ООО «КИБЕРПЛАТ»
Россия, 123610, г. Москва, ЦМТ-2,
Краснопресненская наб., д.12, подъезд №7
Телефон: 8 (495) 967-02-20 Факс: 8 (495) 967-02-08
http://www.cyberplat.ru Email: info@cyberplat.ru

CyberPlat
Russia, 123610, Moscow, WTC-2,
Krasnopresnenskaya nab., 12, Entrance #7
Phone: +7 (495) 967-02-20 Fax: +7 (495) 967-02-08
http://www.cyberplat.com Email: info@cyberplat.com

Часто задаваемые вопросы

CyberFT FAQ

2023

Содержание

1. Правовые и организационные вопросы

1 Кто является владельцем системы?

ООО «КИБЕРПЛАТСОФТ»; ОГРН 1097746423060; ИНН 7731631406

2 Соответствует ли система требованиям следующих нормативных актов:

Положение Банка России от 4 июня 2020 г. № 719-П “О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств”

Положение Банка России от 20 апреля 2021 г. № 757-П "Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций"

В связи с тем, что КиберФТ является системой обмена юридически значимыми в рамках договорного взаимодействия между контрагентами электронными сообщениями (защищённое ЭДО), она не должна соответствовать требованиям ЦБ по защите информации при совершении платежей денежных средств. (Это все равно что просить Ростелеком на уровне каналов защитить передаваемую по этим каналам информацию).

КиберФТ только маршрутизирует сообщения, не имея доступа к их содержимому. Информация расшифровывается уже внутри защищённого контура участника сети КиберФТ, и уже только с этого момента начинаются обязательства участника по тем или иным требованиям законодательства (это касается и требований ЦБ, и требований к ПДн, и т.д.)

Вместе с тем, в КиберФТ реализованы все возможные требования по защите передаваемой информации, в системе используются надежные криптоалгоритмы и криптографические ключи длиной не менее 2048 бит, что обеспечивает достаточную надежность и стойкость шифрования. Кроме того, в системе используются механизмы защиты от несанкционированного доступа к данным и программному коду.

3 Кто выпускает сертификаты ключей (в соответствии с требованиями Федерального закона 63-ФЗ)?

Комплект Криптографических ключей Контролера (Закрытый (секретный) и Открытый ключи) и Сертификат Открытого ключа генерируются Владельцем ключей Участника самостоятельно или при содействии Главного администратора Участника при помощи ПБЗИ OpenSSL, утилиты Genkey (входящей в состав поставляемого ПО КиберФТ) или иного ПО, позволяющего формировать ключи по протоколу RSA (с длиной ключа не менее 2048 бит), либо посредством обращения в удостоверяющий центр.

4 Право какой страны будет использоваться для решения спорных ситуаций?

Договор между Клиентом и «Киберплат» регулируется и толкуется в соответствии с законодательством Российской Федерации.

5 Какие банки в настоящее время используют КиберФТ в качестве альтернативного канала связи для направления финансовых сообщений с банками, в т.ч. с банками-нерезидентами?

Сбербанк, ВТБ, РосБанк, Альфа-Банк, Газпромбанк, ЮниКредит Банк, Райффайзенбанк, РФК-Банк, Совкомбанк. Также нашу систему использовало около 100 других банков, с которыми Киберплат работал до отзыва лицензии Платины.

6 Как реализована возможность вывоза криптоядра за границу?

В КиберФТ «по умолчанию» используется криптография opensource на ключах RSA. Она во всем мире используется и никак не регулируется требованиями нашего законодательства. В рамках отечественной криптографии - вывозить ее за пределы РФ является нарушение законодательства РФ.

Для построения надежной, обязательно дублированной, связи в условиях, приближенных к «боевым», требуется принять от другого узла связи его канал с его шифрованием и дать свой канал со своим шифрованием. Так же отдельным протоколом обговаривается синхронизация/дублирование сообщений по каналам связи.

2. Принципы обмена документами

7 Есть ли портальная версия Терминала или это всегда разворачивание на стороне Клиента?

Да, есть вариант как облачного сервиса, так и вариант развёртывания на стороне клиента.

8 Как обеспечивается маршрутизация сообщений в многоранговой сети? Какие варианты настройки маршрутизации сообщений?

Маршрутизация настраивается на процессинге, между другими процессингами участников обмена. В рамках данных настроек выбирается процессинг получателя, куда изначально поступает документ и процессинг исходного получателя, куда должен в финале поступить документ.

Если у участников обмена есть в наличии собственные не связанные друг с другом процессинги, то в учётной системе данных процессингов можно настроить маршрутизацию отправки документа на другой процессинг, на котором находится получатель отправляемого документа. Каждому участнику присваивается идентификатор процессинга. Наподобие кода терминала из 12 символов, к которому принадлежит участник обмена. Благодаря этому идентификатору определяется, на каком процессинге находится участник обмена и куда отправить документ.

9 Есть ли в сети функция приоритизации трафика? Как реализовано? Есть ли нотификации отправителю о доставке срочных сообщений?

Функции приоритизации трафика у нас не реализована, поскольку мы не видим в ней необходимости в связи с высокой пропускной способностью системы. Киберплат никогда, начиная с 1997 года, не приоритизировал сообщения, обрабатывая в пиковые моменты до 1000 транзакций в секунду.

Есть возможность настройки оповещений о доставке сообщений в рамках терминала.

10 Какой конверт применяется для передачи сообщений участников в сети?

Используется конверт CyberXML. Формат электронного документа или XML конверта, который принят и поддерживается в КиберФТ.

CyberXML может быть как самостоятельным документом, так и содержать ЭД других типов.

Все документы всех форматов MT и 20022 пересылаются только в формате CyberXML, который является транспортным контейнером. При получении Терминалом получателя контейнера CyberXML автоматически делается проверка подписи, он автоматически дешифруется, далее из него автоматически извлекаются документы, у них также автоматически проверяется подпись. После этого документы преобразуются в нативные форматы в соответствии с соответствующим стандартом, которые дальше идут на экспорт в папки экспорта, например 1С, и т.д.

11 Какие реализованы варианты интеграции системы КиберФТ с АБС Банка?

Поддерживается интеграция через API.

Выгрузка документов напрямую из терминала в АБС банка.

Работа через SFTP.

12 Реализована ли в сервер CyberFT Exchange статусная модель обработки сообщений? Есть ли возможность приостановить/возобновить обработку определенных сообщений, от/на определенных клиентов? Есть ли возможность переотправки сообщений?

Данные инструменты реализованы на стороне процессинга КиберФТ.

На стороне терминала, если документ был отправлен, с ним уже ничего не сделать.

3. Форматы документов

13 Какие форматы SWIFT поддерживаются на уровне сети, какими средствами валидируются, кто предоставляет обновления форматов?

На данный момент поддерживается все основные форматы ISO 15022 и ISO 20022.

Валидация осуществляется на стороне процессинга.

Обновление форматов осуществляется на стороне. КиберФТ по запросу одного из участников обмена.

14 Допускаются ли собственные форматы сообщений между участниками сети?

Да допускаются, но могут потребоваться доработки со стороны КиберФТ.

15 Обновление форматов проводится по заявке участника, т.е. каждый участник сам должен обеспечивать обновление?

Если требуется разработка нового формата, то это делается по заявке участника. После разработки формат доступен в виде обновления/новой версии Терминала.

Нами были реализованы только те форматы, использование которых запрашивали наши клиенты. При этом реализация формата силами специалистов «Киберплатсофт» составляет от одной рабочей недели.

16 Если в пакете есть 20022 стандарт, то какие именно схемы поддерживает и как проводит валидации схем, поддерживается ли специфический документооборот стандарта?

Поддерживаются схемы pain.001, pain.002, auth.018, auth.024, auth.025, auth.026, auth.027.

Валидация проходит путем проверки по XSD семейства 20022.

Специфический документооборот поддерживается.

17 Какие рублевые форматы поддерживает ПО КиберФТ?

В любом формате можно выбрать валюту платежа «рубль-RUR».

При этом существуют форматы, подразумевающие валютные операции, в том числе с использованием валюты РФ. Это:

- платежное поручение
- реестр платежных поручений
- выписка
- camt.052
- camt.054
- PROVCSV
- pain.001.RUB

Также по просьбам клиентов были разработаны форматы, используемые ВТБ, Раффайзенбанком Россия и Сбербанком: VTBPayDocRu, VTBStatementRu, VTBRegisterRu, и аналогичные форматы в SBBOL и Raiffeisen. Они допускают использование валюты РФ.

18 Как реализована поддержка форматов SWIFT, ISO, Свободный формат?

Каждый формат представлен отдельным модулем в рамках терминала, что позволяет формировать данные типы документов как в самом интерфейсе терминала, так и выгружать напрямую из системы участника сети.

4. Производительность

19 Чем определяется пропускная способность сети? Как масштабируется сеть? Ориентиры по ключевым метрикам «Время доставки сообщений end-to-end» (в секундах), «Пропускная способность узла сети» (сообщений в секунду, МБ в секунду).

Время доставки стандартного документа **0.21 секунды**, проверялось в рамках канала связи с пропускной способностью **1 гигабит в секунду**.

20 Проводилось ли нагрузочное испытание системы в независимых лабораториях и когда? Можно ли ознакомиться с результатами нагрузочного испытания (внутреннего или внешнего)?

Было одновременно сформировано и отправлено 10 документов. Каждый документ содержит ~1000 платежек (общий размер 25 МБ)

Первый документ - 17:26:35. Последний документ - 17:27:54.

Общее время обработки, начиная с загрузки первого документа, и вплоть до экспорта последнего документа ~ 10 минут. Тысяча платежек в минуту на канале 1 Гб/с

5. Надёжность

21 Как обеспечивается высокая надежность сети (в т.ч. многоранговой)? Как реализована защита от потери информации в сети, в т.ч. при недоступности получателей или сбоя на узлах сети? Как реализован контроль дублирования сообщений в сети. Какие есть инструменты выверки в сети, как быть уверенным что все сообщения и квитанции были доставлены до адресатов?

Каждое сообщение обладает уникальным идентификационным номером uid, на каждом этапе жизненного цикла сообщения фиксируется его статус. Факт каждой доставки фиксируется служебным сообщением (квитанцией) ack. При недоступности получателя сети система либо автоматически будет

предпринимать попытки отправки сообщения, либо оператор может переотправить сообщение через интерфейс учётной системы процессинга.

22 Как реализовано резервирование (в т.ч. георасределение) компонент системы?

Георасределение и резервирование находится за пределами платформы. То есть две разных лицензии разворачиваются на разных площадках. После подписания договора на поставку платформы «CyberFT», мы все покажем и поможем сделать так, как сделано и успешно работает у нас.

23 Как реализована архитектура надежности КиберФТ (как достичь 99,99, георасределение, stand by, stand in, мониторинг, etc.)?

На данный момент надежность, бессбойность и мониторинг должны обеспечиваться внешними средствами, на уровне сети, посредством НА проксирования и т.п.

6. Безопасность

24 Как обеспечивается высокая защищенность сети (в т.ч. многоранговой)? В т.ч. защита от проникновения (на стороне провайдера, на стороне клиента), антивирусная защита с сети, anti-fraud, защита от иных угроз информационной безопасности;

У нас используется данный стек технологий по обеспечению безопасности:

- OpenSSL
- Программный продукт **МагПро КриптоПакет**;
- Поддержка ГОСТ в OpenSSL 0.9.8;
- Поддержка ГОСТ в OpenSSL 1.0.0.
- Поддерживаемая функциональность: В соответствии с RFC 4357
- Электронная подпись **ГОСТ Р 34.10-2001**;
- Распределение ключей VKO 34.10-2001;
- Хэширование **ГОСТ Р 34.11-94**;
- Симметричное шифрование **ГОСТ 28147-89**;

- MAC (имитовставка) ГОСТ 28147-89.
- Работа с защищенными сообщениями по RFC 4490;
- Функциональность PKI по RFC 4491;
- Шифрсьюты TLS на базе российских алгоритмов в соответствии с draft-chudov-cryptopro-cptls.

25 Как реализована защита информации (банковской тайны) в сети?

Все передаваемые сообщения шифруются и подписываются электронными подписями (ЭП).

Поддержка сменных СКЗИ, включая OpenSSL, КриптоПро, Signal-COM, Агава и др.

Использование протокола HTTPS (TLS туннель) при передаче данных.

Передаваемые данные недоступны оператору сети, если он не является стороной в сообщении.

Поддержка VPN и выделенных каналов связи.

Дополнительно можно ознакомиться с нашими рекомендациями по безопасности для клиентов.

7. Поддержка

26 Как реализовано обновление ПО в сети? Как достигается применение участниками сети единой (совместимых) версии ПО?

На данный момент процедура обновления осуществляется участниками обмена вручную.

При выходе новой версии участники получают соответствующие оповещение и выполняют обновление терминала.

27 Кем и как осуществляется техническая поддержка участников сети (провайдеров, клиентов), в т.ч. многоранговой?

Техническая поддержка участников сети осуществляется службой техподдержки ООО «Киберплат» в режиме 24/7 осуществляется в рамках договора ИТО.

8. Дополнения

28 Как организован архив сообщений CyberFT Exchange сервер? Какие средства используются для получения и анализа информации из архива?

Документы в хранилище терминала архивируются автоматически в архивы по 10 000 записей. Логи так же архивируются по достижению размера файла 10 Мб и автоматически удаляется каждый шестой архив.

При желании вы сможете легко настроить автоочистку их или перенос в какое-то хранилище документов из хранилища.

Доступ к информации с документами осуществляется через интерфейс терминала, журналы документов хранятся в MySQL.

29 В качестве БД в архитектуре указана MySQL. Данное решение не входит в целевой техстек. Какие могут быть альтернативы?

Postgres. Но любая альтернатива потребует существенных доработок, которые могут быть произведены по желанию заказчика.

С использованием MySQL проблем возникнуть не должно, так как весь терминал находится в контейнере виртуализации Docker и не требует дополнительного развертывания отдельных программных продуктов типа MySQL.

30 Как обеспечить надежность каналов связи клиент-провайдер, провайдер-провайдер. Какие требования к каналам, резервирование, и т.д.?

Выделить для установки Терминала и работы с ключевыми носителями отдельный сервер (физический или виртуальный), не использовать данный компьютер для других целей;

Обеспечить физические (запираемое помещение с ограниченным доступ; наличие систем кондиционирования, пожаротушения, бесперебойного энергоснабжения, контроля и управления доступом, видеонаблюдения и т.п.) и организационные меры безопасности (назначение ответственных лиц; подготовка организационно-распорядительных документов; организация учета используемых СКЗИ и ключевых носителей; разработка плана обеспечения непрерывности и восстановления работоспособности Терминала);

Расположить сервер с Терминалом в выделенном сегменте демилитаризованной зоны (ДМЗ) ЛВС; на используемом сетевом

оборудовании (межсетевом экране) запретить к серверу любой доступ из сети Интернет, а также доступ с сервера к ресурсам сети Интернет, за исключением следующих ресурсов:

- service.cyberft.ru (109.72.143.4, port 50091);
- cyberft-api.cyberplat.ru (TCP/443);
- cyberft.ru/downloads/soft (109.72.143.4, TCP/443, 80);
- используемые репозитарии ОС Debian (HTTP, FTP), get.docker.com.

Ограничить к серверу доступ на используемом сетевом оборудовании (межсетевом экране) минимально необходимым перечнем взаимодействующих с ним внутренних серверов и рабочих станций (АБС, почтовый сервер, АРМ Главного администратора и пользователей Терминала), расположенных в других сегментах, в том числе, запретить удаленный доступ со стороны системных администраторов (типовые направления и протоколы взаимодействия Терминала с другими элементами системы отображены на Рисунке 1);

Если в выделенном сегменте сети кроме Терминала будет располагаться другое оборудование, целесообразно на программном межсетевом экране, установленном на сервере, запретить взаимодействие с другими серверами сегмента, кроме минимально необходимого доступа, например, с терминала SWIFT (см. Рисунок 1);

На сервере Терминала:

- в BIOS установить пароль на изменение, отключить загрузку с внешних носителей;
- использовать файловую систему Ext4 с включенным журналированием;
- выделить под каталоги /home, /tmp, /var, /boot, /log отдельные разделы; задать квоты использования свободного пространства на диске; каталог /log сделать недоступным для чтения пользователям;
- установить пароль на загрузку (LILO или GRAB), запретить загрузку в режиме BusyBox;
- запретить использование клавиши SysRq;
- в разделах /tmp, /log запретить запуск исполняемых файлов (noexec);
- отключить и деинсталлировать неиспользуемые программные пакеты и демоны (список используемого ПО приведен в Руководстве администратора Терминала);

- при использовании функционала оповещения администраторов по внутренней электронной почте о различных критичных событиях на Терминале, разрешить отправку сообщений только на необходимые внутренние адреса;
- своевременно обновлять операционную систему, проводить установку патчей, критичных обновлений; для установки/обновления операционной системы и ПО использовать доверенные репозитарии;
- не использовать права администратора при отсутствии необходимости; в повседневной практике входить в систему как пользователь, не имеющий прав администратора (при необходимости повышенных привилегий использовать sudo);
- в /etc/security/access.conf запретить удалённый доступ (как минимум, при невозможности отказаться от удаленного доступа, запретить удаленный доступ с правами root);
- включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ. Периодически, как минимум раз в неделю, просматривать журнал аудита и должным образом реагировать на обнаруженные сообщения об ошибках;
- запретить использование незащищенных протоколов (Telnet, FTP);
- для каждого пользователя и АС, получающих доступ к Терминалу, использовать персональные учетные записи (логин/пароль);
- длина пароля должна быть не менее 8 символов, и он должен быть сложным (использовать цифры, буквы разных регистров и специальные символы; не являться последовательностью символов на клавиатуре или словарным выражением);
- установить время жизни пароля не более 3 месяцев (/etc/login.defs) и для исключения возможности автоматического подбора пароля задержку повторного ввода 30 сек (/etc/pam.d/login);
- ограничить права доступа к файловой системе и сервисам для разных ролей пользователей минимально необходимыми правами; установить параметр DIR_MODE в конфигурационном файле /etc/adduser.conf в значение 0750;
- отключить возможность запуска программ с монтируемых отчуждаемых устройств.

31 Как реализован информационный обмен (интеграция) между серверами разных провайдеров?

Обмен между разными процессингами осуществляется с помощью MQ.

32 Какие типы технических сообщений реализованы в сети (ACK/NAK, технические квитки, нотификации о доставке, трекинг я-ля SWIFT GPI, зонды)?

Тип сообщения	Описание
BICDir	Справочник участников сети CyberFT
BICDirRequest	Запрос получения справочника участников
CFTAck	Статус получения ЭД
CFTChkAck	Запрос на проверку доставки
CFTResend	Запрос на повторную отправку
CFTStatusReport	Статус доставки ЭД

33 Ответ по статусу приходит на конверты CyberXML, или на все содержащиеся в них документы тоже?

На CyberXML приходят ответы по транспортным статусам (доставлено/не доставлено). Для документов, находящихся внутри CyberXML, у которых подразумевается отправка бизнес-статусов по каждому конкретному документу, таковые высылаются Терминалом получателя через Процессинг на Терминал отправителя по каждому конкретному документу.

34 В каких точках сети обеспечивается форматно-логический контроль сообщений? Как реализован такой контроль? Как поддерживается единообразие контролей в сети (в т.ч. многоранговой)?

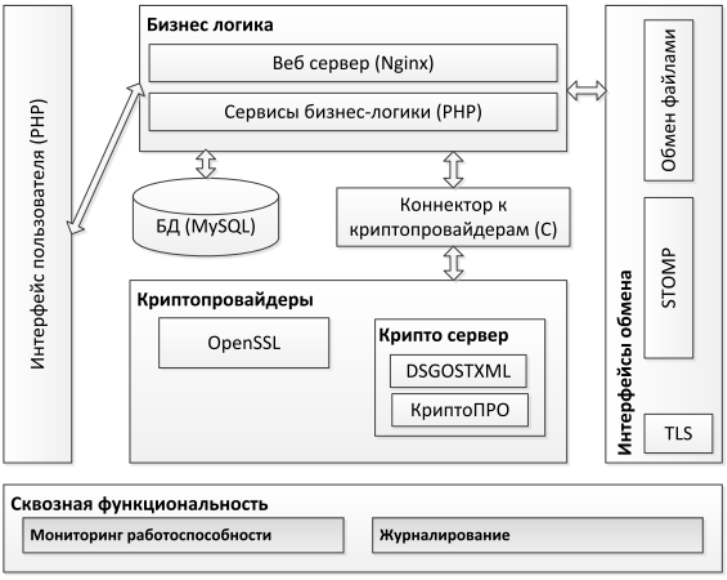
Валидация осуществляется согласно справочнику документов. Актуальность документа поддерживается на самом терминале с помощью уникального идентификатора DocID присваиваемого каждому документу.

35 Как реализована Архитектура CyberFT (ПО провайдера), в т.ч. компонентная архитектура (перечень и назначение компонент/модулей/сервисов и их взаимодействие), техническая архитектура (используемое СПО, продукты, языки программирования)?

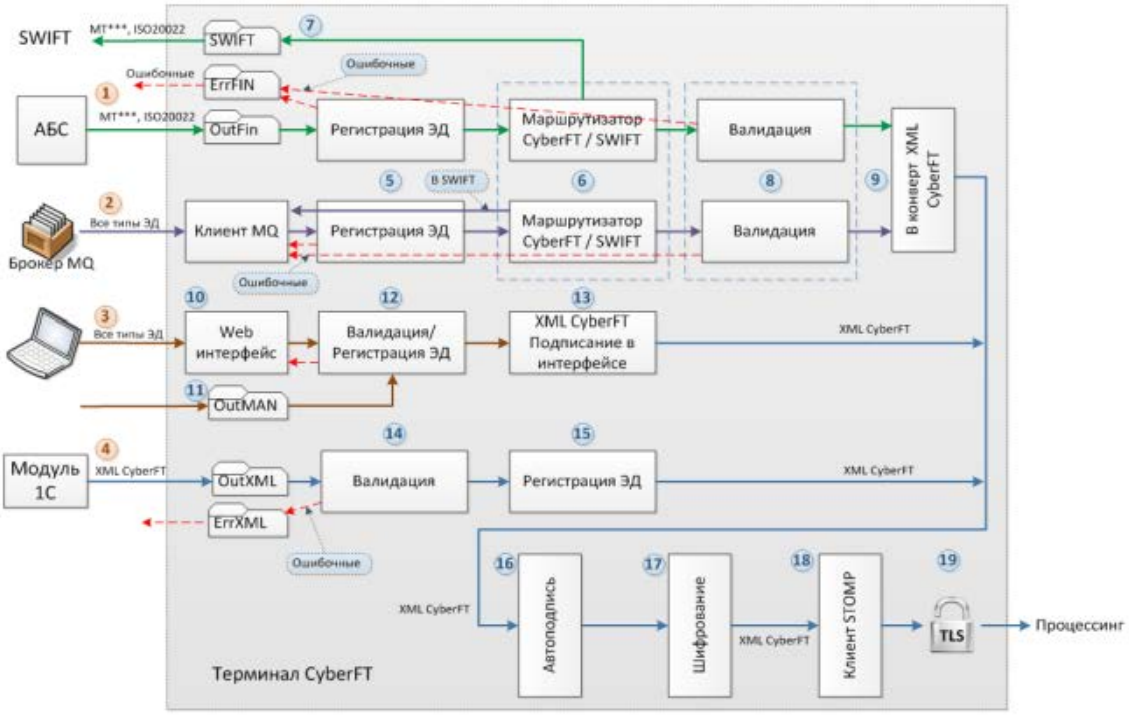
Средства и платформы разработки

1. Язык программирования PHP, PERL.
2. СУБД (MySQL, Redis, TreeDB, postgres) .
3. Операционная система Debian GNU/Linux.
4. Сервер приложений (Nginx)
5. Docker

Описание структуры



Модель данных



Интерфейсы, предоставляемые программным средством

Файловый обмен

Код интерфейса	Обозначение, идентификатор интерфейса в системе
Наименование интерфейса	Файловый обмен
Назначение	Получение входящих документов и отправка исходящих
Формат данных	XML
Транспорт	SFTP
Сценарий работы	Выгрузка документов на SFTP по инициативе банка

Передача персональных данных	Нет
Передается ли информация, регламентированная стандартом PCI DSS *	Да/Нет
Способ идентификации, аутентификации и авторизации	Доступ по sftp
Документация	Ссылка (при наличии)

* Поле не обязательно, до тех пор, пока не пройдена сертификация PCI DSS и не назначен ответственный за соблюдение его требований.

API

Код интерфейса	Обозначение, идентификатор интерфейса в системе
Наименование интерфейса	REST API
Назначение	Передача данных между системой банка и ПС без использования файлового обмена
Формат данных	XML
Транспорт	HTTPS
Сценарий работы	Request-Response
Передача персональных данных	Нет
Передается ли информация, регламентированная стандартом PCI DSS *	Да/Нет

Способ идентификации, аутентификации и авторизации	
Документация	Ссылка (при наличии)

* Поле не обязательно, до тех пор, пока не пройдена сертификация PCI DSS и не назначен ответственный за соблюдение его требований.

Интерфейсы, используемые программным средством

Код интерфейса Наименование интерфейса	Полное наименование интерфейса
Формат данных	XML
Транспорт	HTTPS
Сценарий работы	Request-Response
Передача персональных данных	Нет
Передается ли информация, регламентированная стандартом PCI DSS*	Да/Нет
Способ идентификации, аутентификации и авторизации	Доступ к MQ-очереди

* Поле не обязательно, до тех пор, пока не пройдена сертификация PCI DSS и не назначен ответственный за соблюдение его требований.

Используемые криптографические средства и алгоритмы

КриптоПРО, OpenSSL

36 На архитектурной схеме нарисована поддержка интеграции через MQ и Файлы, при этом в спецификации интеграционных сервисов описаны файлы и API, что в итоге реализовано и с какими брокерами сообщений поддерживает работу система?

Есть все из вышеперечисленного.

Документ из другого приложения кладётся в каталог импорта в виде файла. Каталог также может находиться на sftp. Терминал отправителя опрашивает каталоги импорта и найденные в них файлы загружает в своё хранилище. Далее они могут быть вручную подписаны и отправлены, либо отправляются сразу автоматически.

MQ используется не как источник документов, а как механизм для пересылки конвертов CyberXML между Терминалом и Процессингом.

37 Для интеграции между процессингами используется STOMP протокол, который запрещен у нас ИБ и Архитектурой. Есть ли альтернативы?

STOMP используется как между процессингами, так и между терминалом и процессингом. Работает в туннеле TLS stunnel4 и передача данных защищена.