



Общество с ограниченной ответственностью «СКАНТЕК»
119049 Россия Москва ул. Донская, д.15
ИНН 7706433591 · КПП 770601001 · ОГРН 1167746144664
тел.: +7 (499) 271-96-61, 271-96-62, 271-96-63

SmartEngine

Версия 6.3.0

РУКОВОДСТВО АДМИНИСТРАТОРА

ДАТА СОЗДАНИЯ:	17.04.2011
ПОСЛЕДНЯЯ РЕДАКЦИЯ:	10.02.2016
ВСЕГО СТРАНИЦ:	30

История изменений

Дата	Автор	Версия	Примечания
17.12.2015	Скоробогачева И.А.	6.3.0	Повторяет редакцию документа «SmartEngine. Версия 6.30. РУКОВОДСТВО АДМИНИСТРАТОРА» от 18.03.2015. Изменения внесены в связи с получением ЗАО «СКАНТЕК» исключительных прав на ПО.
10.02.2016	Скоробогачева И.А.	6.3.0	Изменения внесены в связи реорганизацией юридического лица правообладателя в форме преобразования в ООО «СКАНТЕК»

Аннотация

Руководство администратора содержит необходимые сведения для работы специалиста программно-технических средств.

Данный документ содержит инструкцию по применению программного обеспечения SmartEngine версии 6.3.0 (далее «ПО»).

Правообладателем ПО является ООО «СКАНТЕК».

Содержание

Общее описание	5
1.1 Назначение.....	5
1.2 Системные требования	5
1.3 Состав ПО	5
1.4 Установка ПО и конфигурационных файлов	6
1.5 Загрузка первоначальных ключей	6
1.6 Процедура отмены обновления или удаления продукта.....	6
1.7 Журнал выпусков.....	6
2 Административное приложение	7
2.1 Назначение и основные возможности.....	7
2.2 Управление мастер ключами	7
2.3 Краткое описание процедуры загрузки ключей с хоста EPS.....	7
2.4 Настройка коммуникационных параметров приложения.....	8
2.5 Настройка подключения к FTP серверу.....	9
2.6 Идентификация терминала на FTP сервере.....	11
3 Платежное приложение	12
3.1 Назначение и основные возможности.....	12
3.2 Интерфейс пользователя	12
3.3 Выполнение транзакции по карте с магнитной полосой	13
3.4 Выполнение транзакции по чиповой EMV-карте.....	13
3.5 Файл конфигурации	15
Формат файла конфигурации.....	15
Параметры файла конфигурации.....	15
3.6 Файл настройки коммуникационных параметров	26
Примечание 1.....	28
3.7 Установка настроек для обеспечения требований PCI DSS	29
4 Приложение взаимодействия с торговой системой	30
4.1 Назначение и основные возможности.....	30
4.2 Настройки	30

Общее описание

1.1 Назначение

Программный продукт SmartEngine предназначен для выполнения платежных транзакций по банковским, топливным, бонусным и дисконтным картам с использованием магнитной полосы, контактного интерфейса микропроцессорных карт стандарта EMV или бесконтактного интерфейса стандартов MasterCard PayPass, Visa PayWave, ScanTech PayCORN в рамках терминального оборудования Ingenico на платформе Telium 2.

Поддерживаются следующие модели оборудования и режимы работы:

- Интеллектуальный ПИН-пад *ipr320/350* в связанном с управляющей системой режиме;
- Настольный терминал *ict220/250* в автономном или связанном с управляющей системой режимах;
- Переносной терминал *iwl220/250* в автономном режиме;
- Встраиваемый терминал *iSelf (iUP250 + iUR250 + iUC150)* в связанном с управляющей системой режиме.

1.2 Системные требования

Программный продукт SmartEngine предназначен для использования в ПИН-падах Ingenico под управлением операционной системы Telium2 версий 10.XX. Предполагается совместная работа с мастер-приложением Telium Manager под управлением торговой системы в соответствии с протоколом SETIP4.

Оборудование должно содержать не менее 32 Мб RAM и 128 Мб Flash памяти.

Поддерживаются следующие встраиваемые коммуникации:

- Ethernet;
- WiFi;
- GPRS.

1.3 Состав ПО

В состав ПО SmartEngine входят:

- пакет с платежным модулем (в зависимости от конфигурации в терминал может быть загружено несколько платежных приложений) - *8224870630.agn*;
- пакет с административным модулем - *8224040400.agn*;
- пакет с модулем реализации протокола SETIP4 и интерфейсом взаимодействия с оператором автономного терминала - *8224880300.agn*;
- пакеты с ресурсами приложений;
- данное руководство по установке и настройке;
- PA DSS Implementation Guide;
- программа настройки EMV-параметров (*Configuring EMV.exe*);
- набор конфигураций соответствующий требованиям VISA ADVT и MasterCard TIP тестам.

Для обеспечения возможности удаленной загрузки ПО предоставляется полный дистрибутив (Комплект Программного Обеспечения, КПО), включающий в себя все загружаемые в терминал модули. Загрузка данного КПО в систему управления терминалами SmartTMS позволяет удаленно обновить ПО в уже использующихся устройствах.

1.4 Установка ПО и конфигурационных файлов

Установка SmartEngine осуществляется загрузкой соответствующего пакета в ПИН-пад. Загрузка может быть осуществлена как локально, с помощью загрузчика производителя терминалов, LLT, так и удаленно – с FTP сервера или из системы SmartTMS.

Работа приложений определяется настройками конфигурационных файлов. Конфигурационные файлы перед загрузкой могут быть объединены в ZIP-архивы в режиме сжатия по-умолчанию, без использования каталогов.

Рекомендуемое имя архива для приложения – *appN.zip*, где N – идентификатор приложения (1 – платежное, 4 - административное). Загрузка EMV параметров по-умолчанию осуществляется в режиме «обновления», т.е. ранее загруженные EMV параметры сохраняются. В случае, если требуется очистить информацию о ранее загруженных настройках, имя файла архива должно содержать в качестве пятого символа 'C'. Например, *app1C.zip*. Расширение имени файла архива конфигурации должно быть изменено на .PAR.

Загрузка конфигурационных файлов, за исключением коммуникационных параметров, не допускается до закрытия текущего финансового цикла (успешного завершения операции сверки итогов/формирования отчета).

1.5 Загрузка первоначальных ключей

Для работы платежного приложения необходима загрузка мастер-ключа подписи конфигурационного файла и одного или нескольких мастер-ключей для взаимодействия с авторизационным хостом (перечень зависит от используемого хостового решения и его настроек). Рекомендуется осуществлять загрузку первоначальных ключей с использованием специализированных средств – TGTKIT или SEKIT.

1.6 Процедура отмены обновления или удаления продукта

Терминал допускает установку платежного приложения одной из предыдущих версий, тем самым обеспечивая возможность отмены обновления. Удаление приложения возможно как локально из сервисного меню, так и удаленно. При удалении платежного приложения удаляются все его рабочие файлы, но сохраняются ранее загруженные в модуль безопасности терминала ключи.

1.7 Журнал выпусков

Приложения по обслуживанию банковских карт до начала использования проходят различные сертификации (ADVT, MTIP, PA DSS).

Эти сертификации проходят на конкретной версии ОС производителя ПИН-пада, в конкретном окружении.

Выпуски ПО, отражающие интеграцию основных элементов системы зафиксированы в нижеследующей таблице (см. [Таблица1](#)). Подробное описание изменений находится в файлах readme.txt для соответствующих версий.

Таблица

Журнал выпусков

Дата выпуска	Состав ПО	Примечания
18.03.15 (630)	Платформа Telium2 SE 630.0 MN 400.0 OS Telium2 32.10 Telium Manager 78.06	PA DSS сертификация

	EMV Kernel 4.66	

2 Административное приложение

2.1 Назначение и основные возможности

Административное приложение обеспечивает выполнение следующих операций:

- предоставление информации о загруженном в ПИН-пад программном обеспечении и характеристиках устройства;
- управление мастер-ключами ПИН-пада в ручном режиме;
- управление мастер-ключами ПИН-пада в удаленном режиме;
- установка/обновление приложений;
- удаление приложений.

Доступ к функциям административного приложения для закрыт паролем.

Пароль доступа к административным функциям ПИН-пада по умолчанию 567892. Telium Manager позволяет его модифицировать.

2.2 Управление мастер ключами

Для работы платежного приложения в ПИН-пад должны быть загружены соответствующие ключи. Перечень ключей и способ их загрузки зависит от конфигурации платежного приложения. Предполагается возможность использования следующих вариантов загрузки начального ключа:

- Загрузка начального ключа средствами производителя ПИН-падов (для Unicapt32 – KeyInjectionTool или SEKIT, для Telium2 – TGKIT или SEKIT);
- Ручной покомпонентный ввод начального ключа офицерами безопасности;
- Удаленная загрузка ключа с хоста (поддерживается в рамках административного приложения только для хоста EPS).

Остальные, рабочие ключи загружаются либо с хоста, либо в рамках конфигурационных файлов. Подробное описание процедуры загрузки ключей с использованием средств производителя ПИН-падов приведено в «Управление ключами шифрования. Настольный терминал».

В форме отображения ключевой информации для выполнения операций могут быть использованы следующие последовательности клавиш:

- F + 3 + Enter – очистка всей ключевой информации;
- F + 4 + Enter – загрузка ключей с хоста EPS с начальной стадии;
- F + 5 + Enter – инициирование ручного ввода KLK ключа хоста OW;
- F + 6 + Enter – инициирование ручного ввода DSS-CFG ключа, подписания конфигурационных файлов.

Процесс загрузки ключей с хоста EPS описан ниже.

2.3 Краткое описание процедуры загрузки ключей с хоста EPS

Загрузка ключей с хоста EPS базируется на использовании несимметричной (RSA) и симметричной (AES) криптографии.

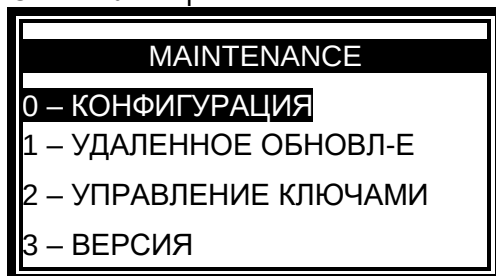
Основными криптоэлементами являются RSA ключ терминала и RSA ключ хоста.

Основными этапами загрузки ключа, с точки зрения терминала, являются:

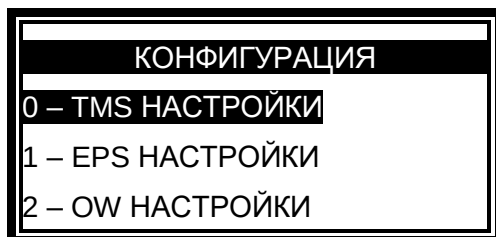
- Генерация RSA ключа терминала (осуществляется при первом запуске приложения);
- Обмен открытыми частями RSA ключей терминала и сервера. Требуется участия двух операторов, на стороне терминала и хоста. Заключается в:
 - Отображении «отпечатка» ключа терминала, который оператор терминала должен сообщить оператору на хосте;
 - Вводе идентификатора доступа, который оператор терминала должен предварительно запросить у оператора хоста;
 - Вводе «отпечатка» ключа хоста, который оператор терминала должен предварительно запросить у оператора хоста;
- Загрузка симметричных ключей в зашифрованном на RSA ключах виде;
- Получение со стороны хоста подтверждения возможности начала обслуживания карт.

2.4 Настройка коммуникационных параметров приложения

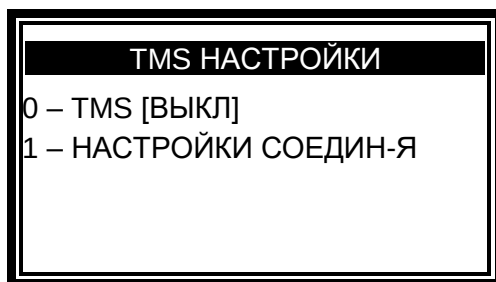
В главном меню выбрать «0 — КОНФИГУРАЦИЯ»



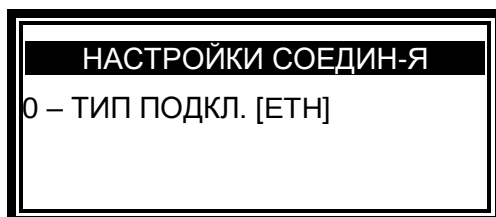
далее выбираем пункт 0 - TMS НАСТРОЙКИ



далее пункт 1 - НАСТР. СОЕДИНЕНИЯ



далее выбираем тип подключения, пункт 0 – ТИП ПОДКЛ. [ETH],



далее выбираем 0 - Ethernet

ТИП ПОДКЛЮЧЕНИЯ
0 – ETHERNET
1 – COM
2 – GPRS
3 – MODEM

2.5 Настройка подключения к FTP серверу

Тип подключения должен быть Ethernet - «TMS [FTP]»

TMS НАСТРОЙКИ
0 – TMS [FTP]
1 – НАСТРОЙКИ СОЕДИН-Я
2 – НАСТРОЙКИ FTP
3 – НАСТРОЙКИ SSL/TLS

Задание пароля доступа к FTP-серверу.

Вводится пароль, заданный на FTP-сервере, для клиента с логином равным серийному номеру данного терминала.

НАСТРОЙКИ FTP
0 - ПАРОЛЬ
1 - IP-АДРЕС
2 - РЕЖИМ FTP
3 – ЛОГ-ФАЙЛ [ВЫКЛ]

ПАРОЛЬ
<u>1</u> 234 >

Задание IP-адреса и IP-порта FTP-сервера.

НАСТРОЙКИ FTP
0- ПАРОЛЬ
1 - IP-АДРЕС
2 - РЕЖИМ FTP
3 – ЛОГ-ФАЙЛ [ВЫКЛ]

ВНИМАНИЕ!

IP-порты для «открытого» и «SSL/TLS» соединений у FTP-сервера **различные!**

IP - АДРЕС
158.251.40 .99
ПОРТ
990

Задание клиентского режима FTP-подключения.

НАСТРОЙКИ FTP
0 - ПАРОЛЬ
1 - IP-АДРЕС
2 - РЕЖИМ FTP
3 – ЛОГ-ФАЙЛ [ВЫКЛ]

ВНИМАНИЕ!

Режим FTP-подключения для «SSL/TLS» соединений только «ПАССИВНЫЙ»!

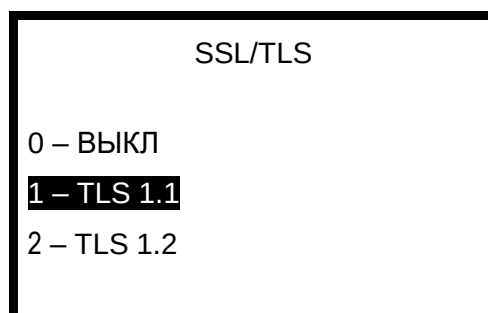
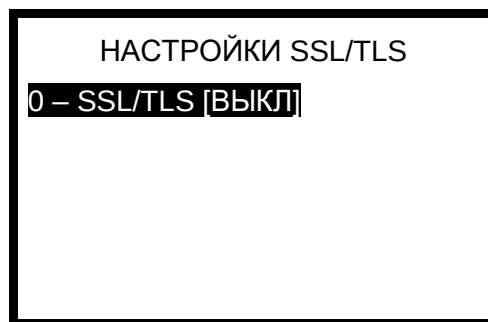
Режим FTP-подключения для «открытых» соединений можно устанавливать как «АКТИВНЫЙ», так и «ПАССИВНЫЙ»!

РЕЖИМ
0 - АКТИВНЫЙ
1 - ПАССИВНЫЙ

Настройки SSL/TLS соединения с FTP-сервером.

TMS НАСТРОЙКИ
0 – TMS [ETH]
1 – НАСТРОЙКИ FTP
2 – НАСТР. СОЕДИНЕНИЯ
3 - НАСТРОЙКИ SSL/TLS

Включение/Отключение SSL/TLS для обмена с FTP-сервером.



ВНИМАНИЕ!

IP-порты для «открытого» и «SSL/TLS» соединений у FTP-сервера **различные!**

При отключении SSL/TLS для обмена с FTP-сервером «ОТКЛЮЧЕНО» все остальные параметры «НАСТРОЙКИ SSL/TLS» не играют роли, но вводимые для них значения сохраняются.

Задание версии SSL/TLS означает его включение.

ВНИМАНИЕ!

PA DSS требует использование SSL /TLS версии «TLS 1.1» или «TLS 1.2»!

2.6 Идентификация терминала на FTP сервере

Терминал идентифицируется на FTP-сервере как клиент с параметрами:

LOGIN: <серийный номер> (например 10081394)

TELIUM MANAGER -> Consultation -> Configuration -> Hardware:

----- General Infos -----

Serial Number : xxxxxxxx

PASSWORD: задаётся в меню MN

НАСТРОЙКИ FTP -> ПАРОЛЬ

3 Платежное приложение

3.1 Назначение и основные возможности

Платежное приложение обеспечивает работу с картами с магнитной полосой, EMV-чипом, бесконтактными картами стандартов PayPass и PayWave. Выполняются следующие операции:

- оплата, в том числе с выдачей наличных;
- предавторизация;
- расчет по предавторизации (без использования карты по транзакции в текущем финансовом цикле);
- отмена предавторизации (без использования карты по транзакции в текущем финансовом цикле);
- возврат;
- учетный возврат (без использования карты по транзакции в текущем финансовом цикле);
- просмотр баланса;
- пополнение карт-счета;
- сверка итогов и выгрузка транзакций.

Прием запроса на выполнение операции и возврат результатов осуществляется в соответствии с протоколом SETIP. Возможность выполнения тех или иных операций может дополнительно настраиваться в зависимости от типа карт.

3.2 Интерфейс пользователя

Приложение SmartEngine осуществляет взаимодействие с владельцем карты в соответствии с требованиями стандарта EMV. Для отображения и ввода данных используется экран и ПИН-клавиатура ПИН-падов, обладающие следующими характеристиками:

- четырехстрочный экран по 16 символов в каждой строке;
- цифровые клавиши 0-9;
- функциональные клавиши для перемещения по меню («стрелка вверх» и «стрелка вниз»);
- управляющие клавиши “C” (корректировка), “STOP” (отмена ввода), “OK” (завершение ввода);
- возможно наличие дополнительных клавиш, нажатия на которые не обрабатываются (игнорируются).

При выполнении сервисных или административных команд приложение не обращается к экрану и/или клавиатуре.

Взаимодействие с клиентом реализовано только при обработке команды на выполнение транзакции. Очистка экрана (сброс предыдущей информации) осуществляется непосредственно перед отображением на экран.

При определенных условиях транзакция может быть выполнена вообще без каких-либо интерфейсных операций со стороны SmartEngine. Сообщения об ошибках приложением SmartEngine клиенту не отображаются.

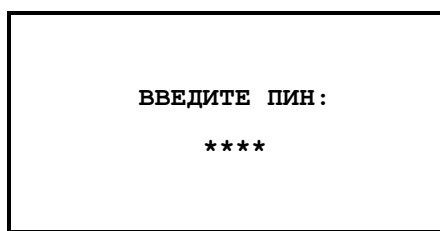
Интерфейс с владельцем карты реализуется на языке терминала (определяется в настройках приложения). Для чиповых EMV-карт существует возможность переключения на язык владельца карты, при условии поддержки данного языка в SmartEngine, либо выбора языка

из перечня поддерживаемых терминалом (если язык владельца карты не поддерживается). Перечень поддерживаемых различными версиями приложения языков приеден в журнале выпусков.

Для отображения используется нормальный шрифт, информация выровнена по центру, сообщения из одной строки выводятся на третью строку экрана, сообщения из двух строк – на вторую и третью, меню – начиная с первой строки.

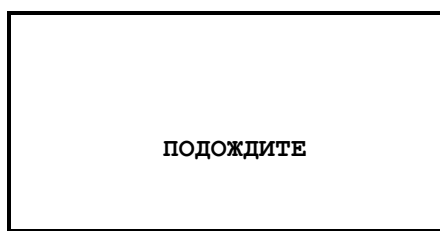
3.3 Выполнение транзакции по карте с магнитной полосой

В процессе обработки команды на выполнение транзакции возможно появление приглашения на ввод ПИН-кода.



Обрабатываются нажатия цифровых клавиш, "С" (корректировка – удаление всех ранее набранных символов), "STOP" (отмена ввода), "OK" (завершение ввода).

Отмена ввода фактически означает отказ от выполнения операции. По завершению интерфейсной операции, независимо от результата выводится экранная форма:



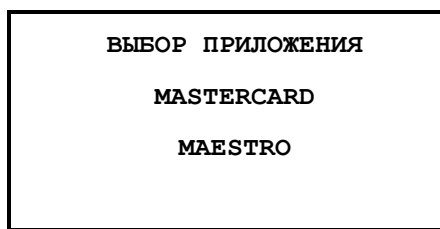
При выполнении операций, не требующих ввода ПИН-кода (ОТМЕНА, ВОЗВРАТ или ОПЛАТА по кредитной карте) отображения на экран в процессе выполнения транзакции не осуществляется.

3.4 Выполнение транзакции по чиповой EMV-карте

При выполнении транзакции по чиповой EMV-карте возможно приглашение на выбор/подтверждение приложения. Необходимость подтверждения выбора EMV приложения определяется установками карты.

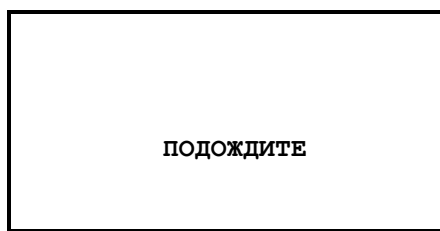
Заголовок меню отображается на языке терминала, пункты меню – на языке терминала или на английском.

Например:



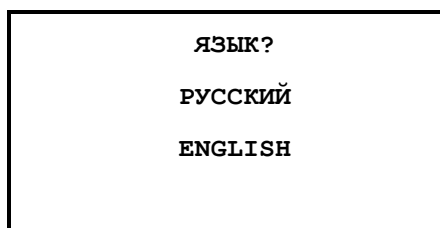
Обрабатываются нажатия цифровых и функциональных клавиш, "STOP" (отмена ввода), "OK" (завершение ввода).

Отмена ввода фактически означает отказ от выполнения операции. По завершению интерфейсной операции, независимо от результата выводится

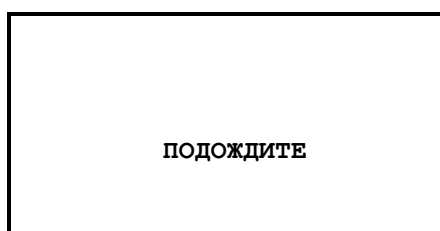


Если выбора/подтверждения приложения не осуществлялось, то экран сохраняет свое текущее состояние.

В случае, если на карте не указаны предпочтительные языки для взаимодействия с владельцем карты, либо перечень предпочтительных языков не пересекается с поддерживаемыми приложением SmartEngine языками клиенту выводится меню выбора языка (заголовок на языке терминала):



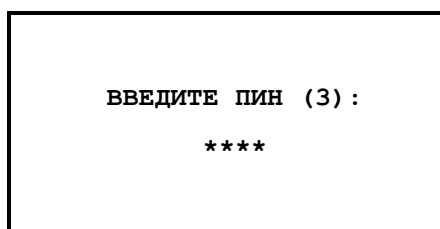
Отмена ввода фактически означает отказ от выполнения операции. По завершению интерфейсной операции, независимо от результата выводится:



В процессе выполнения транзакции возможно появление приглашения на ввод ПИН-кода на установленном в соответствии с требованиями EMV или выбранном клиентом языке:

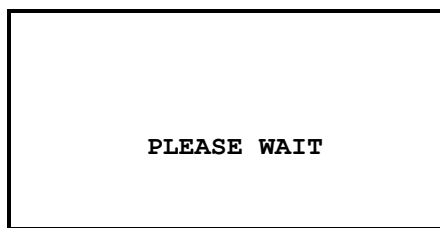


В случае проверки ПИН-кода в OFFLINE режиме, экранная форма принимает несколько иной вид (в скобках указывается число оставшихся попыток проверки ПИН-кода в OFFLINE режиме):



Обрабатываются нажатия цифровых клавиш, "С" (корректировка), "STOP" (отмена ввода), "ОК" (завершение ввода).

Отказ от ввода ПИН-кода по EMV-картам не всегда означает отказ от выполнения операции. Дальнейший ход выполнения транзакции определяется EMV параметрами эквайера. В случае использования операторного решения возможна передача запроса на хост с указанием, что клиент отказался от ввода ПИН-кода. По завершению интерфейсной операции ввода ПИН-кода, независимо от результата выводится:



3.5 Файл конфигурации

Формат файла конфигурации

Имя файла конфигурации – **CONFIG.CFG**

Строки файла конфигурации, начинающиеся с символа ';', рассматриваются как комментарии.

Формат всех остальных (значащих) строк:

Имя параметра = значение параметра

Между именем параметра и символом '=', а также между символом '=' и значением параметра может быть один или несколько пробелов.

Регистр ввода букв значения не имеет.

Максимальная длина строки файла конфигурации – 1023 байта, включая символы перевода строки CR (код 0x0D) и LF (код 0x0A).

Параметры файла конфигурации

Имя параметра	Значение параметра
FIT	Описание карточного продукта в формате: «a» b,c,d,e,f,g₁,h₁,g₂,h₂,...,g_n,h_n <i>Должен быть указан хотя бы один параметр FIT.</i> <i>При обслуживании карты поиск соответствующего описания карточного продукта ведется в порядке их расположения в файле конфигурации.</i>
FIT, a	Наименование карточного продукта, которое может использоваться в чеке. При этом регистр, в котором были введены буквы, сохраняется. Заключается в двойные кавычки. Максимальная длина без кавычек – 16 символов. Если длина больше 16, остаток игнорируется. Может отделяться от следующего поля одним или несколькими пробелами. <i>Необязательное поле</i>
FIT, b	Нижний предел диапазона номеров обслуживаемых карт
FIT, c	Верхний предел диапазона номеров обслуживаемых карт
FIT, d	Режим обслуживания карточного продукта A – карточный продукт относится к American Express F – обслуживаемые топливные карты I – топливные карты, по которым возможна только проверка

	ПИН-кода L – карты лояльности D – дисконтные карты U – необслуживаемые банковские карты <i>Необязательное поле</i>
FIT, e	Дополнительные данные о карточном продукте. Указываются сразу после режима обслуживания карточного продукта до запятой. Могут включать следующие опции: - Признак необходимости проверки срока действия карты – E0 (не проверять) или E1 (проверять). <u>Проверка выполняется, если прочитана МП (в т.ч. Fallback)</u> или данные карты введены вручную. - ES – карты euroShell. - EU – признак принадлежности карточного продукта к «европейскому» проекту Ликард. <i><u>Признак EU имеет более высокий приоритет, чем признак ES, т.е. если оба признака присутствуют в дополнительных данных о карточном продукте, то применяется признак EU, а признак ES игнорируется.</u></i> - Признак возможности OFFLINE при авторизации – F0 (OFFLINE невозможен) или F1 (OFFLINE возможен). Если признак = F1, то при авторизации по топливным картам в случае невозможности ONLINE допускается одобрение транзакции картой в режиме OFFLINE. При одобрении тип операции изменяется на оплату. - F1xxxx – минимальный интервал в мин. между OFFLINE-операциями по одной топливной карте на терминале ТПК (xxxx – от 1-й до 4-х десятичных цифр). Если минимальный интервал между OFFLINE-операциями по данной карте на терминале ТПК не истёк, то при оплате/выдаче наличных и оплате с выдачей наличных в случае невозможности ONLINE не допускается одобрения транзакции картой в режиме OFFLINE. - LIC_SH – ввод дополнительных данных в соответствии с правилами euroShell. - Mxx-xx – маска вывода PAN (xx – одна или две десятичные цифры). Цифра(ы) до дефиса – количество первых цифр PAN, выводимых в открытом виде, цифра(ы) после дефиса – количество последних цифр PAN, выводимых в открытом виде. Для вывода всего PAN в открытом виде необходимо указать маску с любыми двумя значениями, сумма которых больше или равна 19 (максимальная длина PAN) –например, M10-9, M9-10 или M99-99. Для банковских карт (режим обслуживания карточного продукта – A или не указан) максимальная маска принудительно устанавливается равной M6-4. - NOFB – Fallback запрещён. - NOW4 – карты лояльности, необслуживаемые хостом Way4, надо только вернуть данные 2-й дорожки. - Признак необходимости проверки последних 4-х цифр PAN – P0 (не проверять) или P1 (проверять). <u>Проверка выполняется (оператору предлагается ввести последние 4 цифры PAN, после чего они сравниваются с данными МП), если:</u> - ПИН-код клиента <u>не</u> введён - прочитана МП (в т.ч. Fallback) <u>выполняется не расчёт (в т.ч. обязательный), не кредитование, не</u>

	отмена, не возврат, не Deposit Confirm Euro Fleet и не Loaylty Notification Euro Fleet • терминал обслуживается оператором. RFNDxx... – параметры возврата в обслуживаемом оператором автономном терминале, где xx... – одна, две или более десятичных цифр. В настоящее время специфицированы две первые позиции: • позиция 1 0 – карта не требуется 1 – карта обязательно д.б. предъявлена • позиция 2 0 – сумма м.б. изменена 1 – сумма не м.б. изменена Признак необходимости проверки по стоп-листу – S0 (не проверять) или S1 (проверять). Признак актуален, если BlackList <u>=</u> 1. • Признак необходимости проверки Service Code топливных карт – SC0 (не проверять) или SC1 (проверять). Признак актуален, если тип процессинга – OpenWay. <u>Опции, необходимые для ввода OFFLINE ПИН-кода</u> • Axx – алгоритм проверки OFFLINE ПИН-кода (допустимые значения больше 2) • Kxx – номер ключа в Security Area, на котором проверяется OFFLINE ПИН-код • Oxx – смещение проверочного значения на 2-й дорожке (9 – 35) (xx – одна или две десятичные цифры). <u>Признаки необходимости ввода клиентом доп. данных при обслуживании всех топливных карт, кроме euroShell</u> • DN – необходим ввод идентификатора водителя • DS – необходим ввод пробега • RVN – необходим ввод регистрационного номера автомобиля • VHN – необходим ввод идентификатора автомобиля Признаки актуальны, если тип процессинга – OpenWay. • Список операций, запрещённых в карточном продукте. Запрещённые операции указываются с помощью следующих обозначений: ONB – запрос ONLINE-баланса OFB – запрос OFFLINE-баланса AUT – авторизация ATC – расчёт ACM – обязательный расчёт PUR – оплата/выдача наличных PCB – оплата с выдачей наличных CRD – кредитование TUP – пополнение OFFLINE-баланса по решению клиента
--	---

	CAN – отмена REF – возврат PAY – платёж ONH – ONLINE-история операций OFH – OFFLINE-история операций PUN – разблокирование OFFLINE ПИН-кода PSH – смена ПИН-кода PRC – подтверждение операции CDC – расчёт скидки без блокировки средств на карте лояльности ЛУКОЙЛ FLI – Fleet Inquiry Euro Fleet DPI – Deposit Inquiry Euro Fleet DPA – Deposit Auth Euro Fleet DPC – Deposit Confirm Euro Fleet LTI – Loyalty Inquiry Euro Fleet LTN – Loyalty Notification Euro Fleet <u>Пример режима обслуживания карточного продукта и дополнительных данных о карточном продукте:</u> F*E0*EU*F1*M10-9*P0*S1*SC0*TUP <u>Не указаны режим обслуживания карточного продукта, маска вывода PAN и признак необходимости проверки по стоп-листу:</u> *E0*EU*F1*P0*SC0*TUP - Первый символ дополнительных данных о карточном продукте должен быть любым (кроме запятой, букв и цифр) разделителем. - Максимальная длина дополнительных данных – 128 символов. Если длина больше 128, остаток игнорируется. - Между опциями и между обозначениями запрещённых операций должны быть разделители – любые (кроме запятой, букв и цифр) и в любом количестве (с учётом ограничения длины дополнительных данных). <i>Дополнительные данные о карточном продукте – необязательное поле.</i> <i>По умолчанию:</i> - признак необходимости проверки срока действия карты = E1 - признак возможности OFFLINE при авторизации = F0 - маска вывода PAN = M6-4 (банковские карты) и M10-9 (все остальные карты) - признак необходимости проверки последних 4-х цифр PAN = P1 - параметры возврата в обслуживаемом оператором автономном терминале = RFND00 - признак необходимости проверки по стоп-листу = S0 - признак необходимости проверки Service Code топливных карт = SC1
FIT, f	Ввод ONLINE ПИН-кода клиента 0 – запрещён 1 – на усмотрение оператора

	2 – обязателен 3 – запрещён для всех операций, кроме запроса ONLINE-баланса и ONLINE-истории операций, а также смены ПИН-кода 4 – обязателен. Запрос ONLINE-баланса запрещён 5 – обязателен, если значение позиции 3 сервис-кода карты = 0, 3, 5, 6 или 7 6 – обязателен, если: - значение позиции 3 сервис-кода карты = 0, 3, 5, 6, 7 или - значение позиции 2 сервис-кода = 2 (positive authorization is mandatory) и номер карты начинается не на 4 7 – обязателен, если значение позиции 3 сервис-кода карты = 0, 3, 5, 6 или 7, но при отказе клиента от ввода ПИН-кода транзакция продолжается, кроме операций, при выполнении которых ввод ONLINE ПИН-кода обязателен (запрос ONLINE-истории операций и смена ПИН-кода) 8 – обязателен ввод OFFLINE ПИН-кода, кроме операций, при выполнении которых обязателен ввод ONLINE ПИН-кода (<i>при этом в FIT, е должны быть указаны параметры К, А и О</i>) • При запросе ONLINE-истории операций и при смене ПИН-кода: • если f = 0, то операция прекращается • если f = 1, 5, 6 или 7, то ONLINE ПИН-код вводится безусловно. • При запросе ONLINE-баланса: - если f = 4, то операция прекращается • При выполнении всех остальных операций признак f применяется только при обслуживании карт с магнитной полосой, бесконтактных «полосатых» карт и ручном вводе данных карты. • Если f = 5, 6 или 7, и данные карты введены вручную, то ONLINE ПИН-код клиента не вводится и операция продолжается. • ONLINE ПИН-код продавца всегда вводится при кредитовании.
FIT, g	Символьный код валюты в формате ISO 8583
FIT, h	Процент автоматической комиссии/скидки по данной валюте (неотрицательное значение – процент комиссии, отрицательное – процент скидки) <i>(в данной версии не используется)</i>
Currency	Поддерживаемая приложением валюта в формате: a,b,c a – символьный код валюты в формате ISO 8583 b – цифровой код валюты в формате ISO 8583 c – экспонента валюты Может быть указано до 8 валют (до 8 параметров Currency).

	<i>Должен быть указан хотя бы один параметр Currency</i>
Processing	Тип процессинга OW – процессинг OpenWay SP – процессинг SmartPay SV – процессинг Smart Vista CTL – процессинг CTL <i>Обязательный параметр</i>
AcquirerID	Идентификатор банка-эквайера в формате ISO 8583
MerchantID	Идентификатор торговой точки/пункта выдачи наличных в формате ISO 8583
TermMode	Режим работы терминала SALE – торговый терминал CASH – терминал выдачи наличных UNIQUE – Unique (Quasi-Cash)-терминал <i>По умолчанию TermMode = SALE</i>
TerminalID	Идентификатор терминала в формате ISO 8583 <i>Обязательный параметр</i>
KeysFromHost	Загрузка ключей ON – с хоста OFF – локально • <u>Если</u> тип процессинга – не OpenWay, ключи загружаются только локально (KeysFromHost = OFF принудительно). Если KeysFromHost = ON: - Ключевая информация в файле конфигурации игнорируется. - Используется только схема формирования ПИН-блока <u>ISO TPK</u> (PINBlockScheme = ISO TPK принудительно). <i>По умолчанию KeysFromHost = OFF</i>
MAC	Использование MAC 0 – MAC не используется 1 – MAC используется <i>По умолчанию MAC = 0</i>
SecureISO	Режим Secure ISO ON – включён (при этом все сообщения между терминалом и хостом OpenWay Net Server зашифровываются) OFF – выключен • <u>Если</u> тип процессинга – не OpenWay, SecureISO = OFF принудительно. <i>По умолчанию SecureISO = OFF</i>
SecureISOAlg	Алгоритм шифрования сообщений между терминалом и хостом OpenWay Net Server 0 – 3DES 1 – DSCipher <i>Параметр должен быть указан, если SecureISO = ON</i>

PMSSecure	Режим безопасного обмена данными с хостом OpenWay POS Management Server (PMS) ON – включён (при этом все сообщения между терминалом и PMS защищаются MAC и зашифровываются <i>с использованием ключа Secure ISO</i>) OFF – выключен Если тип процессинга – не OpenWay, PMSecure = OFF принудительно. По умолчанию PMSecure = OFF
PINBlockScheme	Схема формирования ПИН-блока ISO TPK – ANSI X9.8 ISO 0, ПИН-блок зашифровывается на TPK (Terminal PIN Key) ISO TMK – ANSI X9.8 ISO 0, ПИН-блок зашифровывается на TMK (Terminal Master Key) DUKPT – ANSI X9.24 2002, DUKPT – 3DES - Схема DUKPT поддерживается не при всех типах процессинга. - Если KeysFromHost = ON, PINBlockScheme = ISO TPK принудительно. - При схеме ISO TMK параметр PinKey игнорируется. Параметр MpinKeySlot1 рассматривается как номер мастер-ключа, на котором зашифровывается ПИН-блок, а параметр PinKeyCheck – как контрольная сумма этого мастер-ключа. - При схеме DUKPT параметры MpinKeySlot1, PinKey и PinKeyCheck игнорируются. По умолчанию PINBlockScheme = ISO TPK
MpinKeySlot1	Номер мастер-ключа (0-7), на котором зашифрован ПИН-ключ (ТПК) - Если KeysFromHost = ON или PINBlockScheme = DUKPT, параметр MpinKeySlot1 игнорируется. - Если PINBlockScheme = ISO TMK, параметр MpinKeySlot1 рассматривается как номер мастер-ключа, на котором зашифровывается ПИН-блок. Параметр должен быть указан, если KeysFromHost = OFF и PINBlockScheme = ISO TPK и указан параметр PinKey ИЛИ PINBlockScheme = ISO TMK
PinKey	ПИН-ключ (ТПК, ключ шифрования ПИН-блока), зашифрованный на мастер-ключе номер MpinKeySlot1. Указывается в 16-ричном виде. Длина – 16 байт (32 16-ричные цифры). Если KeysFromHost = ON или PINBlockScheme = ISO TMK или PINBlockScheme = DUKPT, параметр PinKey игнорируется. Параметр должен быть указан, если KeysFromHost = OFF и PINBlockScheme = ISO TPK и чиповые карты обслуживаются (ChipUse = ON) и в параметрах терминала указано, что есть возможность ввода зашифрованного ONLINE ПИН-кода (для контактных или бесконтактных чиповых карт).
PinKeyCheck	Контрольная сумма ПИН-ключа (ТПК). Указывается в 16-ричном виде. Длина – 3 байта (6 16-ричных цифр). Если KeysFromHost = ON или PINBlockScheme = DUKPT, параметр PinKeyCheck игнорируется.

	Если PINBlockScheme = ISO_TMК, параметр PinKeyCheck рассматривается как контрольная сумма мастер-ключа, на котором зашифровывается ПИН-блок. Параметр должен быть указан, если KeysFromHost = OFF и PINBlockScheme = ISO_TPK и указан параметр PinKey ИЛИ PINBlockScheme = ISO_TMК
MMACKeySlot1	Номер мастер-ключа (0-7), на котором зашифрован MAC-ключ (Terminal Authentication Key, TAK) Если KeysFromHost = ON, параметр MMACKeySlot1 игнорируется. Параметр должен быть указан, если KeysFromHost = OFF и MAC = 1
PinKeyMAC	MAC-ключ (TAK), зашифрованный на мастер-ключе номер MMACKeySlot1. Указывается в 16-ричном виде. Длина – 16 байт (32 16-ричные цифры). Если KeysFromHost = ON, параметр PinKeyMAC игнорируется. Параметр должен быть указан, если KeysFromHost = OFF и MAC = 1
PinKeyMACCheck	Контрольная сумма MAC-ключа (TAK). Указывается в 16-ричном виде. Длина – 3 байта (6 16-ричных цифр). Если KeysFromHost = ON, параметр PinKeyMACCheck игнорируется. Параметр должен быть указан, если KeysFromHost = OFF и MAC = 1
MSIKeySlot	Номер мастер-ключа (0-7), на котором зашифрован ключ Secure ISO (Terminal Derivation Key, TDK) Если KeysFromHost = ON или тип процессинга – не OpenWay, параметр MSIKeySlot игнорируется. Параметр должен быть указан, если KeysFromHost = OFF и Processing = OW и SecureISO = ON или PMSSecure = ON
SecureISOKey	Ключ Secure ISO (TDK), зашифрованный на мастер-ключе номер MSIKeySlot. Указывается в 16-ричном виде. Длина – 16 байт (32 16-ричные цифры). Если KeysFromHost = ON или тип процессинга – не OpenWay, параметр SecureISOKey игнорируется. Параметр должен быть указан, если KeysFromHost = OFF и Processing = OW и SecureISO = ON или PMSSecure = ON
SecureISOCheck	Контрольная сумма ключа Secure ISO (TDK). Указывается в 16-ричном виде. Длина – 3 байта (6 16-ричных цифр). Если KeysFromHost = ON или тип процессинга – не OpenWay, параметр SecureISOCheck игнорируется. Параметр должен быть указан, если KeysFromHost = OFF и Processing = OW и SecureISO = ON или PMSSecure = ON
ManualEntry	Ручной ввод данных карты

	0 – запрещён 1 – разрешён <i>По умолчанию ManualEntry = 0</i>
Sync_Time	Синхронизация даты и времени с хостом в формате: a,b,c a – признак синхронизации даты и времени 0 – запрещена 1 – разрешена b – разница во времени между терминалом и хостом от –12 до 12 (значение, которое надо прибавить ко времени хоста, чтобы получить время терминала) c – разница между временем терминала и GMT от –12 до 12 (значение, которое надо прибавить ко времени терминала, чтобы получить GMT) Если SecureISO = ON или PMSSecure = ON, значение поля [c] должно быть реальным. <i>По умолчанию Sync_Time (a, b и c) = 0</i>
Authorization	Операции авторизации и расчёта (в т.ч. обязательного) 0 – запрещены 1 – разрешены <i>По умолчанию Authorization = 0</i>
Balance	Запрос ONLINE-баланса 0 – запрещён 1 – разрешён <i>По умолчанию Balance = 0</i>
Reconcile	Сверка итогов и выгрузка транзакций ON – разрешены, «нулевая» сверка итогов при отсутствии учитываемых в итогах пакета транзакций запрещена ON2 – разрешены, «нулевая» сверка итогов разрешена (после успешной «нулевой» сверки итогов идентификатор пакета увеличивается на 1) OFF – запрещены (при этом OFFLINE-операции не могут быть выполнены) <i>По умолчанию Reconcile = ON</i>
ChipUse	Обслуживание чиповых карт (контактных и бесконтактных) ON – обслуживаются OFF – не обслуживаются <i>По умолчанию ChipUse = ON</i>
PINByPass	«Обход» ПИН-кода при обслуживании чиповых карт ON – поддерживается OFF – не поддерживается <i>По умолчанию PINByPass = ON</i>

F55Tags	Список тегов поля 55 запроса к хосту - Теги указываются в 16-ричном виде. - Длина каждого тега – 2 байта (4 16-ричные цифры). - Между тегам и внутри тегов могут быть разделители – любые (кроме 16-ричных цифр) и в любом количестве (с учётом ограничения длины строки файла конфигурации). - Максимальное количество тегов – 50. Независимо от указанного списка тегов: - Теги 4F (Application ID) и 9F10 (Issuer Application Data) всегда помещаются в поле 55. - При оплате с выдачей наличных тег 9F03 (Amount, Other) всегда помещается в поле 55. - При обслуживании карт MPAD тег CB (Upper Cumulative Offline Amount Limit) всегда помещается в поле 55. <u>Справочно</u> Список обязательных тегов поля 55 при Processing = OW: 9F26,9F27,9F10,9F37,9F36,0095,009A,009C,9F02,5F2A,0082, 9F1A,9F33,9F34 <i>По умолчанию используется следующий список тегов:</i> 9F26,9F27,9F10,9F37,9F36,0095,009A,009C,9F02,5F2A,0082, 9F1A,9F03,9F33,004F,9F08,9F34,9F35,9F1E,9F53,0084,9F09, 9F41
ConfirmPrice	Подтверждение суммы операции клиентом, если ПИН-код не вводился, при авторизации, расчёте (<u>в т.ч. обязательном</u>), оплате/выдаче наличных, оплате с выдачей наличных, кредитовании, пополнении OFFLINE-баланса по решению клиента и возврате, кроме бесконтактных карт и производных бескарточных операций ON – сумма подтверждается OFF – сумма не подтверждается <i>По умолчанию ConfirmPrice = ON</i>
BlackList	Проверка по стоп-листу 0 – не выполняется 1 – выполняется Проверяются: - контактные чиповые карты при OFFLINE- и потенциально OFFLINE-операциях - бесконтактные карты при оплате/выдаче наличных и оплате с выдачей наличных, если решение карты – OFFLINE APPROVED ЕСЛИ: - данную карту надо проверять по стоп-листу (в FIT, е признак необходимости проверки по стоп-листу = S1) - загружен актуальный стоп-лист. <i>По умолчанию BlackList = 0</i>
BlackListTimeDomain	Период актуальности стоп-листа в днях <i>По умолчанию BlackListTimeDomain = 7</i>

PurchaseOnly	Режим Purchase Only (только оплата) при оплате с выдачей наличных ON – поддерживается OFF – не поддерживается <i>По умолчанию PurchaseOnly = ON</i>
Loyalty	Поддержка loyalty (битовая маска – набор поддерживаемых технологий) (0 – 255) 0 – loyalty не поддерживается 0x01 – апплет лояльности Ликард (кобренд ПКБ/Ликард) 0x02 – зашифрованный PAN как ссылка на идентификатор лояльности (Лукойл Балтия) <i>По умолчанию Loyalty = 0</i>
F12_13	Включение в запрос полей 12 и 13 ON – поля 12 и 13 включаются в запрос OFF – поля 12 и 13 не включаются в запрос <i>По умолчанию F12_13 = ON</i>
RequestRepeatNo	Максимальное количество повторов запроса в случае незавершённости транзакции (0 – 99) 99 – о повторе запрашивается оператор, если терминал обслуживается оператором • Параметр актуален, если повтор запроса в случае незавершённости транзакции поддерживается при данном процессинге (в текущей версии установлено, что повтор запроса поддерживается только если Processing = OW). <i>По умолчанию RequestRepeatNo = 99</i>
AuthDuration	Максимальная длительность блокирования средств на счёте при авторизации в мин. (до 12 цифр, не цифры игнорируются) Если AuthDuration > 0, то она включается в запрос авторизации, а при расчёте и обязательном расчёте вместо операции Authorisation Confirmation используется операция AFD Completion. <i>По умолчанию AuthDuration = 0</i>
TotalOfflineLimit	Лимит общей суммы исходных дебетовых OFFLINE-операций в руб. за финансовый цикл на терминале ТПК (0 – 999999999) При оплате/выдаче наличных и оплате с выдачей наличных в случае невозможности ONLINE не допускается одобрения транзакции картой в режиме OFFLINE, если после этой OFFLINE-операции лимит общей суммы OFFLINE-операций будет превышен. <i>По умолчанию TotalOfflineLimit не установлен (общая сумма OFFLINE-операций не ограничена).</i>
AutoCompleteClose	Автоматическое завершение незавершённого закрытия финансового цикла ON – выполняется OFF – не выполняется <i>По умолчанию AutoCompleteClose = ON</i>

3.6 Файл настройки коммуникационных параметров

Имя файла коммуникационных параметров – **SPDOS.INI**

Строки файла конфигурации, начинающиеся с символа ‘;’, рассматриваются как комментарии. Процедуры установления и разрыва соединения с хостом осуществляются банковским приложением автономно; предполагается использование в устройстве встроенного Ethernet/GPRS/WiFi/DialUp модуля.

Коммуникационные параметры, которые должны быть установлены в файле SPDOS.INI определены в нижеследующей таблице.

Таблица 1

Коммуникационные параметры

Наименование	Описание	Пример (рекомендуемое значение)	Примечание
ModemType	Тип модема	1 – внешний Dialup модем 2 – внутренний Dialup модем 5 – Ethernet 7 - внутренний GPRS модем 9 – WiFi	
Port	Номер порта	1 – RS232-1 для внешнего Dialup модема 2 - RS232-2 для внешнего Dialup модема 7 – для встроенного Dialup модема 9 – для встроенного Ethernet адаптера 12 – для встроенного GPRS модема 13 - виртуальный порт 14 – для встроенного WiFi адаптера	
BufferSize	Максимальный размер буфера приема/передачи	1024	
TimeZone	Временная зона	-3 - Москва (значение по умолчанию)	
HostPhone	Адрес доступа к серверу авторизации	159.251.40.100:7777 – если используется соединение по TCP/IP (159.251.40.100 – адрес; 7777 – номер порта) T8W1234567 – если используется соединение по Dialup (T (tone) или P (pulse)– режим набора	Возможно использование двух адресов доступа к авторизационному хосту см. Примечание 1.

		номера; 8 – префикс набора; W – пауза, после набора номера; 1234567 – номер телефона)	
POSMngServPhone	IP адрес и порт хоста сервера управления терминалами	159.251.40.100:7070 – если используется соединение по TCP/IP (159.251.40.100 – адрес; 7070 – номер порта) P9W7654321 – если используется соединение по Dialup (P (pulse) или T (tone)– режим набора номера; 9 – префикс набора; W – пауза, после набора номера; 7654321 – номер телефона)	Возможно использование двух адресов доступа к серверу управления терминалами см. Примечание 1.
Script	Имя файла скрипта установления соединения с банковским хостом	netserv.scr	
POSMngServScript	Имя файла скрипта установления соединения с OpenWay.PMS	pmsserv.scr	
NumberAttempt	Число повторов установления соединения	3 (по умолчанию равно 2)	
ConnectTime	Тайм-аут установления TCP соединения в секундах	30 (по умолчанию равно 75)	
Timeout	Время ожидания ответа хоста в секундах	60 (по умолчанию равно 60)	
InitString	Строка инициализации модема	ATE0V1	
ScriptTimeOut	Общее разрешенное время выполнения коммуникационного скрипта в сек.	70 (по умолчанию равно 60)	

ScrCmdWait	Разрешенное время выполнения одной команды скрипта в сек.	20 (по умолчанию равно 5)	
CmdRepeatCount	Число попыток выполнения неуспешно завершенной команды скрипта	3 (по умолчанию равно 3)	
LastIPAddress	флаг использования последнего успешного IP-адреса при повторном соединении	0 - не используется (по умолчанию) 1 – используется	
TLS	Флаг использования протокола, гарантирующего безопасную передачу данных по сети	0 – не использовать (по умолчанию) 1 – использовать TLS 1.1 2 – использовать TLS 1.2	В случае использования TLS сертификаты терминала должны быть предварительно загружены административным приложением в модуль безопасности терминала

Примечание 1.

В случае если используется два адреса доступа, то они должны быть разделены между собой символом '|' (0x7C), например, 159.251.40.100:7777|159.251.40.100:1234. Правило обработки данных, в случае использования двух адресов доступа:

- Из списка адресов выбирается первый и осуществляется попытка соединения с хостом, число попыток определяется параметром NumberAttempt. В случае успешного соединения второй адрес игнорируется. Если соединение по первому адресу установить не удалось, осуществляется переход ко второму адресу.
- В случае успешного соединения с хостом и установленным параметром LastIPAddress в 1, приложение запоминает адрес, по которому состоялось соединение с хостом, и использует этот адрес в следующей коммуникационной сессии в качестве первого адреса для установки соединения. В случае если параметр LastIPAddress равен 0, приложение начинает новую коммуникационную сессию, используя порядок адресов определенным в файле коммуникационных параметров.
- При изменении в файле параметров хотя бы одного адреса доступа к хосту, терминал возвращаться в исходное состояние, т.е. начинает обработку адресов, как определено в файле параметров.

3.7 Установка настроек для обеспечения требований PCI DSS

Для удовлетворения требований PCI DSS необходимо сконфигурировать параметры config.cfg в соответствии с прилагаемым SmartEngine PA DSS Implementation Guide.

4 Приложение взаимодействия с торговой системой

4.1 Назначение и основные возможности

Приложение для взаимодействия с торговой системой реализует протокол SETIP2/SETIP4 и обеспечивает дополнительную кастомизацию интерфейса взаимодействия ПИН-пада с клиентом в IDLE режиме.

4.2 Настройки

Приложение SETIP может быть сконфигурировано по следующим параметрам:

Наименование	Описание	Значение по умолчанию	
		T2	U32
ECR_PORT	Идентификатор коммуникационного порта для обмена с торговой системой (при обмене ПИН-пад выступает в качестве «сервера») <число> - номер TCP порта COM0 – RS232 подключение USB – USB подключение	7654	7654 (поддерживается только Ethernet подключение)
TRANSDATATIMEOUT	Тайм-аут ожидания запроса транзакции от торговой системы в случае предъявления карты до подготовки заказа (сотые доли секунды). По истечении тайм-аута предлагается удалить смарт карту и устройство переходит в ожидание ожидания карты.	12000	12000
MSGTIMEOUT	Время отображения сообщений (сотые доли секунды).	500	500
LOGO	Имя BMP-файла с заставкой, отображаемой в IDLE режиме		Не поддерживается
LOGOUTCARDTURNOFF	Флаг отключения реакции ПИН-пада на установку/прокат карты в случае отсутствия связи с торговой системой	0	Не поддерживается