

ДОГОВОР № _____
на обслуживание в системе
«iBank 2»

г. _____

« ____ » _____ 20__ г.

КОММЕРЧЕСКИЙ БАНК «АГРОПРОМКРЕДИТ» (Открытое акционерное общество), именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, вместе в дальнейшем именуемые «Стороны», заключили настоящий Договор о нижеследующем.

1. Предмет Договора

1.1. В соответствии с настоящим Договором Банк осуществляет обслуживание следующих счетов Клиента:

№ _____ в Банке (далее по тексту — «Счет») с использованием системы Интернет-Банкинг (далее по тексту — «Система»), позволяющей посредством сети Интернет отправлять в Банк расчетные и иные документы, указанные в п. 3.5. настоящего Договора, а также самостоятельно получать информацию о текущем состоянии Счета.

1.2. Настоящий Договор является приложением к Договорам _____, заключенным Сторонами (далее по тексту — «Договор банковского счета»). Во всем ином, что не предусмотрено настоящим Договором, Стороны в своих взаимоотношениях в отношении каждого из указанных в п. 1.1 настоящего Договора счетов руководствуются положениями соответствующего данному счету одному из указанных выше договоров.

2. Термины, применяемые в настоящем Договоре

Термины, применяемые в тексте настоящего Договора, используются в следующем значении.

2.1. **«Система «Интернет Банк-Клиент» (Система)»** – автоматизированная организационно-техническая система «iBank 2» обеспечения электронного документооборота и безбумажных расчетов, согласованно эксплуатируемая Клиентом и Банком, обеспечивающая подготовку, защиту и обработку документов в электронном виде с использованием электронно-вычислительных средств обработки информации и публичной сети Интернет. Система «Интернет Банк-Клиент» является корпоративной информационной системой и имеет Свидетельство об официальной регистрации программы для ЭВМ Системы для Интернет-Банкинга «iBank» (iBank) № 2000610712, выданное Российским агентством по патентам и товарным знакам (Роспатент) ООО «БИФИТ», зарегистрированное в Реестре программ для ЭВМ 08.08.2000 г.

2.2. **«Документ в электронной форме» (Электронный документ – ЭД)** – документ, в котором информация представлена в электронно-цифровой форме, содержащий сообщение Банка Клиенту или Клиента Банку, в т.ч. поручение Клиента Банку о совершении операции по Счету. Данный документ представлен в виде файла или записи в базе данных.

2.3. **«Электронная цифровая подпись» (ЭЦП)** – вид аналога собственноручной подписи, предназначенный для защиты Электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием Закрытого ключа ЭЦП и позволяющий идентифицировать владельца Сертификата ключа ЭЦП, а также установить отсутствие искажения информации в Электронном документе. ЭЦП однозначно увязывает в одно целое содержание документа и закрытый ключ подписывающего и делает невозможным изменение документа без нарушения подлинности данной подписи. Для создания и проверки ЭЦП используется средство криптографической защиты – программная библиотека защиты информации «Крипто-КОМ 3.2» (вариант исполнения 5) в составе согласно формуляру ШКНР.032-07 30 01 ФО (Сертификат соответствия выдан ФСБ РФ 07.11.2007г, регистрационный номер СФ/114-1069).

Банк вправе в одностороннем порядке менять перечень средств криптографической защиты, используемых в Системе, без дополнительного согласования и уведомления Клиента. При изменении средств криптографической защиты информации Банк уведомляет об этом Клиента любым не запрещенным законом способом, в том числе по Системе, а Клиент обязан получить (принять) от Банка такие средства криптографической защиты и использовать их в работе с Системой.

2.4. **«ЭЦП Клиента»** – электронная-цифровая подпись уполномоченного Клиентом лица.

2.5. **«ЭЦП Банка»** – электронная-цифровая подпись уполномоченного Банком лица.

2.6. **«Владелец сертификата ключа подписи»** – физическое лицо, владеющее соответствующим закрытым ключом ЭЦП, позволяющим создавать свою ЭЦП в электронных документах (подписывать Электронные документы).

2.7. **«Закрытый ключ ЭЦП»** – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в Электронных документах ЭЦП. Закрытый ключ изготавливается (генерируется) абонентом Системы «Интернет Банк-Клиент» при помощи указанных выше криптобиблиотек и предназначен для формирования им ЭЦП ЭД. Секретный ключ хранится в цифровом виде, например в файле на дискете 3,5" – или ином носителе информации.

2.8. **«Открытый ключ ЭЦП»** – уникальная последовательность символов, соответствующая Закрытому ключу ЭЦП, предназначенная для подтверждения подлинности ЭЦП в Электронном документе. Открытый ключ, автоматически формируемый программными средствами Системы «Интернет Банк-Клиент» при изготовлении секретного ключа подписи и однозначно зависящий (производный) от него. Открытый ключ предназначен для проверки ЭЦП ЭД, сформированной данным участником системы «Интернет Банк-Клиент» при подписании ЭД. Открытый ключ считается принадлежащим абоненту, если он был зарегистрирован в установленном порядке (в Банк представлен Сертификат ключа ЭЦП).

2.9. **«Сертификат ключа ЭЦП»** – подписанный владельцем ЭЦП и заверенный подписью руководителя и оттиском печати Клиента документ на бумажном носителе с указанным в шестнадцатеричном виде Открытым ключом ЭЦП Клиента (по форме Приложения №4). Банк имеет право в одностороннем порядке изменить форму Сертификата в Системе.

2.10. **«Пара ключей ЭЦП»** – Закрытый ключ и соответствующий ему Открытый ключ ЭЦП.

2.11. **«Подлинность ЭД»** – означает, что данный документ (экземпляр документа) создан в Системе без отступлений от принятой технологии. ЭД считается подлинным, если он был, с одной стороны, должным образом оформлен, заверен (подписан) ЭЦП и передан на обработку, а с другой, был принят к исполнению. Свидетельством того, что ЭД принят к исполнению, является уведомление «принят к исполнению» в строке статуса в соответствующем модуле, загруженном с банковского сервера Системы.

2.12. **«Компрометация ключа»** – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых элементов;
- утрата ключевых элементов с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
- несанкционированное копирование или подозрение на копирование хранилища (носителя) с секретными ключами;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- случаи, когда нельзя достоверно установить, что произошло с носителями электронных ключей, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

2.13. **«СКЗИ»** – средства криптографической защиты конфиденциальной информации. К ним относятся: носитель информации с dll-файлами (программные библиотеки защиты информации) и USB-токен.

2.14. **«Статический IP-адрес»** – это уникальный цифровой адрес компьютера в сети Интернет, который выдается провайдером, и не изменяется при подключении к сети Интернет.

2.15. **ОТР-токен** – устройство дополнительной аутентификации Клиента, являющееся генератором одноразовых паролей, действительных для подтверждения одной операции Клиентом в Системе.

3. Соглашения Сторон

3.1. Стороны согласны с тем, что алгоритмы создания и функционирования Электронной цифровой подписи в Системе при передаче Электронных документов, реализация которых осуществляется в соответствии со

стандартами ГОСТ Р34.10-94, ГОСТ Р34.11-94, достаточны для обеспечения защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых Электронных документах, а также сохранения банковской тайны.

3.2. Стороны согласны с тем, что положительный результат проверки ЭЦП Клиента в Системе на сервере Банка является подтверждением того, что:

- полученный Электронный документ подписывался соответствующей ЭЦП Клиента,
- Электронный документ получен в том виде, в котором он исходил от Клиента.

3.3. Стороны согласны с тем, что хранящиеся в контрольных архивах Системы Электронные документы, подписанные ЭЦП Клиента, проверка которой ключом ЭЦП Клиента дала положительный результат, являются доказательным материалом для решения спорных вопросов в соответствии с действующим законодательством и Приложением № 1 – «Положение о порядке разрешения спорных ситуаций».

Проверка осуществляется путем использования функции «Проверить ЭЦП» в модуле операциониста Системы, положительным результатом выполнения которой является выведенное на экран монитора сообщение «ЭЦП верна», а также информация о номере идентификатора ключа, дате и времени подписания документа.

3.4. Стороны согласны с тем, что при изменении Электронного документа, заверенного к моменту внесения изменений электронной цифровой подписью, ЭЦП становится некорректной, то есть проверка ЭЦП открытым ключом ЭЦП дает отрицательный результат. Исправление или изменение Электронного документа, заверенного электронной цифровой подписью, возможно только путем создания нового Электронного документа.

3.5. Стороны считают, что любые Электронные документы, заверенные ЭЦП Клиента, хранящиеся в виде записи в контрольных архивах Системы или извлеченные из нее в виде отдельного файла, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным уполномоченным(и) представителем(ями) Клиента и имеющим оттиск печати Клиента, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы, исходящие от Клиента, без ЭЦП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

Стороны считают, что Электронные документы: «письмо», заверенное ЭЦП Банка, «выписка по счету», юридически эквивалентны соответствующим документам на бумажном носителе, подписанным уполномоченными лицами Банка и имеющим оттиск печати Банка. Электронные документы, исходящие от Банка, без ЭЦП Банка не имеют юридической силы.

Вышеуказанный перечень Электронных документов может изменяться Банком с предварительным уведомлением Клиента сообщением по Системе.

Направление Клиентом Банку иных видов Электронных документов может осуществляться после предварительного согласования с Банком посредством обмена подтверждающими Электронными документами, направляемыми по Системе.

3.6. Стороны согласны с тем, что Открытый ключ ЭЦП, указанный в заверенном подписью руководителя и оттиском печати Клиента Сертификате открытого ключа ЭЦП, принадлежит Клиенту и достаточен для определения Банком корректности ЭЦП.

3.7. Стороны признают в качестве единой шкалы времени при работе с системой Московское поясное время. Контрольным является время системных часов Системы. Стороны признают информацию о дате и времени поступления, исполнения, неисполнения Электронных документов в Банк, содержащуюся в контрольных архивах Банка, необходимым и достаточным доказательством даты и времени передачи, исполнения, неисполнения Клиентом Банку Электронного документа.

3.8. Стороны согласны с тем, что наличие у Банка надлежаще оформленного Электронного документа, подписанного ЭЦП Клиента, проверка корректности которой Открытым ключом ЭЦП Клиента дала положительный результат, является необходимым и достаточным основанием для проведения Банком соответствующей операции на основании указанного Электронного документа.

3.9. Стороны согласны с тем, что использование всемирной телекоммуникационной сети общего доступа Интернет может вызывать перерывы в приеме и обработке Электронных документов в Системе, связанные с отказами телекоммуникационного оборудования провайдеров телекоммуникационных услуг, а также вирусными и иными атаками на систему. Стороны обязаны принимать все доступные способы защиты от указанных угроз.

3.10. Стороны согласны с тем, что контроль за сроком действия ЭЦП, а также контроль за наличием соответствующих полномочия у Владельца сертификата ключа подписи осуществляется Клиентом, а не Банком.

4. Права и обязанности Банка

- 4.1. Банк обязан исполнять принятые от Клиента Электронные документы, указанные в п. 3.5. Договора, подписанные корректной ЭЦП Клиента, в соответствии с условиями настоящего Договора, Договоров банковского счета и действующим законодательством.
- 4.2. Банк обязан по получении от Клиента уведомления по форме Приложения № 2 временно блокировать (досрочно прекратить действие) ключа ЭЦП Клиента в Системе. Банк не обязан проверять подлинность подписи Клиента на полученном уведомлении, а обязан только установить путем обычного визуального контроля соответствие данной подписи имеющемуся у Банка образцу. Наложённая блокировка снимается только на основании требования Клиента не позднее дня, следующего за днем получения такого требования.
- 4.3. Банк обязан обеспечить строго контролируемый и ограниченный доступ к помещениям, в которых находятся программно-аппаратные средства, содержащие контрольные архивы Системы.
- 4.4. Банк обязан хранить в секрете и не передавать третьим лицам Закрытые ключи ЭЦП Банка и Открытые ключи ЭЦП Клиента, используемые при работе в Системе. Риск неблагоприятных последствий, связанных с использованием Закрытого Ключа ЭЦП Банка третьими лицами в случае несоблюдения условий сохранности, несет Банк.
- 4.5. Банк имеет право по своему усмотрению прекратить принятие от Клиента Электронных документов по Системе и потребовать от Клиента смены пары ключей ЭЦП Клиента, направив уведомление по форме Приложения № 3. По письменному требованию Клиента Банк обязан объяснить причину прекращения принятия Электронных документов от Клиента.
- 4.6. Банк имеет право приостановить работу Клиента в Системе и (или) не производить исполнения полученного Электронного документа, сообщив об этом Клиенту не позднее дня, следующего за днем его получения, путем направления сообщения по Системе и, соответственно, затребовать от Клиента оформления документа на бумажном носителе (подлинника) с подписью уполномоченных лиц и оттиском печати Клиента. По письменному требованию Клиента Банк обязан объяснить причину приостановления работы Клиента и неисполнения принятого Электронного документа, которая может быть иной, чем несоответствие Электронного документа положениям настоящего Договора или действующего законодательства.
- 4.7. Банк вправе не принимать Сертификат открытого ключа ЭЦП Клиента, если подписи Владельца сертификата ключа подписи или руководителя Клиента проставлена не в присутствии уполномоченного представителя Банка или если подлинность вышеуказанных подписей не заверена нотариально.
- 4.8. Банк имеет право отказать в исполнении Электронного документа Клиента в случае несоответствия реквизитов такого документа обязательным реквизитам, установленным действующим законодательством РФ и банковскими правилами.
- 4.9. Банк имеет право приостановить работу Клиента в Системе в случае невнесения платы за пользование Системой в соответствии с Тарифами. В этом случае Банк предварительно уведомляет Клиента по Системе либо иным способом о предстоящей приостановке и приостанавливает работу Клиента по истечении 30 календарных дней с момента направления уведомления.
- 4.10. Банк обязан передать Клиенту носитель информации, содержащий программные библиотеки, в которых реализованы СКЗИ, использующиеся в системе iBank2, по Акту приема-передачи СКЗИ по форме Приложения № 7, являющегося неотъемлемой частью настоящего Договора, а Клиент обязан принять соответствующий носитель информации.
- 4.11. Банк обязан передать USB-токен по Акту приема-передачи СКЗИ (USB-токена) по форме Приложения № 8, являющегося неотъемлемой частью настоящего Договора в случае, предусмотренном п. 5.11 Договора.
- 4.12. Банк обязуется отсылать сообщения в формате SMS, предназначенные для Клиента на номер(а) телефона(ов), указанный Клиентом при подключении к Услуге. При этом, информация, указанная в SMS (в том числе относительно счета Клиента и операций по нему) может стать известной лицам и организациям, участвующим в передаче SMS (операторы сотовой связи, их контрагенты, задействованные в процессе передачи данной информации).
- 4.13. Банк обязуется подключить Клиента к услуге в течение двух рабочих дней со дня подачи в Банк заявления по форме Приложения № 9, подписанного уполномоченным лицом.
- 4.14. Для реализации услуги по использованию средства дополнительной аутентификации Банк обязан передать OTP-токен по форме Приложения № 14, являющегося неотъемлемой частью настоящего Договора в случае, предусмотренном п. 5.16 Договора.

5. Права и обязанности Клиента

5.1. Клиент имеет право требовать от Банка предоставления на бумажном носителе копий полученных Банком Электронных документов с проставлением на них соответствующих отметок Банка (об исполнении и др.). Указанные документы предоставляются уполномоченному лицу Клиента при его явке в Банк.

5.2. Клиент имеет право досрочно прекращать действие Открытых ключей ЭЦП Клиента (вместе с соответствующим Закрытым ключом ЭЦП Клиента), направив уведомление по форме Приложения № 2, подписанное уполномоченным лицом (данное уведомление может быть направлено в Банк с использованием Системы, либо в письменном виде (передано в Банк, направлено в Банк по факсу)). Для продолжения дальнейшей работы в Системе уполномоченный представитель Клиента должен сгенерировать новую пару ключей ЭЦП Клиента и передать Банку Сертификат нового Открытого ключа ЭЦП Клиента.

5.3. Клиент имеет право блокировать Открытый ключ ЭЦП Клиента, т.е. приостановить свою работу в Системе, направив уведомление по форме Приложения № 2, подписанное уполномоченным лицом (данное уведомление может быть направлено в Банк с использованием Системы, либо в письменном виде: передано в Банк, направлено в Банк по факсу). Блокировка снимается не позднее дня, следующего за днем получения Банком письменного требования Клиента о снятии блокировки.

5.4. Клиент обязан при создании Электронных документов в Системе соблюдать условия настоящего Договора, нормы действующего законодательства и банковские правила в отношении обязательных реквизитов данных документов.

5.5. Клиент обязан обеспечить хранение в секрете и отсутствие доступа неуполномоченных лиц к Закрытому ключу ЭЦП Клиента и Открытому ключу ЭЦП Банка, используемым при работе в электронной Системе, а также обеспечить отсутствие доступа неуполномоченных лиц к телефонам, к которым подключена услуга SMS-информирование. Риск неблагоприятных последствий, связанных с использованием закрытого Ключа ЭЦП Клиента неуполномоченными лицами, несет Клиент.

5.6. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к Системе или к закрытому ключу ЭЦП Клиента в день ее обнаружения и блокировать свою работу в Системе, направив в Банк уведомление по форме Приложения № 2. Клиент несет риск всех последствий, связанных с несанкционированным доступом к Системе или Закрытому ключу ЭЦП Клиента.

5.7. Клиент обязан по требованию Банка приостановить работу в Системе и для ее возобновления сгенерировать новую ЭЦП Клиента и передать Банку Сертификат нового открытого ключа ЭЦП Клиента. Сертификат открытого ключа ЭЦП Клиента должен передаваться в Банк уполномоченным лицом Клиента (единоличным исполнительным органом либо через доверенное лицо при наличии доверенности (например, по форме Приложения № 6) либо иным способом, позволяющим установить, что документ исходит от Клиента).

5.8. Клиент обязан уведомлять Банк о смене лиц, уполномоченных работать с Системой и распоряжаться Счетом, а также об изменении полномочий лиц, к телефонам которых подключена услуга SMS – информирование. Для возможности работы с Системой новых лиц обеспечить им возможность сгенерировать Пару ключей ЭЦП Клиента. Риск неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о том, что необходимо приостановить действие ЭЦП Клиента несет Клиент.

5.9. Клиент обязан регулярно производить оплату за пользование Системой в соответствии с Тарифами, являющимися неотъемлемой частью Договора.

5.10. Клиент обязан хранить свой закрытый ключ в течение срока действия данного Договора, а также не менее 8 (восьми) лет после расторжения данного Договора. В случае если Клиент после расторжения настоящего Договора оспаривает операции, проведенные Банком с использованием его ЭЦП (в т.ч. закрытого ключа) и не может предъявить используемый закрытый ключ для проведения проверки, то считается что Клиент подтверждает правильность проведения операций Банком с использованием данной ЭЦП (в т.ч. закрытого ключа).

5.11. В целях повышения эффективности противодействия хищениям вредоносными программами секретных ключей ЭЦП Клиент вправе воспользоваться услугой по использованию устройства USB-токен, позволяющего формировать ЭЦП Клиента внутри SIM-карты токена (Сертификат ФСБ РФ, регистрационный номер СФ/114-1009 от 14.05.2007). Для этого Клиент должен предварительно (за 1 месяц) до планируемой даты начала использования USB-токена подать заявление в письменном/электронном виде и оплатить его стоимость в соответствии с действующими Тарифами.

5.12. Клиент обязуется обеспечить условия сохранения переданных СЗКИ в соответствии с требованиями действующего законодательства (в т.ч. Приказа ФАПСИ РФ № 152 от 13.06.2001.)

5.13. Клиент несет персональную ответственность за сохранность носителя, содержащего СКЗИ, и USB-токена после подписания сторонами соответствующего Акта приема-передачи (Приложение №№ 7, 8 к

настоящему Договору).

5.14. В случае утраты Клиентом мобильного телефона (SIM-карты) Клиент обязан:

- при подключении к режиму SMS-уведомления о событии Клиент обязан в максимально короткие сроки самостоятельно сменить настройки в Системе, в том числе номер(а) мобильного(ых) телефона(ов);
- при подключении Клиента к режиму расширенной аутентификации, Клиент обязан позвонить в Банк и заблокировать режим расширенной аутентификации. При блокировке режима расширенной аутентификации и подозрении на компрометацию Ключа, Клиент обязан предоставить в Банк в течение 3 (Трех) рабочих дней письменное уведомление о прекращении действия открытого ключа и соответствующего ему закрытого ключа ЭЦП (по форме Приложения № 2 – являющегося неотъемлемой частью настоящего Договора) и оформить новые сертификаты открытых ключей по правилам п. 4.7. Договора. Для продолжения дальнейшей работы в режиме расширенной аутентификации, Клиенту необходимо предоставить в Банк Заявление в соответствии с п. 7.1.2. Договора.

5.15. Клиент обязан самостоятельно обеспечить поддержку функции SMS на своём мобильном телефоне, а также подписку на услугу SMS у своего оператора сотовой связи.

5.16. Для увеличения степени противодействия возможным попыткам хищения средств Клиента в Системе, Клиент вправе воспользоваться услугой по использованию средства дополнительной аутентификации OTP-токен. Данное устройство является генератором одноразовых паролей и служит дополнительным средством для аутентификации Клиента. Для подключения к услуге Клиент должен предварительно (за 1 месяц) до планируемой даты начала использования OTP-токена подать заявление (Приложение № 13 к настоящему Договору) в письменном/электронном виде и оплатить его стоимость в соответствии с действующими Тарифами.

В случае использования Клиентом OTP-токена отправка Электронных документов в Системе без введения одноразового пароля невозможна. При получении Банком Электронного документа с корректной ЭЦП, Банк считает, что Клиентом введен одноразовый пароль, сгенерированный OTP-токеном и документ отправлен Клиентом. OTP-токен не заменяет ЭЦП, а является дополнительным средством защиты.

5.17. Клиент несет персональную ответственность за сохранность OTP-токена после подписания сторонами Акта приема-передачи по форме Приложения № 14 к настоящему Договору.

5.18. Клиент обязан обеспечить секретное хранение и отсутствие доступа неуполномоченных лиц к OTP-токену. При работе в электронной Системе Клиент также обязан обеспечить отсутствие доступа к OTP-токену неуполномоченных лиц. Риск неблагоприятных последствий, связанных с использованием OTP-токена Клиента неуполномоченными лицами, несет Клиент.

5.19. При одновременном пользовании услугой SMS-информирование в режиме расширенной аутентификации и услугой по использованию средства дополнительной аутентификации OTP-токен, Клиент обязан для авторизации в Системе и отправки Электронных документов вводить одноразовый пароль. В этом случае, Клиент выбирает следующий способ подтверждения для авторизации в Системе и отправки Электронных документов: путем получения SMS-сообщения на мобильный телефон или генерации одноразового пароля с помощью OTP-токена.

При получении Банком Электронного документа с корректной ЭЦП Банк считает, что Клиентом введен одноразовый пароль, выбранный Клиентом при помощи одного из вышеуказанных способов, и документ отправлен Клиентом.

При авторизации Клиента в Системе путем подтверждения одноразовым паролем, выбранным Клиентом одним из вышеуказанных способов, Банк считает, что доступ к Системе имеет уполномоченное лицо Клиента.

6. Совместные обязательства и ответственность Сторон

6.1. Каждая Сторона обязана за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые при работе с Системой.

6.2. В случае возникновения конфликтных ситуаций между Сторонами при использовании Системы Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Положением о порядке разрешения спорных ситуаций» (Приложение № 1), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. В случае, если Клиент отказывается от принятия на себя обязательств по Электронному документу (оспаривает факт или время передачи Электронного документа, его содержание), бремя доказывания обстоятельств, на основании которых он отказывается от принятия на себя обязательств, ложится на него. Ответственность может быть возложена на Банк в случае если создание Электронного документа обусловлено противоправными действиями Банка.

6.3. Стороны обязуются при разрешении споров, которые могут возникнуть в связи с использованием электронной Системы, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу противоположной Стороны.

6.4. Банк не несет ответственности за ущерб, причиненный Клиенту в результате использования третьими лицами Закрытого ключа Клиента (компрометация ключа).

6.5. Банк не несет ответственности за техническое состояние компьютерного оборудования Клиента, возможные помехи в телефонных линиях связи, прекращение работы Системы из-за отключения электроэнергии и повреждения линий связи, программно-аппаратные сбои Системы, если возникновение указанных обстоятельств не связано с виновными действиями Банка.

6.6. Банк не несет ответственности перед Клиентом, в случае, если Электронный документ подписан корректной ЭЦП, но исходил не от Клиента.

6.7. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение принятых по настоящему Договору обязательств на период действия обстоятельств непреодолимой силы и их последствий. К таким обстоятельствам относятся, в частности, стихийные бедствия, пожары, аварии, 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 или ограничивающих указанные в настоящем Договоре виды деятельности или препятствующие выполнению сторонами своих обязательств по настоящему Договору. Сторона, пострадавшая от влияния обстоятельств непреодолимой силы, обязана в возможно короткий срок, но не более чем через 7 (Семь) дней после возникновения этих обстоятельств, довести до сведения другой Стороны информацию о случившемся.

6.8. Банк несет ответственность за неисполнение (ненадлежащее исполнение) обязательств по настоящему Договору только при наличии своей вины.

6.9. Банк не несет ответственности за задержки и сбои, возникающие в сетях операторов сотовой связи, которые могут повлечь за собой задержку или даже недоставку SMS Клиенту.

6.10. Клиент несет ответственность за правильность данных, указанных в заявлении (в том числе номера мобильного телефона, на который будет отправляться соответствующая информация). Недостоверность информации, указанной в заявлении, может служить отказом в подключении Клиента к Услуге.

6.11. Стороны признают, что SMS-сообщения, переданные Банком в соответствии с условиями настоящего Договора, являются сообщениями, надлежащим образом переданные Клиенту.

6.12. Банк не несет ответственности за разглашение информации, связанное с ненадлежащим хранением телефона(ов) SIM-карты, к которым подключена услуга SMS-информирование.

7. Порядок обслуживания Клиента

7.1. Для начала работы по настоящему Договору Клиент обязан произвести оплату за установку Системы в соответствии с Тарифами Банка и предоставить Банку Сертификат (ы) открытого ключа ЭЦП Клиента (согласно карточке с образцами подписей и оттиском печати).

При этом при генерации ЭЦП, Сертификата открытого ключа ЭЦП Клиент обязан использовать СЗКИ, полученные согласно п. 4.10. и (или) 4.11. настоящего Договора.

7.1.1. В целях минимизации вероятности проведения платежей от имени Клиента третьими лицами в случае хищения секретных ключей, Клиент вправе обратиться в Банк с Заявлением о подключении к услуге IP-фильтрации по форме Приложения № 11, являющегося неотъемлемой частью настоящего Договора. Данная услуга позволяет обрабатывать информацию только в случае совпадения статического IP-адреса передающего компьютера со статическим IP-адресом Клиента, хранящемся в базе данных Банка. Банк принимает к исполнению Электронные документы, поступающие только с зарегистрированных в Системе статических IP-адресов (количество адресов IP-фильтрации в Системе не ограничено). Попытки доступа с неразрешенного (незарегистрированного) IP-адреса блокируются Системой. При этом Клиент подтверждает, что Электронный документ, исходящий с зарегистрированных статических IP-адресов Клиента исходит от Клиента.

Новый статический IP-адрес может быть добавлен Банком в список разрешенных IP-адресов по письменному заявлению Клиента, поданному по форме Банка (Приложение № 12, являющееся неотъемлемой частью настоящего Договора), подписанному и переданному в Банк уполномоченным лицом Клиента.

В случае не подключения к услуге IP-фильтрации и последующим хищением средств, ставшим возможным вследствие отправки подписанного корректной электронно-цифровой подписью, но отправленного с IP-адреса третьих лиц, Банк ответственности не несет.

При получении Банком Электронного документа с корректной ЭЦП, Банк считает, что документ отправлен с IP- адреса Клиента независимо от того подключен ли Клиент к услуге IP – фильтрации.

7.1.2. В целях информационного обслуживания Клиента и минимизации рисков проведения платежей от имени Клиента третьими лицами, Клиент вправе обратиться в Банк с Заявлением о подключении к услуге SMS-информирования по форме Банка (Приложение № 9 являющееся неотъемлемой частью настоящего Договора). Услуга SMS-информирования предоставляется в двух режимах: SMS-уведомление о событии и расширенная аутентификация. Клиент вправе подключиться к одному или обоим режимам одновременно. Отключение от Услуги осуществляется на основании заявления Клиента по форме Приложения № 10.

Режим SMS-уведомления о событии предназначен для уведомления Клиента о событиях, которые произошли в Системе. Условия и параметры сообщений Клиент настраивает в Системе самостоятельно. Клиент имеет право самостоятельно изменять в Системе набор рассылок в режиме SMS-уведомления о событии при наступлении определенных событий (утрата мобильного телефона, SIM-карты и др.), номера телефонов, список обслуживаемых счетов и др. Клиент вправе выбрать следующие сообщения:

- об отвержении документа;
- о поступлении в Банк документа;
- о входящих банковских письмах;
- о движении средств по счету;
- о входе в систему;
- о текущих остатках;
- выписка по счету.

Режим расширенной аутентификации предназначен для минимизации вероятности проведения платежей от имени Клиента третьими лицами. Данный режим позволяет при авторизации в Системе получать SMS - сообщения на мобильный(е) телефон(ы) Клиента. Режим расширенной аутентификации устанавливается Банком по Заявлению Клиента, в котором указывается номер(а) мобильного(ых) телефона(ов), на который(е) Клиент рассчитывает получать SMS-сообщения с дополнительным кодом. При подключении режима расширенной аутентификации работа в Системе без введения дополнительного кода невозможна.

Комиссия за фактически предоставленные Услуги за период, в который произошло подключение или отключение (как по инициативе Банка, так и по инициативе Держателя), приравнивается к комиссии за полный месяц предоставления Услуги. Комиссия за предоставление услуги SMS-информирования взимается в соответствии с Тарифами Банка.

7.1.3. Банк начинает прием Электронных документов от Клиента не позднее рабочего дня следующего за днем предоставления в Банк надлежаще оформленных Сертификатов и оплаты. До этого момента Банк не принимает Электронные документы Клиента.

При получении Банком Электронных документов, либо соответствующих документов на бумажных носителях, подтверждающих прекращение полномочий какого-либо из представителей Клиента, Банк прекращает прием Электронных документов, подписанных ЭЦП данного лица.

При предоставлении Клиентом полномочий по работе с Системой и распоряжению Счетом новому лицу, Банк начинает прием от Клиента Электронных документов, подписанных ЭЦП данного лица, начиная со дня, следующего за днем получения Сертификата ключа ЭЦП Клиента, содержащего Открытый ключ ЭЦП данного лица.

При авторизации Клиента в Системе путем подтверждения одноразовым паролем, Банк считает, что доступ к Системе имеет уполномоченное лицо Клиента.

7.2. Банк осуществляет прием Электронных документов, передаваемых по электронной Системе, круглосуточно, за исключением времени проведения требуемых работ, связанных с обновлением Системы, о времени и длительности которых Клиент извещается заранее электронным письмом из Банка, отправляемым по Системе. Использование Системы не лишает Клиента права предоставлять Банку расчетные и иные документы на бумажном носителе.

7.3. Исполнение документов осуществляется в сроки, установленные Договором банковского счета.

7.4. При получении Электронного документа Банк производит проверку:

- корректности ЭЦП Клиента Открытым ключом ЭЦП Клиента;
- правильности заполнения реквизитов Электронного документа в соответствии с требованиями законодательства РФ и Банка России;
- возможности возникновения дебетового сальдо на Счете Клиента, за исключением случаев, когда возникновение дебетового сальдо допустимо в соответствии с соглашением Сторон.

При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный Электронный документ Банком не принимается, считается возвращенным Клиенту, поручение, содержащееся в нем, Банком не исполняется. Статус документа «отвергнут» в Системе информирует

Клиента о неисполнении переданного им по Системе Электронного документа. Иного информирования Клиента о неисполнении Электронного документа Банк не осуществляет. Свидетельством того, что документ принят, является статус Электронного документа «исполнен» в Системе.

7.5. Дальнейшее оформление Электронных документов, переданных в Банк по Системе, осуществляется Банком без участия Клиента, в том числе оформление копий таких документов на бумажном носителе для передачи иным участникам расчетов. При этом дополнительное оформление документов по сравнению с установленными Банком России правилами безналичных расчетов осуществляется Банком только по требованию Клиента при явке его представителя в Банк.

7.6. Если по истечении 10 (десяти) рабочих дней с момента проведения Банком операции по Счету на основании полученного от Клиента Электронного документа, Клиентом не заявляется претензий по такой операции, признается, что Клиент подтвердил правильность проведения операции по его Счету.

7.7. Клиент имеет право с использованием Системы самостоятельно получать информацию о состоянии своего Счета на начало текущего операционного дня.

7.8. Работа с Системой осуществляется через сеть Интернет по электронному адресу, который сообщается Клиенту сотрудником Банка. Об изменении адреса в сети Интернет Банк уведомляет Клиента по Системе.

8. Действие Договора

8.1. Настоящий Договор вступает в силу с момента его подписания обеими сторонами и заключается на неопределенный срок.

8.2. Каждая из Сторон вправе расторгнуть настоящий Договор в одностороннем порядке не ранее, чем через 5 (Пять) рабочих дней после письменного уведомления об этом противоположной Стороны. При этом обязательства по настоящему Договору, возникшие в период его действия, не прекращаются до полного исполнения их Сторонами.

8.3. Расторжение настоящего Договора не влечет недействительности Электронных документов, содержащих корректную ЭЦП Клиента, переданных Клиентом по Системе до дня расторжения настоящего Договора включительно.

8.4. Настоящий Договор прекращает свое действие в случае расторжения всех, указанных в п.1.2. Договоров банковского счета.

9. Заключительные положения

9.1. Споры по настоящему Договору решаются путем переговоров в соответствии с Приложением № 1, а при не достижении согласия — в Арбитражном суде г. Москвы. Применимым правом является право РФ.

9.2. Все приложения, изменения и дополнения к настоящему Договору оформляются в письменном виде, подписываются полномочными представителями Сторон и являются его неотъемлемой частью.

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

10. Юридические адреса Сторон

ПОЛОЖЕНИЕ о порядке разрешения спорных ситуаций

1. В соответствии с настоящим Положением подлежат рассмотрению споры, связанные с наличием у Клиента к Банку претензий по поводу:

- факта передачи Клиентом Банку Электронного документа;
- дня передачи Клиентом Банку Электронного документа;
- содержания переданного Клиентом Банку Электронного документа.

Стороны договорились считать наличие корректной ЭЦП Клиента в оспариваемом Электронном документе необходимым и достаточным доказательством, подтверждающим принадлежность данного Электронного документа Клиенту и, соответственно, фактом, удостоверяющим передачу Электронного документа или содержание переданного Электронного документа. Стороны признают информацию о дате и времени поступления Электронных документов в Банк, содержащуюся в контрольных архивах Банка, необходимым и достаточным доказательством даты и времени передачи Клиентом Банку Электронного документа, если разрешительной комиссией не будет установлен факт внесения Банком изменений в указанную информацию в части, касающейся предмета спора. Корректность ЭЦП Клиента в оспариваемом Электронном документе устанавливается разрешительной комиссией в установленном ниже порядке. Иные споры разрешаются в соответствии с действующим законодательством в Арбитражном суде г. Москвы.

Проверка ЭЦП осуществляется путем использования функции «Проверить ЭЦП» в модуле операциониста Системы, положительным результатом выполнения которой является выведенное на экран монитора сообщение «ЭЦП верна», а также информация о номере идентификатора ключа, дате и времени подписания документа.

Стороны согласны с тем, что совпадение идентификатора ключа при проверке ЭЦП с идентификатором на Сертификате ключа ЭЦП Клиента на бумажном носителе, представляемом Клиентом при регистрации ключа, подтверждает подлинность ЭЦП Клиента на документах, подвергавшихся проверке.

Электронные документы, не имеющие Электронной цифровой подписи, при наличии спорных вопросов не являются доказательным материалом.

2. Клиент предоставляет Банку заявление, содержащее существо претензий с указанием на Электронный документ, содержащий ЭЦП Клиента, на основании которого Банк выполнил, не выполнил или ненадлежаще выполнил какую-либо операцию.

3. Банк обязан в срок не более пяти дней рассмотреть указанное заявление Клиента. При несогласии Банка с претензиями Клиента Банк направляет Клиенту письмо с предложением о формировании разрешительной комиссии. Письмо должно содержать фамилии представителей Банка, которые будут участвовать в работе комиссии.

4. Окончательное формирование комиссии осуществляется в течение трех рабочих дней с даты получения Клиентом указанного в п. 3 настоящего Положения письма Банка. В состав комиссии включаются в равном количестве представители Клиента и представители Банка (не более пяти с каждой стороны, включая Владельца оспариваемой ЭЦП), и, при необходимости, независимые эксперты, в т.ч. представители компании-разработчика Системы. Независимый эксперт считается назначенным только при письменном согласии обеих Сторон. Место работы комиссии — местонахождение Банка, если иное не будет согласовано Сторонами. Если разрешительная комиссия без уважительных причин (под уважительными причинами

подразумеваются: согласование Сторонами иного срока начала работы комиссии, временная нетрудоспособность одного из членов комиссии и др.) не приступит к работе по истечении пяти рабочих дней с даты получения Клиентом вышеуказанного письма Банка с предложением о ее формировании, считается, что Клиент отказался от заявленных им претензий.

5. Стороны обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов (информации), если предоставление таких документов (информации) будет допустимо в соответствии с действующим законодательством. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых для обмена Электронными документами по Системе.

6. Разрешительная комиссия в срок не более пяти дней проводит рассмотрение спорного вопроса. Рассмотрение в обязательном порядке должно включать следующие этапы.

6.1. Разрешительная комиссия проводит проверку Открытого ключа ЭЦП Клиента в Системе на его соответствие сертификату Открытого ключа ЭЦП Клиента, предоставленного Клиентом, (т.е. устанавливает его принадлежность Клиенту), проверяет период действия Открытого ключа ЭЦП Клиента.

6.2. Разрешительная комиссия проводит проверку Электронного документа, подписанного Электронной цифровой подписью Клиента, на основании которого Банком выполнены (не выполнены) оспариваемые Клиентом действия, т.е. принадлежность Клиенту и неизменность содержания спорного Электронного документа проверяется Открытым ключом ЭЦП Клиента. **Проверка производится в соответствии с п. 3.3. Договора.**

6.3. На основании полученных данных в результате указанной в п.п. 6.1 и 6.2 проверки разрешительная комиссия составляет акт, содержащий выводы по указанным выше вопросам. Выводы, содержащиеся в акте, являются обязательными для Сторон.

7. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение Стороны, несущей ответственность согласно выводу о корректности Электронной цифровой подписи Клиента под Электронным документом.

8. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

8.1. Банк не предъявляет Электронного документа, на основании которого Банк выполнил оспариваемую операцию.

8.2. Электронная цифровая подпись Клиента в Электронном документе оказалась некорректной.

УВЕДОМЛЕНИЕ

о прекращении (приостановлении) действия Закрытого и соответствующего ему Открытого ключей ЭЦП (Наименование Владельца ЭЦП Клиента)

(Наименование Клиента) уведомляет Банк о том, что с «___» _____ 20__ г. следует считать недействительным / следует заблокировать на срок _____ (ненужное вычеркнуть) Открытый ключ ЭЦП (Наименование Владельца ЭЦП Клиента), имеющий регистрационный номер: _____ и соответствующий ему Закрытый ключ ЭЦП (Наименование Владельца ЭЦП Клиента).

Прошу заблокировать режим расширенной

аутентификации*

(должность, наименование организации, ФИО)

(подпись)

М.П.

* Отметка ставится Клиентом в случае подключения к режиму расширенной аутентификации.

УВЕДОМЛЕНИЕ

о прекращении действия Закрытого и соответствующего ему Открытого ключей ЭЦП
(Наименование Владельца ЭЦП Клиента)

Банк уведомляет (Наименование Клиента) о том, что с «___» _____ 20__ г. следует считать недействительным Открытый ключ (Наименование Владельца ЭЦП Клиента), имеющий следующий регистрационный номер: _____.

С вышеуказанной даты соответствующий ему Закрытый ключ ЭЦП (Наименование Владельца ЭЦП Клиента) утрачивает силу для дальнейшего применения.

(должность, наименование организации, ФИО)

(подпись)
М.П.

**СЕРТИФИКАТ ОТКРЫТОГО КЛЮЧА ЭЦП СОТРУДНИКА КЛИЕНТА
В СИСТЕМЕ «Internet-Банкинг» ОАО КБ «АГРОПРОМКРЕДИТ»**

1. Наименование организации _____
2. Юридический адрес _____
3. ОГРН _____ дата регистрации «___» _____ года
4. Тел. _____ 5. ИНН _____ 6. КПП _____
7. Факс _____ 8. E-mail _____
9. Сведения о владельце ключа
Фамилия, имя, отчество _____
Должность _____
Удостоверение личности _____, серия _____
номер _____, дата выдачи «___» _____ года,
кем выдан _____
11. Примечания _____
**необязательно для заполнения*

Открытый ключ ЭЦП сотрудника клиента

Идентификатор ключа _____
Наименование криптосредств _____ Алгоритм _____
Дата начала действия «___» _____ 20__ г. (заполняется Банком)
Дата окончания действия «___» _____ 20__ г. (заполняется Банком)
Представление открытого ключа ЭЦП в шестнадцатеричном виде

Личная подпись владельца ключа ЭЦП

Сертификат открытого ключа ЭЦП клиента действует в рамках договора на обслуживание в системе «iBank 2»
N ___ от «___» _____ 20__ г.

Группа подписи _____

Достоверность приведенных данных подтверждаю

Руководитель организации

Уполномоченный представитель Банка

Подпись / Ф.И.О.

подпись / Ф.И.О.

Оттиск печати

Оттиск печати
Банка

Дата приема сертификата
Открытого ключа ЭЦП
«___» _____ 20__ г.

Администратор безопасности системы

подпись / Ф.И.О.

Дата регистрации сертификата
Открытого ключа ЭЦП
«___» _____ 20__ г.

Для работы с системой Клиент должен иметь:

1. Персональный компьютер, совместимый с IBM PC AT, с процессором Intel Celeron 1 GHz и выше, с оперативной памятью не менее 512 Mb и свободным объемом жесткого диска не менее 50 Mb.
2. Установленную на компьютере операционную систему Windows 98/NT/2000/XP или выше
3. Браузер Internet Explorer v. 5.0 и выше с установленной Java-машинкой Sun Java версии 1.6 выше (рекомендуется использовать последнюю рекомендованную разработчиком версию продукта для той платформы, которую использует Клиент).
4. Выход в Интернет со скоростью обмена данных не менее 33 600 кб/с и возможностью использования для обмена порт 443.
5. Кроме вышеперечисленных требований рекомендуется наличие в компьютере пользователя USB-порта, съемного носителя информации (flash-карты, гибкий диск 3.5" и т.д.) Для хранения ключей ЭЦП рекомендуется использовать крипто-токены iBank 2 Key. Съемный носитель информации необходим для записи на него файла с Хранилищем ключей ЭЦП клиента. Необходимо также наличие принтера, на котором будет распечатан Сертификат открытого ключа ЭЦП клиента.

Доверенность № _____

Г. _____
(место выдачи)

_____ (дата выдачи)

_____ (полное наименование организации) (далее именуемый Клиент)

в лице _____,
(должность, фамилия, имя, отчество)

действующего на основании _____, уполномочивает _____
(должность, фамилия, имя, отчество полномочного представителя)

- паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи;
- телефон для связи,
- E-Mail,

на выполнение следующих действий от имени Клиента¹:

- передать в ОАО КБ «АГРОПРОМКРЕДИТ» подписанный _____ Договор на обслуживание по электронной системе Internet-Банкинг № _____ от «___» _____ 20__ г. (далее – Договор)
- передать в ОАО КБ «АГРОПРОМКРЕДИТ» Сертификат открытого ключа ЭЦП КЛИЕНТА № _____, подписанный Владелец ЭЦП _____ к Договору.

Настоящая доверенность действительна до «___» _____ 20__ г. (включительно)

Подпись (фамилия, инициалы) _____ удостоверяю.
(личная подпись)

Руководитель организации _____ (инициалы, фамилия)
(личная подпись)

М.П.

¹ Могут указываться иные полномочия передаваемые Доверенному лицу

АКТ
приема-передачи СКЗИ

г. _____

«___» _____ 20__ г.

ОАО КБ «АГРОПРОМКРЕДИТ», именуемое в дальнейшем «Банк», в лице _____, действующ _____ на основании _____, с одной стороны и _____, именуемый в дальнейшем «Клиент», в лице _____, действующ _____ на основании _____, с другой стороны, вместе в дальнейшем именуемые Стороны, подписали настоящий Акт о нижеследующем:

Для выполнения электронных платежей в системе «iBank 2» Банк передает Клиенту, а Клиент принимает программные библиотеки, в которых реализованы СКЗИ, использующиеся в системе iBank 2 на магнитном носителе в составе, размере и конфигурации, установленной разработчиком СКЗИ:

– файл (-ы): ibank2ccom.dll (размер 311296 байт)

При передаче программных библиотек СКЗИ представителями Сторон проверены комплектность и размер СКЗИ. Претензии у Клиента к программным библиотекам СКЗИ и факту их передачи отсутствуют. Настоящий Акт составлен в двух экземплярах для каждой из сторон.

БАНК:

КОММЕРЧЕСКИЙ БАНК «АГРОПРОМКРЕДИТ» (Открытое акционерное общество)

К/сч. 30101810500000000710 в 5 отделении Московского ГТУ Банка России, БИК044552710

ИНН 5026005919

Адрес: Россия, Московская обл., г. Лыткарино, 5 микрорайон, квартал 2, дом 13.

КЛИЕНТ:

БАНК:

КЛИЕНТ:

Заместитель Председателя Правления

Генеральный директор

Главный бухгалтер

Главный бухгалтер

Передал от имени Банка: _____

Принял от имени Клиента: _____

М.П.

М.П.

АКТ
приема-передачи СКЗИ (USB-токен)

г. _____

«___» _____ 20__ г.

ОАО КБ «АГРОПРОМКРЕДИТ», именуемое в дальнейшем «Банк», в лице _____, действующ _____ на основании _____, с одной стороны и _____, именуемый в дальнейшем «Клиент», в лице _____, действующ _____ на основании _____, с другой стороны, вместе в дальнейшем именуемые Стороны, подписали настоящий Акт о нижеследующем:

Для выполнения электронных платежей в системе "iBank2" Банк передает Клиенту, а Клиент принимает USB-токен. Данное устройство предназначено для создания и хранения секретных ключей Клиента, а также для выполнения требуемых криптографических операций при работе Клиента в системе «iBank2».

При передаче USB-токена представителями Сторон проверены комплектность СКЗИ. Претензии у Клиента к USB-токену и факту его передачи отсутствуют. Настоящий Акт составлен в двух экземплярах для каждой из сторон.

БАНК:

КОММЕРЧЕСКИЙ БАНК «АГРОПРОМКРЕДИТ» (Открытое акционерное общество)
К/сч. 30101810500000000710 в 5 отделении Московского ГТУ Банка России, БИК044552710
ИНН 5026005919
Адрес: Россия, Московская обл., г. Лыткарино, 5 микрорайон, квартал 2, дом 13.

КЛИЕНТ:

БАНК:

Заместитель Председателя Правления

Главный бухгалтер

Передал от имени Банка: _____

М.П.

КЛИЕНТ:

Генеральный директор

Главный бухгалтер

Принял от имени Клиента: _____

М.П.

От _____

_____ указывает Клиент / Уполномоченное лицо Клиента

_____ указывает Головной офис/ филиал/ доп. офис Банка,
куда предоставляется заявление

ЗАЯВЛЕНИЕ
о подключении к услуге SMS-информирования

В целях информационного обслуживания и/или минимизации рисков проведения платежей от имени _____
_____ третьими лицами прошу подключить:
(указать наименование юридического лица)

Режим SMS-уведомления о событии

Режим расширенной аутентификации.

Прошу высылать дополнительный код на следующий(ие) номер(а) мобильного телефона(ов):

Я согласен(на) с тем, что для предоставления мне услуги «SMS–информирование» Банку необходимо предоставлять информацию относительно моего счета и операций по счету лицам и организациям, участвующим в передаче данной информации (операторы сотовой связи, их контрагенты, задействованные в процессе передачи данной информации) и прошу считать их моими представителями. Я согласен(на) с тем, что Банк не несет ответственности за задержки, сбои, возникающие в сетях операторов связи, которые могут повлечь за собой задержку, недоставку, искажение SMS.

_____ Должность

_____ /_____/ Ф.И.О.

_____ Подпись

М.П. «___» _____ 20__ г.

Приложение № 10

к Договору на обслуживание
в системе «iBank2»

№ _____

от «___» _____ 20__ г.

От _____

указывается Клиент / Уполномоченное лицо Клиента

указывается Головной офис/ филиал/ доп. офис Банка,
куда предоставляется заявление

ЗАЯВЛЕНИЕ
на отключение услуги SMS-информирования

В настоящее время _____

указывается Головной офис/ филиал/ доп. офис Банка

предоставляется услуга SMS-информирования в режиме SMS-уведомления о событии и/или режиме расширенной аутентификации по договору на обслуживание по электронной системе Internet-Банкинг (iBank 2).

Прошу произвести отключение услуги SMS-информирования

Режим SMS-уведомления о событии

Режим расширенной аутентификации.

Должность

_____ / _____ /

Ф.И.О.

Подпись

М.П.

«___» _____ 20__ г.

Приложение № 11

к Договору на обслуживание
в системе «iBank2»

№ _____

от «___» _____ 20__ г.

От _____

указывается Клиент / Уполномоченное лицо Клиента

указывается Головной офис/ филиал/ доп. офис Банка,
куда предоставляется заявление

Заявление

С целью подключения услуги IP-фильтрации сообщаю список разрешенных IP-адресов, с которых необходимо принимать электронные документы (ЭД) и производить их исполнение:

IP-адрес _____,

IP-адрес _____,

IP-адрес _____.

С других IP-адресов просьба не осуществлять прием ЭД и их исполнение.

При замене или дополнении IP-адресов обязуюсь письменно уведомить Банк путем подачи Заявления по форме Банка.

Должность

_____ / _____ /

Ф.И.О.

Подпись

М.П. «___» _____ 20__ г.

От _____

указывается Клиент / Уполномоченное лицо Клиента

указывается Головной офис/ филиал/ доп. офис Банка,
куда предоставляется заявление

Заявление

- Прошу дополнить список разрешенных IP-адресов новым статическим IP-адресом
IP _____
- Прошу исключить IP-адрес _____ из списка разрешенных IP-адресов
- Прошу отключить услугу IP-фильтрации*

*В настоящее время

указывается Головной офис/ филиал/ доп. офис Банка

предоставляется услуга IP-фильтрации по договору на обслуживание в системе «iBank2».

Я понимаю, что использование встроенного в систему «iBank2» механизма IP-фильтрации минимизирует вероятность проведения платежей от имени _____

указывается Клиент

третьими лицами в случае хищения секретных ключей.

Кроме этого, мне разъяснено, что в случае отказа от предоставления данной услуги и использования электронного документа Банком, и последующим хищением средств, ставшим возможным вследствие отправки подписанного корректной электронно-цифровой подписью, но отправленного с IP-адреса третьих лиц, Банк ответственности не несет.

Должность

_____ / _____ /

Ф.И.О.

Подпись

М.П. «___» _____ 20__ г.

От _____

_____ /
указывается Клиент / Уполномоченное лицо Клиента

_____ /
указывается Головной офис/ филиал/ доп. офис Банка,
куда предоставляется заявление

ЗАЯВЛЕНИЕ
на предоставление услуги по использованию
дополнительной аутентификации с помощью OTP-токена

Для увеличения степени противодействия возможным попыткам хищения средств Клиента в системе iBank2, прошу предоставить мне услугу дополнительной аутентификации с помощью OTP-токена, в порядке и на условиях, установленных настоящим Договором, а также Тарифами и ставками комиссионного вознаграждения, взимаемыми с клиентов юридических лиц, индивидуальных предпринимателей, а также физических лиц, занимающихся в установленном порядке частной практикой по операциям в валюте РФ и иностранной валюте:

Я понимаю, что процедура подтверждения является обязательной для всех созданных электронных документов, со дня, следующего за днем подписания Акта приема-передачи в рамках реализации услуги по использованию средства дополнительной аутентификации.

Я понимаю, что использование OTP-токена минимизирует вероятность проведения платежей от имени

_____ /
указывается Клиент

третьими лицами в случае хищения секретных ключей и обязуюсь хранить недоступном месте от неуполномоченных лиц.

_____ /
Должность

_____ / _____ /
Ф.И.О.

_____ /
Подпись

М.П. «__» _____ 20__ г.



Приложение № 14
к Договору на обслуживание
в системе «iBank2»
№ _____
от «___» _____ 20__ г.

От _____

_____ указывает Клиент / Уполномоченное лицо Клиента

_____ указывает Главной офис/ филиал/ доп. офис Банка,
куда предоставляется заявление

АКТ
приема-передачи OTP-токена в рамках
реализации услуги по использованию средства дополнительной аутентификации

г. _____ «___» _____ 20__ г.

ОАО КБ «АГРОПРОМКРЕДИТ», именуемое в дальнейшем «Банк», в лице _____, действующ _____ на основании _____, с одной стороны и _____, именуемый в дальнейшем «Клиент», в лице _____, действующ _____ на основании _____, с другой стороны, вместе в дальнейшем именуемые Стороны, подписали настоящий Акт о нижеследующем:

Для выполнения электронных платежей в системе «iBank2» Банк передает Клиенту, а Клиент принимает OTP-токен. Данное устройство предназначено для генерации одноразовых паролей в целях дополнительной защиты электронного документооборота между Банком и Клиентом при работе в Системе «iBank2».

№ п/п	Название	количество	№ ID OTP – токена
1	Генератор одноразовых паролей OTP-токен		

При передаче OTP-токена представителями Сторон проверена комплектность OTP-токена. Претензии у Клиента к OTP-токену и факту его передачи отсутствуют. Клиент предупрежден о порядке работы с OTP-токеном и необходимости обеспечения хранения OTP-токена в недоступном для неуполномоченных лиц месте. Настоящий Акт составлен в двух экземплярах для каждой из сторон.

БАНК:

КОММЕРЧЕСКИЙ БАНК «АГРОПРОМКРЕДИТ» (Открытое акционерное общество)
К/сч. 30101810500000000710 в 5 отделении Московского ГТУ Банка России, БИК 044552710
ИНН 5026005919
Адрес: Россия, Московская обл., г. Лыткарино, 5 микрорайон, квартал 2, дом 13.

КЛИЕНТ:

БАНК:

Заместитель Председателя Правления

Главный бухгалтер

Передал от имени Банка: _____

М.П.

КЛИЕНТ:

Генеральный директор

Главный бухгалтер

Принял от имени Клиента: _____

М.П.