

KDH (Key Distribution Host)

Схема взаимодействия

Версия 3.0.4

История изменений документа

Версия	Дата	Перечень изменений
1.0	17.10.2018	Первоначальная версия документа

Содержание

1. Введение	4
2. Термины и определения	5
3. Общая схема решения	6
3.1. Компонентный состав	6
3.2. Схема взаимодействия удаленной загрузки KLK в POS-терминал	7
3.3. Сценарий смены KLK на POS-терминале	9
3.4. Настройка ПО	9
3.4.1. PSP.....	9
3.4.2. KDH	9
3.4.3. UCM	10

1. Введение

Данный документ описывает взаимодействие между ПО «**PSP**», системы «**RKL**» и «**UCM**», чтобы выполнять загрузку KLK в физический POS-терминал удаленного, без ручного ввода компонент KLK.

2. Термины и определения

Download Server	UniPOS Config Manager Download Server – сервер удаленной параметризации и обновления ПО POS-терминалов.
DS	Download Server
HSM	Hardware Security Module – аппаратный модуль безопасности, предназначенный для безопасной работы с криптографическими ключами и выполнения криптографических операций с использованием ключей.
KCV	Key Check Value – проверочное значение криптографического ключа. Используется для проверки целостности ключа при его передаче.
KDH	Keys Distribution Host – Сервер удаленной загрузки ключей. Один из компонентов RKL, служащий для безопасной передачи ключей на POS-терминал по открытым каналам связи.
KLK	Key Loading Key – ключ загрузки других ключей. Используется как шифрующий ключ для формирования криптограммы другого ключа.
LMK	Local Master Key – внутренний ключ HSM.
POS-терминал	Устройство для безопасного проведения платежей с использованием платежных карт. В контексте данного ТЗ – устройство, принимающее, хранящее и использующее криптографические ключи для обеспечения безопасности проведения платежей.
PSP	Payment Service Provider – сервер, предоставляющий владельцу POS-терминала сервис проведения платежей на стороннем банковском хосте. В контексте данного ТЗ – аналог авторизационного хоста для POS-терминала.
RKL	Remote Key Loading – система удаленной загрузки криптографических ключей в POS-терминалы.
S/N	Серийный номер.
TMK	Terminal Master Key – мастер-ключ POS-терминала.
TMS	Terminal Management System – система параметризации и загрузки ПО на POS-терминалы.
UCM	UniPOS Config Manager – система параметризации и загрузки ПО на POS-терминалы.
ZMK	Zone Master Key – зональный мастер-ключ, используемый для безопасной передачи других ключей.
ПО	Программное обеспечение.
ЦП	Цифровая подпись. Служит для проверки подлинности сформированных данных. Формируется с использованием приватной компоненты RSA-ключа, проверяется с использованием публичной компоненты RSA-ключа.

3. Общая схема решения

3.1. Компонентный состав

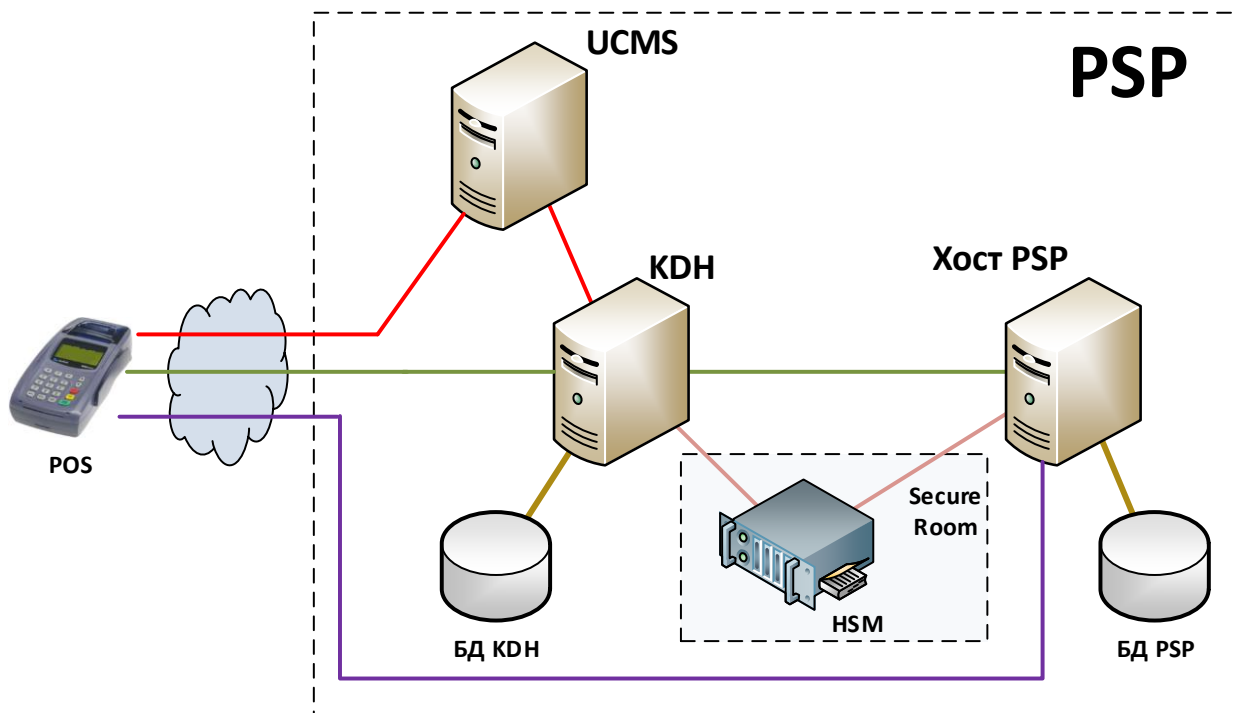


Рисунок 1. Компонентный состав решения

Решение включает в себя следующие компоненты:

1. UCMS (UniPOS Config Manager System) / TMS (Terminal Management System). Система параметризации POS-терминалов.
2. KDH (Keys Distributing Host). Сервер удаленной загрузки ключей. Принимает из PSP, хранит и передает на POS-терминал ключи KLK.
3. POS-терминал. Является целевым устройством, которое удаленным способом получает KLK с сервера удаленной загрузки ключей (KDH).
4. HSM. Аппаратный модуль безопасности, необходимый для перешифрования KLK, предназначенных для загрузки в POS-терминал, с ключа ZMK на публичный ключ POS-терминала. Также используется для формирования цифровой подписи KDH над пакетом данных, содержащим отправляемый на POS-терминал KLK.
5. Хост PSP. Генерирует и хранит KLK POS-терминалов. Получает от KDH информацию о «привязке» определенного KLK к определенному POS-терминалу после получения POS-терминалом KLK с KDH.

3.2. Схема взаимодействия удаленной загрузки KLK в POS-терминал

На рисунке ниже представлена схема взаимодействия компонент при загрузке KLK в POS-терминал:

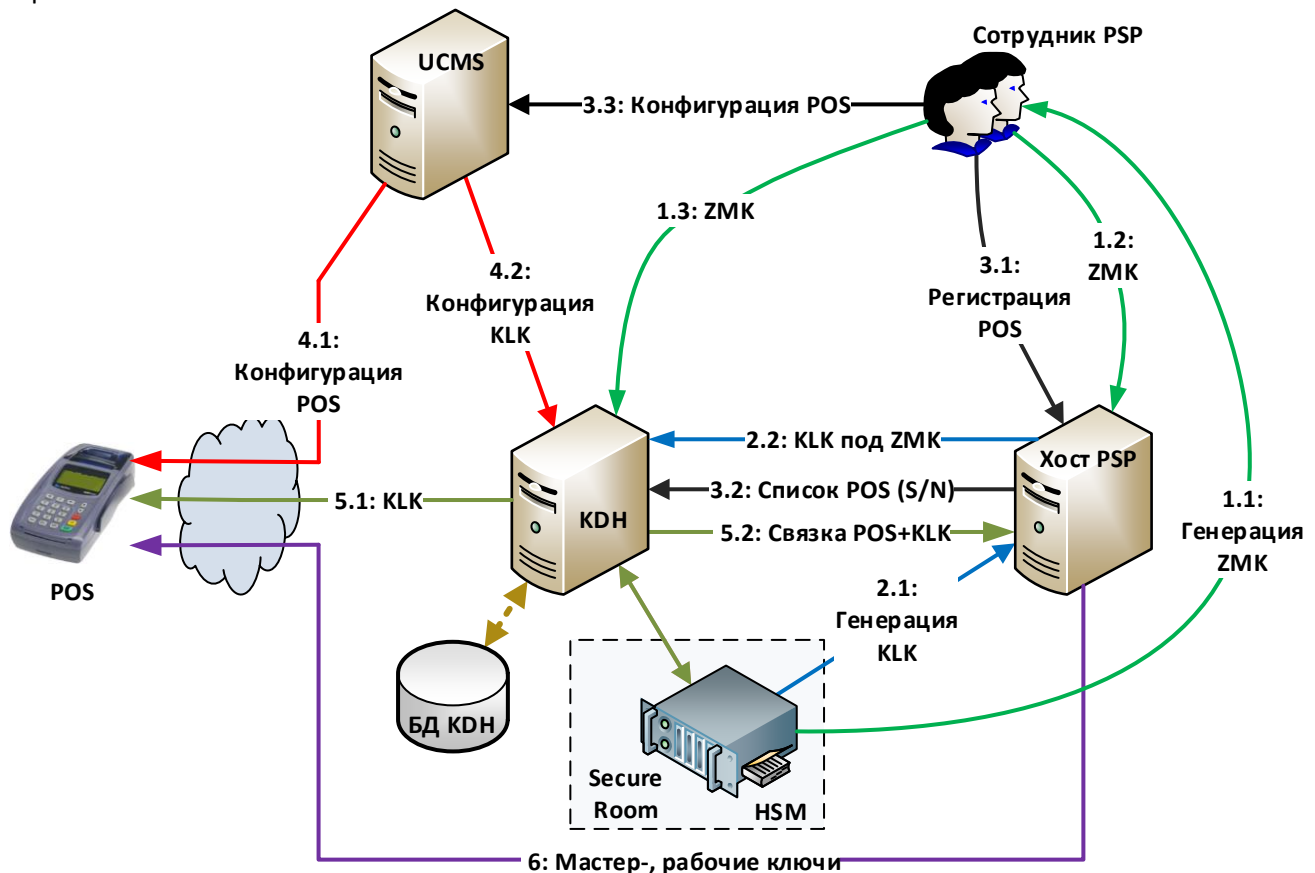


Рисунок 2. Схема взаимодействия компонент

Процедура состоит из следующих шагов:

1. Загрузка ZMK.
 - 1.1. ZMK генерируется на HSM PSP.
 - 1.2. Криптограмма ZMK под LMK загружается в PSP.
 - 1.3. Криптограмма ZMK под LMK загружается в KDH.
2. Формирование KLK:
 - 2.1. Пачка KLK генерируется на HSM PSP. Каждый KLK имеет уникальный идентификатор, по которому в дальнейшем осуществляется привязка KLK к POS-терминалу.
 - 2.2. Сгенерированные KLK экспортируются на ZMK и передаются по HTTP на KDH в виде файлов (один файл может содержать множество KLK). На момент загрузки KLK на KDH эти KLK «обезличены», т.е. не привязаны ни к какому POS-терминалу.
3. Регистрация POS-терминалов в системе. Выполняется по мере ввода POS-терминалов в эксплуатацию и состоит из следующих шагов:
 - 3.1. Сотрудник PSP регистрирует POS-терминал в PSP. При регистрации в числе прочих данных фиксируется S/N POS-терминала.
 - 3.2. Для каждого зарегистрированного, либо для группы зарегистрированных POS-терминалов PSP формирует файл со списком S/N этих POS-терминалов. Список S/N POS-терминалов передается по HTTP на KDH в виде файла. Без такой регистрации POS-терминал не сможет получить ключи с KDH.
 - 3.3. Для каждого вводимого в эксплуатацию POS-терминала в системе параметризации (UCMS / TMS) создается конфигурация.

4. Получение POS-терминалом и KDH конфигурации POS-терминала (в том числе конфигурации KLK):
 - 4.1. Получение POS-терминалом конфигурации из системы параметризации (UCMS / TMS).
 - 4.2. Автоматическая передача из UCMS на KDH по HTTP конфигурации KLK.
5. Удаленная загрузка KLK в POS-терминал с KDH и синхронизация на Хосте PSP информации о привязке KLK к POS-терминалу:
 - 5.1. Получение KLK POS-терминалом состоит из следующих шагов (на графической схеме не детализировано):
 - 5.1.1. POS-терминал и KDH обмениваются сертификатами своих публичных ключей и проверяют сертификаты друг друга, удостоверившись, в том числе, что цепочки сертификатов сходятся на сертификате корневого УЦ ИНПАС.
 - 5.1.2. POS-терминал запрашивает у KDH ключи.
 - 5.1.3. KDH, найдя в БД S/N POS-терминала, а также конфигурацию ключей данного POS-терминала:
 - 5.1.3.1. Выбирает из БД первый «свободный» KLK и «привязывает» выбранный KLK к POS-терминалу.
 - 5.1.3.2. Перешифровывает выбранный KLK с ZMK (под которым хранится KLK в БД KDH) на публичный ключ POS-терминала, полученный из сертификата POS-терминала.
 - 5.1.3.3. Формирует пакет, содержащий:
 - Криптограмму KLK.
 - KCV KLK.
 - Номер слота.
 - 5.1.3.4. Формирует ЦП пакета с использованием своего приватного ключа.
 - 5.1.3.5. Отправляет пакет на POS-терминал.
 - 5.1.4. POS-терминал, получив пакет от KDH:
 - 5.1.4.1. Проверяет ЦП с использованием полученного ранее сертификата KDH.
 - 5.1.4.2. С использованием своего приватного ключа расшифровывает криптограмму KLK.
 - 5.1.4.3. Проверяет KLK по KCV.
 - 5.1.4.4. Сохраняет KLK в пинпаде в нужной ячейке (слоте).
 - 5.1.5. POS-терминал отправляет на KDH подтверждение об успешной загрузке KLK.
 - 5.1.6. KDH, получив подтверждение, меняет в БД статус POS-терминала и статус отправленного ему KLK.
 - 5.2. KDH уведомляет хост PSP о привязке KLK (по идентификатору KLK) к POS-терминалу (по S/N POS-терминала) путем отправки на PSP HTTP-пакета с указанными идентификаторами KLK и POS-терминала.

В результате выполнения всех вышеприведенных шагов в POS-терминале имеется KLK, а на хосте PSP аналогичный KLK «привязан» к данному POS-терминалу. Как следствие, при помощи данного KLK POS-терминал может получить с хоста PSP мастер-ключи, а затем с помощью этих мастер-ключей – рабочие ключи (шаг 6 на схеме).

3.3. Сценарий смены KLK на POS-терминале

При необходимости смены KLK в POS-терминале выполняется следующая последовательность действий:

1. Оператор KDH через web-интерфейс меняет статус POS-терминала с «USED» на «READY». В результате KDH «отвязывает» от POS-терминала текущий (теперь уже бывший) KLK, одновременно меняя статус KLK на «EXPIRED». После этого KDH готов принять от POS-терминала запрос на загрузку нового KLK.
2. Оператор POS-терминала из меню POS-терминала запускает загрузку ключей с KDH, в результате чего выполняется штатная процедура загрузки KLK, шаги которой описаны в п.п.5 пункта 3.2 Схема взаимодействия удаленной загрузки KLK в POS-терминал.
3. Хост PSP, получив от KDH уведомление о привязке нового KLK к POS-терминалу, отвязывает от POS-терминала старый KLK, привязывает новый. Старый KLK помечается на PSP соответствующим образом, и не должен быть использован в дальнейшем.

3.4. Настройка ПО

3.4.1. PSP

1. Наименование хоста, зарегистрированного на KDH как хост PSP.
2. Группу параметров для выгрузки S/N POS-терминалов:
 - 2.1. URL, по которому KDH принимает HTTP-запрос со списком S/N POS-терминалов.
 - 2.2. Логин и пароль пользователя, зарегистрированного на KDH.
 - 2.3. Таймаут установки соединения с KDH и получения HTTP-ответа от KDH.
 - 2.4. Признак (флаг: вкл./выкл.) необходимости осуществления повторных попыток отправки HTTP-запросов на KDH.
 - 2.5. Параметры email-уведомлений, рассылаемых с целью информирования о неуспешной отправке на KDH информации со списком S/N POS-терминалов.
3. Группа параметров для выгрузки набора KLK:
 - 3.1. URL, по которому KDH принимает HTTP-запрос с набором KLK.
 - 3.2. Логин и пароль пользователя, зарегистрированного на KDH.
 - 3.3. Таймаут установки соединения с KDH и получения HTTP-ответа от KDH.
 - 3.4. Признак (флаг: вкл./выкл.) необходимости осуществления повторных попыток отправки HTTP-запросов на KDH.
 - 3.5. Параметры email-уведомлений, рассылаемых с целью информирования о неуспешной отправке на KDH набора KLK.



ПРИМЕЧАНИЕ: Более подробное описание настроек можно посмотреть в документе «Руководство оператора UniPort PSP».

3.4.2. KDH

1. В числе хостов, необходимо зарегистрировать хост с наименованием, заданным в настройках сервера PSP в параметре «Наименование хоста PSP для KDH».
2. Для хоста PSP из пункта выше необходимо указать:
 - 2.1. URL, по которому PSP ожидает HTTP-запрос с привязкой KLK к POS-терминалу.
 - 2.2. Имя и пароль пользователя, зарегистрированного на PSP в качестве учетной записи.
3. Для хоста PSP из пункта выше необходимо зарегистрировать ZMK.



ПРИМЕЧАНИЕ: Более подробное описание настроек можно посмотреть в документе «KDH_User_Guide».

3.4.3. UCM

1. В конфигурации POS-терминала задать идентификатор Хоста, совпадающий с идентификатором хоста PSP, зарегистрированным на KDH (или, что равнозначно, со значением параметра «Наименование хоста PSP для KDH» в настройках PSP).
2. В настройках DownloadServer «включить» использование плагина RKL.



ПРИМЕЧАНИЕ: Более подробное описание настроек можно посмотреть в документе «Руководство по использованию плагина RKL».