

SunMi P2Pro

Инструкция

Версия 1.2

История изменений документа

Версия	Дата	Перечень изменений
1.0	04.09.2019	Первоначальная версия документа
1.1	28.11.2019	Добавлен пункт 2 со всеми подпунктами, пункт 3 и пункт 4. Удалено последнее «Примечание» из пункта 4.
1.2	24.03.2020	Изменена картинка в пункте 2.1.1

Содержание

1. Введение.....	4
2. Настройка соединения с серверами «САН», «KDH» и «UCM».....	5
2.1. Настройка соединения с серверами «САН», «KDH» и «UCM»	5
2.1.1. Создание zip-архива	5
2.1.2. Загрузка в терминал	7
2.2. Ручная настройка соединений с серверами «KDH», «САН» и «UCM»	8
3. Удаленная загрузка ключей	12
4. Ручной ввод ключей в терминал.....	15
5. Приложение	18

1. Введение

Данный документ является пошаговой инструкцией по загрузке ключей, сертификатов и настройке взаимодействия с «RKL» в терминал «**SunMi T6920 P2 PRO**» на базе Android.

ВАЖНО!!!

Пропуск одного из пунктов может привести к неработоспособности дальнейшей схемы действий.

2. Настройка соединения с серверами «САН», «KDH» и «UCM»

Для ручной загрузки файлов сертификатов, ключей сервера («KDH» и «САН»), ключей клиента и настройки подключения к серверам «KDH» и «САН» нужно использовать утилиту «Generate SSL zip package», которая позволяет сформировать zip-архив (с вложенными сертификатами, ключами и адресами серверов) для последующей загрузки в терминал.

Внимание! Утилита запускается только на ПК с операционной системой «Windows x64». На ОС «Windows x32» - не работает.

2.1. Настройка соединения с серверами «САН», «KDH» и «UCM»

2.1.1. Создание zip-архива

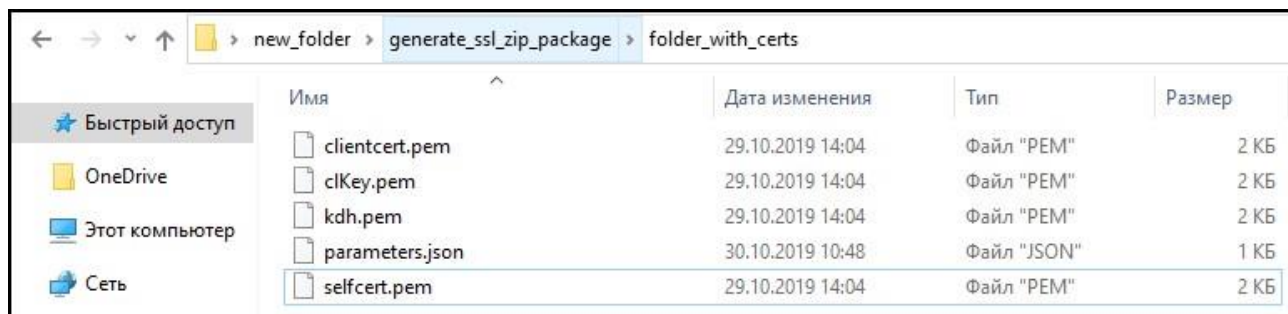
1. Создать новую (рабочую) папку для работы с утилитой. Расположение папки может быть любым;
2. Скопировать и развернуть архив с утилитой «Generate SSL zip package» в созданной папке;
3. Открыть файл «parameters.json» расположенный по пути [Созданная (рабочая) папка] / «generate_ssl_zip_package» / «folder_with_certs»;

```
{
  "ucm": {
    "connections": [
      {
        "name": "default UCM 1",
        "address": "82.196.67.120",
        "port": "24003",
        "useSsl": true,
        "ca": "RCAORCA_ITS.pem",
        "useCahSsl": true
      }
    ]
  },
  "cah": {
    "connection": {
      "address": "10.129.106.105",
      "port": "1801"
    }
  },
  "kdh": {
    "useRklLoaded": True,
    "connection": {
      "address": "82.196.67.120",
      "port": "24001",
      "useSsl": True,
      "ca": "RCAORCA_ITS.pem"
    }
  }
}
```

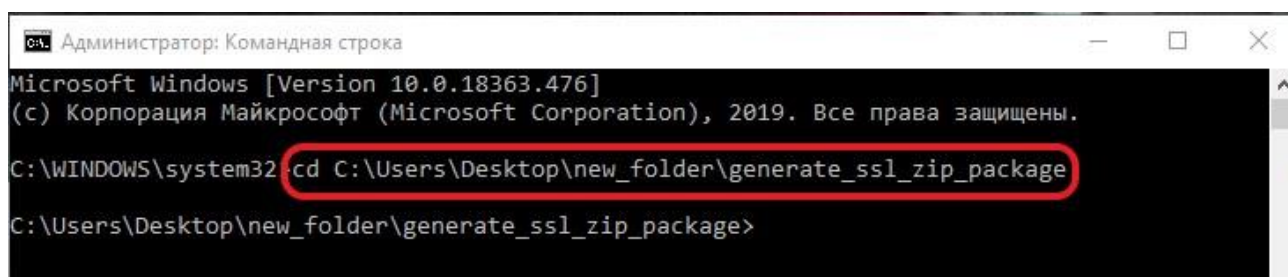
4. Заполнить файл параметров данными (см. п. «5 Приложение»):
 - IP-сервера;
 - Порт сервера;
 - Признак SSL-соединения;
 - Имена файлов сертификатов и ключей с расширением.

Примечание. Корректность содержимого файла после корректировки возможно проверить с помощью «json online validator» (например, <https://jsonformatter.curiousconcept.com/>).

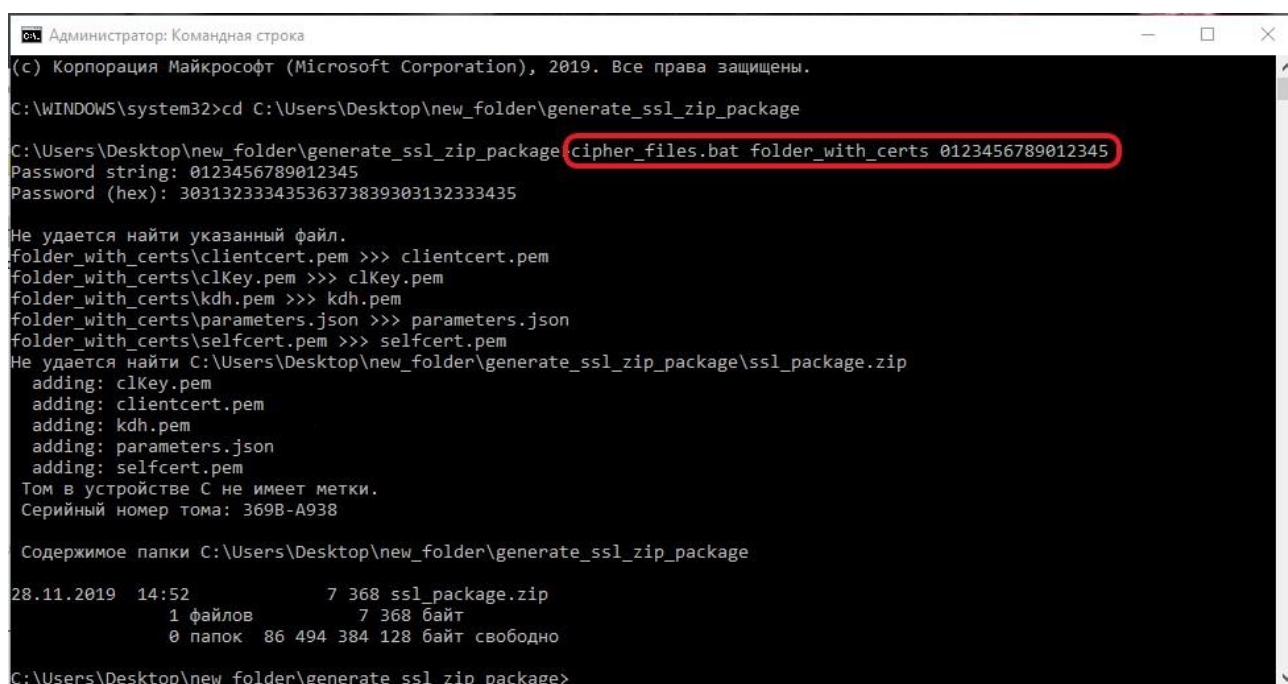
- В папку «**folder_with_certs**» скопировать все файлы сертификатов и ключей, имена которых указаны в файле «**parameters.json**»;



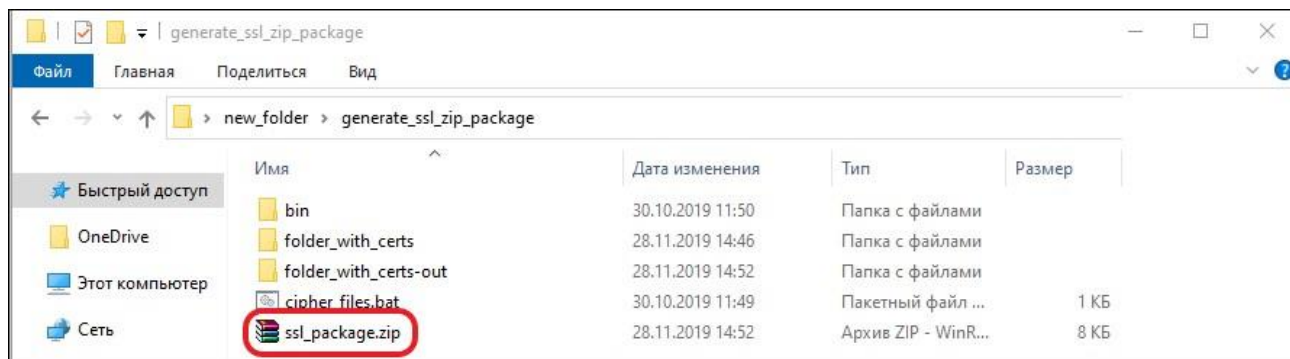
- Запустить командную строку «**cmd.exe**»;
- В окне командной строки для перехода в нужный каталог необходимо выполнить команду «**cd [имя_рабочей_папки]\generate_ssl_zip_package**» (пример, «**cd new_foulder\generate_ssl_zip_package**»);



- Далее запустить процесс сборки zip-архива (с вложенными сертификатами, ключами и адресами серверов) для последующей загрузки в терминал с помощью команды «**cipher_files.bat folder_with_certs yourZipPasswOrd'**», где:
 - cipher_files.bat** – имя используемого (запускаемого) файла;
 - folder_with_certs** – имя папки с файлом параметров «**parameters.json**» и соответствующими файлами (сертификаты, ключи и адреса серверов)
 - yourZipPasswOrd'** – пароль для защиты сформированного zip-архива (пример, «**yourZipPasswOrd'**», «**0123456789012345**»).



9. По окончании выполнения процесса в папке «**generate_ssl_zip_package**» должен появиться zip-архив с названием «**ssl_package.zip**»;



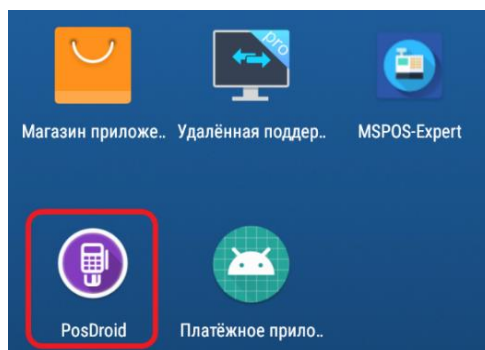
Примечание. Содержимое файла «**ssl_package.zip**» можно проверить, открыв файл в проводнике «**Windows**». В zip-архиве должны быть все файлы, содержащиеся в папке «**folder_with_certs**».

2.1.2. Загрузка в терминал

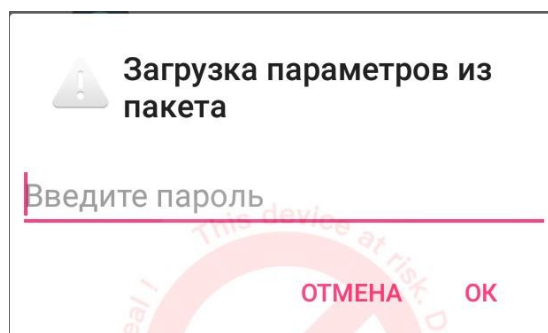
10. Загрузить файл «**ssl_package.zip**» в терминал в папку «**Download**» или «**Bluetooth**» с помощью «**Bluetooth**» стандартными средствами «**Android**»;

Примечание. В случае загрузки файла «**ssl_package.zip**» через «**Bluetooth**», терминал автоматически сохраняет его в папку «**Bluetooth**» (переносить в папку «**Download**» - **не обязательно**).

11. Далее на экране терминала выбрать приложение «**PosDroid**»;



12. Если приложение при старте обнаружило файл «**ssl_package.zip**» в какой-либо из указанных в шаге 10 папок, то терминал запросит предоставление соответствующих прав доступа, нажать кнопку «**Разрешить**» на экране терминала;
13. Далее терминал выполнит запрос пароля от zip-архива;
14. Ввести пароль, указанный при создании zip-архива на шаге 8 и нажать кнопку «**Ок**»;



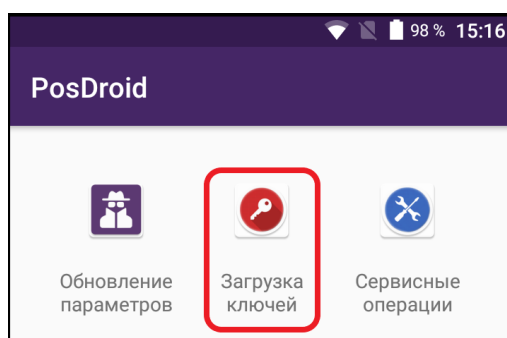
15. Терминал отобразит результат обработки zip-архива.

- a. При успешном завершении обработки zip-архива, приложение (во время работы) будет применять указанные в файле параметры;
- b. При неуспешном завершении обработки zip-архива в первую очередь проверить правильность формирования файла параметра «**parameters.json**», правильность введенного пароля.

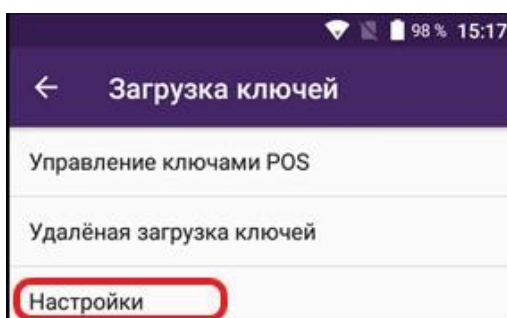
2.2. Ручная настройка соединений с серверами «KDH», «САН» и «UCM»

Примечание. При настройке соединений с серверами «KDH», «САН», «UCM» вручную, нужно удалить файл «**parameters.json**» из папки «**folder_with_certs**».

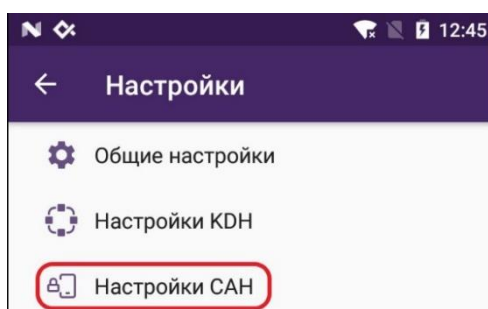
1. В главном окне приложения «PosDroid» выбрать пункт «Загрузка ключей»;



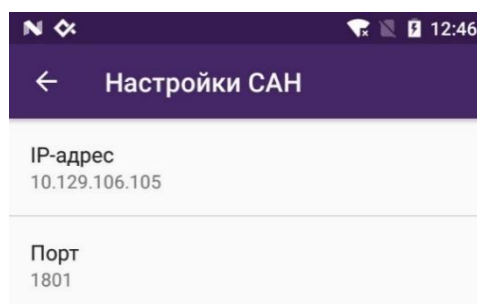
2. В открывшемся меню «Загрузка ключей» выбрать пункт «Настройки»;



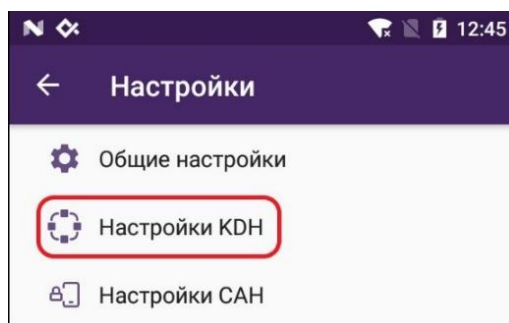
3. Для настройки соединения с сервером «САН» нужно выбрать пункт «Настройки САН»;



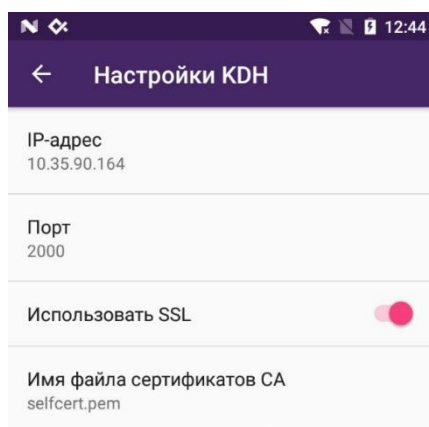
4. В отобразившемся окне «Настройки САН» нужно указать IP-адрес и порт хоста «САН»;



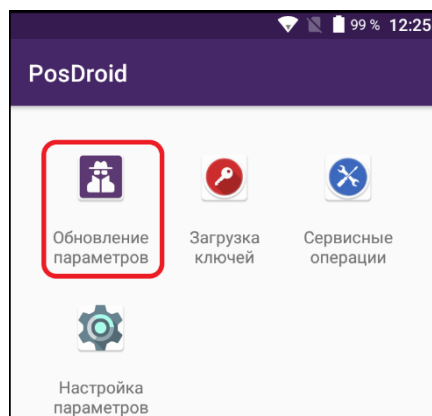
5. Для настройки соединения с сервером «KDH» нужно выбрать пункт «**Настройки KDH**»;



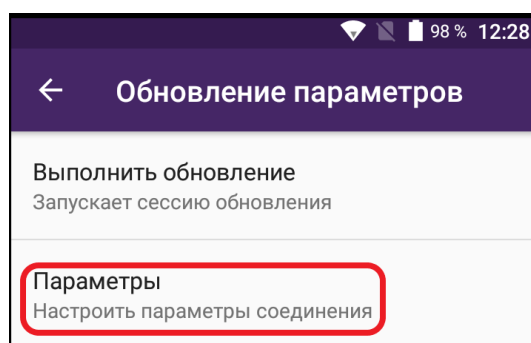
6. В отобразившемся окне «**Настройки KDH**» нужно указать IP-адрес и порт хоста «KDH». Если на сервере используется защищенное SSL-соединение, то нужно установить флаг в чек боксе «**Использовать SSL**» и указать имя файла сертификата, содержащего цепочку сертификатов CA;



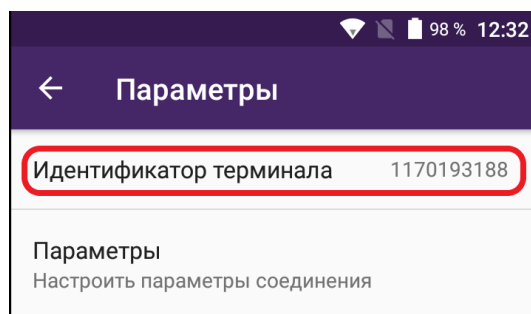
7. В окне приложения «**PosDroid**» нажать на пункт «**Обновление параметров**»;



8. В открывшемся меню выбрать пункт «**Параметры**»;



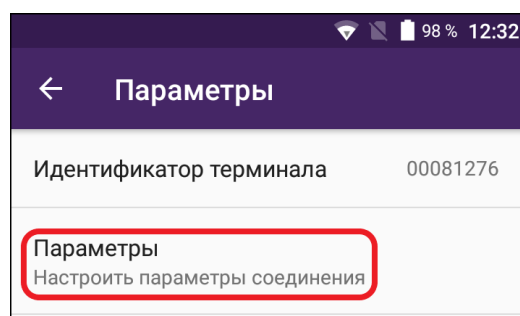
9. Далее выбрать пункт «Идентификатор терминала»;



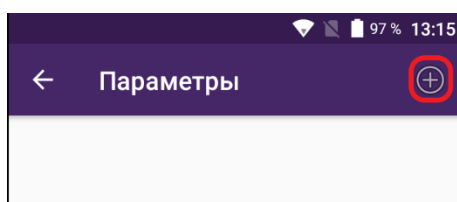
10. В открывшемся окне ввести «Идентификатор терминала» и нажать кнопку «Ок»;



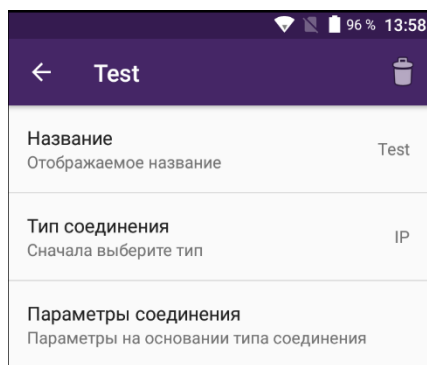
11. В меню «Параметры» нужно выбрать пункт «Параметры» для настройки параметров соединения с сервером параметризации;



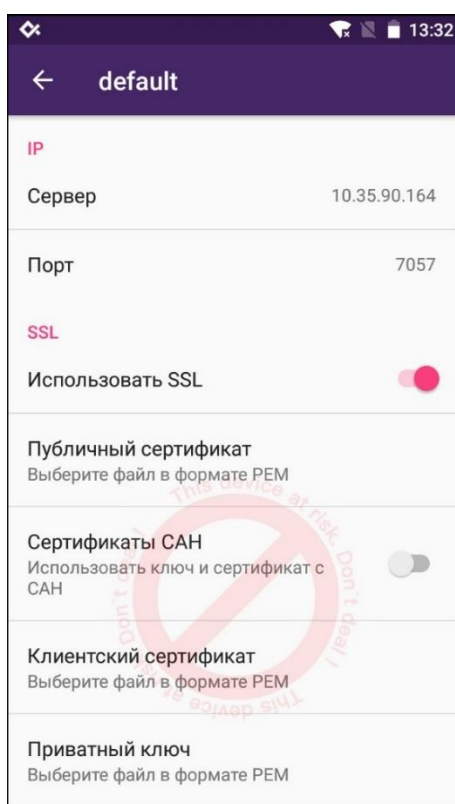
12. Далее нажать на кнопку  в правом верхнем углу экрана терминала;



13. Отобразятся параметры настройки соединения с хостом параметризации:
- **Название** – указать название соединения с хостом параметризации;
 - **Тип соединения** – указать тип соединения «IP»;



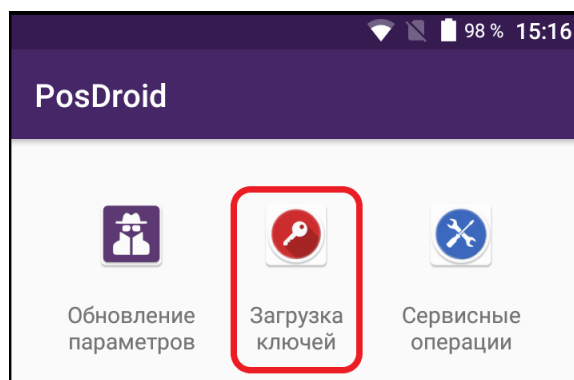
- **Параметры соединения:**
 - **IP**
 - **Сервер** - казать адрес сервера параметризации;
 - **Порт** – указать порт сервера параметризации.
 - **SSL:**
 - **Использовать SSL** – включает использование защищенного соединения;
 - **Публичный сертификат** – выбирается файл публичного сертификата с расширением «*.pem»;
 - **Сертификаты CAH** – включает использование сертификатов и ключа с сервера «CAH»;
 - **Клиентский сертификат** - выбирается файл клиентского сертификата с расширением «*.pem»;
 - **Приветный ключ** - выбирается файл приватного ключа с расширением «*.pem».



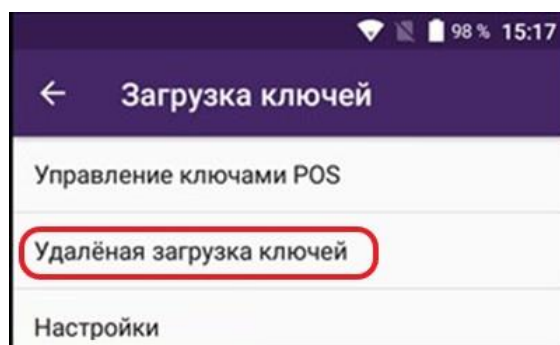
Примечание. Для удаления соединения необходимо нажать на кнопку .

3. Удаленная загрузка ключей

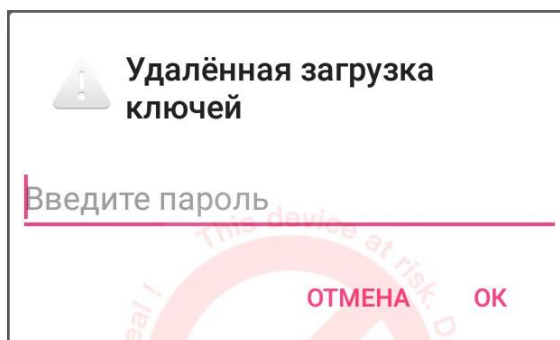
1. В главном окне приложения «PosDroid» выбрать пункт «Загрузка ключей»;



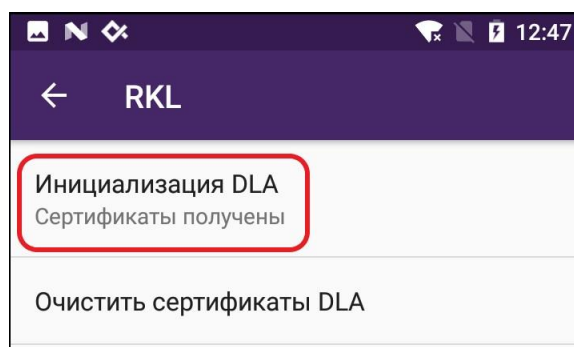
2. В открывшемся меню «Загрузка ключей» выбрать пункт «Удаленная загрузка ключей»;



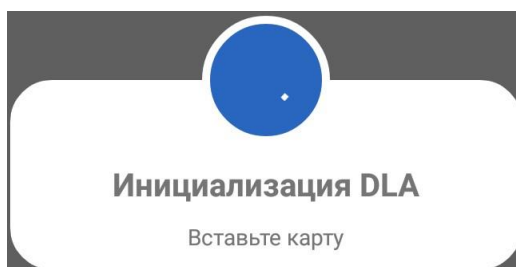
3. Терминал запросит ввод пароля. Ввести пароль (по умолчанию «98765») и нажать кнопку «Ок» на экране терминала;



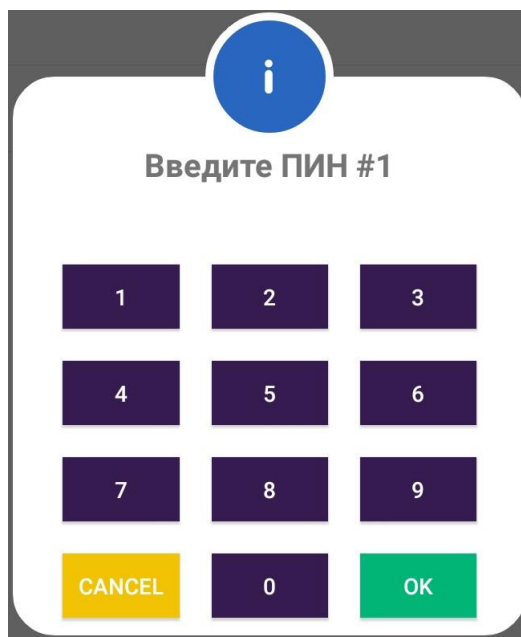
4. Терминал отобразит меню «RKL» где необходимо выбрать пункт «Инициализация DLA»;



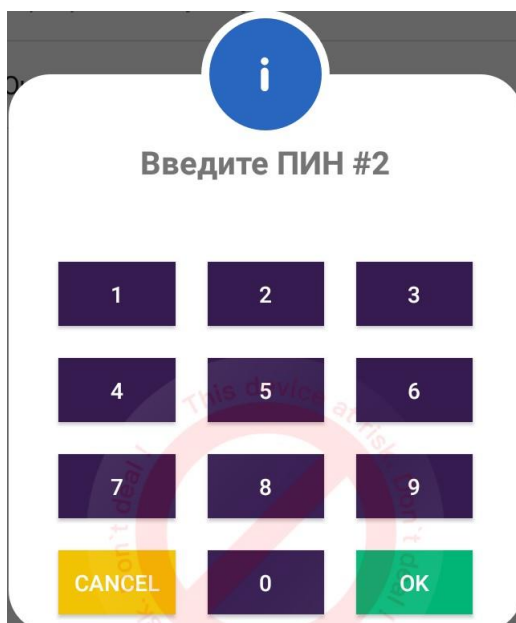
5. Терминал запросит ввести sam-карту



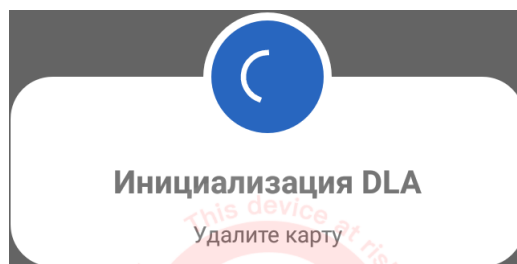
6. Терминал запросит ввести ПИН-код #1 и нажать кнопку «**Ок**» на экране терминала;



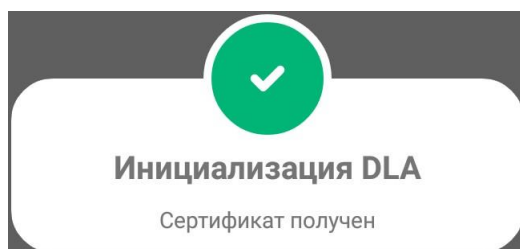
7. Терминал запросит ввести ПИН-код #1 и нажать кнопку «**Ок**» на экране терминала;



8. Терминал запросит удалить sam-карту;



9. После успешной инициализация DLA и получения сертификатов с «САН» будет выведено соответствующее сообщение «**Сертификаты получены**».

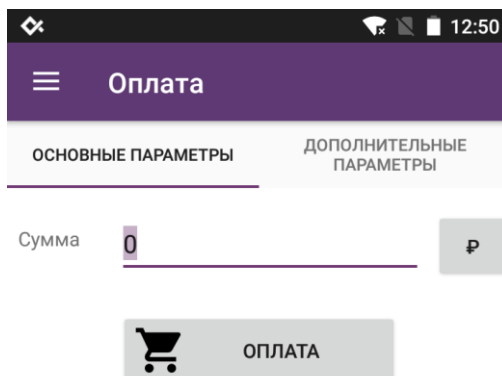


Примечание. В случае если сертификаты уже получены под пунктом «Инициализация DLA» будет отображаться соответствующий статус. При выборе пункта «Инициализация DLA» будет запрошено подтверждение повторной инициализации.

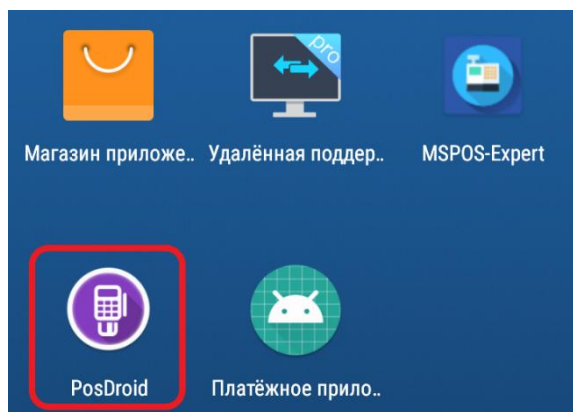
4. Ручной ввод ключей в терминал

Для ввода ключей нужно выполнить следующие действия:

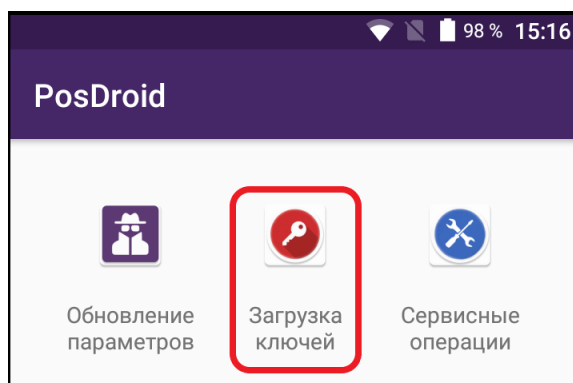
1. Необходимо закрыть платежное приложение с помощью кнопки ;



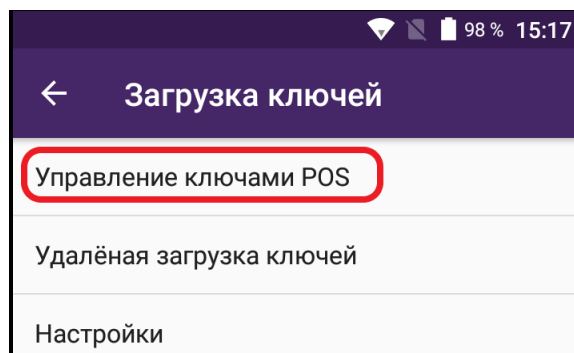
2. Далее на экране терминала выбрать приложение «PosDroid»;



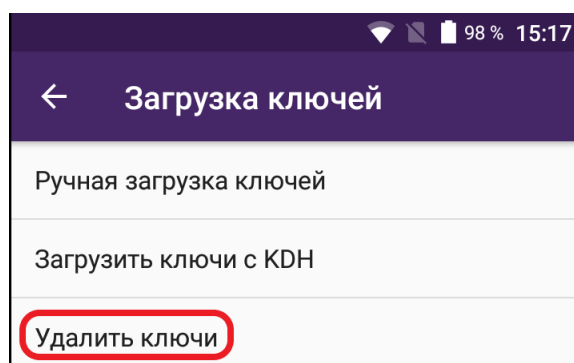
3. В открывшемся окне приложения нажать на пункт «Загрузка ключей»;



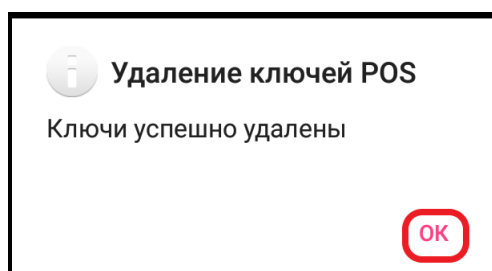
4. В отобразившемся меню выбрать пункт «Управление ключами POS»;



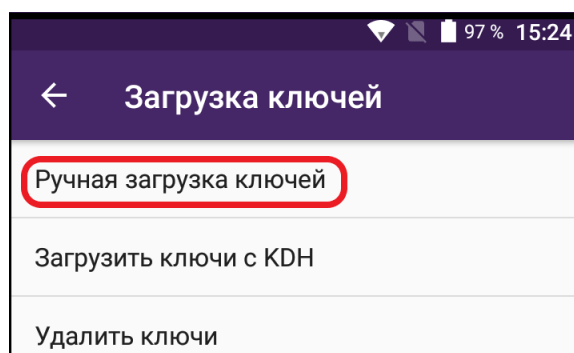
5. Далее выбирать пункт «**Удалить ключи**». При необходимости ввести пароль «**9876**»;



6. Отобразится информационное сообщение «**Ключи успешно удалены**», в котором нужно нажать кнопку «**Ок**»;



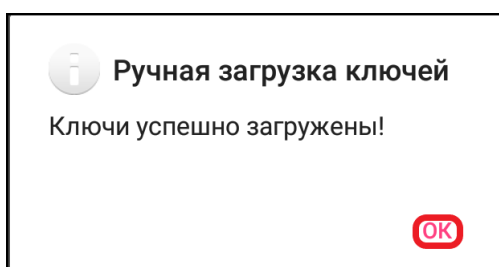
7. Терминал вернется в меню «**Загрузка ключей**», где нужно выбрать пункт «**Ручная загрузка ключей**»;



8. Заполнить все параметры и нажать кнопку «**Загрузить ключи**».
- **Тип ключа** – выбрать из списка тип ключа: «**Мастер ключ**», «**KLK ключ**», «**Ключ для дешифрации**»;
 - **Номер слота** – указать номер слота ячейка, куда будет загружен ключ;
 - **Компонента 1** – ввести компоненту 1;
 - **Компонента 2** – ввести компоненту 2;

Примечание. По окончании ввода компоненты терминал выводит окно для проверки контрольной суммы, в котором нужно проверить контрольную сумму и нажать кнопку «Ок».

9. Отобразится информационное сообщение об успешной загрузке ключей, в котором нужно нажать кнопку «Ок».



5. Приложение

Подключение к «UCM» через SSL соединение используя свои/custom сертификаты сервера и клиента (проверка клиента на сервере).

Файл параметров «parameters.json»

```
{
  "ucm": {
    "connections": [
      {
        "name": "default UCM",
        "address": "192.168.88.208",
        "port": "2001",
        "useSsl": true,
        "clientCertificate": "client.pem",
        "clientKey": "client_key.pem",
        "ca": "ca.pem",
        "useCahSsl": false
      }
    ]
  },
  "cah": {
    "connection": {
      "address": "10.129.106.105",
      "port": "1801"
    }
  },
  "kdh": {
    "useRklLoaded": true,
    "connection": {
      "address": "192.168.88.208",
      "port": "7008",
      "useSsl": true,
      "ca": "ca.pem"
    }
  }
}
```

Пример блока настроек «Stunnel»

```
[DLA]
cert = /etc/stunnel/client.pem
key = /etc/stunnel/client_key.pem
verify = 2
CAfile = /etc/stunnel/ROOT_RKL_CA.pem
accept = 192.168.88.208:7008
connect = 10.35.1.42:1801
```

```
[UCM]
cert = /etc/stunnel/server.pem
key = /etc/stunnel/server_key.pem
verify = 2
CAfile = /etc/stunnel/server.pem
accept = 192.168.88.208:2000
connect = 192.168.88.217:2000
```

Подключение к «UCM» через SSL соединение используя RKL сертификаты сервера и клиента (проверка клиента на сервере).

Файл параметров «**parameters.json**»

```
{
  "ucm": {
    "connections": [
      {
        "name": "default UCM",
        "address": "192.168.88.208",
        "port": "2001",
        "useSsl": true,
        "ca": "ca.pem",
        "useCahSsl": true
      }
    ]
  },
  "cah": {
    "connection": {
      "address": "10.129.106.105",
      "port": "1801"
    }
  },
  "kdh": {
    "useRklLoaded": true,
    "connection": {
      "address": "192.168.88.208",
      "port": "7008",
      "useSsl": true,
      "ca": "ca.pem"
    }
  }
}
```

Пример блока настроек «**Stunnel**»

```
[DLA]
cert = /etc/stunnel/client.pem
key = /etc/stunnel/client_key.pem
verify = 2
CAfile = /etc/stunnel/ROOT_RKL_CA.pem
accept = 192.168.88.208:7008
connect = 10.35.1.42:1801
```

```
[UCM]
cert = /etc/stunnel/server.pem
key = /etc/stunnel/server_key.pem
verify = 2
CAfile = /etc/stunnel/ROOT_RKL_CA.pem
accept = 192.168.88.208:2000
connect = 192.168.88.217:2000
```

Используемые файлы в примерах:¹

- **ca.pem** – файл содержащий цепочку доверительных сертификатов;
- **server.pem, server_key.pem** – файл сертификата и ключа сервера;
- **client.pem, client_key.pem** – файл сертификата и ключа клиента;

¹ Расширение файлов должно быть в строго в нижнем регистре (пример, «**ca.pem**»)

- **ROOT_RKL_CA.pem** – файл содержащий доверительные сертификаты серверов RKL.