Порядок организации подключения

Оглавление

Типы подключений

Система портового сообщества поддерживает следующие типы подключений клиентов

- B2C – интерактивное рабочее место СПС с прямым доступом к информации в системе в режиме реального времени

- B2B – интерфейс (шлюз) для подключения системы клиента к СПС.

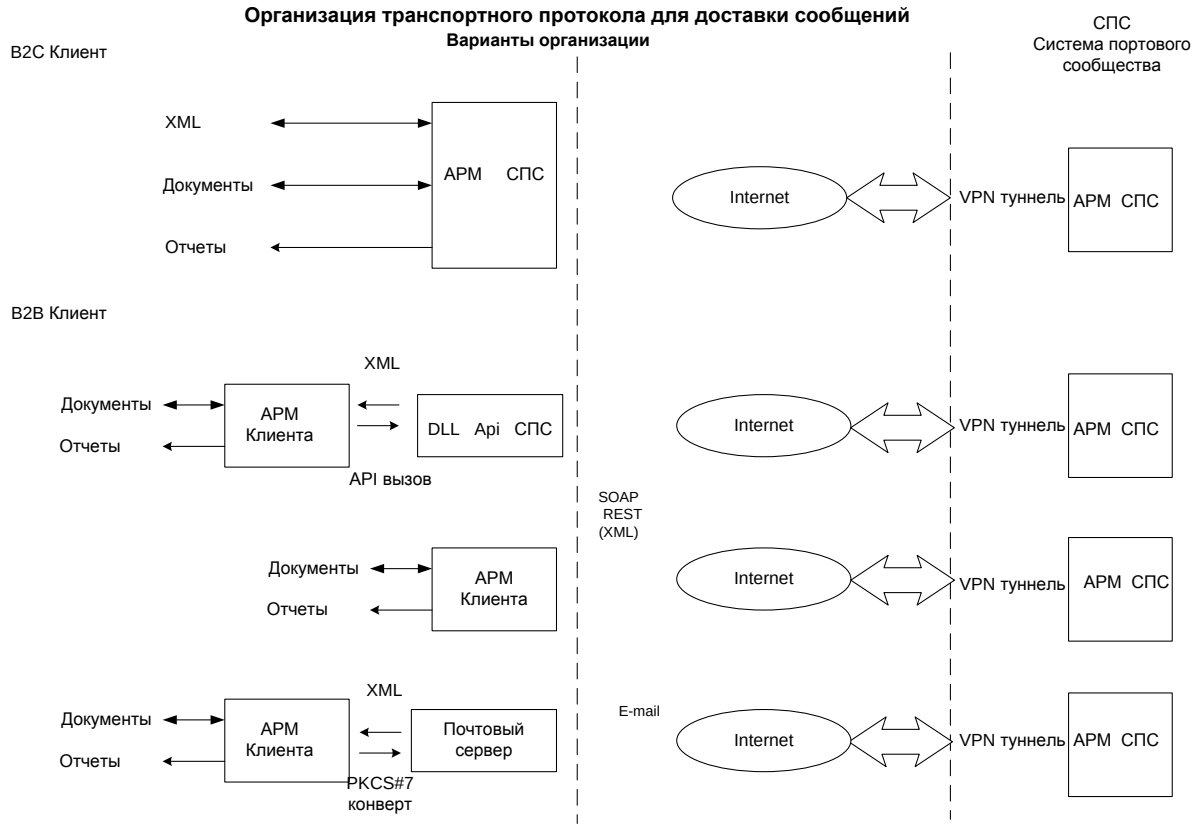
Варианты подключений B2B

Шлюзы могут быть реализованы с использованием следующих технологий:

1. REST – система клиента реализует подключение к СПС по протоколу REST и индицирует вызов функций СПС. Для реализации возможности инициации вызова со стороны СПС на стороне клиента поднимается серверная часть REST. Обмен происходит синхронно.

   1.1. DLL Api – реализует функционал организации подключения по REST протоколу (как клиентскую, так и серверную часть) и работу с ЭЦП. От системы клиента требуется только передача либо прием сообщений в формате XML и обработка сообщений об ошибках (за исключением транспортного уровня). Обмен происходит синхронно.

2. e-mail – в качестве транспорта используется электронная почта. Обмен происходит асинхронно. Каждое сообщение подтверждается квитанцией.



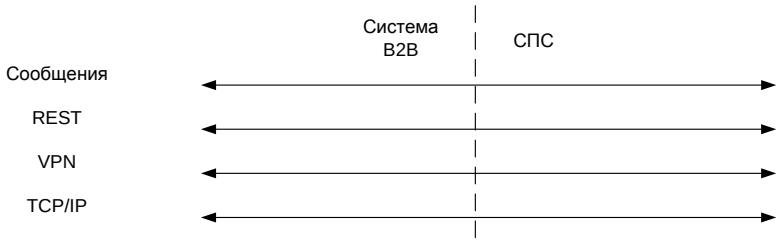
Интеграция через REST

Порядок подключения через REST

- уровни подключения
- порядок взаимодействия систем с СПС (B2B)
- порядок обработки очереди сообщений
- Физические параметры подключения через REST

Организация стека уровней подключения при использовании протокола REST приведена на рисунке:

Уровни подключения



Общая схема взаимодействия систем при построении шлюза B2B приведена на рисунке:

Порядок взаимодействия систем с СПС (B2B)
Общий вариант

При этом последовательность отправки сообщения следующая:

1. Клиент инициирует отправку сообщения путем обращения к соответствующему функционалу сервера (приложений) собственной ИС.
2. Сервер (приложений) клиента передает сообщение серверу приложений ЕИС ПС по одному из описанных выше вариантов подключения.

Сервер приложений ЕИС ПС выполняет предварительную обработку сообщения (проверка транспортной подписи, расшифровка сообщения), выполняет семантическую обработку сообщения, формирует ответ в соответствие с бизнес-процессом, подписывает его собственной ЭЦП.

3. Сервер приложений ЕИС ПС оформляет полученное сообщение в виде конверта PKCS#7, подписывает его транспортной подписью и передает серверу (приложений) клиента по одному из описанных выше вариантов подключения.

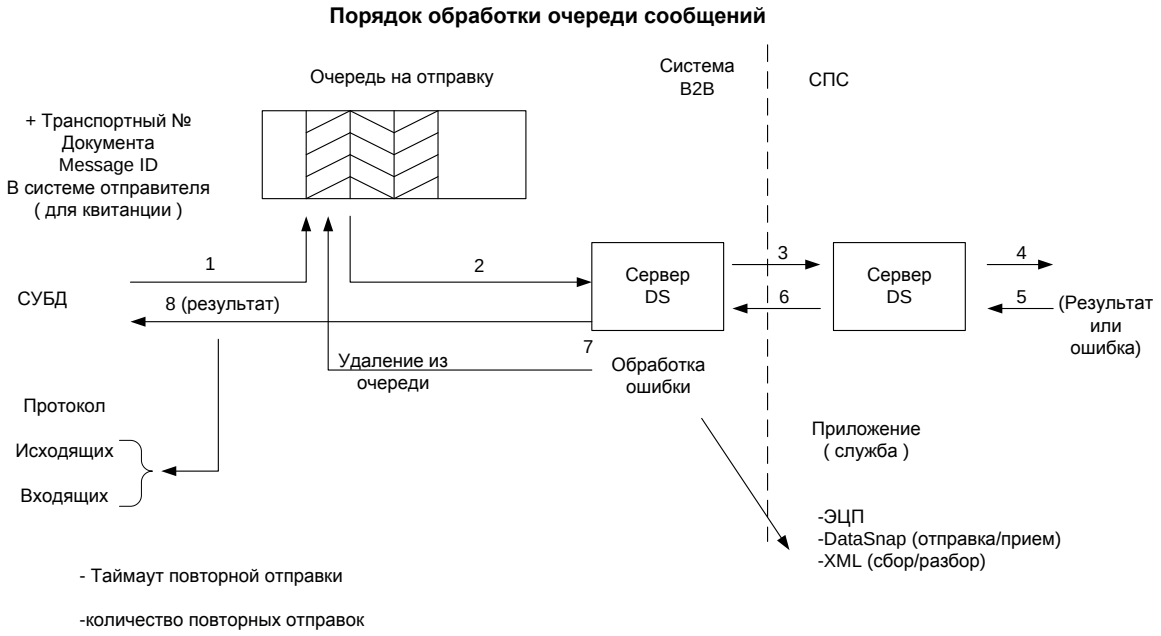
4. Сервер (приложений) клиента возвращает полученное ответное сообщение клиенту.

Примечание. В зависимости от выбранной клиентом архитектуры приложения, на шаге 1 и 6 сервером (приложений) клиента может выполняться операция упаковки сообщения в конверт PKCS#7 и обратной распаковки ответного сообщения, а также обработка ошибок канального уровня в соответствие с приведенной выше диаграммой уровней подключения.

В случае построения систем с использованием DLL Api ЕИС ПС, весь транспортный функционал реализуют библиотеки ЕИС ПС. Библиотеки DLL Api могут находится как в выделенном серверном ПО, так и в составе клиентского рабочего места. DLL реализует формирование XML с подписью, транспортную подпись и поддержку протокола REST. В общем виде, клиентское приложение должно выполнять следующие функции:

- При отправке:
    - формирование заголовка сообщения в виде строки (потока)
    - формирование тела сообщения в виде строки (потока)
    - передача строк в DLL для подписи и отправки
- При приеме:
    - Получение строк из DLL
    - Обработка заголовка сообщения
    - Обработка тела сообщения
    - Обработка ошибок

Порядок обработки очереди сообщений.



Организация КСЗИ осуществляется с использованием механизма VPN (см. «Модель безопасности»).

Физические параметры подключения через REST

Перечень параметров подключения к серверам системы:

```
Сервер VPN: vpn.ppl33-35.net
Тип VPN: L2TP over IPSec
UDP:1701(l2tp),500(isakmp),4500(nat-t)
IP:   50(esp),51(ah)
```

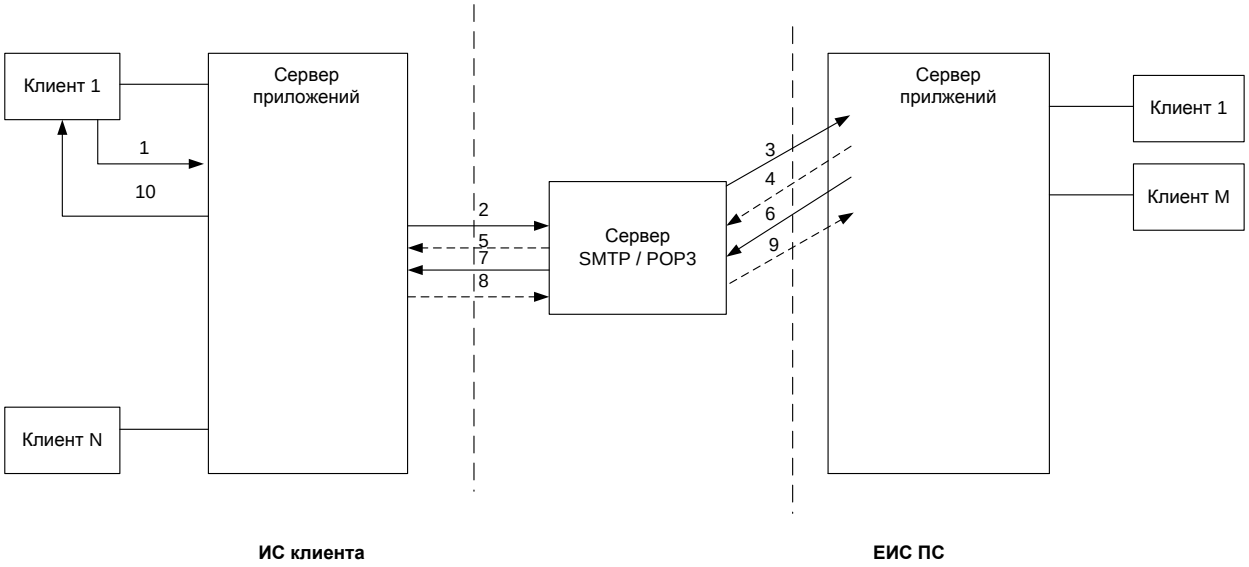
Кроме того, на стороне клиента должны быть доступны адреса АЦСК ГТСУ и ИВК. Перечень IP адресов и требуемых портов перечислены на сайтах соответствующих АЦСК.

Интеграция через e-mail

Порядок подключения через e-mail

- порядок взаимодействия систем с СПС (B2B)
- порядок обработки очереди сообщений
- Физические параметры подключения через e-mail

Порядок взаимодействия систем с СПС (B2B)
Вариант с использованием транспорта E-mail



1. Клиент инициирует отправку сообщения путем обращения к соответствующему функционалу сервера (приложений) собственной ИС.

2. Сервер (приложений) клиента передает сообщение на почтовый сервер (SMTP)

3. Сервер приложений ЕИС ПС опрашивает почтовый сервер (POP3) и получает сообщение.

4. Сервер приложений ЕИС ПС выполняет предварительную обработку сообщения (проверка транспортной подписи, расшифровка сообщения) и возвращает ответное сообщение-квитанцию на почтовый сервер (SMTP).

5. Сервер (приложений) клиента опрашивает почтовый сервер (POP3) и получает сообщение-квитанцию. Отправленное сообщение убирается из очереди отправки.

6. Сервер приложений ЕИС ПС выполняет семантическую обработку сообщения, формирует ответ в соответствие с бизнес-процессом, подписывает его собственной ЭЦП и передает его серверу приложений ЕИС ПС, оформляет полученное сообщение в виде конверта PKCS#7, подписывает его транспортной подписью и передает на почтовый сервер (SMTP).

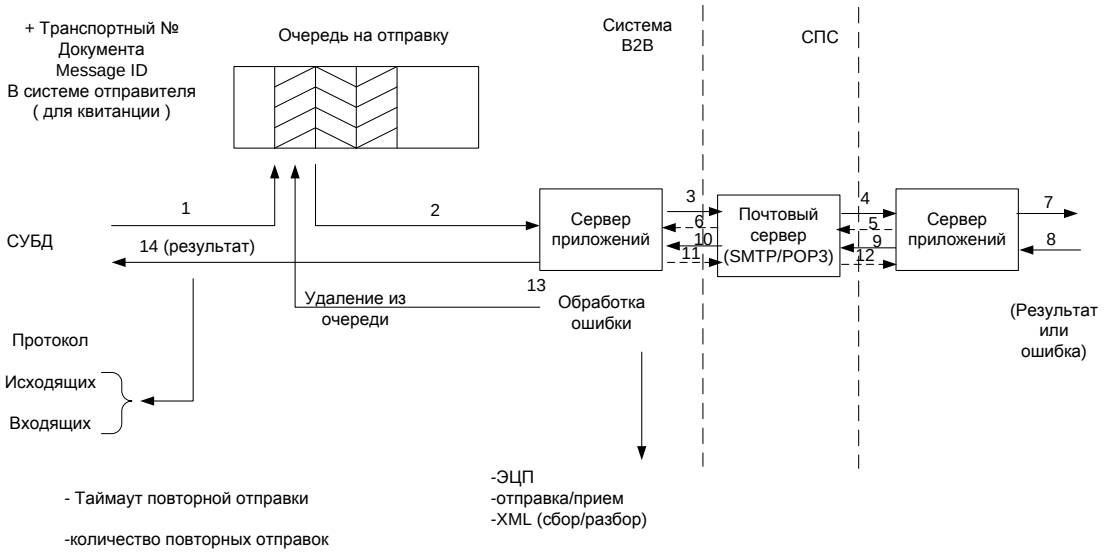
7. Сервер (приложений) клиента опрашивает почтовый сервер (POP3) и получает сообщение.

8. Сервер (приложений) клиента выполняет предварительную обработку сообщения (проверка транспортной подписи, расшифровка сообщения) и возвращает ответное сообщение-квитанцию на почтовый сервер (SMTP).

9. Сервер приложений ЕИС ПС опрашивает почтовый сервер (POP3) и получает сообщение-квитанцию. Отправленное сообщение убирается из очереди отправки.

Примечание. Сервер SMTP может находиться в зоне ЕИС ПС, в этом случае подключение к нему со стороны клиентов должно выполняться с соблюдением требований безопасности (VPN или иное шифрование канала, на которое есть заключение ГСТЗИ)

Порядок обработки очереди сообщений
(при работе через E-mail)



Физические параметры подключения через REST

Перечень параметров подключения к серверам системы:

```
Сервер SMTP/POP3: mail.ppl33-35.com
Порты TCP:
      SMTP: 25, 465
      Pop3: 110, 995
      Imap: 143, 993
```

Кроме того, на стороне клиента должны быть доступны адреса АЦСК ГТСУ и ИВК. Перечень IP адресов и требуемых портов перечислены на сайтах соответствующих АЦСК.

Обобщенный порядок взаимодействия систем

Первоначальные настройки и подключение

1. Клиент оформляет заявку на подключение. По заявке клиент получает параметры для настройки подключения.
2. Клиент настраивает VPN соединение в соответствие с инструкцией по подключению VPN
3. Клиент устанавливает и настраивает библиотеки ЭЦП, ИИТ г.Харьков (www.iit.com.ua)
4. Клиентское ПО (собственная система клиента либо установленное ПО СПС) подключается к системе по протоколу REST.
5. Для подключения к системе любым из доступных способов клиент проходит процедуру регистрации. Для этого необходим действующий ключ ЭЦП с опцией «Таможенное декларирование».
6. Клиентское ПО разрывает соединение REST
7. Клиентское ПО (либо клиент) разрывает соединение VPN.

Примечание:

1. В случае подключения через ПО СПС пункты 3 и 4 выполняются инсталлятором автоматически.

Процедура взаимодействия зарегистрированного клиента

1. Клиент устанавливает соединение VPN
2. Клиентское ПО (собственная система клиента либо установленное ПО СПС) подключается к системе по протоколу REST
3. Клиентское ПО отправляет сообщение авторизации (№19).
4. Клиентское ПО в случае успеха получает ответное сообщение с реальным ID отправителя (№20).
5. Клиентское ПО производит обмен сообщениями в соответствие с бизнес-процессом.
6. Клиентское ПО разрывает соединение REST
7. Клиентское ПО (либо клиент) разрывает соединение VPN.

Организация обмена сообщениями

Синхронный и асинхронный обмен

При организации обмена с использование протокола REST подключение к серверу приложений инициируется со стороны клиента. Обмен происходит синхронно, т.е. любое сообщение с клиента завершается ответом сервера и только после этого транзакция считается завершенной.

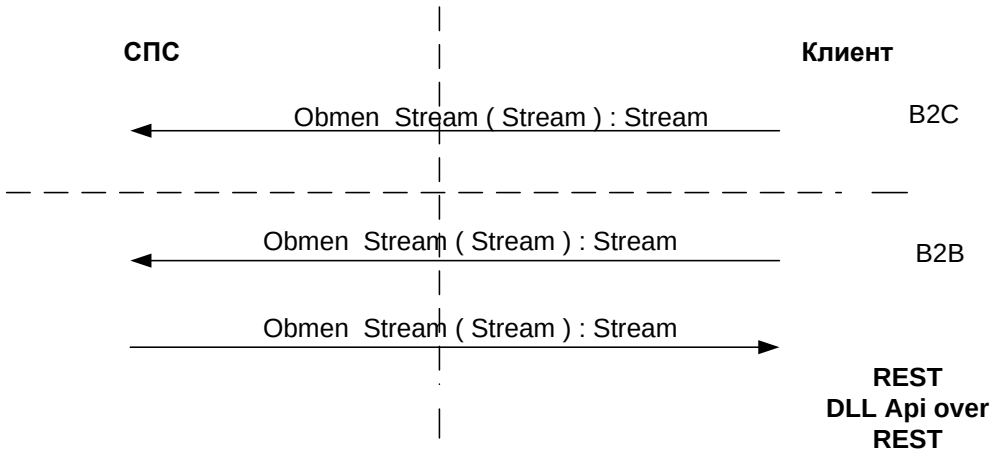
Если по технологии необходимо передать несколько сообщений, это делается либо сообщением-списком (при наличии), либо несколькими транзакциями.

При необходимости инициации передачи сообщения с сервера на клиент задействуется механизм обратного вызова (callback). Порядок работы и параметры вызова аналогичны прямому варранту.

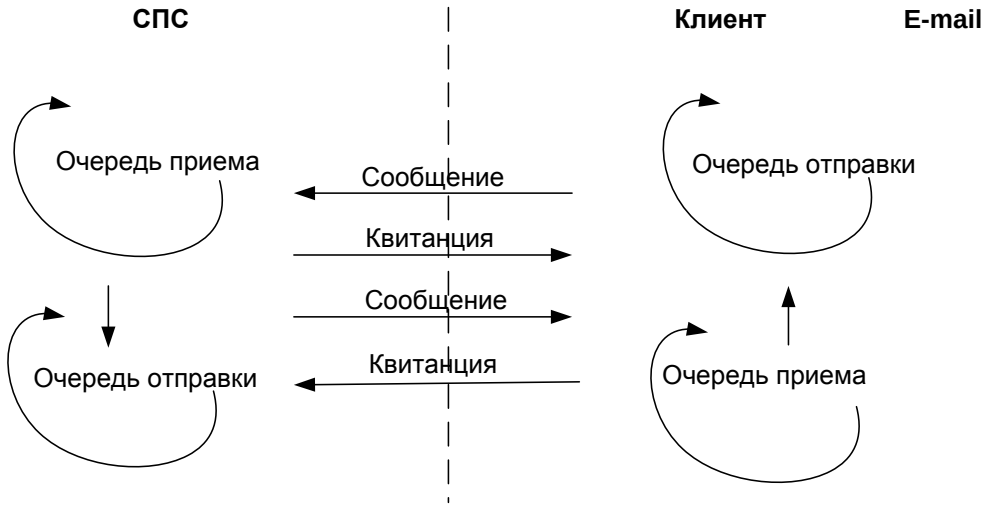
При организации обмена сообщениями через электронную почту задействуется асинхронный механизм. В этом случае каждое отправленное сообщение подтверждается квитанцией. Сообщение – ответ также подтверждается квитанцией.

ПОРЯДОК ОРГАНИЗАЦИИ ОБМЕНА СООБЩЕНИЯМИ

Синхронный обмен



Асинхронный обмен



В виду синхронности алгоритма обработки сообщений в общем виде, при обработке входящего сообщения, которое требует отправки одного либо нескольких сообщений одному либо нескольким получателям, в момент обработки типа сообщения создается соответствующая запись в очередь на отправку сообщений на сервере.