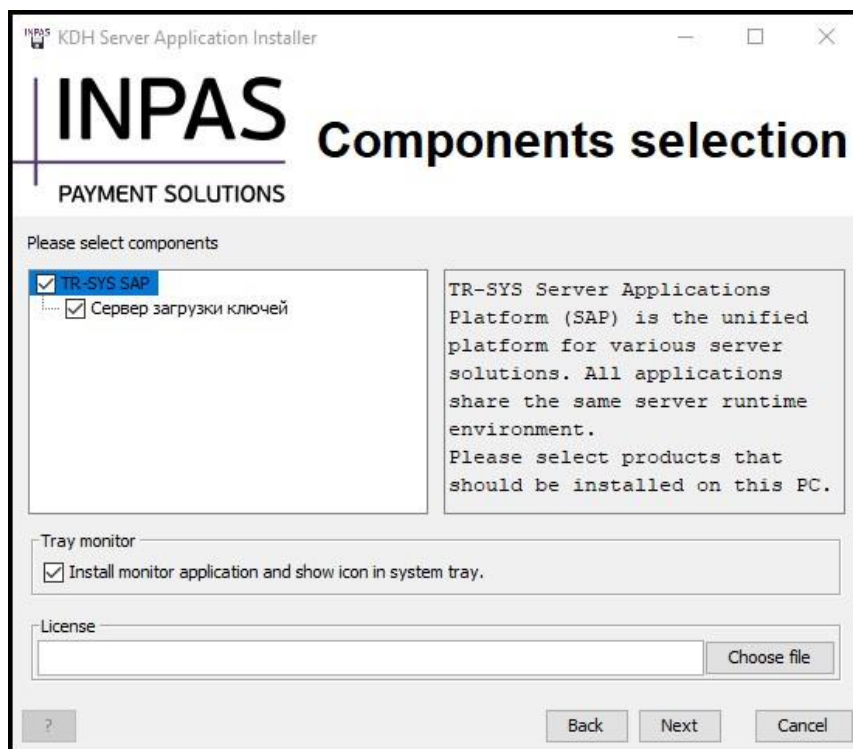
| Type                | Version   | Bits    | Home directory                           |
|---------------------|-----------|---------|------------------------------------------|
| Runtime Environment | 1.8.0_241 | x86     | C:\Program Files (x86)\Java\jre1.8.0_241 |
| Development Kit     | 1.8.0_181 | 64 bits | C:\Program Files\Java\jdk1.8.0_181       |
| Runtime Environment | 1.8.0_241 | 64 bits | C:\Program Files\Java\jre1.8.0_241       |

Выберите виртуальную машину и нажмите кнопку «**Next**».

### 3.1.7. Выбор компонентов для установки

В окне «**Components selection**»:

- Выберите продукт для установки «**Сервер загрузки ключей**».
- Поставьте галочку «**Install monitor application and show icon in system tray**» для установки программы управления сервером KDH и отображения в трее его состояния.
- Укажите файл лицензии в поле «**License**»
- Нажмите кнопку «**Next**» для продолжения установки.



### 3.1.8. Выбор TCP/ IP портов

В окне «**TCP/IP configuration**» укажите TCP/IP порты, которые будет обслуживать система. На эти порты от POS-терминалов будут поступать запросы на удаленную загрузку ключей с KDH.

В списке отображаются текущие используемые порты с указанием номера порта, сетевого интерфейса и режим работы порта.

Справа находятся кнопки удаления, добавления или изменения параметров порта. По нажатию кнопки добавления или изменения порта открывается диалоговое окно, где настраиваются следующие параметры порта:

#### Номер порта (Port).

Номер TCP/IP порта от 1024 до 65535. Данный порт необходимо открыть в брандмауре (см. документацию по Windows) или в iptables (Linux).

#### Режим (Port Mode)

Данная настройка определяет типы подключения терминалов к системе для данного порта. Доступны следующие режимы:

**On demand with TPDU autodetection** - режим, при котором поддерживается автоопределение TPDU для протоколов семейства ISO8583, а также поддерживаются все остальные протоколы с обязательным наличием TPDU. Режим предназначен для обслуживания прямого соединения терминалов с сервером. Если в обслуживающей инфраструктуре терминалы подключены через IEN, то в нем необходимо настроить режим "on demand", то есть по одному TCP/IP соединению на сессию.

#### Port Preset

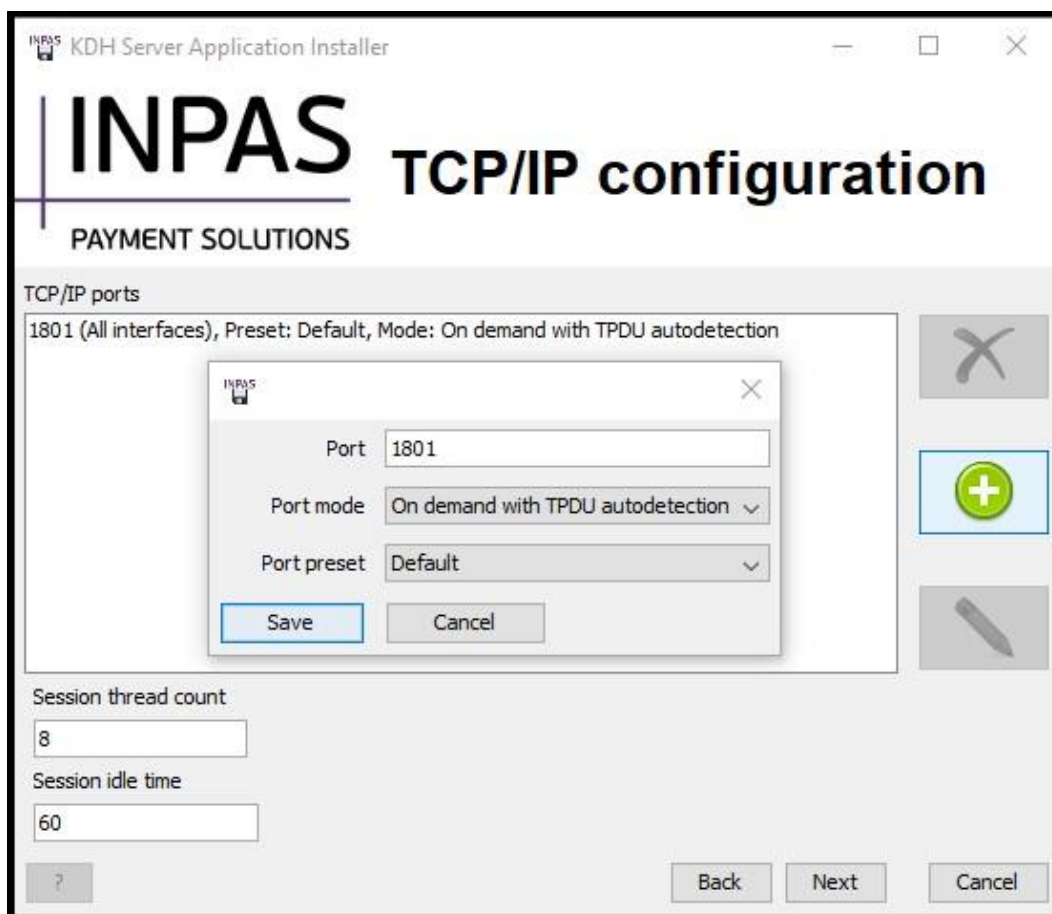
В выпадающем списке для выбора доступны следующие значения: «**Default**», «**Ethernet**», «**GPRS**», «**Dual-Up**».

Под списком с TCP/IP портами расположены два параметра:

**Session thread count** — указывается количество потоков, обрабатывающих запросы от терминалов. Значение по умолчанию — 8. Рекомендуемое значение — количество ядер процессора + 1.

**Session idle time** — указывается таймаут соединения в секундах. Значение по умолчанию (рекомендованное) — 60.

**Примечание:** нельзя добавить несколько портов с одним номером.



После настройки нажмите «Next».

### 3.1.9. Настройка доступа к web-интерфейсу

В окне «Web interface» укажите параметры доступа к web-интерфейсу.



Если в параметре «Host» указать 127.0.0.1 или другой локальный IP-адрес, то подключиться к системе будет возможно только с ПК где установлена система. Если указать 0.0.0.0, то подключиться к системе будет возможно с любого ПК.

После настройки веб доступа нажмите «Next».

### 3.1.10. Настройка уведомлений

В окне «**Notification**» настройте параметры соединения с SMTP сервером для получения уведомлений по E-mail.

Данный шаг может быть пропущен.

Нажмите кнопку «**Next**» для продолжения инсталляции.

### 3.1.11. Настройка связи с HSM

В окне «**HSM configuration**» настройте параметры связи с HSM.

Справа находятся кнопки удаления, добавления или изменения параметров соединения. При необходимости изменить параметры в секциях:

- **Timeout setting:**
  - **Connection timeout (sec)** – время установки соединения с HSM;
  - **Response timeout (sec)** – время ожидания ответа от HSM;
  - **Connection idle (sec)** – время неактивности соединения.
- **HSM LMK number** – номер ячейки в которой хранится LMK на HSM.

По нажатию кнопки добавления или изменения соединения с HSM открывается диалоговое окно, где настраиваются параметры соединения с HSM.

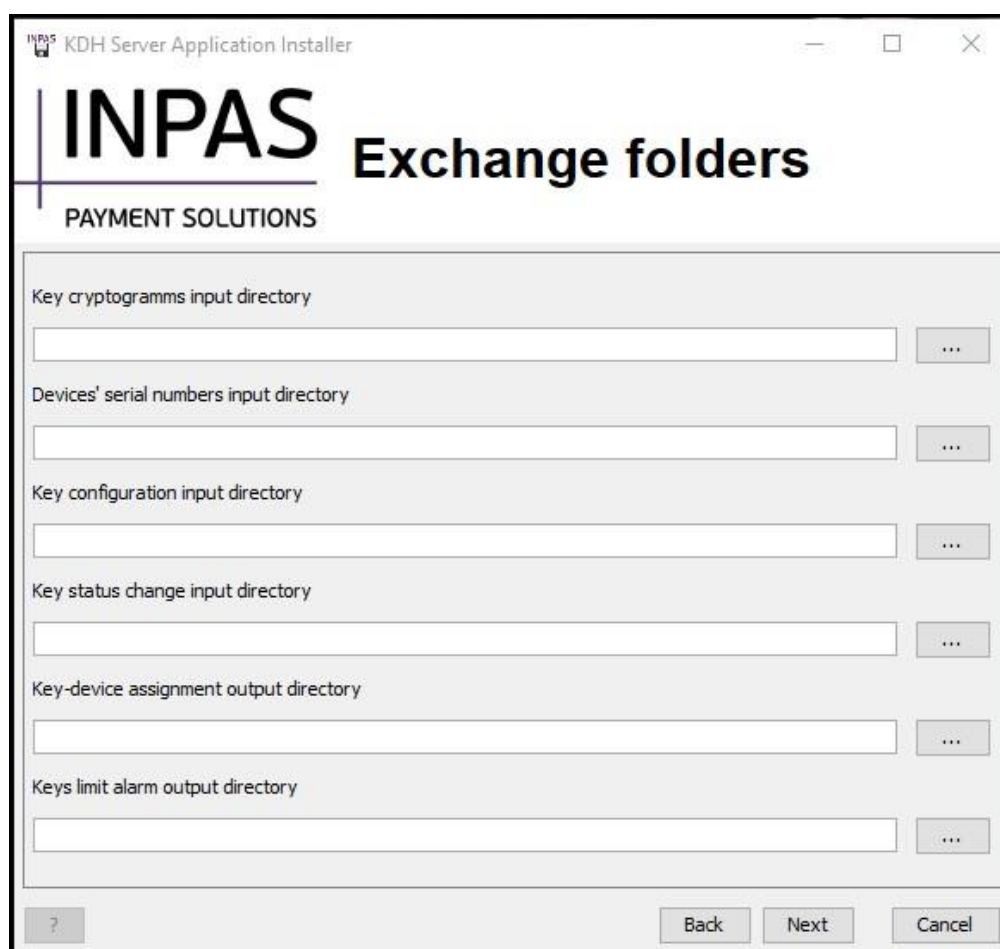
- Создайте соединение нажатием кнопки  в правой части окна.
- В открывшемся окне введите параметры соединения с HSM.
- Нажмите кнопку «**Save**» для сохранения изменений.
- Нажмите кнопку «**Next**». Будет выполнена попытка установить соединение с HSM.

### 3.1.12. Настройка папок обмена

Рекомендуемое место указания директорий для обмена «**/opt/trsys/\***» – данные директории уже имеют права за запись и чтение для «**etp-user**».

При выборе любых других директорий для обмена, необходимо убедиться, что все директории в пути имеют права на запись и чтение для «**etp-user**».

Например, «**/root/kdh/catalog1**». Все три директории должны иметь права для «**etp-user**» на запись и чтение.



В окне «**Exchange folder**» укажите папки обмена:

**Key cryptograms input directory.**

Входящая папка, в которой KDH ожидает файл со списком ТМК.

**Devices' serial numbers input directory.**

Входящая папка, в которой KDH ожидает файл со списком S/N POS-терминалов.

**Key configuration input directory.**

Входящая папка, в которой KDH ожидает файл с конфигурацией ключей POS-терминала.

**Key status change input directory.**

Входящая папка, в которой KDH ожидает файл со статусами ТМК.

**Key-device assignment output directory.**

Исходящая папка, в которую KDH сохраняет файлы с информацией о привязке и выдаче ключей терминалу.

**Keys limit alarm output directory.**

Исходящая папка, в которую KDH сохраняет файл с заявкой на генерацию ТМК.

Нажмите кнопку «Next».

### 3.1.13. Настройка доступа к БД

В окне «KDH Database» настройте доступ к БД KHD.

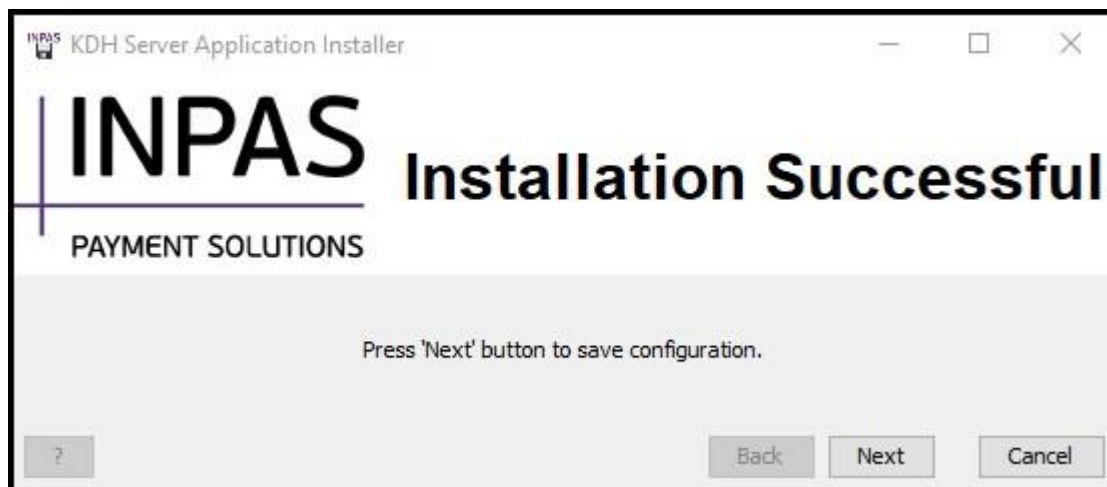
В текущей версии поддерживается только СУБД MySQL версий 5.7

Укажите параметры работы с БД (в «Database name» укажите БД (схему), созданную заранее (см. «Подготовка к установке»)).

**Maximum Pool Size** – указывается максимальное количество подключений к базе данных, которое сможет открыть приложение. Значение по умолчанию – 40.

Нажмите «Next» для перехода к следующему экрану.

В случае неправильной настройки будет выдано сообщение об ошибке. Необходимо устранить проблему.



Нажмите «**Next**» для сохранения конфигурации.

В случае корректной настройки соединения с БД инсталлятор перейдет к следующему окну «**Installation Successful**», нажмите «**OK**».

### **ВАЖНО!**

Рекомендуется после окончания установки KDH в папку «**private**» добавить файл «**X509.properties**».

Данный файл должен содержать строку «**x509.extend=1**».

Данный файл нужен для успешного прохождения проверки цепочки сертификатов УЦ. Он заменяет загрузку CRL-листа УЦ.

Если не подкладывать файл «**X509.properties**» в папку «**private**», то KDH будет выводить в лог информацию вида «**INFO o.s.c.a.ConfigurationClassParser.processPropertySource - Properties location [\${spring.config.location}X509.properties] not resolvable: C:\TRSYS\SAP\private\X509.properties (Не удается найти указанный файл)**».

## 3.2. Инсталляция в «Silent-режиме»

### 3.2.1. Подготовка к установке

Перед началом установки необходимо разместить папку «**private**» в каталог «**c:\sap\_install (Windows)**» или в «**/opt/sap\_install (Linux)**», где уже присутствуют инсталляционные файлы (содержимое поставки).

В папке «**private**» содержатся следующие файлы с параметрами:

- **kdh-db.properties** – параметры подключения к базе данных (8.1);
- **kdh-mc-hsm.properties** - параметры взаимодействия с HSM (8.2);
- **kdh-sinc.properties** – параметры интеграции с другими системами (8.3);
- **licence.properties** – настройки лицензии (8.4);
- **notification.properties** – настройки E-mail уведомлений (8.5);
- **server.properties** – настройки сервера KDH (8.6).

Данные файлы с параметрами возможно настроить самостоятельно, используя стандартное приспособление «**Windows – Блокнот**».

**Примечание.** Если необходимо сделать копию KDH, то нужно выполнить копирование папки «**private**» из каталога с установленным и настроенным KDH (по умолчанию «**C:\TRSYS\sap**»), и выполнить шаги описанные в пункте «**3.2.2**».

### 3.2.2. Запуск командной строки

Для начала установки необходимо запустить командную строку от имени «**Администратора**». Это возможно сделать одним из способов, описанных ниже.

#### Windows 7

Нажать сочетание клавиш «**Windows+R**» и в строку «**Open**» ввести «**cmd.exe**», затем нажать кнопку «**OK**».

Другой способ – нажать кнопку «**Start**», набрать в строке поиска «**cmd**», в результатах поиска в разделе «**Programs**» нажать правой кнопкой мыши на найденную программу и выбрать пункт «**Run as administrator**».

#### Windows 8.x

Создать ярлык на рабочем столе и в качестве пути к программе указать «**c:\windows\system32\cmd**». На закладке «**Security**» поставить флаг «**Run as administrator**».

Запустить консоль двойным кликом на созданный ярлык.

#### Windows 2008 Server/2012 Server

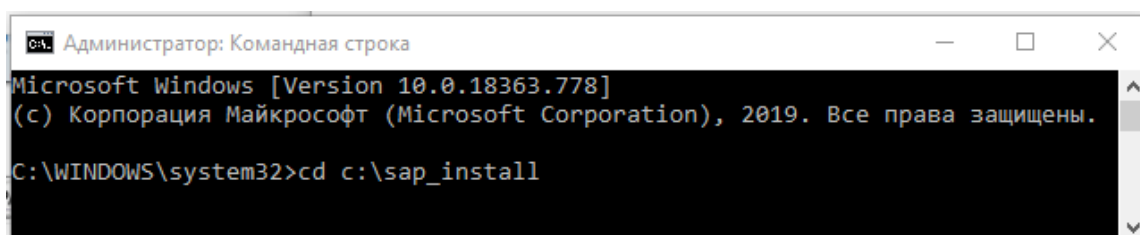
Запустить «**Power Shell**» (иконка находится на панели быстрого запуска, рядом с кнопкой «**Start**»).

#### Linux"

Открыть консоль и выполнить команду «**sudo su root**» При необходимости ввести пароль.

### 3.2.3. Выполнение установки в «Silent-режиме»

После запуска командной строки необходимо перейти в каталог с инсталляционными файлами (содержимое поставки), для этого необходимо выполнить одну из следующих команд: «**cd c:\sap\_install (windows)**» или «**cd /opt/sap\_install (Linux)**».



Затем запустить установку, выполнив команду «`java -jar install.jar --silent --install C:\TRSYS\sap (windows)`» или «`java -jar install.jar --silent --install /opt/trsys/sap (Linux)`».

```
c:\sap_install>java -jar install.jar --silent --install C:\TRSYS\sap
TR-SYS Server Application Platform Installer - 1.3.7 started in silent mode
System is already installed!

c:\sap_install>
```

После появления строки «**System is already installed**», можно приступить к использованию системы.

Для режима silent у инсталлятора добавились параметры:

- `--silent --install <указывается путь для установки>` – выполняется инсталляция с нуля (если система уже установлена – будет ошибка);
- `--silent --uninstall` – выполняется удаление;
- `--silent --upgrade` – выполняется обновление компонентов;
- `--silent --configure` – выполняется изменение конфигурации компонентов.

**Примечание.** При изменении конфигурации компонентов (команда «`--silent --configure`») необходимо разместить папку «**private**» в каталог «`c:\sap_install (Windows)`» или в «`/opt/sap_install (Linux)`», где уже присутствуют инсталляционные файлы (содержимое поставки).

### 3.3. Обновление в «Silent-режиме»

Перед началом обновления нужно внести необходимые изменения в файлы, расположенные в папке «**private**» в каталог «`c:\sap_install (Windows)`» или в «`/opt/sap_install (Linux)`»

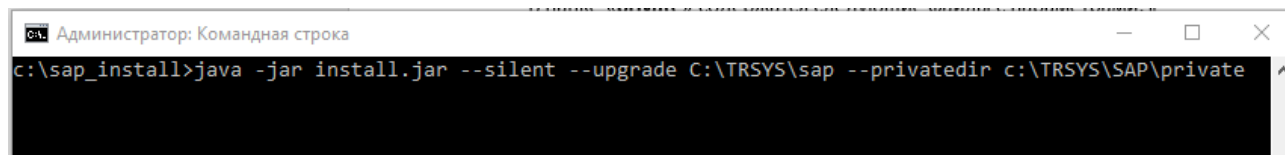
В папке «**private**» содержатся следующие файлы с параметрами:

- ***kdh-db.properties*** – параметры подключения к базе данных (8.1);
- ***kdh-mc-hsm.properties*** - параметры взаимодействия с HSM (8.2);
- ***kdh-sinc.properties*** – параметры интеграции с другими системами (8.3);
- ***licence.properties*** – настройки лицензии (8.4);
- ***notification.properties*** – настройки E-mail уведомлений (8.5);
- ***server.properties*** – настройки сервера KDH (8.6).

Далее запустить командную строку выполнив шаги описанные в пункте «3.2.2».

После запуска командной строки необходимо перейти в каталог с инсталляционными файлами (содержимое поставки), для этого необходимо выполнить одну из следующих команд: «`cd c:\sap_install (windows)`» или «`cd /opt/sap_install (Linux)`».

Затем запустить обновление, выполнив команду «`java -jar install.jar --silent --upgrade C:\TRSYS\sap --privatedir c:\TRSYS\SAP\private (windows)`» или «`java -jar install.jar --silent --upgrade /opt/trsys/sap --privatedir /opt/trsys/sap/private (Linux)`».



```
Администратор: Командная строка
c:\sap_install>java -jar install.jar --silent --upgrade C:\TRSYS\sap --privatedir c:\TRSYS\SAP\private
```

После появления строки «**complete**», можно приступить к использованию системы.

```
15:26:21.954 [main] INFO c.t.t.k.i.MainFrame - Upgrade
15:26:21.955 [main] INFO c.t.t.k.i.MainFrame - complete.
```

## 4. Запуск и остановка

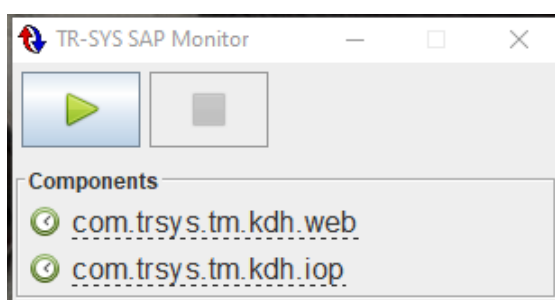
Серверная платформа устанавливается либо как служба (Service) для операционных систем семейства Windows, либо как процесс-демон для ОС семейства Linux.

В Windows служба инсталлируется как служба, запускаемая вручную. При необходимости можно изменить режим запуска на автоматический в панели управления «Control panel».

### 4.1. Программа и управление сервером

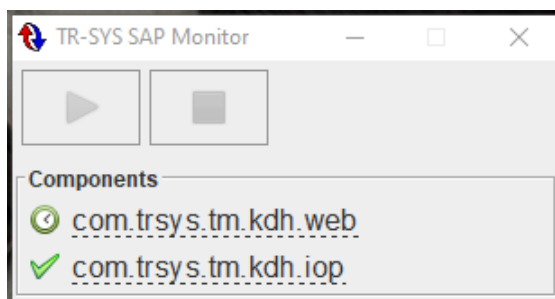
В комплект поставки сервера входит специальная программа для управления сервером KDH. При установке в Windows она запускается сразу после успешной установки. Для Linux потребуется перезагрузка или выход из системы. Данное приложение запускается автоматически и отображает статус в системном трее. При нажатии правой кнопкой на иконку  появляется меню с пунктами «Exit» (закрывает программу) и «Open» (открывает окно управления).

Окно управления выглядит следующим образом:

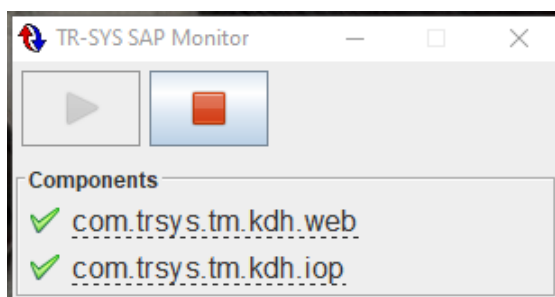


Управление сервером происходит двумя кнопками: «Start» и «Stop».

Ниже отображается статус инсталлированных продуктов:



 - данная пиктограмма означает что продукт ещё не запущен, либо что продукт еще в процессе запуска и следует немного подождать. При успешном запуске отображается зеленая пиктограмма .



В случае, если отобразилась пиктограмма с восклицательным знаком, необходимо диагностировать проблему.

**Примечание:** На Ubuntu автозапуск не работает.

## 4.2. Управление сервером вручную

Сервером также можно управлять вручную. Для «KDH» создано две службы:

- com.trsys.tm.kdh.web;
- com.trsys.tm.kdh.iop.

### Windows.

Для определения текущего состояния службы сервера в Windows используется системная команда «sc», которую необходимо вызывать из консоли.

**E:\SAP>sc query com.trsys.tm.kdh.web**

```
Имя_службы: com.trsys.tm.kdh.web
Тип          : 10  WIN32_OWN_PROCESS
Состояние     : 4  RUNNING
               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
Код_выхода_Win32 : 0  (0x0)
Код_выхода_службы : 0  (0x0)
Контрольная_точка : 0x0
Ожидание      : 0x0
```

Для остановки службы сервера необходимо выполнить команду «sc stop com.trsys.tm.kdh.web».

**E:\SAP>sc stop com.trsys.tm.kdh.web**

```
Имя_службы: com.trsys.tm.kdh.web
Тип          : 10  WIN32_OWN_PROCESS
Состояние     : 3  STOP_PENDING
               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
Код_выхода_Win32 : 0  (0x0)
Код_выхода_службы : 0  (0x0)
Контрольная_точка : 0x2
Ожидание      : 0xbb8
```

Для запуска службы сервера необходимо использовать команду «sc start com.trsys.tm.kdh.web».

**E:\SAP>sc start com.trsys.tm.kdh.web**

```
Имя_службы: com.trsys.tm.kdh.web
Тип          : 10  WIN32_OWN_PROCESS
Состояние     : 2  START_PENDING
               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
Код_выхода_Win32 : 0  (0x0)
Код_выхода_службы : 0  (0x0)
Контрольная_точка : 0x0
Ожидание      : 0x7d0
ID_процесса    : 1888
Флаги         :
```

Для службы «com.trsys.tm.kdh.iop» команды идентичны.

### Linux

Для определения текущего состояния демона сервера необходимо вызвать команду:

Приложение устанавливается от пользователя «root», но запуск происходит от пользователя «etp-user», который создается в процессе инсталляции, если его нет.

***ps -aux |grep com.trsys.tm.kdh.web |grep java:***

```
[oracle@oraclelinux6 ~]$ ps -aux |grep com.trsys.tm.kdh.web |grep java
etp-user  5926 49.6 36.1 2000412 368212 ?    Sl  08:17  ...
```

Если команда выводит процесс, значит демон запущен.

Для запуска демона сервера необходимо вызвать команду:

***sudo /etc/init.d/com.trsys.tm.kdh.web start***

Для остановки демона сервера необходимо вызвать команду:

***sudo /etc/init.d/com.trsys.tm.kdh.web stop***

#### **Права на управление демоном для Linux**

Так как сам демон работает под другим пользователем, для его управления нужны права на выполнение под «**sudo**» скрипта:

- «**/etc/init.d/com.trsys.tm.kdh.web**»;
- «**/etc/init.d/com.trsys.tm.kdh.iop**».

Для этого в файле «**sudoers**» необходимо добавить строку:

```
user ALL=(etp-user) NOPASSWD: /etc/init.d/com.trsys.tm.kdh.web
```

или для группы:

```
%group ALL=(etp-user) NOPASSWD: /etc/init.d/com.trsys.tm.kdh.web
```

где «**user**» и «**group**» - название пользователя и группы соответственно.

## 5. Диагностика проблем с запуском

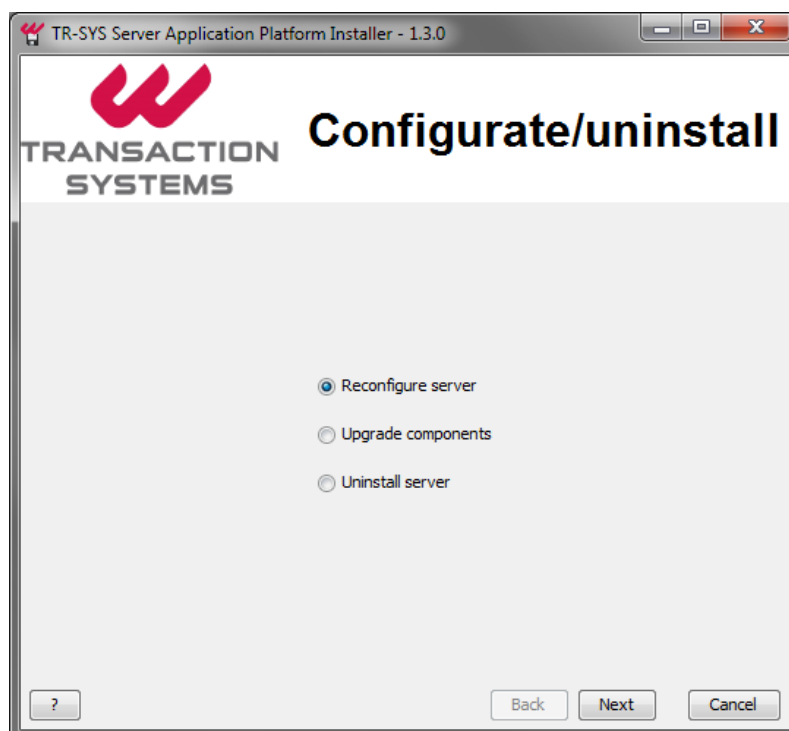
Сервер при запуске записывает информацию в log файл, которая необходима для диагностики проблем. Log файл находится в каталоге каталог-установки «**/serviceability/eventlogs**».

Одна из часто встречающихся ошибок связана с невозможностью соединиться с базой данных. Если проблему по логам диагностировать не получается, выполните следующие действия:

1. остановите сервер;
2. удалите каталог «**serviceability/eventlogs**»;
3. запустите сервер;
4. Через некоторое время, когда в лог перестанет записываться новая информация, отправьте файл в поддержку.

## 6. Изменение текущей установки

Инсталлятор при запуске проверяет наличие установленной серверной платформы. И если она уже установлена, отображает возможные действия.



### 6.1. Повторная конфигурация «Reconfigure server»

При выборе этого действия пользователь проходит по всем шагам настройки для изменения чего-либо.

**Внимание:** сервер должен быть предварительно остановлен.

При повторной конфигурации допускается добавление или удаление каких-либо продуктов. Для этого на странице выбора компонент «**Components selection**» необходимо снять или поставить галочки.

### 6.2. Обновление компонент «Upgrade components»

Это действие используется для обновления версий компонент сервера. Обновления распространяются в виде ZIP архива, который надо развернуть в каталог, куда ранее был развернут пакет установки.

### 6.3. Удаление «Uninstall server»

Это действие удаляет с данного компьютера сервер и все ранее установленные продукты.

## 7. Настройка HTTPS

Для настройки HTTPS начиная с версии 3.0.4, необходимо выполнить следующие действия:

1. выключить сервер KDH одним из описанных вариантов в пунктах «4 Запуск и остановка»;
2. запустить командную строку от имени «Администратора» («ROOT»);
3. выполнить вход в директорию «jre/bin»;

**Примечание.** Директория «jre/bin» располагается:

- Windows x64 – «C:/Program Files/Java/jre/bin»;
- Windows x32 – «C:/Program Files (x86)/Java/jre/bin»;
- Linux – «/usr/lib/jvm/jre/bin».

4. выполнить команду:

```
keytool -genkeypair -noprompt -dname "CN=<1>, OU=OU, O=O, L=L, S=S, C=RU" -alias psb -keyalg RSA -  
keysize 4096 -storetype PKCS12 -storepass <2> -keystore keystore_psb.p12 -validity 365 -ext  
SAN=dns:<1>,ip:<3>
```

Где (далее используются во всех командах):

- <1> - имя сервера, возможно узнать, используя команду «hostnamectl» (Static hostname);
- <2> - пароль хранилища ключей (не менее 6 символов);
- <3> - IP-адрес сервера, возможно узнать, используя команду «ipconfig».

Итогом успешного выполнения команды является появление файла «keystore\_psb.p12» в директории «jre/bin».

5. далее выполнить следующую команду:

```
keytool -export -alias psb -storepass <2> -keystore keystore_psb.p12 -rfc -file psb.cer
```

Итогом успешного выполнения команды является появление файла «psb.cer» в директории «jre/bin».

6. следующей выполнить команду:

```
keytool -import -alias psb -file psb.cer -storepass <2> -keystore truststore_psb.p12
```

7. на отобразившейся вопрос «Trust this certificate?» ввести «yes»;

Итогом успешного выполнения команды является появление файла «truststore\_psb.p12» в директории «jre/bin».

8. далее проверить хранилища «keystore», «truststore» на наличие сертификатов, используя команды:

```
keytool -list -v -storepass <2> -keystore keystore_psb.p12
```

```
keytool -list -v -storepass <2> -keystore truststore_psb.p12
```

**Примечание.** В обоих хранилищах должно лежать по одному сертификату.

9. в файле «server.properties» указать следующие параметры:

```
web.port.https=8443  
web.host.https=<3>  
security.require-ssl=true  
server.ssl.key-store=<4>  
server.ssl.key-store-password=<2>  
server.ssl.key-store-type=PKCS12  
server.ssl.key-alias=psb
```

Где **<4>** - абсолютный путь до файла **«keystore\_psb.p12»**, например **«/opt/jre/bin/keystore\_psb.p12»**.

10. включить сервер KDH одним из описанных вариантов в пунктах **«4 *Запуск и остановка*»**;
11. скопировать файл **«psb.cer»** на машину клиента и добавить его в корневые центры сертификации;
12. в браузере (рекомендуется Chrome) ввести **«https://<3>:8443/kdh»**.

## 8. Приложение

### 8.1. kdh-db.properties

Таблица 1.

|                      |                                                                                                                                                                                                                                                                            |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jdbc.url             | Указывается путь/ адрес для подключения к БД<br>Примеры формата для MySQL<br><a href="https://dev.mysql.com/doc/connector-j/8.0/en/connector-j-reference-jdbc-url-format.html">https://dev.mysql.com/doc/connector-j/8.0/en/connector-j-reference-jdbc-url-format.html</a> |
| jdbc.maximumPoolSize | Указывается максимальное количество подключений к базе данных, которое сможет открыть приложение. Пример значения – 40 (по умолчанию)                                                                                                                                      |
| jdbc.username        | Указывается имя пользователя для подключения к БД                                                                                                                                                                                                                          |
| db.type              | Указывается тип базы данных. Пример значения – mysql                                                                                                                                                                                                                       |
| jdbc.drive           | Указывается тип драйвера для подключения к БД<br>Для mysql – “com.mysql.jdbc.Driver”                                                                                                                                                                                       |
| jdbc.isEncrypted     | Указывает на наличие зашифрованного пароля. Параметр может отсутствовать                                                                                                                                                                                                   |
| jdbc.password        | Указывается пароль пользователя для подключения к БД                                                                                                                                                                                                                       |

### 8.2. kdh-mc-hsm.properties

Таблица 2.

|                       |                                            |
|-----------------------|--------------------------------------------|
| hsm.connectionTimeout | Время установки соединения с HSM           |
| hsms.1.pool           | Количество подключений                     |
| hsm.lmk               | Номер ячейки в которой хранится LMK на HSM |
| hsm.responseTimeout   | Время ожидания ответа от HSM               |
| hsms.1.host           | IP-адрес для соединения с HSM              |
| hsm.idle              | Время неактивности соединения              |
| hsms.1.port           | Порт для соединения с HSM                  |

### 8.3. kdh-sinc.properties

Таблица 3.

|                  |                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------|
| folder.ucms      | Полный путь к папке, в которой KDH ожидает файл с конфигураций ключей POS-терминала                   |
| folder.dts       | Полный путь к папке, в которой KDH ожидает файл со списком S/N POS-терминалов                         |
| folder.raptor    | Полный путь к папке, в которой KDH ожидает файл со списком ТМК                                        |
| folder.host_keys | Полный путь к папке, в которую KDH сохраняет файлы с информацией о привязке и выдаче ключей терминалу |
| folder.two       | Полный путь к папке, в которой KDH ожидает файл со статусами ТМК                                      |
| folder.keyLimit  | Полный путь к папке, в которую KDH сохраняет файл с заявкой на генерацию ТМК                          |

### 8.4. licence.properties

Таблица 4.

|              |                                    |
|--------------|------------------------------------|
| license.file | Указывается путь до файла лицензии |
|--------------|------------------------------------|

## 8.5. notification.properties

Таблица 5.

|                   |                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------|
| notify.email.port | Порт SMTP сервера                                                                                             |
| notify.email.host | IP-адрес SMTP сервера                                                                                         |
| notify.email      | Включение использования SMTP сервера для получения уведомлений по E-mail. Возможные значения: «true», «false» |
| notify.email.from | E-mail, куда будут отправляться уведомления                                                                   |

## 8.6. server.properties

Таблица 6.

|                                |                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------|
| web.host.http                  | IP-адрес по которому будет доступен веб интерфейс KDH                                              |
| web.port.http                  | Порт по которому будет доступен веб интерфейс KDH                                                  |
| web.host.https                 | IP-адрес, по которому будет доступен веб интерфейс KDH (имеет приоритет перед web.host.http)       |
| web.port.https                 | Порт, по которому будет доступен веб интерфейс KDH (имеет приоритет перед web.port.http)           |
| security.require-ssl=          | необходимость использовать SSL.(true/false)                                                        |
| server.ssl.key-store=          | путь к keystore (например, /opt/jre/keystore_psb.p12, C:/TRSYS/jre/keystore_psb.p12)               |
| server.ssl.key-store-password= | пароль                                                                                             |
| server.ssl.keyStoreType=       | Тип шифрации пароля (например, PKCS12)                                                             |
| server.ssl.keyAlias=           |                                                                                                    |
| server.tcpip.1.protocol        | Выбор протокола для связи с терминалом. Варианты : sa, iso8583                                     |
| server.tcpip.1.preset          | Пресеты настроек порта для связи с терминалами. Возможные варианты: deflt, ethernet, gprs, dial-up |
| server.tcpip.1.port            | Номер порта для связи с терминалами                                                                |
| session.thread.count           | Максимальное количество потоков для сессии                                                         |
| session.idle.time              |                                                                                                    |
| logging.file                   | Имя файла логов                                                                                    |
| logging.path                   | Путь для хранения логов                                                                            |
| web.ctx.path                   |                                                                                                    |
| web.redirect.https             | true – чтобы всегда перенаправляла на защищенный порт, false чтобы не перенаправлять               |
| process.monitor.turnOnOnStartu | Если нужно включать монитор при включении сервера то true, иначе false                             |

## 8.7. x509.properties

Таблица 7.

|              |                                                                                                |
|--------------|------------------------------------------------------------------------------------------------|
| x509.extend= | Должно иметь значение 1. Необходимо для успешного прохождения проверки цепочки сертификатов УЦ |
|--------------|------------------------------------------------------------------------------------------------|