

Договор об использовании автоматизированной системы «iBank» при осуществлении расчетно-кассового обслуживания Клиентов ПАО КБ «РусьРегионБанк»

СТАТУС ДОГОВОРА

Настоящий договор об использовании автоматизированной системы «iBank» при осуществлении расчетно-кассового обслуживания Клиентов ПАО КБ «РусьРегионБанк» (далее - Договор), является Договором присоединения, регулирующим отношения по обслуживанию по системе «iBank» Клиентов - юридических лиц, индивидуальных предпринимателей, адвокатов и нотариусов в Публичном Акционерном Обществе Коммерческий Банк «Русский Региональный Банк», сокращенное наименование - ПАО КБ «РусьРегионБанк» (далее – Банк).

Опубликование Договора, включая распространение его текста и приложений к нему в сети Интернет на официальном сайте Банка <https://www.rrb.ru/>, необходимо рассматривать как публичное предложение (оферта) Банка, адресованное юридическим лицам, индивидуальным предпринимателям, адвокатам и нотариусам заключить Договор на предлагаемых условиях в соответствии со ст. 428 Гражданского Кодекса Российской Федерации.

Заключение Договора производится путем присоединения к его условиям в следующем порядке: Клиенты представляют в Банк подписанное со своей стороны Заявление о подключении к системе «iBank» (Приложение № 1 к настоящему Договору).

1. ПРЕДМЕТ ДОГОВОРА

1.1. Предметом настоящего Договора является предоставление Банком Клиенту возможности осуществления платежей со всех своих счетов, открытых в Банке, а также получение иных услуг в соответствии с настоящим Договором посредством дистанционного банковского обслуживания (именуемого далее «iBank»).

1.2. Настоящий Договор является неотъемлемой частью всех договоров банковского счета, заключенных между Сторонами как на момент подписания настоящего Договора, так и заключенных в будущем.

2. ТЕРМИНЫ, ПРИМЕНЯЕМЫЕ В ДОГОВОРЕ И ПРИ ПОЛЬЗОВАНИИ СИСТЕМЫ «iBank»

2.1. Система «iBank» – совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, с целью предоставления Клиенту услуг по настоящему Договору.

2.2. «**Электронный документ**» – совокупность байт, содержащая платежное поручение или информационное сообщение Клиента.

2.3. «**Электронная подпись**» (ЭП) – совокупность байт, формируемая Клиентом, однозначно сопоставляемая электронному документу и используемая для аутентификации (подтверждение авторства и целостности) электронного документа.

При обеспечении функционирования системы «iBank» в соответствии с настоящим Договором используются следующие виды электронных подписей:

- усиленная квалифицированная электронная подпись;
- усиленная неквалифицированная электронная подпись;
- неквалифицированная электронная подпись с имитозащитой.

Термины усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись используются в значении, установленном Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

2.4. «**Секретный ключ ЭП Клиента**» – ключ (последовательность байт), самостоятельно генерируемый Клиентом с использованием средств системы «iBank» и предназначенный для формирования Клиентом электронной подписи электронных документов.

2.5. «**Открытый ключ ЭП Клиента**» – ключ (последовательность байт), зависящий от секретного ключа ЭП Клиента, самостоятельно генерируемый Клиентом с использованием средств системы «iBank» и предназначенный для проверки Банком корректности электронной подписи электронного документа, сформированного Клиентом.

2.6. **«Корректная электронная подпись Клиента»** – электронная подпись электронного документа Клиента, дающая положительный результат ее проверки с открытым ключом ЭП Клиента.

2.7. **«Сертификат открытого ключа ЭП Клиента»** – бумажный документ, с представленным в шестнадцатеричном виде открытым ключом ЭП Клиента, датой начала и окончания действия открытого ключа ЭП Клиента, заверенный подписью руководителя и имеющий оттиск печати Клиента.

2.8. **«Активный открытый ключ ЭП Клиента»** – открытый ключ ЭП Клиента, зарегистрированный Банком в системе «iBank», и используемый Клиентом в текущее время для работы в системе «iBank».

2.9. **«Пара ключей ЭП Клиента»** – секретный ключ ЭП Клиента и соответствующий ему открытый ключ ЭП Клиента.

2.10 **MAC-токен BIFIT; Рутокен ЭП 3.0, Рутокен ЭП 3.0 3120, Рутокен ЭП 3.0 3220; MS_KEY K - АНГАРА Исп.8.1.1** - персональный аппаратный криптопровайдер с неизвлекаемыми секретными ключами ЭП и формирующий ЭП под электронным документом непосредственно внутри USB-устройства.

2.11. **«Компрометация ключа ЭП Клиента»** - утрата доверия к тому, что используемый ключ шифрования обеспечивает безопасность конфиденциальной информации.

К событиям, связанным с компрометацией действующих криптографических ключей, относятся следующие:

- * утрата ключевых носителей (USB-токен MAC-токен BIFIT; Рутокен ЭП 3.0, Рутокен ЭП 3.0 3120, Рутокен ЭП 3.0 3220; MS_KEY K - АНГАРА Исп.8.1.1);

- * утрата (в том числе хищение) ключевых носителей (USB-токен MAC-токен BIFIT; Рутокен ЭП 3.0, Рутокен ЭП 3.0 3120, Рутокен ЭП 3.0 3220; MS_KEY K - АНГАРА Исп.8.1.1) с последующим их обнаружением;

- * увольнение сотрудников, имевших доступ к ключевой информации;

- * передача ключевой информации по линии связи в открытом виде (если это не предусмотрено правилами пользования);

- * нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;

- * возникновение подозрений на утечку информации или ее искажение;

- * не расшифровывание входящих или исходящих сообщений Пользователей (Клиентов);

- * отрицательный результат при проверке электронной подписи документа;

- * нарушение целостности упаковки ключевых носителей и (или) печати на сейфе, где хранились ключевые носители;

- * несанкционированное копирование ключевых носителей;

- * случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате злоумышленных действий).

Первые пять событий должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

2.12. **«Абонентский пункт системы»** – техническое оборудование, предназначенное для эксплуатации Клиентом системы «iBank».

3. ОСНОВНЫЕ ПОЛОЖЕНИЯ

3.1. Банк осуществляет подключение аппаратно-программных средств Абонентского пункта Клиента к системе электронного документооборота Банка и обслуживание Клиента с использованием системы «iBank» в соответствии с договорами банковского счета, заключенными Сторонами.

3.2. Банк осуществляет операции по счетам на основании принятых по системе «iBank» расчетно-платежных документов, подписанных ключами шифрования и электронными подписями (далее ЭП) соответствующих должностных лиц Клиента. Ключи шифрования и ЭП прекращают действие на основании заявления Клиента с момента его получения Банком.

3.3. Стороны признают метод шифрования информации и ЭП используемые при передаче документов между Банком и Клиентом. При замене лиц, имеющих право подписи, ключи шифрования подлежат замене.

3.4. Для защищенного хранения секретных ключей ЭП Клиента в обязательном порядке используется USB-токен MAC-токен BIFIT; Рутокен ЭП 3.0, Рутокен ЭП 3.0 3120, Рутокен ЭП 3.0 3220; MS_KEY K - АНГАРА Исп.8.1.1.

USB-токен MAC-токен BIFIT; Рутокен ЭП 3.0, Рутокен ЭП 3.0 3120, Рутокен ЭП 3.0 3220; MS_KEY K - АНГАРА Исп.8.1.1 Банк передает, а Клиент обязуется принять на основании акта и оплатить в соответствии с действующими тарифами Банка.

3.5. К использованию в системе «iBank» допустимы следующие документы:

3.5.1 от Клиента:

- а) рублевые документы;
- б) валютные документы;
- в) текстовые и иные сообщения по установленной Банком форме.

3.5.2 от Банка:

- а) выписки по счету за период до предыдущего рабочего дня включительно;
- б) остаток по счету на дату до предыдущего рабочего дня включительно;
- в) сведения о доставке документов Клиента в Банк;
- г) результаты обработки документов Клиента в Банке;
- д) произвольные документы (обновления системы, обновления справочников, текстовые сообщения).

3.6. Стороны признают, что получение указанных в п. 3.5 Договора документов, заверенных ЭП Клиента, юридически эквивалентно получению документов на бумажном носителе, подписанных лицом (лицами), уполномоченными распоряжаться денежными средствами, находящимися на счете Клиента, и скрепленных печатью Клиента.

Подлинность электронной подписи подлежит обязательной проверке согласно требованиям Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» и иным нормативно-правовым актам.

3.7. Стороны признают, что контрольные архивы документов, создаваемые системой «iBank» в Банке, являются доказательным материалом для решения спорных вопросов.

4. ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ И ПРАВИЛА ЭКСПЛУАТАЦИИ СИСТЕМЫ «iBank»

4.1. Для работы с сервисом пользователю необходимы:

- Современный компьютер с операционной системой (ОС).

Работа с сервисом возможна на следующих ОС:

- Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
- Apple Mac OS X: 10.12 и выше;
- Ubuntu и прочие deb-дистрибутивы (последние версии x64);
- Монитор с разрешением не менее 1280x1024.

● Web-браузер с поддержкой BIFIT Signer для использования электронной подписи с применением аппаратных устройств. Поддержка BIFIT Signer обеспечена в браузерах: Microsoft Edge; Google Chrome; Яндекс.Браузер; Firefox; Opera; Safari (при условии, что браузер используется совместно с Mac OS X).

● Персональное аппаратное USB-устройство с возможностью использования цифровой ЭП или съемный USB-накопитель (при использовании файловых ключей).

Аппаратное устройство (аппаратный криптопровайдер) предназначено для генерации ключей ЭП внутри самого устройства и обеспечения их защищенного неизвлекаемого хранения. Формирование ЭП под электронным документом происходит внутри самого устройства.

Сервис поддерживает работу с такими аппаратными устройствами (токенами), которые имеют действующий сертификат соответствия ФСБ на встроенное СКЗИ:

- MAC-токен BIFIT;
- Рутокен ЭП 3.0, Рутокен ЭП 3.0 3120, Рутокен ЭП 3.0 3220;
- MS_KEY K - АНГАРА Исп.8.1.1.

5. РЕЖИМ ОБСЛУЖИВАНИЯ КЛИЕНТОВ

5.1. Система «iBank» доступна для формирования документов круглосуточно. При невозможности передачи информации в Банк с использованием системы «iBank», документы могут поступить от Клиента в виде подлинника на бумажном носителе.

5.2. Для дополнительной аутентификации Клиента и в целях защиты от несанкционированного проведения операций в системе «iBank» Банк предоставляет возможность использования системы одноразовых паролей.

Система одноразовых паролей используется, если это предусмотрено Заявлением о подключении к системе «iBank».

5.3. Одноразовые пароли используются:

- при первичном входе в систему;
- при совершении Клиентом расходных операций с использованием системы «iBank».

5.4. Одноразовый пароль направляется Клиенту Банком способом и на условиях, установленных в Заявлении о подключении к системе «iBank».

5.5. Банк осуществляет контроль аутентичности (подтверждения подлинности) одноразового пароля. В случае отрицательного результата проверки аутентичности одноразового пароля Банк отказывает в доступе к системе «iBank», либо в исполнении электронного документа.

5.6. Документы, поступившие от Клиента в Банк по системе «iBank», на списание денежных средств, полученные до 16 часов текущего рабочего дня, а в пятницу до 15 часов, Банк принимает к исполнению в тот же день; документы, поступившие позже указанного времени - на следующий рабочий день. Выписки по Счетам Клиента за текущий рабочий день формируются к 10:00 часам следующего рабочего дня. Для получения вышеуказанных документов Клиент должен осуществить сеанс связи с Банком, используя систему «iBank», в соответствии с «Инструкцией по работе с системой «iBank» (Приложение № 2 к настоящему Договору).

5.7. Клиент поручает Банку дальнейшее оформление платежных документов, переданных Клиентом в Банк по системе «iBank».

5.8. Банк не несет ответственности за задержку в формировании выписки по Счетам Клиента, если она связана с неполучением Банком информации о проведенных операциях по его корреспондентскому счету от Межрегионального Центра Информатизации при Банке России, обеспечивающего взаиморасчеты между банками.

5.9. Клиент вправе установить ограничения по параметрам операций по осуществлению переводов денежных средств с использованием системы «iBank». Клиентом могут быть установлены следующие ограничения:

- на максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени;
- на перечень возможных получателей денежных средств;
- на временной период, в который могут быть совершены переводы денежных средств;
- на географическое местоположение устройств, с использованием которых может осуществляться подготовка и (или) подтверждение клиентом электронных сообщений;
- на перечень идентификаторов устройств, с использованием которых может осуществляться подготовка и (или) подтверждение клиентом электронных сообщений;
- на перечень предоставляемых услуг, связанных с осуществлением переводов денежных средств;
- иные ограничения, если такая возможность будет установлена нормативно-правовыми актами.

Банк может применить иные ограничения по параметрам операций по осуществлению переводов денежных средств в случаях, когда такая возможность допускается нормативными актами Банка России.

Для установления ограничений Клиент направляет в Банк заявление по установленной Банком форме (Приложение № 3 к настоящему Договору). Клиент вправе изменить/отменить установленные в соответствии с настоящим пунктом ограничения, направив в Банк заявление по установленной Банком форме (Приложение № 4 к настоящему Договору).

6. ПОРЯДОК ОПЛАТЫ

6.1. Банк осуществляет обслуживание Клиента по системе «iBank» в соответствии с действующими в Банке «Тарифами комиссионного вознаграждения» (далее – Тарифы), размещенными в сети Интернет на официальном сайте Банка <https://www.rrb.ru/>. Банк имеет право, а Клиент выражает согласие на списание со своих счетов в Банке без дополнительных распоряжений и без акцепта соответствующих сумм. Списание производится ежемесячно, в течении последних трех банковских дней текущего месяца, при условии использования системы «iBank» Клиентом в этом месяце.

6.2 Началом оказания услуг считается дата принятия Банком от Клиента Сертификата открытого ключа ЭП Клиента, при этом оплата производится за полный календарный месяц, в котором получен Сертификат.

6.3. В случае расторжения Договора до окончания текущего расчетного месяца, оплата производится за весь месяц.

6.4. Банк оставляет за собой право изменения Тарифов за обслуживания по системе «iBank» в одностороннем порядке, о чем уведомляет Клиента путем размещения информации на доске объявлений или в сети Интернет на официальном сайте Банка <https://www.rrb.ru/>.

7. ПРАВА И ОБЯЗАННОСТИ СТОРОН ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ «iBank»

7.1. Клиент обязан:

7.1.1. Самостоятельно и за свой счет провести работы по созданию условий, необходимых для установки системы «iBank», в том числе по согласованию с Банком:

- приобрести или выделить необходимую для установки системы «iBank» вычислительную технику;

- приобрести USB-токен MAC-токен BIFIT; Рутокен ЭП 3.0, Рутокен ЭП 3.0 3120, Рутокен ЭП 3.0 3220; MS_KEY K - АНГАРА Исп.8.1.1;

- приобрести аппаратно-программный комплекс для защиты технических средств СИСТЕМЫ от несанкционированного доступа;

- определить потребность в каналах связи и обеспечить их подключение.

7.1.2. Заполнять документы в соответствии с действующими нормативными актами, регулирующими безналичные расчеты в Российской Федерации и Инструкции по работе с системой «iBank».

7.1.3. Предоставлять права доступа к системе «iBank» только лицам, уполномоченным распоряжаться денежными средствами, находящимися на счете Клиента, в соответствии с банковской карточкой Клиента, предоставленной в Банк. Не допускать к автоматизированной банковской системе лиц, не имеющих права на распоряжение банковским счетом (не включенных в банковскую карточку).

7.1.4. Оплачивать услуги согласно Тарифам Банка.

7.1.5. Выполнять требования соглашений, руководящих документов и эксплуатационной документации, необходимых для функционирования в системе «iBank».

7.1.6. Незамедлительно информировать Банк по телефону о всех случаях утраты и (или) компрометации ключа ЭП Клиента (или подозрения на компрометацию) и представлять Банку в течение 1 (одних) суток официальное письменное уведомление о случившемся.

7.1.7. В случае утраты и (или) компрометации (или подозрения на компрометацию) ключа ЭП Клиента немедленно отключать свой Абонентский пункт от системы «iBank» и приостановить все банковские операции по своим счетам с использованием электронной системы расчетов.

7.1.8. Обеспечивать сохранность, подлинность и конфиденциальность коммерческой и иной информации, которая станет известной Клиенту вследствие выполнения им своих обязательств по настоящему Договору.

7.1.9. Обеспечивать сохранность и конфиденциальность полученного от Банка программного обеспечения Абонентского пункта, включая программное обеспечение средств криптографической защиты информации, индивидуальных криптографических ключей шифрования и ЭЦП.

7.1.10. Не передавать ни при каких обстоятельствах третьим лицам полученное от Банка программное обеспечение Абонентского пункта, включая программное обеспечение средств криптографической защиты информации, а также USB-токен MAC-токен BIFIT; Рутокен ЭП 3.0, Рутокен ЭП 3.0 3120, Рутокен ЭП 3.0 3220; MS_KEY K - АНГАРА Исп.8.1.1.

7.1.11. В течение 1 (одного) банковского дня письменно сообщать Банку о происшедших изменениях, связанных с полномочиями должностных лиц по распоряжению счетом, в 3-х дневный срок с момента получения предоставлять документы, подтверждающие произошедшие изменения статуса или внесение изменений и дополнений в учредительные и иные документы, не предоставление которых может оказать негативное воздействие на проведение банковских операций.

7.1.12. В случае наступления изменений, связанных с полномочиями должностных лиц по распоряжению счетом, Клиент обязан предоставить Банку «Уведомление об отмене действия секретного и соответствующего ему открытого ключей ЭП Клиента» (Приложение № 5 к настоящему Договору) и новый сертификат открытого ключа ЭП Клиента в системе «iBank».

7.1.13. По требованию Банка генерировать новую пару ключей ЭП Клиента и зарегистрировать новый открытый ключ ЭП Клиента в Банке.

7.1.14. В случае блокирования или удаления открытого ключа ЭП Клиента, Клиент обязан предоставить Банку «Уведомление об отмене действия секретного и соответствующего ему открытого ключей ЭП Клиента».

7.1.15. При уведомлении Банком о смене программного обеспечения осуществить все необходимые действия для своевременного получения и установки новой версии системы «iBank».

7.1.16. Предоставлять Банку достоверную информацию для связи и направления уведомлений, установленных п. 7.3.11 настоящего Договора, а в случае ее изменения, не позднее одного дня предоставлять обновленную информацию. Обязанность Банка по направлению Клиенту уведомлений, предусмотренных пунктом 7.3.11 настоящего Договора, считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи с Клиентом.

7.1.17. До осуществления перевода денежных средств с использованием системы «iBank» ознакомиться с правилами проведения Банком расчетно-кассовых операций, установленных ЦБ РФ и разработанных на их основе внутренними Банковскими правилами (Приложение № 6 к настоящему Договору) и «Тарифами комиссионного вознаграждения» Банка, реквизитами и корреспондентскими счетами Банка, размещенными в операционном зале Банка и в сети Интернет на официальном сайте Банка <https://www.rrb.ru/>.

7.2. Клиент имеет право:

7.2.1. Запросить у Банка предоставления бумажной копии платежных документов, переданных по системе «iBank» и принятых Банком, с исполнением в день проведения операций Банком по вышеуказанным платежным документам.

7.2.2. Клиент имеет право приостановить или досрочно прекратить действие своего активного открытого ключа ЭП и потребовать от Банка заблокировать этот активный открытый ключ ЭП Клиента, посредством направления в Банк уведомления по форме Приложения № 5 к настоящему Договору любым доступным способом: по факсу, по системе Банк-Клиент, по электронной почте, нарочно.

7.2.3. Клиент имеет право по своему усмотрению генерировать новые пары ключей ЭП Клиента и регистрировать в Банке новые открытые ключи ЭП Клиента.

7.2.4. До 5-го числа месяца, следующего за отчетным, получить в Банке сводный реестр проведенных платежей по счетам Клиента за прошедший месяц.

7.2.5. Не позднее 10-го числа месяца, следующего за отчетным, вернуть Банку реестр платежей (п. 7.2.4), подписанный лицом (лицами), уполномоченными распоряжаться денежными средствами, находящимися на счете Клиента. Заверяется подписями и печатью Клиента каждый лист реестра. Если в указанные сроки Клиент не предоставил в Банк заверенный вышеуказанным способом сводный реестр платежей, то все платежи данного реестра считаются подтвержденными Клиентом.

7.3. Банк обязан:

7.3.1. Произвести комплекс работ, связанных с первоначальной установкой Клиенту системы «iBank».

7.3.2. Предоставить Клиенту комплект руководящих документов и эксплуатационной документации, необходимых для функционирования в системе «iBank».

7.3.3. Обеспечивать сохранность, подлинность и конфиденциальность открытых ключей ЭП Клиента, а также иной конфиденциальной и коммерческой информации Клиента, которая станет известной Банку вследствие выполнения им своих обязательств по настоящему Договору.

7.3.4. Принимать к исполнению только те платежные документы, которые оформлены в соответствии с п. 7.1.2, надлежащим образом зашифрованы ключами шифрования, подписаны ЭП и признаны подлинными программой контроля ЭП. В случае отбраковки документа программой контроля ключей шифрования или программой контроля ЭП, документ Банком к исполнению не принимается, о чем Клиент получает извещение с указанием причины.

7.3.5. Осуществлять техническое сопровождение и оказать необходимую консультационную помощь по техническим вопросам эксплуатации системы «iBank».

7.3.6. По требованию Клиента заблокировать в системе «iBank» существующий активный открытый ключ ЭП Клиента и зарегистрировать новый открытый ключ ЭП Клиента.

7.3.7. Информировать Клиента о всех случаях компрометации ключей ЭП Клиента, обеспечивать локализацию последствий и восстановление конфиденциальной связи.

7.3.8. Обеспечивать отключение Клиента, чьи ключи ЭП подверглись компрометации, и приостанавливать банковские операции по их счетам и (или) платежным поручениям.

7.3.9. Обеспечивать возобновление конфиденциального документооборота и электронных расчетов в системе «iBank» после генерации Клиентом новой пары ключей ЭП и регистрации нового открытого ключа ЭП Клиента в Банке.

7.3.10. Организовывать проведение расследования обстоятельств компрометации индивидуальных секретных ключей шифрования и ЭП.

7.3.11. Информировать Клиента о совершении каждой операции с использованием электронного средства платежа путем направления клиенту соответствующего уведомления в системе «iBank».

7.3.12. Банк обязан предоставлять Клиенту бумажные копии платежных документов, переданных по системе «iBank» и принятых Банком, и информацию по вышеуказанным платежным документам, которые связаны с использованием системы «iBank», в течение одного дня после обращения Клиента.

7.3.13. Информировать Клиента об изменениях правил проведения расчетно-кассовых операций, устанавливаемых Банком России и разработанных на их основе внутренних правил и «Тарифов комиссионного вознаграждения Банка», реквизитов и корреспондентских счетов Банка, посредством размещения информации в доступном для обозрения Клиента месте в операционном(ых) зале(ах) Банка и в сети Интернет на официальном сайте Банка <https://www.rrb.ru/>.

7.4. Банк имеет право:

7.4.1. Банк имеет право по своему усмотрению без уведомления Клиента блокировать активный открытый ключ ЭП Клиента и потребовать от Клиента смены пары ключей ЭП Клиента.

7.4.2. Банк имеет право без объяснения причин затребовать от Клиента оформления документа на бумажном носителе (подлинника) с подписью уполномоченных лиц и оттиском печати Клиента, в соответствии с карточкой с образцами подписей и оттиска печати Клиента и не производить полученного по системе «iBank» исполнения электронного документа, сообщив об этом Клиенту. В случае если Клиент не предоставит в день требования Банком оформленный документ на бумажном носителе (подлинник) Банк вправе не исполнять соответствующий электронный документ.

7.4.3. Изменять «Тарифы кассового обслуживания Банка» на обслуживание в системе «iBank» согласно п. 6.4 настоящего Договора.

7.4.4. Приостановить или прекратить использование Клиентом системы «iBank» при нарушении Клиентом порядка использования системы «iBank», установленного настоящим Договором. Приостановление или прекращение использования Клиентом системы «iBank» не прекращает обязательств Клиента и Банка по переводу денежных средств, возникших до момента приостановления или прекращения указанного использования.

7.4.5. Банк имеет право отказать в приеме платежного поручения по тем же причинам, по которым возможен возврат документов на бумажном носителе. Причина отказа обязательно должна быть занесена в поле «возврат» электронного платежного документа.

8. СОВМЕСТНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН.

8.1. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования неуполномоченными на то лицами секретного ключа ЭП Клиента. Банк не несет ответственности за несанкционированный доступ к электронной системе «iBank» совершенный через компьютер Клиента. Банк не несет ответственности в случае неисполнения Клиентом положений п. 7.1 настоящего Договора.

8.2. При невозможности использования системы «iBank» Стороны обязаны в течение 24 часов связаться друг с другом любыми доступными способами, осуществить обмен платежными документами и принять меры к восстановлению компьютерной связи.

8.3. В случае возникновения конфликтных ситуаций между Клиентом и Банком при использовании электронной системы «iBank» Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций» (Приложение № 6), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации.

8.4. Стороны обязуются принять все организационные меры для обеспечения безопасности носителей ключей шифрования и ЭП, баз данных документов и контрольных архивов для исключения несанкционированного доступа к информации. При возникновении угрозы

несанкционированного доступа к системе Стороны обязуются немедленно прекратить использование ключей шифрования и ЭП и в течение 24 часов связаться друг с другом для выяснения обстоятельств происшедшего.

8.5. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием электронной системы «iBank», предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной стороны, участвующей в настоящем Договоре.

8.6. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по настоящему Договору обязательств в случае возникновения обстоятельств непреодолимой силы, к которым относятся: стихийные бедствия, пожары, аварии, отключения электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, актов органов федеральных или местных органов власти и обязательных для исполнения одной из сторон, прямо или косвенно запрещающих указанные в Договоре виды деятельности или препятствующие выполнению сторонами своих обязательств по Договору, если сторона, пострадавшая от их влияния, доведет до сведения другой стороны известие о случившемся в возможно короткий срок после возникновения этих обстоятельств с предоставлением подтверждающих документов, выданных уполномоченными органами. При этом срок исполнения обязательств по договору отодвигается соразмерно времени, в течение которого будут действовать такие обстоятельства или их последствия.

9. СРОК ДЕЙСТВИЯ ДОГОВОРА

9.1. Настоящий Договор вступает в силу с момента его подписания обеими Сторонами и сохраняет силу на период действия договоров банковского счета.

9.2. Стороны вправе расторгнуть Договор в одностороннем порядке по истечении 15 дней после письменного уведомления об этом противоположной Стороны.

10. ПРОЧИЕ УСЛОВИЯ

10.1. Споры по настоящему Договору разрешаются путем переговоров с учетом взаимных интересов Сторон в порядке, предусмотренном Приложением № 6, а при недостижении соглашения - в соответствии с действующим законодательством в арбитражном суде г. Москвы.

10.2. При осуществлении электронных платежей стороны руководствуются действующим законодательством, правилами и техническими требованиями, установленными в Положении о безналичных расчетах в РФ, а также в настоящем Договоре.

10.3. Все Приложения, изменения, дополнения и особые условия к настоящему Договору оформляются в письменном виде, подписываются уполномоченными лицами и являются неотъемлемой его частью.

10.4. Настоящий Договор составлен в двух экземплярах по одному для каждой Стороны, причем оба экземпляра имеют одинаковую юридическую силу.

5. Перечень идентификаторов устройств, с использованием которых может осуществляться формирование (подготовка) и (или) подтверждение клиентом оператора по переводу денежных средств электронных сообщений

6. Перечень предоставляемых услуг, связанных с осуществлением переводов денежных средств

7. Иные
ограничения

(наименование должности)

_____ /
(подпись)

_____ /
(Ф.И.О.)

(дата)

М.П.

<i>Отметки Банка о принятии Заявления</i>			
Должность сотрудника Банка	Подпись сотрудника Банка	Ф.И.О. сотрудника Банка	Дата принятия Заявления Банком
<i>Отметки Банка об акцепте Заявления</i>			
Должность сотрудника Банка	Подпись сотрудника Банка	Ф.И.О. сотрудника Банка	Дата акцепта

М.П.

<i>Отметки Банка о принятии Заявления</i>			
Должность сотрудника Банка	Подпись сотрудника Банка	Ф.И.О. сотрудника Банка	Дата принятия Заявления Банком
<i>Отметки Банка об акцепте Заявления</i>			
Должность сотрудника Банка	Подпись сотрудника Банка	Ф.И.О. сотрудника Банка	Дата акцепта

М.П.

УВЕДОМЛЕНИЕ

об отмене действия секретного и соответствующего ему открытого ключей
ЭП Клиента

Клиент уведомляет Банк о том, что с «____» _____ 20__ г. считать
недействительным открытый ключ ЭП Клиента, со следующим идентификатором
открытого ключа ЭП Клиента _____

Соответствующий ему секретный ключ ЭП Клиента утрачивает силу для
дальнейшего применения с вышеуказанной даты.

ПОДПИСИ СТОРОН:

БАНК:

КЛИЕНТ:

_____ (_____)

_____ (_____)

М. П.

М. П.

ПОЛОЖЕНИЕ
о порядке проведения технической экспертизы
при возникновении спорных ситуаций

1. В настоящем Положении под спорной ситуацией понимается существование претензий у **Клиента** к **Банку** по обслуживанию через систему «iBank», справедливость которых может быть однозначно установлена по результату проверки ЭП **Клиента** под электронным документом.
2. **Клиент** представляет в **Банк** заявление, содержащее существо претензии с указанием на документ с ЭЦП, на основании которого **Банк** выполнил или не выполнил операции по счету **Клиента**.
3. **Банк** обязан в течение не более пяти дней от даты подачи заявления **Клиента** сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включается равное количество представителей **Клиента** и представителей **Банка**. По соглашению сторон в состав комиссии могут быть включены другие независимые эксперты. При невозможности согласованного выбора других независимых экспертов, комиссия приступает к работе без их участия.
4. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение стороны, несущей ответственность согласно выводу об истинности ЭП **Клиента** под приложенным документом.
5. Разрешительная комиссия в течение не более пяти дней проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:
 - 5.1. Разрешительная комиссия проводит техническую экспертизу электронного документа, заверенного ЭП **Клиента**, на основании которого **Банком** выполнены оспариваемые **Клиентом** действия с его счетом.
 - 5.2. Разрешительная комиссия проводит техническую экспертизу открытого ключа ЭП **Клиента**, период действия и статус открытого ключа ЭП **Клиента**, и установление его принадлежности **Клиенту**.
 - 5.3. Разрешительная комиссия проводит техническую экспертизу корректности ЭП **Клиента** в электронном документе.
 - 5.4. На основании данных технической экспертизы разрешительная комиссия составляет акт.
6. **Банк** несет ответственность перед **Клиентом** в случае, когда имело место хотя бы одна из следующих ситуаций:
 - 6.1. **Клиент** предъявляет электронный документ, заверенный ЭП **Клиента**, а **Банк** необоснованно не исполнил данное распоряжение по счету **Клиента**.
 - 6.2. **Банк** не предъявляет электронного документа, переданного **Клиентом**, на основании которого **Банк** выполнил операции по счёту **Клиента**.
 - 6.3. ЭП **Клиента** в электронном документе оказалась некорректной.
 - 6.4. **Клиент** предоставляет Уведомление об отмене действия секретного и соответствующего ему открытого ключей ЭП **Клиента**, подписанное должностным лицом **Банка** и при этом, указанная в Уведомлении дата окончания действия пары ключей ЭП **Клиента** раньше даты, указанной в спорном электронном документе.
7. **Банк** не несет ответственность перед **Клиентом** в следующих случаях:
 - 7.1. **Банк** предъявляет электронный документ, ЭП **Клиента** которого признана разрешительной комиссией как корректная, принадлежность **Клиенту** открытого ключа ЭП **Клиента** подтверждена.
 - 7.2. **Клиент** отказался участвовать в проведении технической экспертизы.