Приложение № 4
к Общим условиям использования
электронных документов

ИНСТРУКЦИЯ
О ПОРЯДКЕ ВЗАИМОДЕЙСТВИЯ СТОРОН ПО ОСУЩЕСТВЛЕНИЮ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

1. Обмен Электронными документами

1.1. Для работы в Системе Пользователь Системы использует программно-технические средства, удовлетворяющие требованиям, приведенным в Списке технических и программных средств, необходимых для работы подсистемы “Клиент” (далее – Список).

1.2. В процессе работы Пользователь Системы выполняет в Системе следующие действия:

- Регистрация в Системе – формирование специального ЭД “регистрация”, подписанного ЭП Клиента (далее – ЭПК). Работа в Системе возможна только после успешной проверки ЭПК сервером Системы.
- Работа с ЭД, исходящими от Клиента, предполагает формирование новых ЭД на основе ЭД, имеющихся в Системе и предусмотренных в Заявлении. Для каждого типа ЭД в Системе имеется соответствующая экранная форма. Для документов “Платежное поручение” возможен импорт в Систему файлов определенного Банком формата. Описание структуры файла импорта имеется на сервере Банка.
- Проставление для каждого ЭД одной или нескольких ЭПК. Количество ЭПК для каждого типа ЭД определено в Заявлении. После подписания ЭД всеми необходимыми ЭПК в соответствии с Заявлением происходит автоматическая пересылка ЭД в Банк для исполнения.
- Просмотр, печать, сохранение в файл поступивших из Банка ЭД.
- Выход из Системы.

1.3. Процедура обработки ЭД сервером Системы происходит следующим образом:

- По окончании формирования ЭД Пользователи Системы проставляют ЭПК в количестве, определенном в Заявлении и отправляют ЭД в Банк.
- Сервер Банка получает ЭД и проверяет корректность всех имеющихся в нем ЭПК.
- Основанием для принятия Банком ЭД, переданного Клиентом по Системе, является наличие в количестве, установленном в соответствии с Заявлением, и корректность всех ЭПК в ЭД. При положительном результате проверки сервер Банка проставляет в документе отметку о времени приема ЭД и ЭП Банка (далее – ЭПБ), свидетельствующую о получении Банком ЭД, и сохраняет данный ЭД в Системе. При отрицательном результате проверки ЭПК ЭПБ в ЭД не проставляется, Клиент получает сообщение об ошибке средствами Системы. Ключи проверки электронной подписи Банка и копии соответствующих Сертификатов ключей размещаются на сервере системы https://www.bankline.ru. Сертификат Ключа проверки электронной подписи Банка подписывается только уполномоченным представителем Банка. Срок действия Комплекта ключей Банка составляет 5 лет.

1.4. Процедуры, описанные в п.1.3 настоящей Инструкции, представляют собой единый и неделимый на части процесс получения Банком ЭД, не могут быть выполнены в другой последовательности и рассматриваться независимо друг от друга.

1.5. Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл должен содержать ЭПК, отметку о времени приема документа Банком и ЭПБ. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.

1.6. Переданный Клиентом в Банк ЭД в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус ЭД изменяется Банком. Клиент имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в

том числе о времени его изменения) переданного в Банк ЭД. Сервер Банка присваивает полученным от Клиента ЭД следующие статусы:

- Рублевые платежные поручения:
  - “получен банком”;
  - “документ отправлен на исполнение”;
  - “в очереди у операциониста”/ “обработка успешно завершена …“;
  - “обработано без ошибок” или “обработано с ошибкой” с указанием причины, по которой документ отвергнут;
  - “включен в рейс для РКЦ”;
- Остальные типы документов:
  - “получен банком”;
  - “документ отправлен на исполнение”;
  - “в очереди у операциониста”/ “обработка успешно завершена …“;
  - “обработано без ошибок” или “обработано с ошибкой” с указанием причины, по которой документ отвергнут.

Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться присвоение Банком ЭД Клиента статуса “документ отправлен на исполнение”, а при работе в Депозитарном модуле Системы - получение Клиентом документа типа «Статус обработки распоряжения/запроса», в котором указано, что статус обработки соответствующего ЭД Клиента «Принято к исполнению».

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

Примечание: Перечень и описание статусов ЭД, присваиваемых сервером Банка в Депозитарном модуле Системы, приведены в руководстве пользователя Депозитарного модуля Системы.

1.7. При формировании ЭД для Клиента Банк проставляет в нем ЭПБ. ЭД считается переданным Банком Клиенту, если он подписан ЭПБ и выложен на сервер Банка, то есть имеется в списке входящих ЭД Клиента на сервере Банка. Клиент может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.

1.8. Банк фиксирует электронные архивы полученных от Клиента ЭД, содержащих ЭПК и ЭПБ, и доставленных Клиенту ЭД, содержащих ЭПБ, и хранит их способом, обеспечивающим Клиенту доступ к данным ЭД на сервере Банка.

1.9. Клиент с помощью программы проверки ЭП CryptoManager.exe, установленной на Персональном компьютере, имеет возможность в любой момент времени проверить ЭПБ и ЭПК любого файла архива. Вышеуказанная программа проверки ЭП позволяет выполнять проверку типов ЭП (раздел 3 настоящей Инструкции), разрешенных для использования в Системе.

1.10. Программу проверки ЭП CryptoManager.exe можно получить у фирмы-разработчика Системы – ЗАО “ИНИСТ” (Лицензия ФСБ России № 12818Н от 16.04.2013), зарегистрированной по адресу 115035, г. Москва, Космодамианская наб., д.40-42, стр.3.

2. Порядок получения, замены и хранения ключей

2.1. Для Комплектов ключей, сгенерированных для работы на Персональном компьютере:

2.1.1. Клиент, относящийся к корпоративному сегменту, может генерировать Комплекты ключей своих Пользователей Системы согласно Заявлению с помощью программных средств, предоставленных Банком, на USB-токенах с использованием своих технических средств.

2.1.2. Клиент, относящийся к сегменту предпринимателей, может генерировать Комплекты ключей своих Пользователей Системы согласно Заявлению с помощью программных средств, предоставленных Банком, на USB-токенах или иных носителях информации (жесткий диск, съемные носители (оптические диски, флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств.

2.1.3. Ключ проверки электронной подписи каждого Пользователя Системы регистрируется Банком на основании подписанного Сторонами Сертификата ключа.

2.1.4. Срок действия Комплекта ключей указывается в Сертификате ключа. Срок действия Комплекта ключей 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 трех лет. До истечения установленного срока Клиент обязан инициировать процедуру смены Комплектов ключей. По заявлению Клиента, направленному в Банк средствами Системы до окончания срока действия Комплекта ключей, его действие может быть продлено на срок не более 3 месяцев. По инициативе Клиента Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.

2.1.5. Оформленные со стороны Банка Сертификаты ключей Клиента вручаются лично представителю Клиента, курьеру Клиента, либо направляются Клиенту посредством почтовой связи. Сертификаты ключей должны храниться у каждой из Сторон не менее пяти лет после окончания их срока действия.

2.2. Для Комплекта ключей, сгенерированного посредством Мобильного приложения:

2.2.1 Пользователь вправе генерировать Комплект ключей для Мобильного приложения с помощью программных средств, предоставленных Банком, при наличии действующего Комплекта ключей, сгенерированного для работы на Персональном компьютере.

2.2.2 Срок действия Комплекта ключей указывается в Сертификате ключа. Срок действия Комплекта ключей, сгенерированного посредством Мобильного приложения, не может превышать срок действия Комплекта ключей Пользователя, сгенерированного для работы на Персональном компьютере. До истечения установленного срока Клиент обязан инициировать процедуру смены Комплектов ключей. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.

2.2.3 Статус ЭП Пользователя Системы, сгенерированной посредством Комплекта ключей для Мобильного приложения, соответствует Статус ЭП Пользователя Системы, указанному в Заявление, при генерации Комплекта ключей на USB-токенах.

2.3. Обязательная замена Комплекта ключей проводится в следующих случаях:

- истек срок действия Комплекта ключей;
- произошла Компрометация ключей.

2.4. В случае лишения Клиентом Пользователя Системы права подписывать ЭП ЭД соответствующие Комплекты ключей выводятся из действия на основании письменного заявления Клиента или ЭД свободного формата, отправленного средствами Системы.

3. Обеспечение безопасности процедуры обмена документами

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

3.1.1. Для Персонального компьютера:

- Средство криптографической защиты информации (СКЗИ) на базе Программного комплекса «Бикрипт 5.0.» (вариант исполнения 2), разработанного ООО Фирма «ИнфоКрипт» (сертификат соответствия ФСБ РФ СФ/114-3021 от 30 декабря 2016 года). Клиент, относящийся к сегменту предпринимателей, имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (жесткий диск, съемные носители (оптические диски, флеш-память, внешний винчестер) и т.п.). Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов.

- Использованием СКЗИ «Криптотокен ЭП 2» в составе USB-токенов JaCarta ГОСТ/JaCarta-2 ГОСТ, разработанных ЗАО «Алладин Р.Д.» (сертификат соответствия ФСБ России № СФ/124-3473 от 10.08.2018 г и № СФ/124 – 3502 от 11.09.2018 г.). 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 пароля.
- Шифрования данных в телекоммуникационных каналах с использованием СКЗИ КриптоПро CSP версии 4.0 и выше. Для защиты данных от несанкционированного доступа в

телекоммуникационных каналах используется протокол Transport Layer Security (TLS v. 1.2, RFC 2246 и выше[1]).

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

3.1.2. Для Мобильного приложения:

- Средства криптографической защиты информации с использованием алгоритма RSA для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v.1.2, RFC 2246), применяются криптографические международные алгоритмы шифрования RSA (3072 bit), обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с SHA 512.
- Симметричное шифрование AES с длиной ключа 256 bit., генерация и хранение Ключа электронной подписи, а также подписание ЭД производится во внутренней защищенной памяти Мобильного устройства. Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации, предназначенных для генерации и хранения ключа ЭП, за исключением USB-токенов.

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

3.2.1. Для работы на Персональном компьютере:

- Организовать выделенный компьютер подсистемы «Клиент», предназначенный исключительно для работы с Банком;
- Генерацию и хранение ключевой информации, а также подписание документов производить с использованием USB-токенов JaCarta ГОСТ/JaCarta -2 ГОСТ;
- В случае генерации Клиентом, относящимся к сегменту предпринимателей, Ключей электронной подписи своих Пользователей на носители, отличные от USB-токенов, осуществлять эксплуатацию рабочего места и обеспечение его безопасности организационными и техническими мерами в соответствии с требованиями эксплуатационной документацией для СКЗИ «Бикрипт 5.0» для класса КС1: «Средство криптографической защиты информации «Бикрипт 5.0». Правила пользования» (ИНФК.11485466.4012.027.31). Данный документ размещен на официальном сайте Банка в сети Интернет по адресу http://www.rosbank.ru.
- Ввести ограничение сетевого взаимодействия компьютера подсистемы «Клиент» только с необходимым доверенным перечнем IP-адресов;
- Проверять, что установлено защищенное TLS-соединение с официальным ресурсом сервиса https://www.bankline.ru
- Средствами подсистемы «Клиент» закрепить за Пользователями Системы IP-адрес/список IP-адресов компьютеров подсистемы «Клиент» в целях обеспечения контроля на стороне Банка;
- Обеспечить на выделенном компьютере наличие средств защиты от вредоносного программного обеспечения, их работоспособность и регулярное обновление;
- Исключить на выделенном компьютере открытие писем с вложениями, полученными от неизвестных или недоверенных источников;
-
- Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;
- Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;
- Исключить использование средств удаленного администрирования;
- Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана;

[1] Рекомендуется использовать версию TLS v.1.2.

- 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.);
- Контролировать соблюдение требований безопасности.

3.2.2. Для работы с Мобильным устройством:

- Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;
- Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;
- Исключить использование средств удаленного администрирования;
- Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты);
- Контролировать соблюдение требований безопасности;
- Обеспечить наличие антивирусного программного обеспечения.

3.3. Пользователи Системы, уполномоченные использовать Систему Клиентами, относящимися к сегменту предпринимателей, должны в Системе ввести номер телефона сотовой связи для получения на указанный номер информационных сообщений в соответствии с Договором.

3.4. Клиент обязан:

- Исключить появление на Персональном компьютере или Мобильном устройстве подсистемы “Клиент” 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;
- Исключить возможность несанкционированных Банком изменений в технических и программных средствах Клиента, определенных в Списке;
- Исключить возможность Компрометации ключей в процессе их транспортировки, эксплуатации и хранения.

3.5. Стороны обязаны:

- обеспечивать конфиденциальность Ключей электронных подписей, в частности не допускать использование принадлежащих им Ключей электронных подписей без их согласия;
- уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- 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 Персональном компьютере и/или Мобильном устройстве Пользователя Системы вирусов или других программ деструктивного действия. Блокировка Ключа электронной подписи. Пользователя Системы снимается Банком по факту получения от Клиента подтверждения об удалении с Персонального компьютера и/или Мобильного устройства Пользователя Системы вирусов или других программ деструктивного действия.

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

Если произошла Компрометация ключей любого Пользователя Клиента, последний обязан:

- В случае доступности Комплекта ключей (подозрение на несанкционированное копирование) немедленно послать в Банк ЭД “Блокировка ключа”. При этом Система автоматически заблокирует возможность использования данного Комплекта ключей Пользователя Системы;

- В случае недоступности (утрата, хищение и т.п.) Комплекта ключей сообщить Администратору Системы по телефону (телефон и электронный адрес Администратора системы указаны на сайте www.bankline.ru, а также в Заявлении, используя для авторизации кодовую фразу, приведенную в Сертификате ключа, о факте Компрометации ключей;
- В случае утраты Пользователем Системы кодовой фразы 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 предоставления необъективной 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;
- В срок не более 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 Комплекта ключей;
- В случае принятия решения о замене Комплекта ключей, сгенерированного для Персонального компьютера, сгенерировать новый Комплект ключей самостоятельно и направить своего представителя в Банк для его регистрации. В случае принятия решения о замене Комплекта ключей, сгенерированного посредством Мобильного приложения, сгенерировать новый Комплект ключей самостоятельно в соответствии с Инструкцией.

Если произошла Компрометация ключей Банка, последний обязан:

- 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;
- Произвести внеплановую смену Комплекта ключей Банка, опубликовать новый Ключ проверки электронной подписи и копию Сертификата ключа Банка, содержащего новый Ключ проверки электронной подписи Банка, на сервере Системы.

3.8. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного по кодовой фразе Клиента Банк немедленно приостанавливает использование Системы данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде.

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 предоставленную фирмой-разработчиком ЗАО “ИНИСТ” программу проверки ЭП, указанную в п.1.10 настоящей Инструкции

4.4.1. Сторона, отстаивающая подлинность спорного ЭД, обязана предоставить спорный ЭД, действовавшие в момент создания спорного ЭД Сертификаты ключей Стороны, подписавшей спорный ЭД, Банк обязан предоставить сами Ключи проверки электронной подписи, 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 ключей, 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 проверки ЭП, указанной в п.1.10 настоящей Инструкции, и каждого Ключа проверки электронной подписи, 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 Ключи проверки электронной подписи, 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 Ключи проверки электронной подписи, содержащиеся в Сертификатах ключей, с соответствующими Ключами проверки электронной подписи, 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 Ключи проверки электронной подписи действующими на момент выработки ЭП спорного ЭД, и внести запись об этом в Протокол (данная запись заверяется подписями членов Согласительной комиссии). Ключ проверки электронной подписи признается действующим на момент создания ЭП спорного ЭД в случае, если дата создания спорного ЭД приходится на период действия Ключа проверки электронной подписи. В противном случае Ключ проверки электронной подписи признается недействующим на момент создания ЭП.

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

- Ключи проверки электронной подписи в Сертификатах ключей и в Протоколе совпадают,
- Все результаты проверки ЭП в Протоколе положительны,
- Согласительная комиссия признала все Ключи проверки электронной подписи, содержащиеся в Протоколе, действующими на момент выработки ЭП.

В противном случае Согласительная комиссия признает ЭД недействительным.