Приложение №3
к Общим условиям использования электронных документов
при прямой интеграции учетных систем клиента с Банком

ПРАВИЛА
ВЗАИМОДЕЙСТВИЯ СТОРОН ПО ОСУЩЕСТВЛЕНИЮ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ ПРИ ПРЯМОЙ ИНТЕГРАЦИИ УЧЕТНЫХ СИСТЕМ КЛИЕНТА С БАНКОМ

1. Общие правила обмена электронными документами

1.1. Клиент самостоятельно определяет способ интеграции учетной системы и Банка.

Банк поддерживает следующие варианты интеграции (каждому из вариант интеграции соответствует свой набор электронных документов):

- через сервис «1С:ДиректБанк»;
- через протокол SOAP/FTPs;
- через сервис «Транзит НРД» (транзит документов Клиентов через систему электронного документооборота Небанковской кредитной организации акционерного общества «Национальный расчетный депозитарий» (ИНН 7702165310);
- через сеть «CyberFT» (транзит документов Клиентов через систему электронного документооборота Общества с ограниченной ответственностью «КИБЕРПЛАТ» (ИНН 7731220815).

1.2. Для работы в Системе Клиент самостоятельно производит настройки учетной системы и выполняет необходимые доработки своей системы в зависимости от выбранного способа интеграции с Банком.

1.3. Банк поддерживает следующие типы электронных документов в зависимости от выбранного варианта интеграции:

1.3.1. «1С:ДиректБанк»:

- документы от Клиента:
  - платежные поручения в рублях РФ;
  - платежные поручения в валюте;
  - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке;
- документы от Банка:
  - статус исполнения платежного поручения;
  - подтверждение зачисления денежных средств на счета сотрудников;
  - выписки по рублевым и валютным счетам.

1.3.2. протокол SOAP/FTPS:

- документы от Клиента:
  - платежные поручения в рублях РФ и валюте;
  - заявления на покупку/продажу валюты;
  - заявления об обязательной продаже валюты;
  - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке;
  - документы валютного контроля;
  - заявления о размещении денежных средств;
  - документы свободного формата;
  - запросы на отзыв документа
- документы от Банка:

- статус исполнения платежного поручения;
- подтверждение зачисления денежных средств на счета сотрудников;
- выписки;
- статус отзыва документа

1.3.3. через «Транзит НРД»/сеть «CyberFT»:

- документы от Клиента:
  - платежные поручения в рублях РФ;
- документы от Банка:
  - статус исполнения платежного поручения;
  - выписки.

1.4. Банк поддерживает следующие форматы электронных документов в зависимости от выбранного варианта интеграции:

1.4.1. «1С:ДиректБанк»: XML-формат технологи DirectBank (ДиректБанк) фирмы 1С. Описание приведено на сайте компании по адресу http://v8.1c.ru/edi/edi_app/bank/

1.4.2. SOAP/FTPS: XML-формат стандарта ISO 20022:

- для платежей в рублях РФ на базе формата pain.001.001.03 (06)
- для статусов исполнения платежей на базе формата pain.002.001.03 (06)
- для выписок по окончанию операционного дня на базе формата camt.053.001.02
- для промежуточных выписок по запросу на базе формата camt.052.001.02
- для платежей в валюте и конверсии на базе формата pain.001.001.03 (06)
- для отзывов поручений клиента на базе формата camt.055.001.06
- для постановки на учет кредитного договора/контракта на базе формата auth.018.001.01
- для внесения изменений в ВБК на базе формата auth.021.001.01
- для снятия с учета контракта на базе формата auth.020.001.01
- для сведений о валютных операциях на базе формата auth.024.001.01
- для справки о подтверждающих документах на базе формата auth.025.001.01
- для статусов по документам Валютного контроля на базе формата auth.027.001.01
- для возврата ранее размещенных денежных средств на базе формата trea.325.001.01.RU
- для подтверждения о размещении депозита на базе формата trea.320.001.01.RU
- для писем свободного формата из/в банк auth.026.001.01

Детальное описание форматов предоставляется Банком в Правилах Имплементации (TIG).

1.4.3. «Транзит НРД»/сеть «CyberFT»: XML-формат стандарта ISO 20022:

- для платежей на базе формата pain.001.001.03 (06)
- для статусов исполнения платежей на базе формата pain.002.001.03 (06)
- для выписок по окончанию операционного дня на базе формата camt.053.001.02

1.5. Для начала работы в Системе Пользователь Системы должен быть зарегистрирован в Системе, иметь действующий Сертификат и соответствующий ему Закрытый ключ.

1.6. Работа с ЭД в Системе происходит с ЭД, подписанными ЭП Клиента с помощью действующего Сертификата. Банк исполняет ЭД, полученные от Клиента, только после успешной проверки ЭП Клиента сервером Системы. ЭП Клиента под пакетом документов приравнивается к ЭП Клиента под каждым документом внутри пакета.

1.7. Клиент может создать неограниченное количество Сертификатов для работы в Системе. При этом количество единовременно используемых Сертификатов для подписания ЭД ЭП Клиента:

- для технологии 1С:ДиректБанк - не более 4 (четырех) Сертификатов;

- для технологий на базе протокола SOAP/FTPS/«Транзит НРД»/сети «CyberFT» – не ограничено.

1.8. Для технологии на базе протокола SOAP/FTPS/«Транзит НРД»/сети «CyberFT» Клиент может установить дополнительные требования к подписанию ЭД по сумме, заполнив Заявление о дополнительной настройке подписей по типам электронных документов (Приложение 5 к Условиям). В этом случае ЭД, получаемый Банком, должен быть сформирован таким образом, чтобы удовлетворять требованиям сочетания ЭП Клиента как для верификации на сервере Системы, так и для дополнительной проверки подписей на базе Заявления о дополнительной настройке подписей по типам электронных документов. В случае, если Клиент уже имеет действующее соглашение для работы в Системе Интернет Клиент-Банк и требования к подписанию ЭД, настроенные в системе Интернет Клиент-Банк, то данные требования будут применяться к ЭД, полученным по Системе до отмены такого требования.

1.9. Процедура обработки ЭД сервером Системы происходит следующим образом:

- сервер Банка получает ЭД и проверяет корректность всех имеющихся в нем ЭП.

- основанием для принятия Банком ЭД, переданного Клиентом по Системе, является наличие в количестве, установленном в соответствии с Заявлением, и корректность всех ЭП Клиента под ЭД. При положительном результате проверки сервер Банка проставляет в ЭД отметку о времени и ЭП Банка, свидетельствующую о получении пакета Банком, и сохраняет данный документ в Системе. При отрицательном результате проверки ЭП Клиента ЭП Банка в документе не проставляется, Клиент получает сообщение об ошибке средствами Системы. Сертификат ключа ЭП Банка выпускается уполномоченным представителем Банка. Срок действия Комплекта ключей Банка составляет 1 (один) год.

1.10. Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. При наличии действующего договора для работы в Системе Интернет Клиент-Банк все входящие документы будут отображаться в «Исходящих документах» Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл содержит ЭП Клиента, отметку о времени приема документа Банком и ЭП Банка. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.

1.11. Переданный Клиентом в Банк документ в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус документа изменяется Банком. Клиент имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк документа. Сервер Банка присваивает полученным от Клиента документам следующие статусы:

1.11.1. для технологии 1С:ДиректБанк:

- Платежные поручения в рублях РФ, платежные поручения в валюте:

  - «Принят» – электронный документ прошел первичный контроль и поступил в обработку;

  - «Исполнен» – платежный документ исполнен Банком;

  - «Отклонен банком» – электронный документ не прошел первичный контроль в Банке и был отклонен;

  - «Приостановлен» – платежный документ отложен Банком по причине недостатка средств на счете Клиента;

  - «Аннулирован» – Электронный документ был отозван Клиентом с одобрения Банка;

  -«Не подтвержден» – Платежный документ ожидает подтверждения по SMS или личном кабинете Клиента;

- Зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке:

  - «Принят» – электронный документ прошел первичный контроль и поступил в обработку;

  - «Исполнен» – электронный документ исполнен Банком;

  - «Отклонен банком» – электронный документ не прошел первичный контроль в Банке и был отклонен.

Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться присвоение Банком ЭД Клиента статуса «Принят». Банк

информирует Клиента об исполнении каждого ЭД Клиента путем направления Клиенту соответствующего уведомления посредством Системы.

1.11.2. для технологии SOAP/FTPS/«Транзит НРД»/сети «CyberFT» используются следующие статусы:

«RCVD» - получено Банком;

«RJCT» - отклонено;

«ACTC» - принято, проверены подлинность и формат;

«ACCP» - принято, документ отправлен на исполнение;

«ACSP» - конечный успешный для внешних платежей;

«ACSC» - конечный успешный для внутренних платежей.

1.12. При формировании ЭД для Клиента Банк проставляет в нем ЭП Банка. Документ считается переданным Банком Клиенту, если он подписан ЭП Банка и помещен во входящие документы Клиента на сервере Банка. При наличии действующего договора для работы в системе Интернет Клиент-Банк, исходящие документы от Банка будут присутствовать в списке «Входящие документы» Клиента на сервере Банка. Клиент может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.

1.13. Банк фиксирует электронные архивы полученных от Клиента ЭД, содержащих ЭП Клиента и ЭП Банка, и доставленных Клиенту ЭД, содержащих ЭП Банка, и хранит их.

2. Порядок получения, замены и хранения ключей

2.1. Клиент может запросить генерацию Сертификатов своих Пользователей Системы согласно Заявлению о настройке пользователей Системы (Приложение 1 к Условиям) в соответствии с Руководством по генерации сертификатов (Приложение 2 к Условиям). В рамках Договора Клиент может использовать ЭП, выпущенные Банком для Пользователей Клиента в рамках заключенного договора об использовании электронных документов.

2.2. Сертификат каждого Пользователя Системы регистрируется Банком на основании подписанного Сторонами Акта о признании (Приложение 6 к Условиям), распечатанного и подписанного в 2 (дух) экземплярах, по одному для каждой из Сторон. Заполненный Акт о признании Система формирует автоматически.

2.3. Срок действия Комплекта ключей указывается в Сертификате и составляет 1 (Один) год. Срок действия Сертификата не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Системы, срок действия Комплекта ключей не может превышать 1 (Одного) года. Клиент несет ответственность за отслеживание срока действия сертификата и полномочий Пользователей Клиента.

2.4. До истечения установленного срока Клиент обязан инициировать процедуру генерации нового Сертификата. Продление срока действия Сертификата невозможно. На основании Заявления на аннуляцию сертификата Сертификат Пользователя Системы аннулируется и не подлежит восстановлению. Каждый новый Акт о признании конкретного Пользователя, подписанный Сторонами, автоматически отменяет действие Сертификата данного Пользователя Системы, выпущенного ранее.

2.5. Оформленный со стороны Банка Акт о признании Клиента вручается лично представителю Клиента, курьеру Клиента, либо направляется Клиенту посредством почтовой связи. Акт о признании должен храниться у каждой из Сторон не менее 5 (Пяти) лет после окончания срока действия Комплекта ключей.

2.6. Обязательное аннулирование Сертификата проводится в случае Компрометации Ключей электронной подписи Клиента.

2.7. В случае лишения Клиентом Пользователя Системы права подписывать ЭП Клиента ЭД, соответствующий Сертификат выводится из действия на основании письменного Заявления об отзыве (аннулировании) сертификатов пользователей Системы (Приложение 4 к Условиям).

3. Обеспечение безопасности процедуры обмена документами

3.1. Безопасность обмена ЭД достигается за счет применения следующих средств:

3.1.1. Средство криптографической защиты информации (СКЗИ) на базе Программного комплекса «Бикрипт 5.0.», разработанного ООО Фирма «ИнфоКрипт» (сертификат соответствия ФСБ РФ СФ/114-3534 от 12 декабря 2018 года);

3.1.2. Использованием СКЗИ «Криптотокен» или «Криптотокен 2» в составе USB-токенов JaCarta ГОСТ (eToken ГОСТ), разработанных ЗАО «Алладин Р.Д.» (сертификат соответствия № СФ/124-3475от 10 августа 2018 года). Ключ электронной подписи никогда не покидает внутренней защищенной памяти USB-токена. Генерация и хранение Ключа электронной подписи, а также подписание документов производится во внутренней защищенной памяти USB-токена. Доступ к ключу электронной подписи осуществляется с использованием ПИН-кода доступа к токену.

3.1.3. СКЗИ КриптоПро CSP версии 4.х и выше. Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v. 1.2, RFC 2246), применяются криптографические алгоритмы шифрования в соответствии с ГОСТ 28147-89, обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с ГОСТ Р 34.11-94;

3.1.4. Удостоверения принадлежности сервера Системы ПАО РОСБАНК с помощью сертификата, выданного ПАО РОСБАНК аккредитованным Удостоверяющим центром ООО "КРИПТО-ПРО".

3.2. На основании дополнительных соглашений между Сторонами возможно применение других технических средств по защите информации.

3.3. Клиенту рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих требований безопасности:

3.3.1. Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;

3.3.2. Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;

3.3.3. Исключить использование средств удаленного администрирования;

3.3.4. Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана);

3.3.5. Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.);

3.3.6. Контролировать соблюдение требований безопасности.

3.4. Клиент обязан:

3.4.1. исключить появление в компьютере вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение подсистемы, скомпрометировать ключи Пользователя Системы посредством применения лицензионных средств защиты от вредоносного кода и регулярного их обновления;

3.4.2. исключить возможность Компрометации ключей в процессе их эксплуатации и хранения.

3.5. Стороны обязаны:

3.5.1. обеспечивать конфиденциальность Ключей электронной подписи, в частности не допускать использование принадлежащих им Ключей электронной подписи без их согласия;

3.5.2. уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении;

3.5.3. не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного Ключа нарушена.

3.6. Банк вправе в одностороннем порядке заблокировать Ключ электронной подписи Пользователя Системы в случае появления обоснованных подозрений в наличии на компьютере

Пользователя Системы вирусов или других программ деструктивного действия. Для возобновления работы Клиенту после удаления с компьютера Пользователя Системы вирусов или других программ деструктивного действия потребуется заново сгенерировать Сертификат и Ключ электронной подписи.

3.7. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон.

3.8. В случае Компрометации ключей любого Пользователя Клиента, Клиент обязан:

3.8.1. В случаях доступности Комплекта ключей (подозрение на несанкционированное копирование), а также в случае недоступности (утрата, хищение и т.п.) Комплекта ключей сообщить Администратору Системы по телефону (телефон и электронный адрес Администратора системы указаны в Заявлении о настройке пользователей системы) о факте Компрометации или угрозе Компрометации), используя для авторизации данные из Сертификата.

3.8.2. При этом, Администратор Системы вправе произвести дополнительные действия по авторизации Пользователя Системы (обратный звонок по указанному в Заявлении телефону, запрос на предоставление дополнительной информации: о фамилии куратора Клиента в Банке/уполномоченного сотрудника Банка, количестве пользователей и т.п.). В случае непредоставления информации Администратор ставит в известность куратора Клиента в Банке/уполномоченного сотрудника Банка и по согласованию с ним решает вопрос о продолжении/блокировании работы Клиента в Системе.

3.8.3. В срок не более 3 (Трех) рабочих дней после сообщения по телефону о факте Компрометации ключей, направить в Банк на бланке Клиента письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Клиента (при наличии). В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены ключей;

3.8.4. В случае принятия решения о замене Комплекта ключей – Клиент обязан сгенерировать новый Комплект ключей самостоятельно и направить своего представителя в Банк для его регистрации.

3.9. В случае Компрометации ключей Банка, последний обязан:

3.9.1. Известить Клиента о факте компрометации Комплекта ключей Банка, продолжении\приостановлении работы Системы и смене Комплекта ключей Банка посредством Системы с указанием даты и точного времени смены вышеуказанного Комплекта ключей;

3.9.2. Произвести внеплановую смену Комплекта ключей Банка и передать Сертификат ключа Банка Клиенту.

3.10. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного Клиента Банк немедленно приостанавливает использование Системы данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде или с использованием иных, не связанных с Системой, средств дистанционного обслуживания.

3.11. Дальнейшее использование Системы Клиентом возможно только после устранения угрозы Компрометации ключей Клиента.

4. Порядок проверки ЭД и ЭП при разногласиях

4.1. Для разрешения споров относительно подлинности ЭД по заявлению заинтересованной Стороны, полагающей, что ее права нарушены, Сторонами в двухнедельный срок с даты подачи заявления создается Согласительная комиссия, в присутствии которой производятся все операции по подготовке и проведению процедуры разрешения спора. В состав Согласительной комиссии включаются представители Банка в количестве двух человек и представители Клиента в количестве двух человек, а в случае необходимости (по соглашению Сторон) – независимые эксперты. Представителями Банка и Клиента могут быть назначены как сотрудники этих организаций, так и иные компетентные лица, полномочия которых подтверждаются соответствующими доверенностями.

4.2. Спорным ЭД является ЭД, в отношении которого одна Сторона предъявляет претензии по его подлинности другой Стороне.

4.3. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка.

4.4. В присутствии членов Согласительной комиссии Банк обязан на свободном от программного обеспечения компьютере установить операционную систему Windows7 и выше и программу КриптоПро CSP версии 4.x и выше.

4.4.1. Сторона, отстаивающая подлинность спорного ЭД, обязана предоставить спорный ЭД, действовавшие в момент создания спорного ЭД Сертификаты Стороны, подписавшей спорный ЭД, Банк обязан предоставить сами Сертификаты, записанные на съемном носителе в виде файлов в формате, применяемом Системой (в случае если Клиент не предоставляет спорный ЭД, он предоставляется Банком).

4.4.2. Стороны обязаны предоставить все имеющиеся в их распоряжении Сертификаты, информацию о проведенных плановых и внеплановых сменах Комплекта ключей Сторон и документы, удостоверяющие факты смены Комплекта ключей. Стороны также обязаны предоставить служебные ЭД Системы, в которых указаны факты получения ЭД из каналов связи и результаты их обработки (проверки).

4.5. Члены Согласительной комиссии должны выполнить следующие действия:

4.5.1. Произвести с помощью программы КриптоПро CSP и каждого Сертификата, использованного при подписании спорного ЭД, операцию проверки ЭП;

4.5.2. Создать Протокол установления подлинности ЭД – документ на бумажном носителе, создаваемый Системой в качестве результата проверки ЭП спорного ЭД (далее – Протокол). Протокол должен содержать распечатанные на бумажном носителе Сертификаты, использованные для установления подлинности ЭП, и заключение об итогах проверки ЭП спорного ЭД. Протокол должен быть подписан собственноручно всеми членами Согласительной комиссии;

4.5.3. Сравнить Сертификаты с соответствующими Сертификатами, зафиксированными в Протоколе установления подлинности ЭП спорного ЭД, и установить, тождественны ли они, внести об этом запись в Протокол (данная запись заверяется подписями членов Согласительной комиссии);

4.5.4. Установить, являлись ли Сертификаты действующими на момент создания ЭП спорного ЭД, и внести запись об этом в Протокол (данная запись заверяется подписями членов Согласительной комиссии). Сертификат признается действующим на момент создания ЭП спорного ЭД в случае, если дата создания спорного ЭД приходится на период действия Сертификата. В противном случае Сертификат признается недействующим на момент создания ЭП.

4.6. Согласительная комиссия признает Электронный документ подлинным, если одновременно выполнены условия:

4.6.1. Сертификаты совпадают с соответствующими Сертификатами, зафиксированными в Протоколе,

4.6.2. Все результаты проверки ЭП в Протоколе положительны,

4.6.3. Согласительная комиссия признала все Сертификаты, содержащиеся в Протоколе, действующими на момент выработки ЭП.

В противном случае Согласительная комиссия признает ЭД недействительным.

5. Интеграция через сервис «1С:ДиректБанк»

5.1. Автоматизированный обмен данными между Банком и Клиентом строится на основе использования сервиса 1С:ДиректБанк, позволяющий создавать, подписывать и отправлять документы в Банк из 1С: Предприятие. Подробное описание, порядок работы и технические детали приведены на сайте разработчика компании 1С по ссылке: http://v8.1c.ru/edi/edi_app/bank/

6. Интеграция по технологии на базе протокола SOAP

6.1. Автоматизированный обмен данными между Банком и Клиентом строится на основе использования Web-сервиса SOAP, в рамках которого стороны обмениваются данными, используя транспортный контейнер. Описание в виде wsdl-файла приведено по ссылке https://www.bankline.ru/h2h/iso/H2HService?wsdl (WSLD схема сервиса).

6.2. Инициатором обмена данными всегда выступает Клиент, посредством обращения к Web-сервису. Все Клиенты обращаются к одному Web-сервису.

6.3. Транспортный контейнер может иметь зашифрованную часть или не иметь таковой.

6.4. Документ, содержащийся в транспортном контейнере, должен иметь ЭП. Для формирования ЭП и шифрации данных должна использоваться одна и та же криптосистема, в зависимости от настроек, ключ для шифрации может совпадать только с одним из ключей для формирования ЭП.

6.5. В канале обмена данными используются следующие запросы со стороны Клиента:

6.5.1. Запрос на аутентификацию

Параметры запроса:

- *Идентификатор Клиента*
- *Номер сертификата*
- *Издатель сертификата*

Ответ модуля H2H:

- *Зашифрованный ID сессии*

Все остальные запросы должны приходить с ID авторизованной сессии в заголовке (или первым параметром в остальных запросах). Сессия имеет таймаут (настраиваемый на стороне Банка параметр).

6.5.2. Запрос – принять файл

Параметры запроса:

- *Транспортный контейнер*
- *ID сессии*

Тип запроса:

- Описание в секции DocTypeType xsd-схемы транспортного контейнера (Приложение 1 к настоящим Правилам)

Ответ модуля H2H:

- *Транспортный контейнер*

6.5.3. Запрос – закрыть сессию

Параметры запроса:

- *ID сессии*

Пояснение: Запрос содержит *ID*-сессии, в общем случае ответ модуля не обязателен, т.к. активная сторона запрашивать модуль не будет, а модуль в любом случае закроет сессию по таймауту.

6.6. Тело входящего сообщения может содержать документ или пакет однотипных документов, описанных в первом разделе типов.

6.7. При получении транспортный контейнер проходит следующие проверки:

- на структуру контейнера
- на наличие Клиента и его Пользователей, как зарегистрированных в Системе
- на корректность дешифрации (если предусмотрено, запрос в криптосервер)
- на корректность разархивирования (если предусмотрено)
- на наличие и корректность необходимых подписей (запрос в криптосервер)

6.8. Описание методов API

6.9.1. Запрос на аутентификацию

createSession

cryptoSystem – используемая криптосистема. Соответствует enum криптостстем из xsd-схемы транспортного пакета. Передавать значение g (одна маленькая буква)

certNum – номер сертификата. Берется из сертификата Клиента в том виде как он есть (со всеми ведущими стартовыми 0). Поскольку на нижнем уровне это массив байтов в hex-кодировке, при передаче case-символов и наличие разделяющих пробелов между байтами не имеет значения –

должно обработаться и в uppercase и в lowercase; и с разделителем между байтами пробелом и без разделителей.

Issuer – издатель сертификата – используется атрибут CN (common name) поля Issuer (издатель) сертификата Клиента

Client – код Клиента в терминах ИКБ

Метод возвращает массив байтов – это бинарное содержимое pkcs7-контейнера, внутри которого содержится зашифрованный ID сессии, который после расшифровки надлежит передавать во всех остальных запросах.

Важно! У сертификата, который используется для создания сессии должно стоять разрешение на шифрование данных (Data Encipherment в Key Usage). Это право не имеет никакого отношения к правам пользователя в ИКБ – только к разрешениям на криптографические операции. При этом у данного сертификата может вообще не стоять права делать подпись (Digital Signature в Key Usage).

Данные условия позволяют создать на стороне клиента на серверной стороне исключительно транспортный уровень, который будет заниматься только шифрованием/расшифровкой данных, все необходимые подписи под которыми уже создали клиенты на своих локальных рабочих местах. Подписи, собранные в пакете, могут быть сделаны другим сертификатом и даже другими пользователями.

6.9.2. Запрос – получение настроек

getSettings

Session – ID сессии, полученный в методе создания сессии

Client – код Клиента в терминах ИКБ

6.9.3. Метод информационного обмена

createRequest

session – ID сессии, полученный в методе создания сессии

client – код клиента в терминах ИКБ

requestBody – байты xml транспортного пакета, соответствующего переданной xsd-схеме

Метод возвращает массив байтов – это бинарное содержимое транспортного пакета, ответа сервера

Для транспортного пакета поддерживаемые кодировки UTF-8 и WINDODS-1251

Для внутренних документов в формате ISO поддерживаемая кодировка UTF-8

6.9.4. Закрытие канала обмена

closeSession

session – ID сессии, полученный в методе создания сессии

7. Интеграция для технологии на базе протокола FTPS

7.1. Механизм обмена данными построен на использовании FTPS-сервера, через который производится обмен файлами между Банком и Клиентом.

7.2. Общее описание работы протокола FTPS:

- подпись файлов выполняется с помощью ГОСТ сертификатов;
- шифрование файлов выполняется с помощью ГОСТ сертификатов;
- для работы необходима программа КриптоПро CSP версии 4.x и выше;
- возможно использование дополнительных средств кодирования информации.

7.3. FTPS-сервер передает зашифрованные файлы на внутренний FTP-сервер, где они расшифровываются. После расшифровки FTP-сервер принимает только файлы со следующими расширениями: txt, pdf, csv, doc, docx, xls, xlsx, jpg, enc, sig, zip, txz, rar, wav, mp3, xlsb, 7z, tif, gz, xml, , raz.

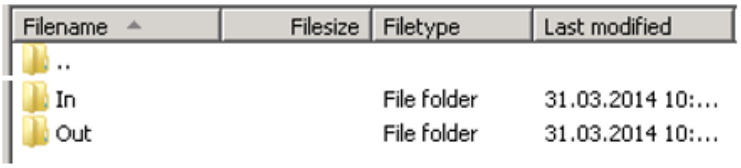
7.4. Для публичных IP адресов и/или подсетей партнера настраивается разрешение на подключение к FTPS-серверу Банка, IP адрес которого 194.8.224.46.

Параметры подключения к серверу:

194.8.224.46 порт 990, требование implicit FTP over SSL. Порты данных 65000-65100.

7.5. На FTPS-сервере создается пользователь. Данные пользователя UserName и Password передаются партнеру. Пользователю даются права чтения/записи на папки, предназначенные для обмена файлами.

7.6. Если поток обмена данными с Клиентом один и не требуется отдельного именования потока, то создаются папки In и Out.



7.6.1. Папка In – папка для файлов от Клиента.

В папку In можно выкладывать только файлы с расширением sig.enc (подписанные и зашифрованные файлы). Имя файла должно содержать только латинские буквы заглавные и строчные, цифры, «-» и «_»,«!». Например, Test_1_3-3!.txt.sig.enc

7.6.2. Папка Out – папка для файлов из Банка.

7.7. Если потоков обмена данными несколько или требуется именование потока, то создаются папки для потока(-ов) вида:

- %NameStream%\In
- %NameStream%\Out

7.8. Для отправки файлов в Банк необходимо файлы скопировать в папку In. Затем эти файлы будут в автоматическом режиме переданы получателям на стороне Банка.

7.9. Файлы из Банка копируются в автоматическом режиме в папку Out.

7.10. Внимание! Файлы с одним и тем же именем будут перезаписываться при перемещении из папки In.

7.11. Срок хранения файлов на FTPS сервере 30 (Тридцать) дней, после истечения этого срока файлы автоматически удаляются из всех папок.

7.12. Ограничения на передачу файлов: максимальный объем загружаемых файлов 100 шт. за одну загрузку (скрипт запускается раз в 10 минут), следующие файлы можно загружать только после того как предыдущие будут скопированы на внутренний сервер, т.е. исчезнут из папки In, и максимальный суммарный объем передаваемых файлов не более 5Гб за одну передачу.

8. Полезные ссылки для работы с Системой

Для теста:

https://www6.bankline.ru/h2htest/iso/H2HService - сервис H2H

https://www6.bankline.ru/h2htest/iso/H2HService?wsdl – WSLD схема

https://www6.bankline.ru/h2htest/db1c_h – сервис для 1С

Для боя:

https://www.bankline.ru/h2h/iso/H2HService – сервис H2H

https://www.bankline.ru/h2h/iso/H2HService?wsdl – WSLD схема сервиса

https://www.bankline.ru/h2h/db1c_h – сервис для 1С

9. Приложения:

Приложение 1. Xsd-схема транспортного контейнера

Приложение 2. Пример транспортного контейнера с опцией шифрования документа

Приложение 3. Пример транспортного контейнера с опцией архивирования документа

Приложение 4. WSDL описание сервиса H2H

Приложение 1. Xsd-схема транспортного контейнера

HostToHost.xsd

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:vc="http://www.w3.org/2007/XMLSchema-versioning"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:hh="urn:rosbank:hh"
        targetNamespace="urn:rosbank:hh"
        elementFormDefault="qualified"
        attributeFormDefault="unqualified"
        version="1.0"
        id="HostToHost"
>
 <xs:element name="Error" type="hh:ErrorType">
  <xs:annotation>
   <xs:documentation>транспортный формат ошибки</xs:documentation>
  </xs:annotation>
 </xs:element>
 <xs:complexType name="ErrorType">
  <xs:annotation>
   <xs:documentation>транспортный формат ошибки</xs:documentation>
  </xs:annotation>
  <xs:sequence>
   <xs:element name="Message" type="xs:string" minOccurs="1" maxOccurs="1">
    <xs:annotation>
     <xs:documentation>Сообщение об ошибке</xs:documentation>
    </xs:annotation>
   </xs:element>
   <xs:element name="Code" type="xs:string" minOccurs="0" maxOccurs="1">
    <xs:annotation>
     <xs:documentation>Код ошибки</xs:documentation>
    </xs:annotation>
   </xs:element>
   <xs:element name="FileName" type="xs:string" minOccurs="0" maxOccurs="1">
    <xs:annotation>
     <xs:documentation>имя исходного фала, при обработке которого произошла
ошибка</xs:documentation>
    </xs:annotation>
   </xs:element>
  </xs:sequence>
 </xs:complexType>
 <xs:element name="Envelope" type="hh:EnvelopeType">
  <xs:annotation>
```

```
   <xs:documentation>транспортный конверт</xs:documentation>
  </xs:annotation>
 </xs:element>
 <xs:complexType name="EnvelopeType">
  <xs:annotation>
   <xs:documentation>транспортный конверт</xs:documentation>
  </xs:annotation>
  <xs:sequence>
   <xs:element name="body" type="hh:BodyType" minOccurs="1" maxOccurs="1">
    <xs:annotation>
     <xs:documentation>тело сообщения</xs:documentation>
    </xs:annotation>
   </xs:element>
   <xs:element name="signature" type="hh:SignatureType" minOccurs="1" maxOccurs="4">
    <xs:annotation>
     <xs:documentation>Подпись</xs:documentation>
    </xs:annotation>
   </xs:element>
  </xs:sequence>
  <xs:attribute name="clientCode" type="xs:string" use="required">
   <xs:annotation>
    <xs:documentation>идентификатор КБ</xs:documentation>
   </xs:annotation>
  </xs:attribute>
  <xs:attribute name="crysys" type="hh:CryptoSysType" use="required">
   <xs:annotation>
    <xs:documentation>идентификатор криптосистемы</xs:documentation>
   </xs:annotation>
  </xs:attribute>
  <xs:attribute name="format" type="hh:FormatType" use="required">
   <xs:annotation>
    <xs:documentation>формат обмена</xs:documentation>
   </xs:annotation>
  </xs:attribute>
  <xs:attribute name="docType" type="hh:DocTypeType" use="required">
   <xs:annotation>
    <xs:documentation>тип документа</xs:documentation>
   </xs:annotation>
  </xs:attribute>
 </xs:complexType>

 <xs:complexType name="BodyType">
  <xs:annotation>
   <xs:documentation>тело сообщения</xs:documentation>
  </xs:annotation>
  <xs:sequence>
```

```
   <xs:choice minOccurs="1" maxOccurs="1">
    <xs:element name="encryptedDoc" type="hh:EncryptedDocType">
     <xs:annotation>
      <xs:documentation>Данные</xs:documentation>
     </xs:annotation>
    </xs:element>
    <xs:element name="doc" type="xs:base64Binary">
     <xs:annotation>
      <xs:documentation>Данные</xs:documentation>
     </xs:annotation>
    </xs:element>
   </xs:choice>
  </xs:sequence>
  <xs:attribute name="compressFormat" type="hh:CompressFormatType" use="optional">
   <xs:annotation>
    <xs:documentation>Формат сжатия данных</xs:documentation>
   </xs:annotation>
  </xs:attribute>
  <xs:attribute name="encrypted" type="xs:boolean" use="optional">
   <xs:annotation>
    <xs:documentation>признак использования шифрованного тела</xs:documentation>
   </xs:annotation>
  </xs:attribute>
 </xs:complexType>

 <xs:complexType name="EncryptedDocType">
  <xs:simpleContent>
   <xs:extension base="xs:base64Binary">
    <xs:attribute name="cert" type="xs:string" use="required">
     <xs:annotation>
      <xs:documentation>сертификат, для которого зашифровано</xs:documentation>
     </xs:annotation>
    </xs:attribute>
    <xs:attribute name="issuer" type="xs:string" use="optional">
     <xs:annotation>
      <xs:documentation>издатель , для которого зашифровано</xs:documentation>
     </xs:annotation>
    </xs:attribute>
   </xs:extension>
  </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="SignatureType">
  <xs:annotation>
   <xs:documentation>подпись</xs:documentation>
  </xs:annotation>
```

```
 <xs:sequence>
  <xs:element name="SignatureValue" type="xs:base64Binary">
   <xs:annotation>
    <xs:documentation>Тело подписи</xs:documentation>
   </xs:annotation>
  </xs:element>
 </xs:sequence>
 <xs:attribute name="signKind" type="hh:SignKindType" use="required">
  <xs:annotation>
   <xs:documentation>тип подписи</xs:documentation>
  </xs:annotation>
 </xs:attribute>
 <xs:attribute name="cert" type="xs:string" use="required">
  <xs:annotation>
   <xs:documentation>сертификат подписанта</xs:documentation>
  </xs:annotation>
 </xs:attribute>
 <xs:attribute name="issuer" type="xs:string" use="optional">
  <xs:annotation>
   <xs:documentation>издатель сертификата подписанта</xs:documentation>
  </xs:annotation>
 </xs:attribute>
</xs:complexType>

<xs:simpleType name="SignKindType">
 <xs:annotation>
  <xs:documentation>тип подписи</xs:documentation>
 </xs:annotation>
 <xs:restriction base="xs:int">
  <xs:enumeration value="0">
   <xs:annotation>
    <xs:documentation>подпись банка</xs:documentation>
   </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="1">
   <xs:annotation>
    <xs:documentation>подпись руководителя</xs:documentation>
   </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="2">
   <xs:annotation>
    <xs:documentation>подпись бухгалтера</xs:documentation>
   </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="3">
   <xs:annotation>
```

```
      <xs:documentation>подпись ст. сотрудника</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="4">
     <xs:annotation>
      <xs:documentation>подпись мл. сотрудника</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
   </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="CryptoSysType">
   <xs:annotation>
    <xs:documentation>идентификатор криптосистемы</xs:documentation>
   </xs:annotation>
   <xs:restriction base="xs:string">
    <xs:enumeration value="g">
     <xs:annotation>
      <xs:documentation>ГОСТ</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="p">
     <xs:annotation>
      <xs:documentation>PGP</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="c">
     <xs:annotation>
      <xs:documentation>Криптопро</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
   </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="CompressFormatType">
   <xs:annotation>
    <xs:documentation>Формат сжатия данных</xs:documentation>
   </xs:annotation>
   <xs:restriction base="xs:string">
    <xs:enumeration value="zip">
     <xs:annotation>
      <xs:documentation>Zip формат с одним файлом в архиве</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
   </xs:restriction>
  </xs:simpleType>
```

```
 <xs:simpleType name="FormatType">
  <xs:annotation>
   <xs:documentation>формат обмена</xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:string">
   <xs:enumeration value="ISO20022.RU 2015.01 RUS">
    <xs:annotation>
     <xs:documentation>ISO 20022 для передачи финансовых сообщений между банком и корпорацией с учетом требований национальной платежной системы. Версия 2015.01</xs:documentation>
    </xs:annotation>
   </xs:enumeration>
   <xs:enumeration value="SWIFT">
    <xs:annotation>
     <xs:documentation>SWIFT..</xs:documentation>
    </xs:annotation>
   </xs:enumeration>
   <xs:enumeration value="OTHER-XML">
    <xs:annotation>
     <xs:documentation>Прочие форматы в xml виде (транспортный контейнер, ошибка...)</xs:documentation>
    </xs:annotation>
   </xs:enumeration>
  </xs:restriction>
 </xs:simpleType>

 <xs:simpleType name="DocTypeType">
  <xs:annotation>
   <xs:documentation>тип документа</xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:string">
   <xs:enumeration value="pain.001.RUB">
    <xs:annotation>
     <xs:documentation>pain.001специальным образом сформированные рублевые платежные инструкции корпорации;</xs:documentation>
    </xs:annotation>
   </xs:enumeration>
   <xs:enumeration value="pain.001.FCY">
    <xs:annotation>
     <xs:documentation>pain.001специальным образом сформированные валютные платежные инструкции корпорации;</xs:documentation>
    </xs:annotation>
   </xs:enumeration>
   <xs:enumeration value="pain.002">
    <xs:annotation>
     <xs:documentation>статусы(квитанции) на платежные инструкции корпорации;</xs:documentation>
    </xs:annotation>
```

```
    </xs:enumeration>
    <xs:enumeration value="camt.053">
     <xs:annotation>
      <xs:documentation>финальная выписка по счету, содержащая все операции за день</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="rsb.hh.lst">
     <xs:annotation>
      <xs:documentation>запрос на список id документов или документ по id</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="MT940">
     <xs:annotation>
      <xs:documentation>Выписка в формате SWIFT MT940</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="MT942">
     <xs:annotation>
      <xs:documentation>Выписка в формате SWIFT MT942</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="MT950">
     <xs:annotation>
      <xs:documentation>Выписка в формате SWIFT MT950</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="TRANSPORT-CONVERT">
     <xs:annotation>
      <xs:documentation>Документ формата транспортного конверта</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ERROR">
     <xs:annotation>
      <xs:documentation>Ошибка приема/разбора документа</xs:documentation>
     </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
 </xs:simpleType>

</xs:schema>
```

Приложение 2. Пример транспортного контейнера с опцией шифрования документа

<?xml version="1.0" encoding="UTF-8"?>

<!--Sample XML file generated by XMLSpy v2011 rel. 2 (http://www.altova.com)-->

-<hh:Envelope xmlns:hh="urn:rosbank:hh" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:rosbank:hh HostToHost.xsd" format="ISO20022.RU 2015.01 RUS" docType="pain.001" clientCode="RSB001" crysys="g">

-<hh:body encrypted="true">

<hh:encryptedDoc cert="50 01" issuer="ПАО РОСБАНК">UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</hh:encryptedDoc>

</hh:body>

-<hh:signature cert="10 21 35" issuer="ПАО РОСБАНК" signKind="1">

<hh:SignatureValue>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</hh:SignatureValue>

</hh:signature>

</hh:Envelope>

Приложение 3. Пример транспортного контейнера с опцией архивирования документа

<?xml version="1.0" encoding="UTF-8"?>

<!--Sample XML file generated by XMLSpy v2011 rel. 2 (http://www.altova.com)-->

-<hh:Envelope xmlns:hh="urn:rosbank:hh" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:rosbank:hh HostToHost.xsd" format="ISO20022.RU 2015.01 RUS" docType="pain.001" clientCode="RSB02" crysys="g">

-<hh:body compressFormat="zip">

<hh:doc>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</hh:doc>

</hh:body>

-<hh:signature cert="22 54 87" signKind="2" issuer="ПАО РОСБАНК">

<hh:SignatureValue>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</hh:SignatureValue>

</hh:signature>

</hh:Envelope>

Приложение 4. WSDL описание сервиса H2H (альтернативный к предоставленному по ссылке)

H2HService.wsdl