

**СИСТЕМА «PETROL PLUS»
ТО PETROL ONLINE (ПОДДЕРЖКА SSL)**

*Руководство администратора
Версия 7.0.0.0*

ВЕДОМОСТЬ ИЗМЕНЕНИЙ

ИЗМЕНЁННАЯ ЧАСТЬ (раздел, страница)	ИЗМЕНЕНИЯ	
	тип (дополнения, удаления) и конкретное описание	
Публикация документа	Дата: 13.01.2016	Версия: 7.0.0.0

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ.....	5
1.1 Используемые термины, определения и сокращения.....	5
2 ОБЩАЯ СХЕМА РАБОТЫ	6
3 ПОДДЕРЖКА СЕРТИФИКАЦИИ НА ТЕРМИНАЛЕ	8
3.1 СПОСОБЫ ЗАГРУЗКИ СЕРТИФИКАТА ПО УМОЛЧАНИЮ	8
3.2 ШТАТНЫЕ СПОСОБЫ ЗАГРУЗКИ И ОБНОВЛЕНИЯ РАБОЧИХ СЕРТИФИКАТОВ.....	8
3.2.1 Особенности загрузки рабочего сертификата при изменении номера терминала и номера эмитента	8
3.3 РУЧНЫЕ ОПЕРАЦИИ СЕРТИФИКАЦИИ.....	9
3.4 ПРОСМОТР ПАРАМЕТРОВ SSL-ОБМЕНА	11
3.5 СООБЩЕНИЯ ТЕРМИНАЛА ОБ ОШИБКАХ ЗАГРУЗКИ СЕРТИФИКАТА.....	12

СПИСОК ИЛЛЮСТРАЦИЙ

Рис. 1. Схема подключений терминала.....	6
Рис. 2. Запрос пароля для получения рабочего сертификата.....	8
Рис. 3. Подтверждение использования пароля по умолчанию	8
Рис. 4. Меню «НАСТР. ПОДКЛЮЧ.».....	9
Рис. 5. Вид меню «Сертификация» (сертификат есть).....	9
Рис. 6. Вид меню «Сертификация» (сертификат отсутствует)	9
Рис. 7. Окно подтверждения выполнения операции получения сертификата	10
Рис. 8. Запрос пароля	10
Рис. 9. Подтверждение использования пароля по умолчанию	10
Рис. 10. Сообщение о наличии RSA-ключей на терминале	10
Рис. 11. Сообщение о генерации RSA-ключей.....	10
Рис. 12. Просмотр параметров SSL-обмена	11

1 ВВЕДЕНИЕ

В данном документе приведено описание особенностей информационного взаимодействия терминала с АС и КС в режиме защищённого обмена данными с использованием протокола SSL(TLS).

1.1 Используемые термины, определения и сокращения

АС	—	авторизационный сервер
БД	—	база данных
КС	—	коммуникационный сервер
ПО	—	программное обеспечение
ТО	—	точка обслуживания
Эмитент	—	организация, выпустившая платёжную карту / талон
Cisco ASA	—	аппаратный межсетевой экран (сетевой фильтр). Осуществляет контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами в целях обеспечения защиты сети от несанкционированного доступа
FleetCor CA	—	FleetCor Certification Authority — центр сертификации FleetCor (удостоверяющий центр)
Citrix	—	Citrix NetScaler VPX — ПО для оптимизации процесса доставки web-приложений. Поддерживает надёжное управление трафиком и обеспечивает защиту web-приложений от различных типов атак
NDES	—	Network Device Enrollment Service — служба управления сертификатами, входящая в состав системы Windows Server 2008 R2
RSA	—	криптографический алгоритм с открытым ключом
SCEP	—	Simple Certificate Enrollment Protocol — «черновой» стандарт Интернета, разработанный компанией Cisco Systems, который помогает решить проблему создания запросов и установки сертификатов вручную, разрешая устройствам запрашивать сертификаты x509 v3 у любых удостоверяющих центров, поддерживающих протокол SCEP
SSL	—	Secure Sockets Layer — криптографический протокол, использующий асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений

2 ОБЩАЯ СХЕМА РАБОТЫ

На Рис. 1 представлена общая схема конфигурации программно-аппаратных средств, обеспечивающих взаимодействие терминала с AC, KC в защищённом режиме обмена данными.

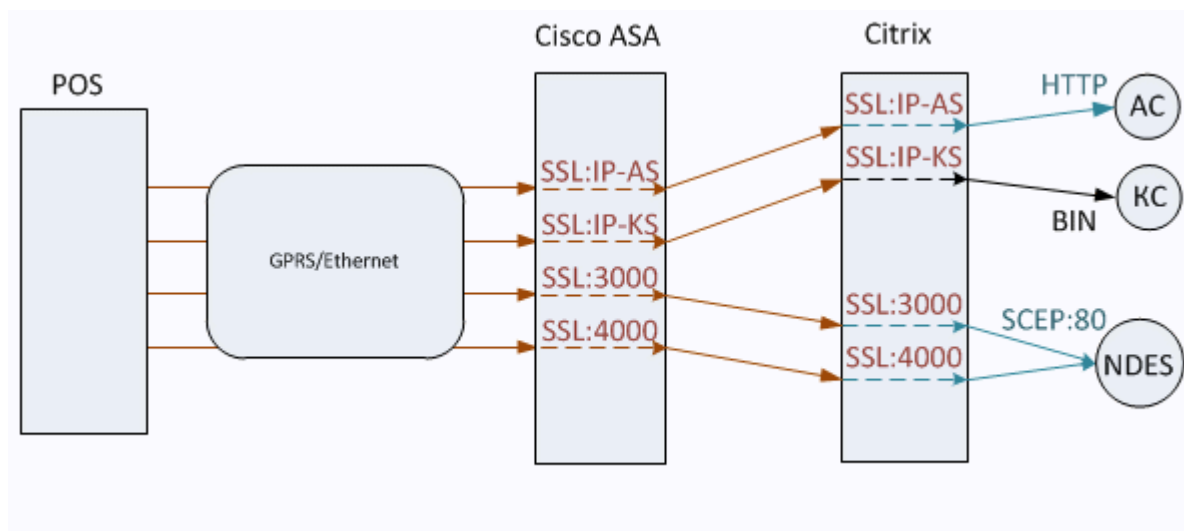


Рис. 1. Схема подключений терминала

Для обмена данными терминала используются следующие способы:

- с AC — передача данных по методу запроса POST (HTTP-протокол);
- с KC — передача бинарных данных;
- два канала обмена данными с NDES — передача данных по методу запроса GET (HTTP-протокол). Используется для работы с сертификатами.

Примечание.

Для работы с сертификатами используются два соединения с Citrix для разделения каналов связи рабочих терминалов и терминалов, которые ещё не сертифицированы. Эти соединения используют разные номера портов соединения с Citrix (порты 3000 и 4000 (см. Рис. 1) по умолчанию), что обеспечивает защиту от DDoS-атак, поскольку каждое соединение использует свой сертификат.

Все подключения терминала с AC, KC и NDES производятся по протоколу TCP/IP через хосты Citrix. При этом на терминале, как обычно, настраиваются только подключения, используемые для авторизации и инкассации (см. документ «Petrol Plus. ПП. ТО»), а сертификация производится по IP-адресам и подключениям авторизационных соединений. Если авторизационные соединения не настроены, для сертификации используются настройки подключений, используемых для инкассации. Сертификационное соединение использует фиксированные номера портов. Их значения прописываются в терминальное ПО при его сборке.

Все данные, передаваемые по каналам обмена с AC, KC и NDES, шифруются с помощью SSL. Работа по SSL-протоколу предусматривает наличие на терминале сертификата, выданного сервером NDES на уникальный RSA-ключ, сгенерированный терминалом. Приватная часть ключа хранится на терминале вместе с выданным сертификатом в специальной БД сертификатов. Этот файл шифруется с помощью криптопроцессора терминала и его данные не могут быть получены извне.

Изначально каждый терминал имеет один исходный набор параметров безопасности (ключ/сертификат/пароль), «прошиваемый» в ПО при его сборке (см. п. 3.1, стр. 8). Для обмена данными с AC и KC в штатном режиме терминал должен заменить исходный сертификат (сертификат по умолчанию) на рабочий. Для этого на терминале реализуется следующая последовательность операций:

- генерация двух RSA-ключей (приватного и публичного);
- подключение к Citrix с использованием исходного сертификата;
- генерация запроса к NDES на получение рабочего сертификата.

В штатном режиме работы терминала данные операции выполняются в автоматическом режиме и не требуют взаимодействия с администратором NDES / Citrix (см. п. 3.2, стр. 8).

Ручные операции получения / удаления / замены сертификата выполняются только в экстренных случаях (терминал скомпрометирован, терминал долго не использовался и сертификат устарел, Citrix не авторизует подключение терминала по причине некорректного сертификата и т. п.). Данные

операции реализуются с вводом пароля и по согласованию с администратором NDES / Citrix. При их выполнении оператору терминала необходимо связаться с администратором, предоставить свои данные и получить пароль на обновление (см. п. 3.2.1, стр. 8).

Информацию о сроке действия текущего рабочего сертификата, а также о других параметрах SSL-обмена можно просмотреть на терминале (см. п. 3.4, стр. 11).

Сертификат выдаётся терминалу службой NDES с привязкой к номеру терминала, номера эмитента терминала и его серийного номера (CN-данные). Изменение этих данных приведёт к тому, что сертификат станет невалидным и оператору потребуется заново получать сертификат. Особенности загрузки сертификатов, выполняемой при изменении данных терминала, приведены в п. 3.2.1 на стр. 8.

Во время каждого рестарта терминал проверяет состояние базы полученных сертификатов. Если обнаруживается какая-либо ошибка (номер терминала или номер эмитента терминала не соответствуют данным выданного сертификата, база сертификатов повреждена и т. п.), база данных удаляется и производится попытка восстановить её из резервной копии. Если резервная копия также повреждена, реализуется попытка получения нового рабочего сертификата.

Описание сообщений терминала об ошибках загрузки сертификатов приведено в п. 3.5 на стр. 12.

3 ПОДДЕРЖКА СЕРТИФИКАЦИИ НА ТЕРМИНАЛЕ

Поддержка сертификации на терминале заключается в выполнении следующих процедур:

- разовая операция загрузки сертификата по умолчанию (см. п. 3.1, стр. 8);
- загрузка и обновление рабочих сертификатов (см. п. 3.2, стр. 8);
- загрузка и обновление сертификатов в ручном режиме (см. п. 3.2.1, стр. 8).

3.1 Способы загрузки сертификата по умолчанию

Сертификат по умолчанию может доставляться на терминал одним из следующих способов:

- при обновлении ПО через TMS — данный способ используется при обновлении сети уже работающих терминалов, имеющих готовые настройки подключения;
- в процессе первоначальной «прошивки» ПО терминала.

3.2 Штатные способы загрузки и обновления рабочих сертификатов

Рабочий сертификат штатно может загружаться на терминал одним из следующих способов:

- автоматическая загрузка рабочего сертификата после обновления ПО терминала. В этом случае, после перезагрузки и обновления ПО терминал генерирует новый рабочий ключ, затем, используя имеющиеся старые настройки АС-соединения (или КС-соединения) и «прошитые» в ПО исходные параметры безопасности (ключ/сертификат/пароль), подключается к NDES и получает рабочий сертификат. Данная процедура не требует никакого вмешательства оператора, но может занимать некоторое время после перезагрузки терминала;
- загрузка рабочего сертификата в процессе инкассации (см. документ «*Petrol Plus. РП. ТО*»). Если на терминале нет настроенного подключения к АС, оператор может настроить подключение к КС и выполнить инкассацию. В этом случае, перед выполнением инкассации терминал попытается получить рабочий сертификат. Данная операция выполняется с запросом пароля (см. Рис. 2).

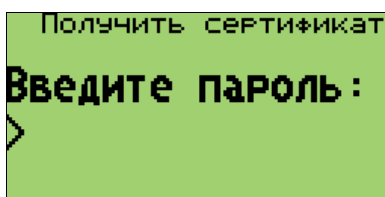


Рис. 2. Запрос пароля для получения рабочего сертификата

Для использования пароля, заданного по умолчанию, следует ввести пустую строку. Появится запрос на подтверждение выполнения операции (см. Рис. 3).

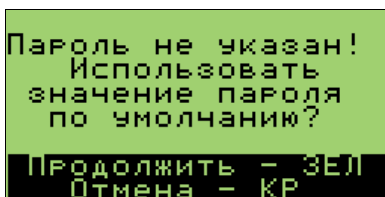


Рис. 3. Подтверждение использования пароля по умолчанию

Для завершения операции подтвердите использование пароля по умолчанию.

- автоматическое обновление рабочего сертификата по истечении срока его действия. Данная процедура запускается автоматически по истечении 80% от периода действия текущего сертификата. Операция выполняется без запроса пароля и без участия оператора.

Примечание.

Просроченный сертификат (например, в случае, когда терминал долго не использовался) не может быть обновлён в автоматическом режиме.

3.2.1 Особенности загрузки рабочего сертификата при изменении номера терминала и номера эмитента

Значения серийного номера терминала, его ID, а также номера эмитента используются на АС для идентификации подключённого терминала. При обмене данными терминала с АС через Citrix в HTTP-заголовок добавляется поле X-SSL-Client-CN: POS-EEEE-TTTTTT-SSSSSS, где EEEE —

Система «Petrol Plus»	ТО Petrol Online (поддержка SSL)	Версия: 7.0.0.0	8/12
-----------------------	----------------------------------	-----------------	------

Все исключительные авторские права принадлежат ООО «НКТ Софтвэр».

Передача данного документа или прав на него третьим лицам, его распространение, равно и использование иным образом без письменного согласия правообладателя ООО «НКТ Софтвэр» запрещены

номер эмитента, TTTT — номер терминала, SSSSSSSS — серийный номер терминала. Эти данные содержатся в сертификате терминала, который Citrix получает при установлении с ним связи.

Ниже приведены особенности загрузки рабочего сертификата, выполняемой при изменении на терминале его номера или изменения номера эмитента.

1. Если на терминале задан номер терминала / эмитента, то при изменении значения любого из этих параметров, независимо от наличия на терминале текущего рабочего сертификата, выполняется подключение к NDES и получение нового рабочего сертификата. При этом старый рабочий сертификат удаляется. Для выполнения процедуры получения нового сертификата используются исходные параметры безопасности (ключ/сертификат/пароль), «прошитые» в ПО.
2. Если на терминале не задан его номер или не задан номер эмитента, то при изменении значения любого из этих параметров, независимо от наличия на терминале текущего рабочего сертификата, процедура получения нового сертификата не выполняется.

3.3 Ручные операции сертификации

Ручные операции получения / удаления / замены сертификата выполняются только в экстренных случаях (терминал скомпрометирован, терминал долго не использовался и сертификат устарел, Citrix не авторизует подключение терминала по причине некорректного сертификата и т. п.). Данные операции выполняются с вводом пароля и по согласованию с администратором NDES / Citrix: оператору терминала необходимо связаться с администраторами, предоставить свои данные и получить пароль на обновление.

Для выполнения операций сертификации в ручном режиме выполните следующие действия:

1. Выберите пункт главного меню «Установки / Настр. подключений» (см. документ «Petrol Plus. РП. ТО»). Откроется меню «НАСТР. ПОДКЛЮЧ.» (см. Рис. 4).

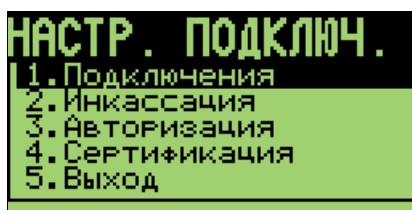


Рис. 4. Меню «НАСТР. ПОДКЛЮЧ.»

2. В меню «НАСТР. ПОДКЛЮЧ.» выберите пункт «Сертификация». Откроется окно «Сертификация». Если на терминале уже имеется рабочий сертификат, меню «Сертификация» будет иметь вид, приведённый на Рис. 5.

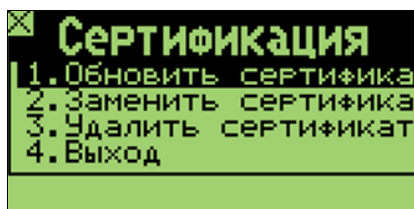


Рис. 5. Вид меню «Сертификация» (сертификат есть)

Если сертификат отсутствует, в меню будет доступен только один пункт «Получить сертификат» (см. Рис. 6).

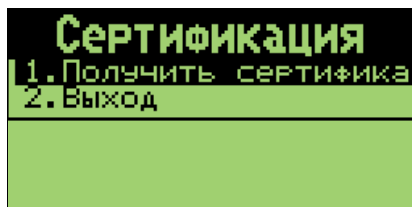


Рис. 6. Вид меню «Сертификация» (сертификат отсутствует)

Для получения сертификата выполните следующие действия:

1. В меню настройки выберите пункт **«Получить сертификат»** (см. Рис. 6). Откроется окно подтверждения выполнения операции (см. Рис. 7).

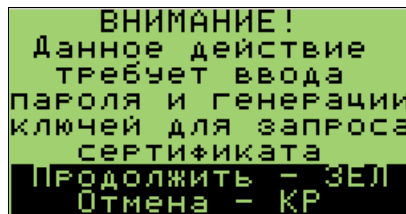


Рис. 7. Окно подтверждения выполнения операции получения сертификата

2. Продолжите операцию. Откроется окно запроса пароля (см. Рис. 8).

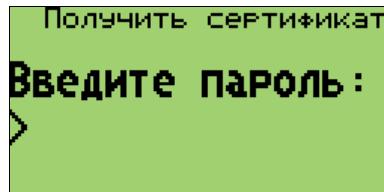


Рис. 8. Запрос пароля

3. Введите пароль. Если используется пароль, заданный по умолчанию, введите пустую строку. Появится запрос на подтверждение использования пароля по умолчанию (см. Рис. 9).

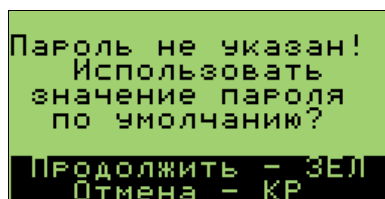


Рис. 9. Подтверждение использования пароля по умолчанию

4. Подтвердите использование пароля по умолчанию. Если на терминале уже имеются сгенерированные ранее RSA-ключи, на дисплее появится сообщение «Ключи загружены» (см. Рис. 10).

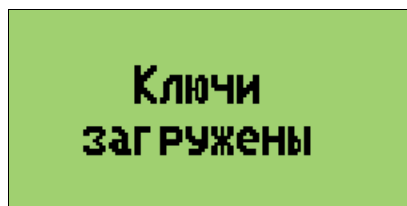


Рис. 10. Сообщение о наличии RSA-ключей на терминале

Если ключи отсутствуют, выполняется их генерация, сопровождаемая соответствующим сообщением на дисплее терминала (см. Рис. 11).

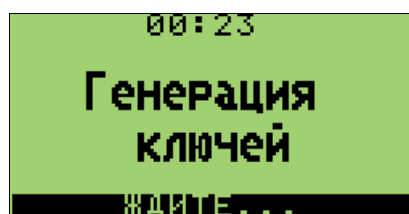


Рис. 11. Сообщение о генерации RSA-ключей

После проверки наличия (загрузки) ключей выполняется подключение к хосту NDES и загрузка рабочего сертификата. По результатам операции на дисплее появляется сообщение об успешном или неуспешном её завершении. Описание сообщений терминала об ошибках загрузки сертификатов приведено в п. 3.5 на стр. 12.

После успешной загрузки сертификата вид меню «**Сертификация**» изменится (см. Рис. 5).

Операции замены и удаления сертификата (пункты пункт «**Заменить сертификат**» и «**Удалить сертификат**», соответственно (см. Рис. 6)) выполняются аналогично операции получения сертификата, с запросом пароля. Операция обновления сертификата (пункт «**Обновить сертификат**») выполняется без запроса пароля.

3.4 Просмотр параметров SSL-обмена

Для просмотра текущих параметров обмена, выберите пункт меню «**Установки / Настр. авторизации / Диаг. авторизации**» и нажмите на кнопку **F2** (см. документ «*Petrol Plus. РП. ТО*»). На дисплее терминала появится информация о параметрах SSL-обмена терминала с АС (см. Рис. 12).

```

Диаг. авторизации
Статус: SSL-сессия
Тип: Ethernet1
IP: 127.0.0.1
Port: 4544
---- Сертификат ----
От: 07:45 18.11.2015
До: 07:45 16.05.2016

```

Рис. 12. Просмотр параметров SSL-обмена

3.5 Сообщения терминала об ошибках загрузки сертификата

В случае возникновения ошибок при выполнении процедуры загрузки рабочего сертификата различными способами на дисплее терминала могут появляться информационные сообщения, перечисленные в Табл. 1.

Табл. 1. Описание сообщений терминала об ошибках в процессе загрузки сертификата

Сообщение	Причина возникновения и способ устранения
Сертификат не получен	Общая ошибка получения сертификата
Ошибка сертиф. [....]	Детальная ошибка проверки сертификата терминала на Citrix. Требуется расшифровки разработчиком
Ошибка получения сертификата: [....]	Детальная ошибка получения сертификата на NDES. Требуется расшифровки разработчиком
Серт. требует подтверждения	Сертификат выдаётся только после подтверждения администратором NDES
Ошибка проверки запроса серт.	Некорректно работает служба NDES. Некорректно работает служба FleetCor CA
Запрос серт. отклонен	NDES не смог обработать запрос
Служба SCEP недоступна	Сервер NDES не запущен или недоступен
Нет ответа на запрос серт.	Сервер WWW не запущен или недоступен
Номер терм. НЕ ИЗМЕНЕН	Ошибка смены номера терминала из-за ошибки получения сертификата
Для смены номера эмитента необходимо закрыть смену	Для изменения номера эмитента необходимо закрытие смены