Описание функциональных характеристик LANKEY

Версия 1.0

Оглавление

ИСПОЛЬЗУЕМЫЕ ОБОЗНАЧЕНИЯ

Таблица 1. Используемые обозначения

Обозначение	Комментарий
Полужирный	Наименование кнопок
Курсив	Наименование пунктов меню, файлов и элементов программного интерфейса на компьютере
⚠	Примечание

ТЕРМИНЫ И АББРЕВИАТУРЫ

Таблица 2. Термины и аббревиатуры

Термины и аббревиатуры	Определение
Банк	Заказчик специального ПО
ГО	Головной офис
KMS	Key Management System – приложение SV Система учета и генерации криптографических ключей
S/N	Серийный номер POS-терминала
POS	POS-терминал, эквайером которого является банк, для установки в ПВН банка или в ТСП
SV	Хост банка
CMS	Бэк-офис банка
RKI	Remote Key Injection – программное обеспечение, вендора POS-терминалов, обеспечивающее удаленную загрузку TMK в POS
Raptor	Сервер приложений, который используется для взаимодействия с HSM с целью генерации криптографических ключей
Stunnel	SSL/STL сервер
TMK	Terminal Master Key – мастер-ключ терминала, под которым проводится обмен рабочими ключами
ZMK	Zone Master Key – ключ DES, которым шифруются ключи TMK, используемые для обмена информацией между двумя субъектами. ZMK используется для передачи TMK на RKI
LMK	Local Master Key – локальный мастер-ключ, представляющий собой ключ верхнего уровня, который используется и хранится в HSM
HSM	Программно-аппаратный модуль безопасности, который генерирует наборы секретных криптографических ключей для последующей загрузки в целевое устройство
ДТС	Департамент терминальной сети
ДРТ	Департамент развития технологий
ДП	Департамент процессинга
ДКР	Департамент контроля рисков
СЗК/KDH	Система Загрузки Ключей (LANKEY)
ПС	Платежные системы (МПС, НСПК, VPAY) или операции on-us в межхосте
Single Merchant	Мерчант, у которого для каждого POS используется отдельный Terminal_ID

Термины и аббревиатуры	Определение
Multi Merchant	Мерчант, у которого для одного POS используется несколько Terminal_ID
TermId	Основной внутренний идентификатор терминала в SV
Terminal_ID	Основной уникальный параметр, по которому: • осуществляется регистрация POS в TMS • осуществляется установка конфигурации, а также взаимодействие POS с СЗК
Host_ID	Уникальный идентификатор хоста внутри банка
Key_ID	Уникальный идентификатор TMK в банке
Check value	Проверочное значение ключа TMK или ZMK
ЖЦ	Жизненный цикл
СГК	Банковский скрипт генерации ключей
GUI	Graphical user interface – графический пользовательский интерфейс
MFT	Managed File Transfer – управляемая передача файлов на базе ПО EFT Server Enterprise компании GlobalScape. Это решение может работать FTP/SFTP/FTPS сервером и запускать по расписанию или иному виду событий какой-либо исполняемый файл
TMS	Система параметризации POS-терминалов

ЛИСТ ИЗМЕНЕНИЙ

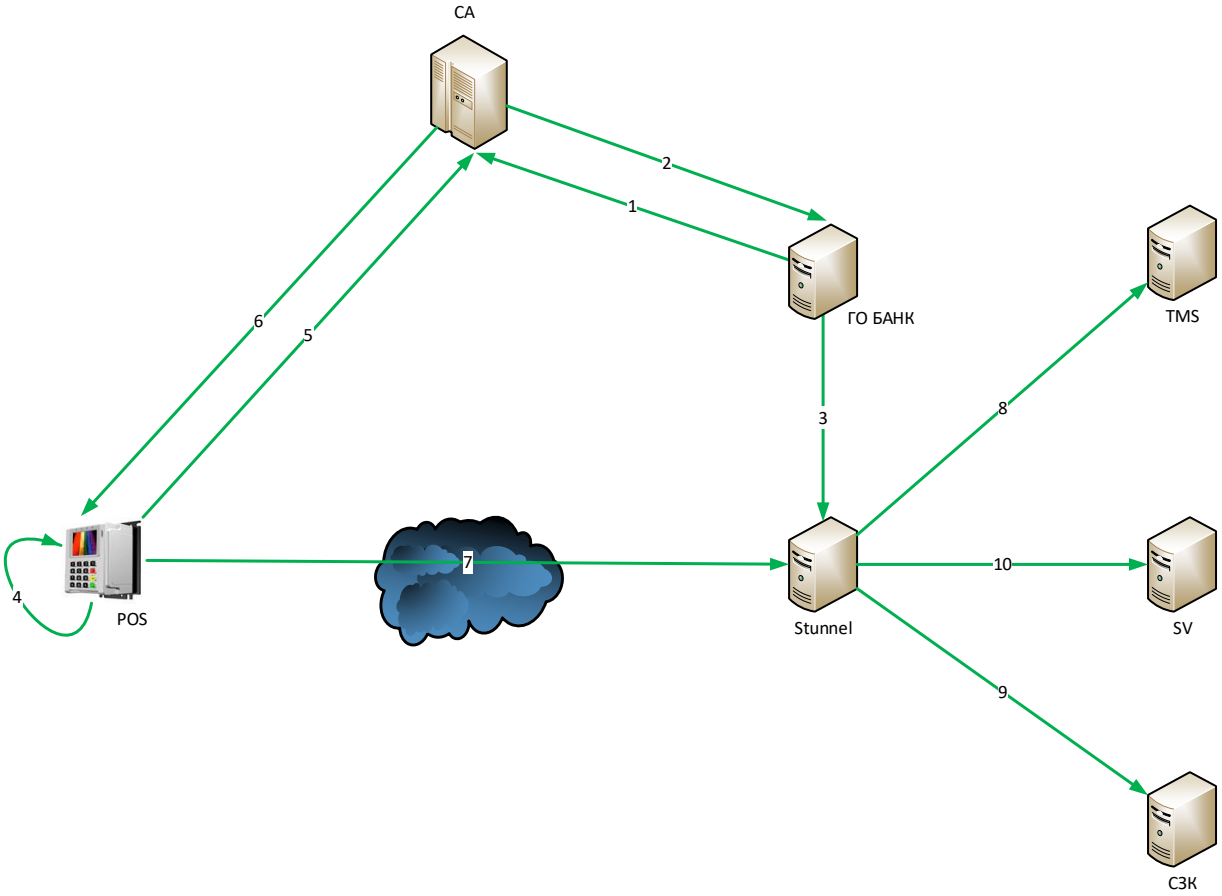
Таблица 3. Лист изменений

Версия	Дата	Автор	Детали
1.0	29.05.2023	Лисайчук Ф.В.	Создание документа

ВВЕДЕНИЕ

В настоящем документе, разработанным компанией «Лантер», описывается СЗК, с помощью которой выполняется автоматическая загрузка криптографических ключей в POS-терминалы.

1. ОБЩАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ ПРИ ВЫПОЛНЕНИИ УДАЛЕННОЙ ЗАГРУЗКИ КЛЮЧЕЙ



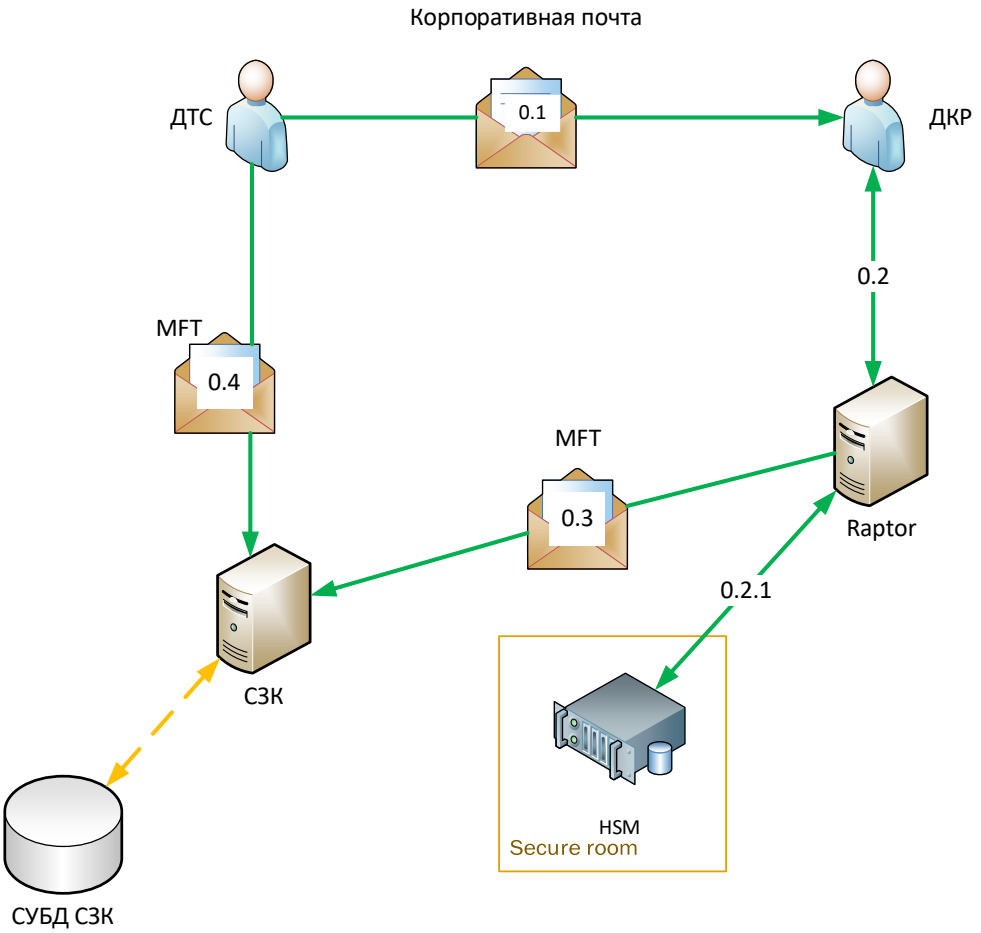
1. Банк выпускает комплект RSA-ключей и передает запрос на подпись публичного ключа вендору POS-терминалов
2. Вендор возвращает банку подписанный сертификат вместе со своим корневым сертификатом
3. Банк использует присланные от вендора сертификаты для поднятия на своей стороне SSL/TLS сервера
4. В POS-терминал устанавливается приложение, созданное компанией «Лантер», которое осуществляет взаимодействие с устройством для подписи сертификата
5. Приложение Лантер, с использованием STLS API, генерирует терминальную пару RSA-ключей и формирует запрос на подпись своего публичного ключа из этой пары, с помощью устройства для подписи, которое выступает в данном случае УЦ

6. POS-терминал получает подписанный сертификат и корневой сертификат и помещает их в свою защищенную зону
7. Корневой сертификат в дальнейшем используется для установки TLS канала связи с SSL/TLS сервером банка для первичной загрузки TMS-параметров и криптографических ключей
8. По защищённому соединению POS отправляет на TMS запрос на загрузку параметров и зашифрованных банковских SSL-сертификатов, которые будут использоваться для всех последующих рабочих операций: повторная загрузка параметров, ключей, проведение транзакций
9. POS загружает с сервера СЗК ТМК и ключ для дешифровки банковских SSL-сертификатов
10. Загрузка рабочих ключей с хоста банка, и все последующие операции, выполняется уже с использованием расшифрованных банковских SSL-сертификатов.

2. ОПИСАНИЕ ПРОЦЕДУР ПОДГОТОВКИ И РЕАЛИЗАЦИИ СЗК

2.1 Подготовка и передача ZMK и S/N

Подготовка и передача ZMK и S/N представлена на схеме №1:



2.1.1 Подготовка и передача ZMK

Описание схемы №1:

- Шаг 0.1

По мере необходимости ДТС направляет через корпоративную почту в ДКР заявку на формирование ZMK для определенного филиала банка, указывая Host_ID

- Шаг 0.2

Для всех Host_ID ДКР, получив заявку от ДТС, инициирует в ручном режиме на сервере Raptor с помощью СГК процесс генерации необходимого количества ZMK на HSM

- Шаг 0.2.1

Генерация ZMK. Ключ должен быть выпущен в виде двух криптограмм (трансляция под LMK авторизационного HSM, и криптограммы под LMK HSM, находящегося в контуре СЗК). ZMK уникальный для каждого Host_ID под одним и тем же LMK. Основные параметры – см. Приложение №12.

- Шаг 0.3

Средствами MFT файл *ZMK для СЗК* передаётся на СЗК. Порядок действий с ZMK следующий:

- ZMK_Status после ввода в СЗК будет *LOADED*.
- Для проверки, что полученная криптограмма ZMK зашифрована именно тем LMK, ID которого передан вместе с ключом, необходимо:
- ✓ Отправить запрос на HSM импорт ZMK с указанным ZMK_ID
- ✓ При отсутствии ошибки в ответе HSM считать проверку успешной (т.е. Response code HSM на соответствующую команду равен 00).

2.1.2 Подготовка и передача S/N

Описание схемы №1:

- Шаг 0.4

ДТС получает информацию по актуальному списку S/N (файл *Список серийных номеров*, см. Приложение №11) и пополняет список S/N в СЗК со S/N_Status *NEW*.

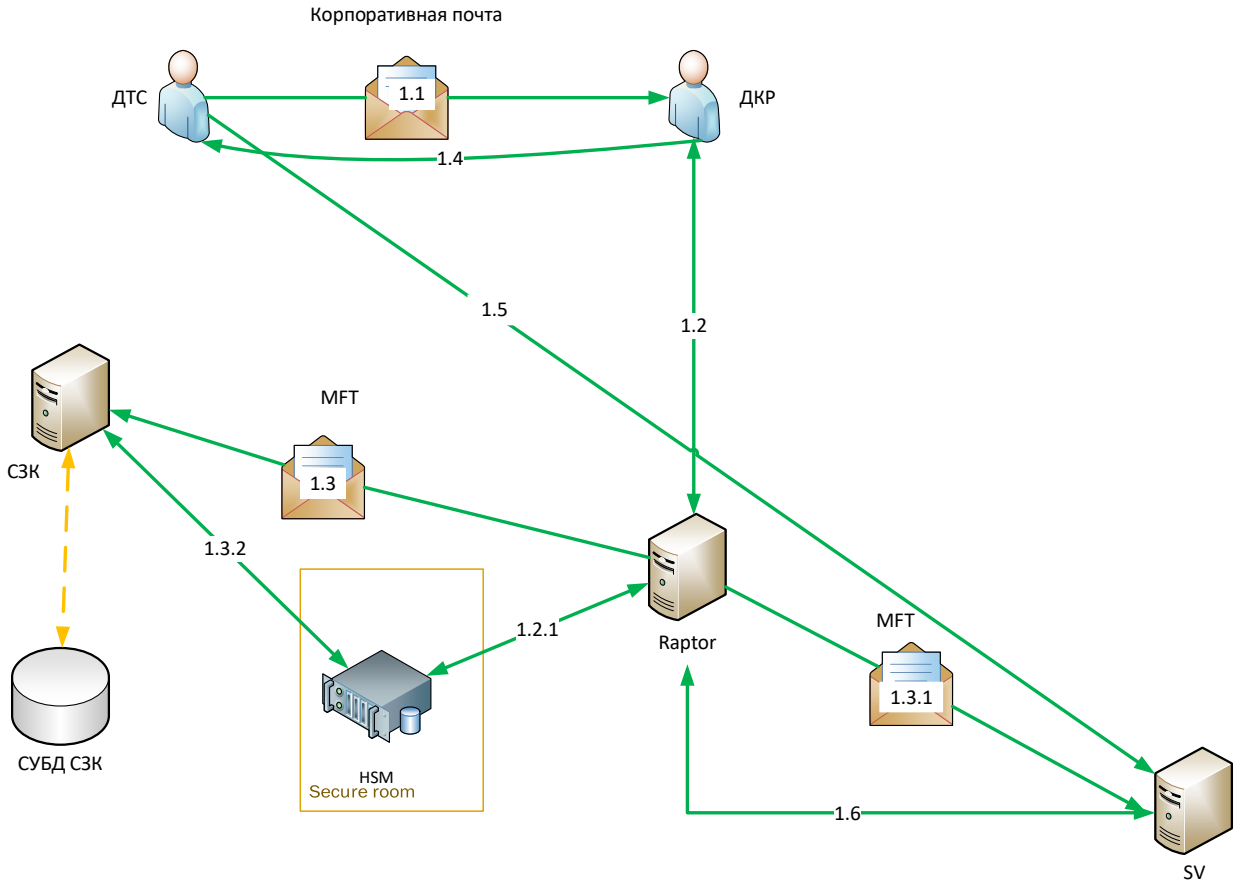
Возможны два режима обновления:

а) В ручном режиме через GUI СЗК

б) Путем обработки файла *Список серийных номеров* (Приложение №5).

2.2 Подготовка и передача TMK для СЗК и SV

Подготовка и передача TMK представлена на схеме №2:



Описание схемы №2:

- Шаг 1.1

ДТС по корпоративной почте направляет в ДКР заявку на формирование определенного количества TMK для POS-терминалов для определенного филиала банка, указывая Host_ID

- Шаг 1.2

ДКР, получив заявку от ДТС, инициирует в ручном режиме на сервере Raptor с помощью СГК процесс генерации необходимого количества TMK на HSM. В случае окончания срока действия ZMK, инициируется генерация ZMK.

- Шаг 1.2.1

Raptor обращается к HSM, передавая команды на генерацию TMK и транслирует полученные TMK:

- под ZMK для СЗК – файл *TMK для СЗК*
- под LMK для SV – файл *TMK для SV*.

ТМК назначается уникальный Key_ID. При формировании для разных систем (SV, СЗК), один и тот же ТМК формируется с тем же Key_ID.

- Шаг 1.3

Из каталога Raptor'а средствами MFT передается на СЗК пакет криптограмм ТМК (ZMK), предназначенных для загрузки в POS (см. Приложение №7). Возможны два режима:

  - В ручном режиме через GUI
  - Путем автоматической обработки файла *ТМК для СЗК*.

- Шаг 1.3.1

Из каталога Raptor'а средствами MFT передается в SV пакет криптограмм ТМК (LMK), предназначенных для загрузки в POS.

- Шаг 1.3.2

- Для проверки, что полученная криптограмма ТМК зашифрована именно тем ZMK, ID которого передан вместе с ключом, необходимо:
  - ✓ послать запрос на HSM импорт (из-под ZMK на LMK) ТМК с указанным ZMK_ID.
  - ✓ при отсутствии ошибки в ответе HSM считать проверку успешной (т.е. Response code HSM на соответствующую команду равен 00)
  - ✓ СЗК проверяет соответствие полученных ключей актуальному ZMK, для этого производится трансляция TMK(ZMK) в TMK(LMK). При отсутствии ошибки в ответе HSM проверка считается успешной – TMK_Status *READY*
  - ✓ СЗК формирует список актуальных криптограмм и сохраняет его в своей СУБД

- Шаг 1.4

ДКР по корпоративной почте передает в ДТС информацию о генерации нового пакета ТМК

- Шаг 1.5

ДТС инициирует пакетную загрузку ТМК в SV в модуль KMS, используется ТМК (LMK) для POS – файл *ТМК для SV*.

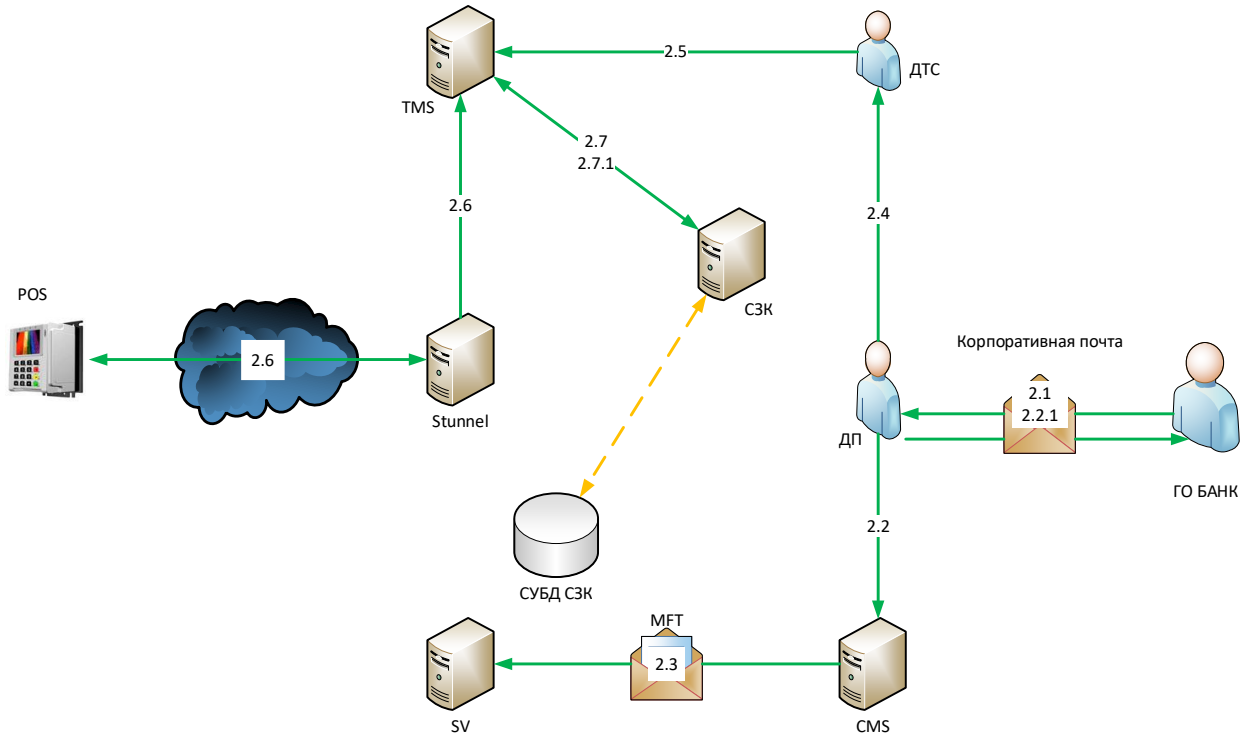
В SV загружается криптограммы вместе с уникальным Key_ID.

- Шаг 1.6

В процессе пакетной загрузки ключей SV обращается к Raptor для получения пакета TMK (LMK) для Банка.

2.3 Подготовка и установка конфигурации POS

Подготовка и установка конфигураций POS представлена на схеме №3:



Описание схемы №3:

- Шаг 2.1

ГО Банк передает заявку на регистрацию Merchant/POS в ДП

- Шаг 2.2

ДП регистрирует Merchant/POS в CMS, присваивая Terminal_ID с уникальным номером

- Шаг 2.2.1

ДП передает результаты обработки заявки на регистрацию Merchant/POS в ГО Банк

- Шаг 2.3

Из CMS регистрационные данные (в т.ч. Terminal_ID) выгружаются и передаются средствами MFT в SV

- Шаг 2.4

ДП передает заявку на регистрацию с заполненным полем *Terminal_ID* в ДТС

- Шаг 2.5

ДТС при подготовке конфигурации в TMS заводит необходимые параметры в т.ч. обязательный параметр Terminal_ID, S/N, признак хоста Host_ID, IP:port сервера СЗК.

ДТС при заведении терминального профиля идентификатором указывает первые 4 и последние 4 цифры серийного номера терминала

- Шаг 2.6

При подготовке терминала к установке в ТСП осуществляется удаленная загрузка конфигурации с TMS, и на POS передается набор необходимых параметров (в т.ч. Terminal_ID). При передаче данных используется TLS 1.2 соединение со взаимной аутентификацией на основе сертификата, полученного при инициализации устройства вендором и встроенного в ПО, для первичной загрузки параметров. В процессе первичной загрузки параметров каждый POS получает зашифрованный набор SSL-сертификатов, в формате PKCS#12, для дальнейшей работы

- Шаг 2.7

По факту успешной загрузки параметров TMS автоматически формируется запрос в СЗК, в котором присутствует S/N и соответствующие ему TerminalD и Host_ID – см. файл *Загрузка конфигурации для POS* (см. Приложение №11).

Передача информации от СЗК логируется на СЗК, а приём информации в TMS – соответственно на TMS

- Шаг 2.7.1

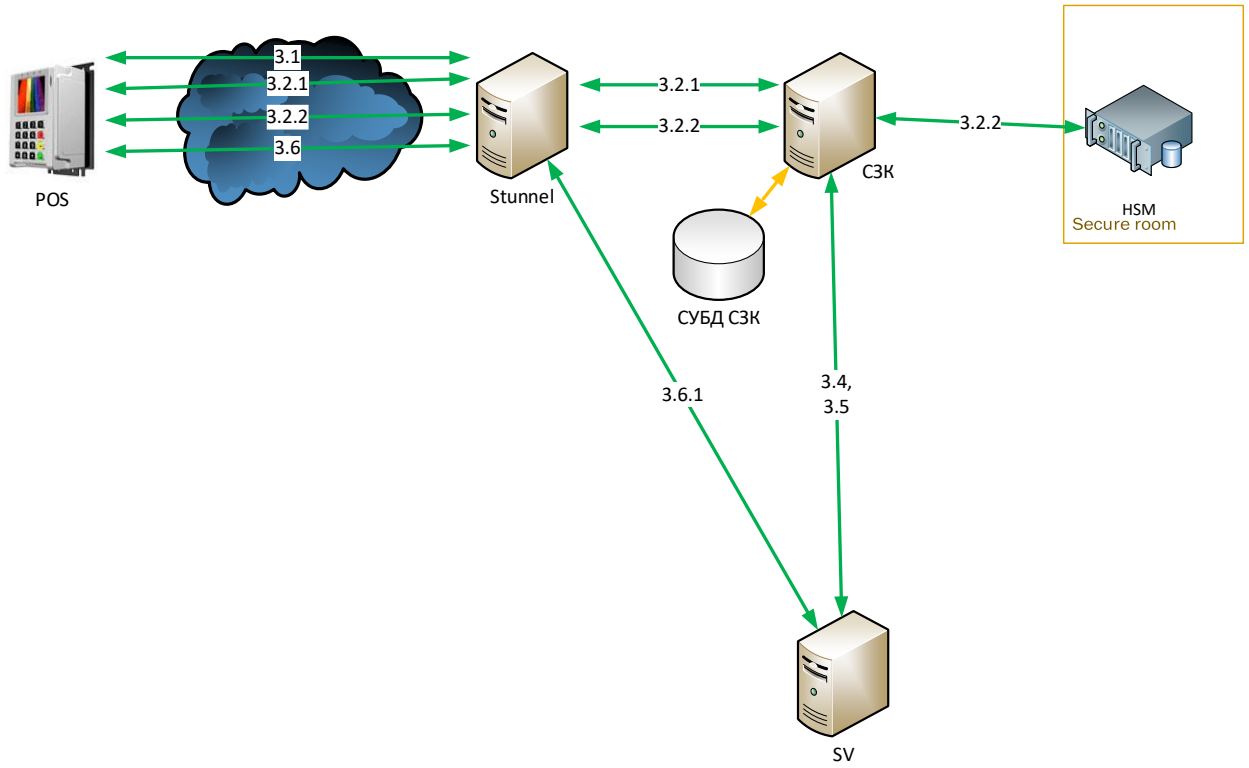
С Multi Merchant добавление вторых и последующих Terminal_ID в СЗК осуществляется по событию Загрузки конфигурации для S/N из TMS в СЗК.

Передаётся файл *Загрузка конфигурации для POS* (Приложение №11) на СЗК, в котором содержатся S/N и соответствующие ему Terminal_ID и Host_ID.

В СЗК S/N ранее привязанный к другому Terminal_ID и имеющий S/N_Status *USED* клонируется для другого Terminal_ID.

2.4 Удалённая загрузка TMK на POS и ключа для дешифрирования SSL-сертификатов полученных от TMS

Удалённая загрузка TMK и ключа для дешифровки на POS представлена на схеме №4:



- Шаг 3.1

POS подключается к Stunnel и устанавливает соединение по протоколу TLS 1.2 с использованием корневого сертификата, выданного УЦ вендора

- Шаг 3.2.1

Между POS и СЗК осуществляется обмен сертификатами и взаимная верификация. POS отправляет на СЗК запрос на получение TMK, включив в запрос такие параметры как: тип запрашиваемого ключа (PIN/MAC), свой серийный номер, случайное число и свой сертификат публичного ключа. СЗК проверяет наличие серийного номера в своём списке серийных номеров

терминалов, где S/N_Status=READY, определяет Host_ID. СЗК проверяет наличие в БД криптограмм ключей для Host_ID, ZMK_Status=READY и TMK_Status=READY. СЗК выбирает из БД нужную криптограмму ключа (самая старшая). Далее СЗК подает на HSM команду перешифрования TMK с LMK на публичный ключ POS, потом СЗК подает на HSM команду генерации подписи на своем Private Key. Подпись осуществляется на набор данных - криптограмма ключа, серийный номер POS и случайное число. СЗК пересылает на POS: зашифрованный на публичном ключе POS TMK, ключ для дешифрования банковских SSL-сертификатов, подпись набора данных и сертификат публичного ключа СЗК. POS сначала проверяет достоверность сертификата публичного ключа СЗК, потом проверяет подпись набора данных на публичном ключе СЗК и потом POS загружает зашифрованный TMK во внутреннее секретное хранилище и ключ для расшифровки пароля от банковских SSL-сертификатов. POS сообщает факт загрузки ключа в СЗК. При возникновении сбоя в процессе загрузки ключа POS сообщает об этом в СЗК. В процессе выполнения данного шага СЗК ведет лог, в котором отражена вся доступная информация о POS-терминале и результаты выполнения отдельных операций данного шага

- Шаг 3.2.2

СЗК обеспечивает параллельную работу по загрузке ключей в несколько терминалов одновременно

- Шаг 3.3

После завершения передачи в СЗК меняется:

  - S/N_Status с *READY* на *USED*
  - TMK_Status с *READY* на *LOADED_IN_POS*
  - В логе СЗК формирует соответствующую запись.

- Шаг 3.4

СЗК получив полный пакет данных (Terminal_ID, S/N, Key_ID, Host_ID), определив хост владельца POS, передает в SV уведомление GetTermList для получения внутреннего ID терминала (TermId).

Получив успешный ответ от SV, СЗК связывает TermId с Terminal_ID

- Шаг 3.5

а) СЗК формирует запрос об успешной загрузке ключа AssignKeyByTerm. В системе учета ключей СЗК производится учет данного действия. SV возвращает ответ на AssignKeyByTerm.

б) В СЗК меняется TMK_Status с *LOADED_IN_POS* на *LOADED_IN_SV*.

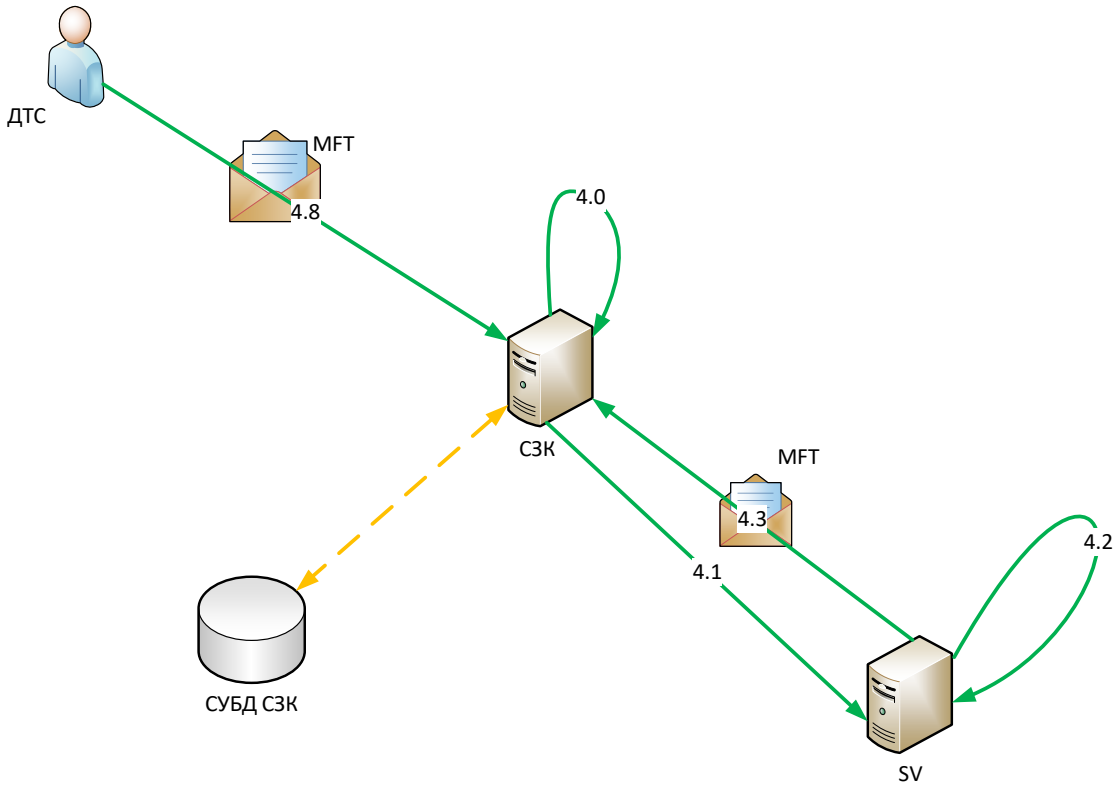
- Шаг 3.6 – 3.6.1

Проведение транзакций в POS, выход в ПС через SV.

3. ДАЛЬНЕЙШИЙ ЖИЗНЕННЫЙ ЦИКЛ СЗК

3.1 Жизненные циклы TMK, ZMK и S/N

Жизненный цикл TMK, ZMK и S/N представлен на схеме №5:



- Шаг 4.0

При появлении в СЗК событий по POS, у которых:

- истек срок действия ZMK (TMK_Status изменился на *EXPIRED*)
- истек срок действия TMK (TMK_Status изменился на *EXPIRED*)
- TMK скомпрометирован (такой TMK_Status вручную меняется оператором СЗК на *COMPROMISED*)

Выполняются следующие действия:

- Шаг 4.1

а) СЗК формирует сообщение в SV об изменении статуса TMK ключей – *ChangeKeyStatus*

Для TMK_Status со значением:

- EXPIRED необходимо оставить поле с криптограммой, контрольная сумма (Check Value) ключа также не удаляется для осуществления контроля невозможности повторной загрузки данного ключа в СЗК
- COMPROMISED требуется оставить поле с криптограммой.

б) SV получив такое сообщение, изменяет статус ключа TMK на истек срок действия *TMK* и по итогам такого события формирует ответное сообщение в СЗК.

⚠ Единовременно для каждого Host_ID должен быть только один активный ZMK. Новый ZMK и пакет ключей к нему выпускаются заранее, но в систему загружаются после вывода из эксплуатации старого пакета ZMK/TMK. Загрузка нового пакета ключей осуществляется в ходе запланированных регламентных работ.

- Шаг 4.2

Оператор SV, при наступлении такого события, в зависимости от ситуации меняет в KMS статус TMK в случаях:

- истек срок действия TMK – *EXPIRED*
- раскрытием третьей стороне – *COMPROMISED*
- удалением при выводе из эксплуатации Host_ID – *CANCELLED*.

После наступления такого события:

- Шаг 4.3

а) SV формирует для СЗК отчет *Key Status Report* (см. Приложение №9). Отчет передается средствами MFT

б) СЗК, получив отчет *Key Status Report*, меняет TMK_Status, не отвечая SV на *EXPIRED, COMPROMISED* или *CANCELLED*.

Для TMK_Status со значением:

- EXPIRED необходимо оставлять поле с криптограммой, контрольная сумма (Check Value) ключа также не удаляется для осуществления контроля невозможности повторной загрузки данного ключа в СЗК

- COMPROMISED и CANCELLED требуется оставить поле с криптограммой.

Возможны два режима обновления:

б.1) В ручном режиме через GUI

б.2) Путем автоматической обработки файла *Key Status Report*.

- Шаг 4.4[1]

ДКР в ручном режиме через GUI в случаях, когда ТМК раскрытием третьей стороне меняет TMK_Status *READY* статус на *COMPROMISED*. ДКР выбирает нужный ТМК из списка по любым из следующих параметров:

- поле Check value
- поле Key_ID.

В этом случае требуется оставить поле с криптограммой ТМК

Далее действие – см. шаги 4.0 и 4.1.

- Шаг 4.5[2]

Необходимо на периодической основе проверять срок действия ТМК. В случае если истек срок действия, то TMK_Status *READY* меняется на *EXPIRED*. В этом случае требуется оставлять поле с криптограммой ТМК.

Контрольная сумма (Check Value) ключа не удаляется для осуществления контроля невозможности повторной загрузки данного ключа в СЗК.

Период действия ТМК – параметр, задаваемый оператором в СЗК.

Также в случае загрузки новых ключей ТМК в терминал (с S/N в статусе *READY*), который уже имеет загруженные / привязанные ключи в БД СЗК, необходимо в момент обращения терминала на СЗК для старых ключей менять статус с *LOADED_IN_POS* или *LOADED_IN_SV* на *EXPIRED*.

Далее действие – см. шаги 4.0 и 4.1.

- Шаг 4.6[3]

[1] Данный шаг на схеме не отображён
[2] Данный шаг на схеме не отображён
[3] Данный шаг на схеме не отображён

ДКР в ручном режиме через GUI, в случаях, когда ZMK:

а) раскрыт третьей стороной, меняет статус ZMK_Status на *COMPROMISED*. В этом случае требуется оставить поле с криптограммой ZMK.

По TMK под этим ZMK, у которых TMK_Status *READY* статус меняется на *COMPROMISED*, СЗК формирует соответствующие запросы в SV об изменении статуса TMK ключей – *ChangeKeyStatus*.

б) удален при выводе из эксплуатации Host_ID, меняет Host_ID и статус ZMK_Status на *CANCELLED*. В этом случае требуется оставить поле с криптограммой ZMK.

TMK под этим ZMK, у которых TMK_Status *READY, LOADED_IN_POS* или *LOADED_IN_SV* меняются на *CANCELLED*, СЗК формирует соответствующие запросы в SV об изменении статуса TMK ключей – *ChangeKeyStatus*.

Далее действие – см. шаги 0.1 – 0.3.

в) окончился срок действия, меняет статус ZMK_Status на *EXPIRED*.

TMK под этим ZMK, у которых TMK_Status *READY*, LOADED_IN_POS, *LOADED_IN_SV* статус меняется на *EXPIRED*, СЗК формирует соответствующие запросы в SV об изменении статуса TMK ключей – *ChangeKeyStatus*.

- Шаг 4.7[4]

Необходимо на периодической основе проверять срок действия ZMK. Если истек срок действия, то необходимо изменить ZMK_Status на *EXPIRED*. В этом случае требуется оставлять поле с криптограммой ZMK.

Контрольная сумма (Check Value) ключа также не удаляется для осуществления контроля невозможности повторной загрузки данного ключа в СЗК.

[4] Данный шаг на схеме не отображён

TMK под этим ZMK, у которых TMK_Status *READY*, *LOADED_IN_POS*, *LOADED_IN_SV* статус меняется на *EXPIRED*. СЗК формирует соответствующие запросы в SV.

Период действия ZMK – параметр, загружаемый во входящем файле. Задается индивидуально для каждого ZMK. Все ZMK должны иметь разные сроки действия (назначение индивидуального срока жизни каждому ZMK).

Таким образом, в СЗК имеется информация о дате ввода в эксплуатацию ZMK и сроке его действия.

Далее действие – см. шаги 0.1 – 0.3.

- Шаг 4.8

ДТС получает информацию о том, что необходимо обновить S/N_Status в СЗК:

- с *NEW* на *USED*
- с *READY* на *USED*
- с *USED* на *NEW*.

Доступны два режима обновления:

а) В ручном режиме GUI обработки файла *Список серийных номеров* (Приложение №5)

б) Путем передачи файла *Список серийных номеров* (Приложение №5) средствами MFT и обработкой его СЗК.

3.2 Отчётность

- Шаг 4.9[5]

ДКР выгружает в ручном режиме через GUI из СЗК через штатный интерфейс отчеты – см. Приложение №1.

[5] Данный шаг на схеме не отображён

4. ФУНКЦИОНАЛ СЗК

Таблица 4. Функционал СЗК

№ шага	Описание требований
Система Загрузки Ключей	
0.3	Возможность пакетной файловой загрузки (пакетный импорт) в СЗК в работу и учета ZMK
0.4	Возможность пакетной файловой загрузки (пакетный импорт) в СЗК файла или в ручном режиме через GUI – см. Приложение №5
1.3	Возможность пакетной файловой загрузки (пакетный импорт) в СЗК в работу и учета криптографических ключей. Набор полей в файле для загрузки в СЗК – см. Приложение №8. Обновление и хранение согласно Приложению №1
1.3.2	Проверка корректности сформированных TMK под ZMK
2.7	Обработка входящих от TMS – см. Приложение №11
2.7.1	Обработка входящих от TMS – см. Приложение №11
3.2.1	Обрабатывание в СУБД СЗК сообщения об удалении TMK+ Key_ID (по указанному Key_ID) и S/N (по указанному в сообщении S/N) Возможность постановки входящих соединений в очередь Хранение и обновление согласно Приложению №1
3.2.2	Расшифровка TMK(ZMK) с помощью HSM и передача на целевой POS Возможность использования нескольких HSM из списка, задаваемого настройками системы. Если недоступен один HSM, то система автоматически обращается к другому
X	Невозможность повторной загрузки ключей в систему (включая ключи, имеющие текущий статус *EXPIRED*, криптограмма которых удалена)
3.3	Пользовательский интерфейс с возможностью управления процессами загрузки/отзыва S/N, TMK в СЗК установкой S/N_Status, TMK_Status. Автоматическая установка статусов загружен, удален, отправлен по соответствующим событиям/действиям оператора Взаимодействие с RKI по контролю и передаче данных о S/N и TMK(ZMK).

№ шага	Описание требований
	По Multi Merchant терминалам направляется в SV несколько запросов на привязку ключа различными Terminal_ID и одним Key_ID. Взаимодействие с двумя комплектами СЗК в режиме master/slave. Синхронизация списков S/N и TMK(ZMK) производится по событию загрузка ключа POS. Авторизация пользователей по логину/паролю в системе СЗК согласно Приложению №1. Логирование операций с ключами и действий операторов Отображение роли загруженных мастер ключей (TMK_PIN, TMK_ MAC)
3.4	Возможность задавать для каждого Host_ID свой набор параметров: IP, port, продукт, login, password. Поддержка жизненных циклов ZMK, TMK и S/N – см. Приложение №10

ПРИЛОЖЕНИЕ №1 ТРЕБОВАНИЯ К СЗК В ЧАСТИ KEY LIFE CYCLE

Таблица 5. KEY LIFE CYCLE

№ поля	Имя поля	Описание	Возможные значения	Комментарии
1	Key_ID			
2	Key Cryptogram			
3	User_ID_KDH			
4	PSP_ID (Key Loading facility)			
5	Type key			
6	ID ZMK (для передаваемых ключей)			
7	Key check value			
8	Terminal_Ser No (S/N)			
9	Terminal_ID			
10	Key_Status (TMK_Status)			
11	Дата и время генерации ключа			
12	Дата и время трансляции под ZMK			
13	Дата и время отправки ключа в KDH			
14	Дата, время загрузки ключа в терминал			.
15	Дата и время привязки к Terminal_ID			

№ поля	Имя поля	Описание	Возможные значения	Комментарии
16	Дата и время удаления в KDH			
17	Status Terminal_Ser No в KDH (S/N_Status)			
18	Host_ID			

ПРИЛОЖЕНИЕ №2 ТРЕБОВАНИЯ К CA

22-8 Minimum cryptographic strength for the CA system shall be:
• Root and subordinate CAs have a minimum RSA 2048 bits or equivalent;
• EPP/PED devices and KDHs have a minimum RSA 1024 bits or equivalent.
Effective 1 January 2017, EPP/PED and KDHs must use a minimum RSA 2048 bits or equivalent.
The key-pair lifecycle shall result in expiration of KDH keys every five years, unless another mechanism exists to prevent the use of a compromised KDH private key.
25-3.2 CA or Registration Authority (RA) software updates must not be done over the network (local console access must be used for CA or RA software updates)
25-3.3 Non-console access must use two-factor authentication. This also applies to the use of remote console access.
25-3.4 Non-console user access to the CA or RA system environments shall be protected by authenticated encrypted sessions. No other remote access is permitted to the host platform(s) for system or application administration
25-6 Audit trails must include but not be limited to the following:
• All key-management operations, such as key generation, loading, transmission, backup, recovery, compromise, and destruction and certificate generation or revocation
• The identity of the person authorizing the operation
• The identities of all persons handling any key material (such as key components or keys stored in portable devices or media)
• Protection of the logs from alteration and destruction
25-6.1 Audit logs must be archived for a minimum of two years.
25-7 CA application logs must use a digital signature or a symmetric MAC (based on one of the methods stated in *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques*) mechanism for detection of alteration.
The signing / MACing key(s) used for this must be protected using a secure cryptographic device in accordance with the key-management requirements stipulated in this document
25-7.1 Certificate-processing system components operated **online must be protected by a firewall(s) from all unauthorized access**, including casual browsing and deliberate attacks. Firewalls must minimally be configured to:
• Deny all services not explicitly permitted.
• Disable or remove all unnecessary services, protocols, and ports.
• Fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a failure.
• Disable source routing on the firewall.
• Not accept traffic on its external interfaces that appears to be coming from internal network addresses.
• Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action can be taken.
• Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled.
25-7.2 Online certificate-processing systems must employ individually or in combination network and host-based intrusion detection systems (IDS) to detect inappropriate access. At a minimum, database servers and the application servers for RA and web, as well as the intervening segments, must be covered.
25-8 Implement user-authentication management for all system components as follows:
25-8.1 Initial, assigned passphrases are pre-expired (user must replace at first logon).
25-8.2 Use of group, shared, or generic accounts and passwords, or other authentication methods is prohibited.
25-8.3 If passwords are used, system-enforced expiration life must not exceed 30 days and a minimum life at least one day.
25-8.4 Passwords must have a minimum length of eight characters using a mix of alphabetic, numeric, and special characters.
25-8.5 Limit repeated access attempts by locking out the user ID after not more than five attempts.
25-8.6 Authentication parameters must require a system-enforced passphrase history, preventing the reuse of any passphrase used in the last 12 months.
25-8.7 Passwords are not stored on any of the systems except in encrypted form or as part of a proprietary one-way transformation process, such as those used in UNIX systems.
25-8.8 The embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.
25-8.9 Where log-on security tokens (for example, smart cards) are used, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN/passphrase to enable their usage. The PIN/passphrase must be at least eight decimal digits in length, or equivalent.
Note: *Log-on security tokens (for example, smart cards) and encryption devices are not subject to the pass-phrase management requirements for password expiry as stated above.*
25-9 Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations.
28-2 CA operations must be dedicated to certificate issuance and management. **All physical and logical CA system components must be separated from key-distribution systems**.

ПРИЛОЖЕНИЕ №3 ШИФРОВАНИЕ ДАННЫХ ПРИ ПЕРЕДАЧЕ МАСТЕР-КЛЮЧЕЙ НА POS

1. Длины используемых 3DES ключей должны быть не менее 16 байт
2. Минимальная длина RSA ключа не менее 2048бит
3. Логи аудита должны содержать полный перечень действий пользователя, включая, аутентификацию, факты просмотра данных, факты изменения данных в системе
4. Логи аудита должны иметь позаписные MAC-и вычисленные с использованием HSM и процедурами менеджмента ключей. Это необходимо для поддержания контроля неизменности записей. Должна быть предусмотрена процедура контроля неизменности записей
5. Логи аудита должны писаться в два независимых хранилища: таблица БД и внешний текстовый файл. Должна быть предусмотрена процедура сравнения двух хранилищ для контроля целостности данных
6. Логи аудита должны храниться не менее двух лет
7. Новый пользователь в системе описывается администратором с указанием логина и пароля, который должен быть заменен пользователем при первом входе в систему
8. Время жизни пароля задается администратором в пределах от одного до тридцати дней, по истечению этого срока пароль должен быть изменен пользователем
9. Пароль должен состоять минимум из восьми символов и должен включать в себя цифры, буквы и печатные спецсимволы
10. Количество попыток предъявления пароля не должно превышать пяти, после чего логин блокируется
11. Пароль может храниться в системе только в хешированном виде
12. Встроенные пароли в шелл скриптах, командных файлах запрещены

ПРИЛОЖЕНИЕ №4 СПРАВОЧНИК HOST_ID

Таблица 6. Справочник Host_ID

#	Значение Host_ID	Описание Host_ID
1		
2		
3		

ПРИЛОЖЕНИЕ №5 ФАЙЛОВЫЙ ОБМЕН «СПИСОК СЕРИЙНЫХ НОМЕРОВ»

Маска имени файла: DTS_SZK_[YYYYMMDD]_[NNNN].TXT

где

Таблица 7. Список серийных номеров

№ поля	Поле	Позиция	Длина поля	Формат	Значение
1	Outgoing System Name	1-3	3		Константа «DTS»
2	Delimiter	4	1	c	Символ «_» (нижнее подчеркивание)
3	Incoming System Name	5-7	3		Константа «SZK»
4	Delimiter	8	1	c	Символ «_» (нижнее подчеркивание)
5	File Date	9-16	8		YYYYMMDD – Дата формирование файла.
6	Delimiter	17	1	c	Символ «_» (нижнее подчеркивание)
7	Number Packet	18-21	4		Номер пачки
8	Delimiter	22	1	c	Символ «.» (точка)
9	Расширение файла	23-25	3		TXT

Каталог, в котором СЗК должен ожидать файл: локальный.

Таблица 8. Формат файла Список серийных номеров

#	Обозначение	Название	Тип	Макс. длина	Справочник	Обязательный	Комментарий
1	Host_ID		Строка	4	См. Приложение №4		
2	S/N		Строка	16			
3	S/N_Status		Строка				

Формат TXT, каждая запись – на отдельной строке, разделитель полей «|».

ПРИЛОЖЕНИЕ №6 ИЕРАРХИЯ HOST_ID -> TERMINAL_ID

На обсуждении.

ПРИЛОЖЕНИЕ №7 ФАЙЛОВЫЙ ОБМЕН «ТМК ДЛЯ СЗК»

Маска имени файла: *Key_KDH_[AAA]_[YYYYMMDDHH24MISS].XML*

где

Таблица 9. ТМК ДЛЯ СЗК

№ поля	Поле	Позиция	Длина поля	Формат	Значение
1	Description	1-3	3		Описание файла. Константа «Key»
2	Delimiter	4	1	c	Символ «_» (нижнее подчеркивание)
3	Incoming System Name	5-7	3		Константа «KDH»
4	Delimiter	8	1	c	Символ «_» (нижнее подчеркивание)
5	Host_ID	9-11	3		[AAA] - См. справочник в примечании Приложения №8
6	Delimiter	12	1	c	Символ «_» (нижнее подчеркивание)
7	Time Stamp	13-28	16		[YYYYMMDDHH24MISS] – Дата и время формирования файла
8	Delimiter	29	1	c	Символ «.» (точка)
9	Расширение файла	30-32	3		XML

Каталог, в котором СЗК должен ожидать файл: локальный.

Пример файла:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
  <KeyCryptograms>
    <Row>
      <HostId>PH2</HostId>
      <Id>300000001</Id>
      <UnderZMK>4AF3197810559E4443DD21C19434280</UnderZMK>
      <KeyCheck>75C790</KeyCheck>
      <Type>TMK</Type>
      <KeySubType>PIN</KeySubType>
      <Status>Ready</Status>
      <OwnerType>POS</OwnerType>
      <Date>20160524</Date>
      <Time>1600</Time>
    </Row>
  </KeyCryptograms>
```

Таблица 10. Структура файла ТМК ДЛЯ СЗК

#	Написание тэга	Обозначение	Название	Макс. длина	Справочник	Обязательный
1	HostId	HostId	Уникальный номер хоста	3	см. Справочник **	Да
2	Id	KeyId *	Уникальный идентификатор: - ТМК для PIN и MAC	9	Диапазон 100 000 000 - 999 999 999 со сквозным счетчиком. В 1-й позиции указывается признак хоста – см. Справочник **	Да
3	UnderZMK	Key Cryptogram	Криптограмма ключа: - PIN и MAC как ТМК	32	---	Да
4	KeyCheck	Key Check Value	Проверочное число: - ТМК для PIN и MAC	6	---	Да
5	Type	Key Type ***	Тип ключа	3	1 вариант: ТМК	Да
6	KeySubType	Key Subtype***	Параметры ТМК	3	2 значения: PIN, MAC	Да
7	Status	Key Status ***	Статус ТМК	5	1 вариант: READY	Да
8	OwnerType	Owner ***	Владелец ТМК	3	Константа: POS	Да
9	Date	Date Key Generation	Дата создания ТМК	8	YYYYMMDD	Да

#	Написание тэга	Обозначение	Название	Макс. длина	Справочник	Обязательный
10	Time	Time Key Generation	Время создания ТМК	6	HHmmSS	Да

⚠ * При формировании для разных систем (SV, СЗК) один и тот же ТМК будет формироваться с тем же Key_ID.

** Справочник – см. Приложение №4.

*** В случае не соответствующего значения в базу данных ключ не добавляется, в логе формируется сообщение об ошибке.

ПРИЛОЖЕНИЕ №8 РОЛИ ПО ДОСТУПУ В СЗК

Таблица 11. РОЛИ ПО ДОСТУПУ В СЗК

№	Действие	Оператор ДТС	Оператор ДКР	Администратор
1	Загрузка TMK(ZMK) в БД	X	---	---
2	Загрузка ZMK(LMK) в БД	---	X	---
3	Установка срока действия TMK	---	X	---
4	Установка срока действия ZMK	---	X	---
5	Загрузка списка S/N	X	---	---
6	Установка статуса *COMPROMISED* на TMK	X	X	---
7	Установка статуса *COMPROMISED* на ZMK	X	X	---
8	Установка статусов *USED*, *NEW* на S/N	X	---	---
9	Загрузка списка S/N со статусом *USED*	X	---	---
10	Загрузка списка скомпрометированных TMK	X	X	---
11	Просмотр в интерфейсе СЗК записей о ключах, работа с фильтрами по каждому полю	X	X	---
12	Просмотр в интерфейсе СЗК записей о S/N, работа с фильтрами по каждому полю	X	X	---
13	Формирование отчетов по ЖЦ S/N	X	X	---
14	Формирование отчетов по ЖЦ TMK	X	X	---
15	Заведение новых пользователей/сброс паролей	---	---	X
16	Настройка сетевых доступов к узлам системы (SV, HSM)	X	---	---
17	Настройка справочников Host_ID	X	---	---
18	Просмотр в интерфейсе СЗК записей по событиям	X	---	---

№	Действие	Оператор ДТС	Оператор ДКР	Администратор
19	Генерация и добавление ключей и сертификатов СЗК и СА	---	X	---
20	Распределение функционала пользователям	---	---	X
21	Настройка параметров *Размер неснижаемого остатка свободных ключей* и *Число генерируемых новых свободных ключей*	X	---	---

ПРИЛОЖЕНИЕ №9 ФАЙЛОВЫЙ ОБМЕН «KEY STATUS REPORT»

Маска имени файла: KSR_KDH_[YYYYMMDD]_[NNNN].TXT

где:

Таблица 12. Маска имени файла key status report

№	Поле	Позиция	Длина поля	Формат	Значение
1	KSR	1-3	3		Константа «Key Status Report»
2	Delimiter	4	1	c	Символ «_» (нижнее подчеркивание)
3	Incoming System Name	5-7	3		Константа «KDH»
4	Delimiter	8	1	c	Символ «_» (нижнее подчеркивание)
5	File Date	9-16	8		YYYYMMDD – Дата формирование файла
6	Delimiter	17	1	c	Символ «_» (нижнее подчеркивание)
7	Number Packet	18-21	4		Номер пачки
8	Delimiter	22	1	c	Символ «.» (точка)
9	Расширение файла	23-25	3		TXT

Каталог, в котором СЗК должен ожидать файл: локальный.

Формат TXT, разделитель полей «|».

Таблица 13. Структура файла key status report

N	Обозначение	Название	Тип	Макс. длина	Значение
1	Date	Дата и время события смены статуса	строка	14	YYYYMMDDHHmmSS
2	Key_ID	Уникальный идентификатор ключа	строка	9	от 910000000 до 919999999

N	Обозначение	Название	Тип	Макс. длина	Значение
3	TMK_Status*	Текущий статус TMK	строка	5	=READY =LOADED_IN_POS =LOADED_IN_SV Текущее значение TMK_Status может отличаться в СЗК от SV, при обработке не обращать на это внимания
4	New_TMK_Status	Новый статус TMK	строка	11	=READY =EXPIRED =COMPROMISED =CANCELLED
5	Check_value		строка	?	

⚠ Примечание к структуре файла приложения ФАЙЛОВЫЙ ОБМЕН ZMK ДЛЯ СЗК:

* Значение в поле «TMK_Status» (Текущий статус TMK) необходимо игнорировать, так как в действительности допускается рассинхронизация TMK статусов между системами СЗК и SV, но в то же время по полю «New_TMK_Status» импортировать статус ровно так как это разрешает ЖЦ TMK. Если ЖЦ не разрешает перехода, то отвергнуть с записью в лог с соответствующей ошибкой.

ПРИЛОЖЕНИЕ №10 ЖИЗНЕННЫЙ ЦИКЛЫ ZMK, TMK И S/N

Таблица 14. Жизненный цикл ZMK в СЗК

№	Исходное состояние ZMK_Status	Итоговое состояние ZMK_Status	Условие перехода
1	Отсутствует (NULL)	LOADED	Шаг 0.3.
2	LOADED	COMPROMISED	Шаг 4.6 подпункт а) Требуется оставить поле с криптограммой ZMK По TMK под этим ZMK, у которых TMK_Status *READY* статус меняется на *COMPROMISED*
3	LOADED	EXPIRED	Шаги 4.0 и 4.7 Требуется обнулять поле с криптограммой ZMK По TMK под этим ZMK, у которых TMK_Status *READY* статус меняется на *EXPIRED*
4	LOADED	CANCELLED	Шаг 4.6 подпункт в) Требуется оставить поле с криптограммой ZMK По TMK под этим ZMK, у которых TMK_Status READY, LOADED_IN_POS или LOADED_IN_SV меняются на CANCELLED

Таблица 15. Жизненный цикл TMK в системе СЗК

№	Исходное состояние TMK_Status	Итоговое состояние TMK_Status	Условие перехода
1	Отсутствует (NULL)	READY	Шаг 1.3.2
2	READY	LOADED_IN_POS	Шаг 3.3
3	READY	COMPROMISED	Шаги 4.1 и 4.3
4	READY	EXPIRED	Шаги 4.1 и 4.3

№	Исходное состояние TMK_Status	Итоговое состояние TMK_Status	Условие перехода
5	LOADED_IN_POS	LOADED_IN_SV	Шаги 3.5 подпункт б)
6	LOADED_IN_POS	COMPROMISED	Шаги 4.1 и 4.3
7	LOADED_IN_POS	EXPIRED	Шаги 4.1 и 4.3
8	LOADED_IN_SV	COMPROMISED	Шаги 4.1 и 4.3
9	LOADED_IN_SV	EXPIRED	Шаги 4.1 и 4.3
10	READY	CANCELLED	Шаг 4.3
11	LOADED_IN_POS	CANCELLED	Шаг 4.3
12	LOADED_IN_SV	CANCELLED	Шаг 4.3

Таблица 16. Жизненный цикл S/N в системе СЗК

№	Исходное состояние S/N_Status	Итоговое состояние S/N_Status	Условие перехода
1	Отсутствует (NULL)	NEW	Шаг 0.4
2	NEW	READY	Шаг 2.7
3	NEW	USED	Шаг 4.8
4	READY	NEW	Шаг 2.6 (POS-терминал может сломаться после того, как сходил на TMS, но не дошел до СЗК)
5	READY	USED	Шаги 3.3 и 4.8
6	USED	NEW	Шаг 4.8 (получение из ремонта POS)
7	USED	USED	Шаг 2.7.1 (для Multi Merchant, добавление 2-ого Terminal_ID)

Изменения могут происходить в ручном варианте через GUI либо при обработке файлов.

ПРИЛОЖЕНИЕ №11 ФАЙЛОВЫЙ ОБМЕН «ЗАГРУЗКА КОНФИГУРАЦИИ ДЛЯ POS»

Маска имени файла:*LANTERTMS_KDH_[YYYYMMDDHHMISSmmm].xml*

где

Таблица 17. Загрузка конфигурации для POS

№ поля	Поле	Позиция	Длина поля	Формат	Значение
1	Outgoing System Name	1-4	4		Константа «TMS»
2	Delimiter	5	1	c	Символ «_» (нижнее подчеркивание)
3	Incoming System Name	6-8	3		Константа «KDH»
4	Delimiter	9	1	c	Символ «_» (нижнее подчеркивание)
5	Time Stamp	10-26	17		YYYYMMDDHHMISSmmm – Дата и время формирование файла.
6	Delimiter	27	1	c	Символ «.» (точка)
7	Расширение файла	28-30	3		xml

Каталог, в котором СЗК должен ожидать файл ключей: локальный.

Пример файла:

```
<POS_ConfigFile >

<!--  SingleMerchant terminal  -->
  <POS>
       <Host_ID>PH2 </Host_ID>
       <Terminal_ID>L0026670</Terminal_ID>
       <Serial_Number>10010001</Serial_Number>
       <SingleMerchant>
                    <Terminal_ID>L002667B</Terminal_ID>
        </SingleMerchant>
  </POS>


<!--  MultiMerchant terminal  -->
  <POS>
    <Host_ID>PH2 </Host_ID>
    <Terminal_ID>L0026680</Terminal_ID>
    <Serial_Number>1001A822</Serial_Number>
    <MultiMerchant>
        <Terminal_ID>L002668P</Terminal_ID>
        <Terminal_ID>L002668B</Terminal_ID>
     </MultiMerchant>
  </POS>

</POS_ConfigFile>
```

ПРИЛОЖЕНИЕ №12 ФАЙЛОВЫЙ ОБМЕН «ZMK ДЛЯ СЗК»

Маска имени файла: ZMK_SZK.xml

где

Таблица 18. ZMK ДЛЯ СЗК

№ поля	Поле	Позиция	Длина поля	Формат	Значение
1	Description	1-3	3		Описание файла. Константа «ZMK»
2	Delimiter	4	1	c	Символ «_» (нижнее подчеркивание)
3	Incoming System Name	5-7	3		Константа «SZK»
4	Delimiter	8	1	c	Символ «.» (точка)
5	Расширение файла	9-11	3		XML

Каталог, в котором СЗК должен ожидать файл: локальный.

Таблица 19.Формат файла ZMK для СЗК

#	Написание тэга	Обозначение	Название	Справочник
1	HostId	HostId	Уникальный номер хоста	см. Приложение №4
2	Id		Идентификатор ZMK	
3	UnderLMK	Key Cryptogram	Криптограмма ключа	---
4	KeyCheck	Key Check Value	Проверочное число	---
5	Date	Date Key Generation	Дата создания ZMK	YYYYMMDD
6	Time	Time Key Generation	Время создания ZMK	HHmm

Пример файла:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Row>
<HostId>PH2</HostId> идентификатор хоста
<Id>100000001</Id> идентификатор ZMK
<UnderLMK>UDC768A28C8906123EFB0499E3A0158A2</UnderLMK> Криптограмма ключа
<KeyCheck>8A0F28</KeyCheck> Контрольная сумма
<Date>20160524</Date> Дата генерации ZMK
<Time>1600</Time> Время генерации ZMK
</Row>
```