«УТВЕРЖДЕНО»
Правлением ПАО КБ «САММИТ БАНК»
Протокол № 32 от «16» марта 2017 года

Президент _____ С.В. Бененов

Договор на использование электронного средства платежа
в системе «iBank2»
(Публичная оферта)

1. СТАТУС ДОГОВОРА

1.1. Настоящий Договор на использование электронного средства платежа в системе «iBank2», (далее — Договор), является Договором присоединения, регулирующим отношения по обслуживанию юридического лица или индивидуального предпринимателя, (далее – Клиента) в системе «iBank2» ПАО КБ «САММИТ БАНК», (далее - «Банк»).

1.2. Опубликование Договора, включая распространение его текста и приложений к нему на web-странице Банка в Интернете (сайт ПАО КБ "САММИТ БАНК" по адресу www.kbsammit.ru) рассматривается как публичное предложение (оферта) Банка, адресованное Клиентам для заключения Договора на предлагаемых условиях в соответствии со ст. 428 Гражданского Кодекса РФ.

1.3. Заключение Договора производится путем присоединения к его условиям в следующем порядке: Клиенты представляют в Банк подписанное со своей стороны Заявление о присоединении в форме, установленной Банком и приведенной в Приложении №1 к настоящему Договору.

1.4. Оригинал Договора, оформленный надлежащим образом (листы прошиты, пронумерованы, скреплены подписью Председателя Правления и печатью Банка), хранится в головном офисе Банка и применяется в качестве доказательства в случае возникновения споров. Копии оригинала Договора размещаются на официальных стендах Банка в головном, операционных и дополнительных офисах.

2. ТЕРМИНЫ, ПРИМЕНЯЕМЫЕ В ДОГОВОРЕ

2.1. **«Клиент»** – юридическое лицо, индивидуальный предприниматель, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, имеющее действующий банковский счет в ПАО КБ «САММИТ БАНК», заключившее с Банком договор об использовании электронного средства платежа в системе «iBank2».

2.2. **Система «iBank2»** - 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. Клиентская часть системы «iBank 2» работает режиме **«РС–банкинг»** через программное обеспечение, установленное на оборудовании Клиента. Все необходимые электронные документы подготавливаются на компьютере Клиента без подключения к сети Интернет и передаются в Банк при установлении связи с сетью Интернет.

2.3. «**Электронный документ**» **(ЭД)** – совокупность байт, содержащая финансовый документ или информационное сообщение Клиента.

2.4. «**Электронная подпись**» (**ЭП**) – совокупность символов, формируемая Клиентом, однозначно сопоставляемая электронному документу и используемая для аутентичности (подтверждение авторства и целостности) электронного документа. ЭП вырабатывается в результате криптографического преобразования информации с использованием секретного ключа ЭП и позволяет идентифицировать владельца ключа ЭП, а также установить отсутствие искажений информации в ЭД с момента выработки ЭП. Каждый ключ ЭП в системе закрепляется для использования за конкретным уполномоченным лицом Клиента, владельцем ключа ЭП. Количество ЭП, необходимых для подтверждения электронного документа, определяется согласно карточке с образцами подписей и оттиска печати Клиента.

2.5. **«Ключ ЭП Клиента»** – уникальная последовательность символов, самостоятельно генерируемая Клиентом с использованием средств системы «iBank2», и предназначенная для формирования Клиентом электронной подписи электронных документов.

2.6. **«Ключ проверки ЭП Клиента»** – уникальная последовательность символов, однозначно связанная с ключом ЭП Клиента, самостоятельно генерируемый Клиентом с использованием средств системы «iBank2», и предназначенная для проверки Банком корректности электронной подписи электронного документа, сформированного Клиентом.

2.7. «**Корректная ЭП Клиента**» – электронная подпись электронного документа Клиента, дающая положительный результат ее проверки с использованием ключа проверки ЭП Клиента.

2.8. «**Сертификат ключа проверки ЭП Клиента**» – документ на бумажном носителе, с представленным в шестнадцатеричном виде ключа проверки ЭП Клиента, заверенный подписью руководителя и имеющий оттиск

печати Клиента, подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП; содержит ключ проверки ЭП Клиента, идентификатор и срок действия ключа проверки ЭП.

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

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

- Утрата ключа ЭП Клиента или носителя с ключом ЭП Клиента (утрата ключа);
- Утрата ключа с последующим обнаружением;
- Увольнение сотрудников, имевших доступ к ключам;
- Нарушение правил хранения и использования ключевых носителей (Приложение №4 к настоящему Договору);
- Случаи, когда нельзя достоверно установить, что произошло с носителями ключей (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

2.11. «Блокировочное слово» - уникальное слово, определяемое Клиентом при регистрации в системе «iBank 2», для блокирования работы Клиента в системе по телефонному звонку.

2.12. «Ключевой носитель» - аппаратное устройство (USB – токен, смарт-карта или другой рекомендуемый Банком криптопровайдер) для обеспечения неизвлекаемого хранения и использования ключа ЭП Клиента в защищенной области памяти устройства, а также формирования ЭП Клиента под электронным документом по Российскому криптографическому алгоритму ГОСТ Р34.10-2001 непосредственно внутри устройства.

2.13. «Персональный аппаратный криптопровайдер с не извлекаемыми секретными ключами ЭП» - USB-токен «iBank 2 Key», смарт-карта «iBank 2 Key» или другой рекомендуемый Банком криптопровайдер (далее по тексту - **Персональный аппаратный криптопровайдер**), является средством усиленной неквалифицированной ЭП, предназначенный для генерации пары ключей ЭП, хранения сгенерированных ключей ЭП (является носителем, содержащим ЭП), формирования ЭП под документами в соответствии с утвержденными стандартами (ГОСТ Р34.10-94, ГОСТ Р34.10-2001, ГОСТ Р34.11-94) с использованием встроенного в устройство сертифицированного СКЗИ. Применяется в целях дополнительного повышения безопасности электронного документооборота между Клиентом и Банком и полного исключения возможности несанкционированного копирования ключей ЭП.

2.14. «Генератор одноразовых паролей» - аппаратное устройство для обеспечения дополнительной авторизации электронных документов и/или аутентификации Клиента в системе «iBank2» персональным одноразовым паролем, действие которого ограничено определенным интервалом времени.

2.15. «**Средство подтверждения**» - электронное или иное средство, используемое для получения/генерации одноразовых паролей. Средство подтверждения является средством простой ЭП, считается действительным на определенный момент времени, если одновременно выполнены следующие условия: на этот момент времени между Банком и Клиентом заключено соглашение об использовании средства подтверждения, срок действия средства подтверждения не истек, средство подтверждения не было отменено Клиентом или Банком.

2.16. «Поставщик» – организация или физическое лицо, осуществляющее продажу Ключевых носителей и/или Генераторов одноразовых паролей.

2.17. «SMS информирование» - услуга, порядок оказания и пользования которой регламентируется настоящим Договором, позволяющая Клиенту (Пользователю) получать информационные сообщения посредством SMS и/или электронной почте при синхронизации Клиента с сервером системы iBank и/или об операциях, совершенных по счету (-ам) Клиента, открытому (ым) в Банке и подключенного (ым) к Системе «iBank2».

2.18. «Одноразовый пароль синхронизации «iBank2» - услуга, порядок оказания и пользования которой регламентируется настоящим Договором, позволяющая клиенту получать посредством SMS-сообщений на мобильный телефон, либо генерировать самостоятельно с помощью приобретаемого в банке устройства (OTP-токена или MAC-токена), одноразовый пароль при выполнения синхронизации для отправки платежных документов и писем, получения выписок, статусов документов и иной информации по системе «iBank2».

2.19. «Дополнительное подтверждение платежных документов» - услуга, порядок оказания и пользования которой регламентируется настоящим Договором, позволяющая клиенту получать посредством SMS-сообщений на мобильный телефон, либо генерировать самостоятельно с помощью приобретаемого в банке устройства (OTP-токена) одноразовый пароль для дополнительного подтверждения отправляемых в банк платежных поручений.

2.20. Клиент» - юридическое лицо или индивидуальный предприниматель.

2.21. «Пользователь» - сотрудник Клиента, номер мобильного телефона которого предоставляется для использования Услуг **«SMS информирование», «Одноразовый пароль на вход в «iBank2», «Дополнительное подтверждение платежных документов», «Фильтрация IP адресов».**

3. ПРЕДМЕТ ДОГОВОРА

3.1. Банк подключает счета Клиента к системе «iBank2» на основании Заявления о присоединении (Приложение № 1 к настоящему Договору). В процессе обслуживания Банк подключает дополнительные счета на основании заявлений Клиента, предоставленных на бумажных носителях или переданных по системе дистанционного банковского обслуживания.

3.2. Банк осуществляет обслуживание банковских (расчетных, текущих, специальных, транзитных и др.) счетов Клиента с использованием системы «iBank2», позволяющей передавать электронные документы и принимать выписки и информационные сообщения.

4. СОГЛАШЕНИЕ СТОРОН

4.1. До заключения договора Клиент проинформирован Банком об условиях использования системы «iBank 2» в качестве электронного средства платежа (ЭСП), в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования системы «iBank 2».

4.2. Банк информирует Клиента о совершении каждой операции с использованием ЭСП путем предоставления:

- уведомления в виде SMS сообщения или сообщения электронной почты (по выбору Клиента - Приложения 1 к Договору на использование электронного средства платежа) о проведенных операциях по счету (списание денежных средств) и выписки об операциях по счету, запрашиваемой Клиентом самостоятельно во время работы в системе «iBank 2».
- информации об изменении статуса ЭПД, принятого системой в обработку, из состояния «Доставлен» до состояния «Исполнен» или «Отвергнут».
- распечатки выписки об операциях по счету при личном посещении Клиентом Банка.

4.3. Стороны признают, что встроенное средство криптографической защиты информации в системе «iBank2» обеспечивает необходимый уровень защиты информации от несанкционированного доступа, подтверждения подлинности и авторства электронных документов, а также разбора конфликтных ситуаций.

4.4. Стороны признают, что при изменении электронного документа, заверенного электронной подписью, ЭП становится некорректной, то есть проверка ЭП дает отрицательный результат.

4.5. Стороны признают, что подделка ЭП Клиента, то есть создание корректной электронной подписи электронного документа от имени Клиента, невозможна без знания пароля и наличия доступа к ключу ЭП Клиента.

4.6. Стороны признают, что электронные документы, заверенные необходимым количеством электронных подписей Клиента, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным Клиентом и имеющим оттиск печати Клиента, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы без необходимого количества электронных подписей Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

4.7. Стороны признают, что электронные документы с электронными подписями Клиента, созданные системой «iBank2» и полученные сервером Банка, являются материалом для решения спорных вопросов в соответствии с «Процедурой проведения технической экспертизы при возникновении спорных ситуаций» (Приложение №3 настоящего Договора).

4.8. Стороны согласны с тем, что наличие у Банка надлежаще оформленного Электронного документа, подписанного ЭП Клиента, проверка подлинности которой ключом проверки ЭП Клиента дала положительный результат, является основанием для проведения Банком соответствующей операции на основании указанного Электронного документа.

4.9. Электронные документы, не имеющие необходимого количества электронных подписей, при наличии спорных вопросов, не являются доказательным материалом.

4.10. Стороны признают, что ключ проверки ЭП Клиента, указанный в заверенном подписью руководителя и оттиском печати Клиента Сертификате ключа проверки ЭП Клиента, принадлежит Клиенту и используется для проверки подлинности ЭП Клиента.

4.11. Стороны признают, что применяемая в Персональном аппаратном криптопровайдере технология генерации и хранения Ключа ЭП, формирования ЭП под документом с использованием Персонального аппаратного криптопровайдера полностью исключает возможность получения прямого доступа к Ключу ЭП с целью его копирования, переноса на внешний носитель или использования для формирования ЭП вне устройства.

4.12. Стороны признают, что применяемые в системе «iBank 2» механизмы дополнительного подтверждения документов с помощью Одноразового пароля, являются надежными. Документы, требующие подтверждения Одноразовым паролем, принимаются Банком к исполнению только в случае надлежащего подтверждения Одноразовым паролем, полученным со Средства подтверждения Клиента.

4.13. В процессе эксплуатации Системы «iBank2» Стороны самостоятельно выполняют на своей территории мероприятия, обеспечивающие безопасность аппаратно-программных средств Системы, защиту ключей, паролей и ресурсов Системы от несанкционированного доступа.

4.14. Стороны признают в качестве единой шкалы времени при работе с системой «iBank 2» Владивостокское поясное время. Контрольным является время системных часов аппаратных средств Банка.

4.15. Банк рассматривает заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом его ЭСП, и доводит информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок не более 30 дней со дня получения таких заявлений, а также не более 60 дней со дня получения заявлений в случае использования ЭСП для осуществления трансграничного перевода денежных средств.

4.16. Использование Клиентом ЭСП может быть приостановлено или прекращено Банком на основании полученного от Клиента уведомления или по инициативе Банка при нарушении Клиентом порядка использования ЭСП в соответствии с договором, но это не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения указанного использования.

4.17. В случае утраты ЭСП и/или его использования без согласия Клиента он обязан направить соответствующее уведомление в Банк незамедлительно после обнаружения факта утраты ЭСП и/или его использования без согласия Клиента (по форме Приложение 5 настоящего договора), но не позднее дня, следующего за днем получения уведомления о совершенной операции.

4.18. После получения Банком уведомления Клиента в соответствии с п. 4.17. настоящего договора Банк обязан возместить Клиенту сумму операции, совершенной без согласия Клиента после получения указанного уведомления.

4.19. Если Банк не информировал Клиента о совершенной операции в соответствии с п.4.2. настоящего договора, Банк обязан возместить Клиенту сумму операции, о которой Клиент не был проинформирован и которая была совершена без согласия Клиента.

4.20. В случае, если Банк информировал клиента о совершенной операции в соответствии с п. 4.2. настоящего договора и Клиент **не** направил в Банк уведомление в соответствии с п. 4.17. настоящего договора, Банк не обязан возмещать Клиенту сумму операции, совершенной без согласия Клиента.

4.21. Банк и Клиент обеспечивают хранение архивов электронных документов в течение срока, установленного для хранения соответствующих документов на бумажном носителе.

5. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

5.1. Для подключения к системе «iBank2» Клиент обязан следовать п.п .9.1 – 9.5 настоящего Договора.

5.2. Клиент обязан назначить из числа своих сотрудников ответственного представителя по взаимодействию с Банком в вопросах использования Клиентом электронного средства платежа в системе «iBank2».

5.3. Клиент для работы в системе дистанционного банковского обслуживания «iBank2» обязан использовать Ключевые носители, передаваемые Банком Клиенту, в качестве устройств для формирования и хранения секретного ключа ЭП, а также для подписания электронных документов. Клиент использует USB-токен для первоначальной генерации пары открытого и закрытого ключей и в дальнейшем при плановой смене ключей по истечении срока их действия, досрочной смены при подозрении на компрометацию ключей или по желанию Клиента, смене руководства; для административных действий с ключевой информацией.

5.4. Ключевые носители предоставляемые другими поставщиками, к использованию не допускаются. При обращении с ключевым носителем Клиент соблюдает правила, изложенные в Руководстве по работе с USB-токеном или иного, полученного от Банка по акту приема-передачи (Приложение №8 к настоящему Договору) ключевого носителя. Оплата устройств производится согласно действующим тарифам Банка.

5.5. Клиент обязан контролировать доставку электронных документов в Банк и их обработку на основе передаваемого Банком результата приема и обработки ЭД. ЭД считается принятым и обработанным системой «iBank2» только в том случае, если Клиент получил соответствующий положительный результат.

5.6. Клиент обязан по требованию Банка заверить подписями и печатью распечатанные Банком, принятые по системе «iBank2» и проведенные по счету Клиента платежные документы или предоставить оригиналы вышеуказанных документов.

5.7. Клиент обязан обеспечить сохранность в тайне от посторонних лиц информацию о ключах ЭП должностных лиц, уполномоченных распоряжаться счетом. Ключевые носители ключа ЭП должны храниться у лиц, для генерации ЭП которых они используются.

5.8. Клиент обязан не передавать третьим лицам программное обеспечение, документацию системы, сведения по форматам ЭД и технологии их обработки Клиентом и Банком, относящиеся к данному Договору.

5.9. Клиент обязан содержать компьютеры, с которых осуществляется работа с системой «iBank2», в технически исправном состоянии и обеспечить их нахождение в служебном помещении, как правило, доступ в которое разрешен только тем сотрудникам Клиента, которые непосредственно работают с системой.

5.10. На любом компьютере/ноутбуке, с которого производится работа с системой «iBank2», Клиент обязан использовать актуальное лицензионно антивирусное программное обеспечение и штатный защитный экран Брандмауэр Windows, либо другой межсетевой экран (*firewall)* в режиме постоянной работоспособности и максимальной степени защиты, а также регулярное полное антивирусное сканирование, своевременное обновление антивирусных баз, операционной системы и прикладного программного обеспечения.

5.11. Клиент обязан допускать к эксплуатации системы только сотрудников, имеющих соответствующую подготовку.

5.12. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к системе «iBank2» не позднее следующего дня с момента обнаружения.

5.13. Клиент обязан незамедлительно извещать Банк обо всех случаях компрометации ключей ЭП.

5.14. Клиент обязан производить генерацию новой пары ключей ЭП должностных лиц, уполномоченных распоряжаться счетом, не реже 1 раза в 2 года.

5.15. В случае изменения в составе руководства Клиента (смена руководителя, главного бухгалтера и иных лиц, указанных в карточке с образцами подписей и оттиска печати) Клиент обязан в течение 3-х рабочих дней с момента такого изменения сообщить об этом Банку (с предоставлением соответствующих документов), сгенерировать новую пару ключей ЭП и зарегистрировать новый ключ проверки ЭП в Банке.

5.16. Клиент обязан в случае прекращения использования системы «iBank2» уничтожить ключ ЭП Клиента.

5.17. Клиент обязан заполнять электронные документы в системе «iBank2» в соответствии с действующим «Положением о правилах осуществления перевода денежных средств» (утв. Банком России 19.06.2012 N 383-П).

5.18. Клиент обязан хранить в секрете и не передавать третьим лицам пароль и носитель с ключом ЭП Клиента.

5.19. Клиент обязан по требованию Банка сгенерировать новую пару ключей ЭП Клиента и зарегистрировать новый ключ проверки ЭП Клиента в Банке.

5.20. Клиент обязан представлять информацию по запросу Банка, необходимую для исполнения Банком требований Федерального Законодательства, включая информацию о своих выгодоприобретателях и бенефициарных владельцах, в срок установленный запросом.

5.21. Клиент имеет право досрочно прекратить действие своего активного ключа ЭП и соответствующего ему ключа проверки ЭП Клиента направив в Банк «Уведомление об отмене действия Пары ключей ЭП Клиента» (Приложение №5 к настоящему Договору) в двух экземплярах и потребовать от Банка блокировать этот активный ключ проверки ЭП Клиента.

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

5.23. Клиент имеет право, позвонив в службу технической поддержки системы дистанционного банковского обслуживания Банка, и произнеся блокировочное слово, впредь до письменного уведомления, блокировать свою работу в системе «iBank2».

5.24. Клиент имеет право отозвать ранее переданный в Банк электронный документ, имеющий корректную подпись ЭП, путем направления в Банк по системе «iBank2» соответствующего уведомления защищенного ЭП, при условии, что Банк к моменту получения уведомления не произвел списание со счета Клиента денежных средств во исполнение ранее полученного от Клиента электронного документа.

5.25. Клиент имеет право выбрать один или несколько видов дополнительных услуг по обеспечению безопасности при работе в системе «iBank2»:

- Рассылка SMS уведомлений Клиенту о состоянии банковских счетов через SMS (услуга «SMS информирование»);
- Дополнитедьная аутентификация при входе в систему «iBank2» с помощью одноразового персонального пароля, полученного Клиентом с использованием OTP – токена, MAC-токена или услуги «Одноразовый пароль на вход в «iBank2»;
- Авторизация с помощью одноразового персонального пароля при совершении платежа в системе «iBank2» с использованием OTP – токена, MAC-токена или услуги «Дополнительное подтверждение платежных документов» на сумму более указанной Клиентом в Приложении №7 к настоящему Договору;
- Ограничение доступа Клиента по IP-адресам (фильтрация IP адресов), с которых разрешена работа с системой «iBank2». Сведения об IP-адресах, с которых будет разрешена работа с системой «iBank2» указывается Клиентом в Приложении №7 к настоящему Договору;

5.26. Клиент обязан регулярно производить подключение к системе «iBank2» для получения выписки по его расчетным счетам.

5.27. Клиент обязан производить подключение к системе «iBank2» для получения входящей корреспонденции не реже одного раза в два дня.

5.28. Клиент обязан при использовании Услуг(и) «SMS информирование», «Одноразовый SMS пароль на вход в «iBank2» и «Дополнительное подтверждение платежных документов» указывать номера мобильных телефонов и/или электронные адреса Пользователей с их согласия.

5.29. Клиент обязуется самостоятельно урегулировать все споры и разногласия с Пользователями по поводу поступления им SMS/email сообщений в рамках Услуг(и) «SMS информирование», «Одноразовый SMS пароль на вход в «iBank2» и «Дополнительное подтверждение платежных документов».

5.30. Клиент имеет право получать консультации Банка в рамках оказания Услуг.

5.31. Клиент обязан оплачивать услуги Банка ежемесячно, с 01 по 15 число, согласно действующим тарифам.

6. ПРАВА И ОБЯЗАННОСТИ БАНКА

6.1. Банк обязан обладать техническим оборудованием, необходимым для эксплуатации системы «iBank2» в исправном состоянии и количестве, достаточном для надлежащего обслуживания Клиента, располагать кадрами, необходимыми для работы с Клиентом с использованием системы «iBank2».

6.2. Банк обязан передать Клиенту по запросу необходимую документацию и предоставить рекомендации для работы с системой, а также до заключения договора информировать клиента об условиях использования электронного средства платежа, в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования электронного средства платежа.

Банк обязан размещать на web-странице в Интернете (сайт ПАО КБ "САММИТ БАНК" по адресу http://www.kbsammit.ru информационные материалы, необходимые для работы Клиента с системой «iBank2», в том числе электронный документ «Руководство пользователя РС-Банкинг», «Основы безопасности работы с компьютером», «Защита от фишинга», «Правила безопасной работы в системе iBank2», а также «Инструкция по настройкам SMS сообщений».

6.3. Банк обязан произвести блокирование ключа проверки ЭП Клиента по письменному «Уведомлению об отмене действия Пары ключей ЭП Клиента» (Приложение №5 к настоящему Договору).

6.4. Банк обязан по требованию Клиента зарегистрировать новые ключи проверки ЭП Клиента на основании предоставленного Сертификата ключа проверки ЭП.

6.5. Банк обязан предупредить Клиента о необходимости смены Ключей ЭП не менее чем за 10 дней до даты окончания срока действующих ЭП Клиента.

6.6. Банк обязан по телефонному звонку Клиента после произнесения Клиентом блокировочного слова, впредь до письменного уведомления об отмене, блокировать работу Клиента в системе «iBank2».

6.7. Банк имеет право отказать Клиенту в совершении перевода денежных средств с использованием системы «iBank 2» в следующих случаях:

- возникновения технических неисправностей или других обстоятельств, препятствующих использованию системы «iBank 2»;

- при наличии оснований, указанных в п.11.ст.7 Федерального закона №115-ФЗ от 07.08.2001 «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма»;

- при нарушении оформления ЭД и сроков их предоставления в Банк;

- при задержке Клиентом оплаты услуг Банка по Договору на обслуживание Клиента по системе «iBank 2».

6.8. Банк имеет право запросить у Клиента документы, необходимые для соблюдения требований законодательства РФ в целях предупреждения, выявления и пресечения деяний, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма и не производить исполнение электронного документа Клиента до момента поступления в Банк соответствующих документов.

6.9. В случае возникновения обоснованных подозрений в подлинности электронных документов или возникновения форс-мажорных обстоятельств Банк имеет право затребовать от Клиента оформления платежного документа на бумажном носителе, заверенного необходимыми подписями в соответствии с карточкой с образцами подписей и печатью, и не производить платеж до оформления бумажного документа, о чем Банк обязан сообщить Клиенту не позднее дня получения электронного документа.

6.10. В случае неполучения от Клиента запрашиваемых документов по истечении срока указанного в запросе Банка, после предварительного предупреждения Клиента по системе «iBank 2», Банк блокирует активный ключ ЭП Клиента и принимает для исполнения расчетные документы Клиента только на бумажных носителях (подлинники) с подписью уполномоченных лиц и оттиском печати Клиента.

6.11. Банк вправе расторгнуть настоящий Договор в одностороннем порядке, уведомив Клиента за 10 рабочих дней до даты расторжения, в случае неполучения от Клиента запрошенных документов, по истечении 14-ти дней с момента блокировки активного открытого ключа ЭП Клиента.

6.12. Клиент предоставляет Банку право без дополнительных распоряжений списывать денежные средства с расчетного и иных счетов Клиента в сроки и в размере стоимости предоставляемых Клиенту услуг согласно действующим Тарифам Банка.

6.13. Банк вправе в одностороннем порядке изменять действующие тарифы и/или вводить новые тарифы на оказываемые услуги. Извещение Клиента об изменении действующих и/или введении новых тарифов в рамках данного Договора осуществляется Банком путем размещения информации на информационных стендах в помещениях Банка, web-странице Банка в Интернете (сайт ПАО КБ "САММИТ БАНК" по адресу www.kbsammit.ru) и направления Клиенту соответствующего уведомления по системе «iBank2». Измененные и/или вновь введенные тарифы на услуги Банка вводятся в действие по истечении 10 календарных дней со дня размещения соответствующей информации на web-странице Банка в Интернете (сайт ПАО КБ "САММИТ БАНК" по адресу www.kbsammit.ru), либо с даты, указанной в соответствующем уведомлении Клиента.

6.14. В случае задержки уплаты Клиентом абонентской платы, согласно действующим тарифам Банка, более 14-ти дней Банк вправе, в последний рабочий день месяца, произвести отключение Клиента от системы в одностороннем порядке и расторгнуть договор с Клиентом. При этом повторное подключение к системе «iBank2» производится на следующий день после погашения задолженности Клиентом в полном объеме, если задолженность была погашена в течении месяца с момента отключения Клиента от системы «iBank2». В случае

если задолженность была погашена более чем через месяц после отключения Клиента от системы, для повторного подключения потребуется заключение нового договора (С оплатой по тарифу «Обслуживание клиентов по системе «iBank2»).

6.15. В случае нарушения клиентом своих обязанностей, Банк имеет право произвести блокирование Клиента (ключа проверки ЭП Клиента) без предварительного уведомления до момента устранения нарушения.

6.16. Банк обязан оказывать Клиентам Услугу(и) «SMS информирование», «Одноразовый пароль на вход в «iBank2», «Дополнительное подтверждение платежных документов», «Фильтрация IP адресов» согласно их заявлениям на подключение по форме Приложение №7 к настоящему Договору.

6.17. Банк обязан подключить/отключить Услугу(и) «SMS информирование», «Одноразовый пароль на вход в «iBank2», «Дополнительное подтверждение платежных документов», «Фильтрация IP адресов» на основании предоставленого Клиентом соответствующего Заявления в произвольной форме.

6.18. Банк не несет ответственность, в том числе и перед третьей стороной в случае указания Клиентом при подключении/настройки Услуг(и) «SMS информирование», «Одноразовый пароль на вход в «iBank2», «Дополнительное подтверждение платежных документов» неверного номера мобильного телефона или адреса электронной почты.

7. СОВМЕСТНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

7.1 Банк не несёт ответственность за ущерб, причинённый Клиенту в результате использования третьими лицами ключа ЭП Клиента.

7.2 При расторжении настоящего Договора Стороны несут ответственность по всем ранее сформированным электронным документам с электронными подписями Клиента в системе «iBank2» в соответствии с действующим законодательством РФ.

7.3 В случае возникновения конфликтных ситуаций между Клиентом и Банком при использовании системы «iBank2» Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Процедурой проведения технической экспертизы при возникновении спорных ситуаций» (Приложение №3 настоящего Договора), выполнять требования данной Процедуры и следовать выводам по рассмотрению конфликтной ситуации.

7.4 Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием системы «iBank2», предоставлять в письменном виде свои оценки, доказательства и материалы по запросу заинтересованной Стороны, участвующей в настоящем Договоре.

7.5 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 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. Сторона, пострадавшая от их влияния, обязана сообщить другой Стороне о случившемся в срок не позднее 30 дней с момента возникновения этих обстоятельств.

8. ПОРЯДОК ОБСЛУЖИВАНИЯ КЛИЕНТА

8.1. Банк осуществляет прием документов, передаваемых по системе «iBank 2», с 8.30 ч. до 17:30 ч. местного времени. При невозможности передачи документов в Банк с использованием системы «iBank 2», документы могут поступить от Клиента в виде подлинника на бумажном носителе, оформленные надлежащим образом..

8.2. Документы, поступившие до 17:00 ч., Банк принимает к исполнению в тот же день; документы, поступившие с 17:00 ч. до 17:30 ч.- на следующий рабочий день. Документы, поступившие в Банк после 17:30 ч. – не принимаются к исполнению.

8.3. Клиент поручает Банку дальнейшее оформление платежных документов, переданных в Банк по системе «iBank 2».

8.4. При получении электронных документов от Клиента Банк производит проверку корректности ЭП Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчётном счёте Клиента, о чем информируется Клиент по системе «iBank2».. В случае отбраковки документ к обработке Банком не принимается.

8.5. ЭД считается принятым Банком к исполнению после присвоения ему в системе «iBank 2» статуса «На исполнении».

8.6. При недостаточности денежных средств на счете Клиента для исполнения всех предъявленных к нему требований списание денежных средств осуществляется в очередности в соответствии со ст.855 ГК РФ.

8.7. При наличии у Клиента расчетного (текущего) счета выписки по счетам, дебетовые и кредитовые приложения по проведенным операциям предоставляются Клиенту в электронном виде посредством

системы «iBank2» с отметками Банка об исполнении документов без последующего их предоставления на бумажных носителях, за исключением документов по кассовым операциям и иных первичных документов, получение которых по системе «iBank2» не представляется возможным (требования кредиторов, налоговых органов и т.п.).

9. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СИСТЕМЕ «IBANK2» И СТОИМОСТЬ РАБОТ

9.1. Для подключения к системе «iBank2» Клиент предоставляет в Банк Заявление о присоединении установленной формы (Приложение №1 к настоящему Договору) в одном экземпляре и обеспечивает технические, программные и коммуникационные ресурсы, необходимые для работы с системой, в том числе:

- персональный компьютер, совместимый с IBM PC с параметрами: Pentium 133 или выше, объем ОЗУ 512 Мб или выше; объем свободной памяти на жестком диске 500 Мб или выше; операционная система Windows XP или выше (а как же Linux и MacOS), поддерживающая Sun Java Plugin;
- подключение к сети Internet;
- принтер.

9.2. Клиент оплачивает услуги по подключению к системе «iBank2», получает Ключевой носитель по Акту (приложение № 8 к настоящему Договору), действует согласно инструкции по установке, опубликованной на сайте банка.

9.3. Клиент самостоятельно выполняет загрузку, установку и настройку программного обеспечения необходимого для работы в системе «iBank2» (Java – машина, драйвер USB-токена, АРМ пользователя) и производит предварительную регистрацию в системе, осуществляет генерацию ключей ЭП в соответствии с полученными инструкциями и предоставляет в Банк два заполненных экземпляра «Сертификата ключа проверки ЭП Клиента» (Приложение №2 к настоящему Договору) на каждую пару ключей, распечатанные после генерации.

9.4. Банк производит окончательную регистрацию Клиента в системе «iBank2».

9.5. Началом оказания услуг считается дата начала действия первого Ключа проверки ЭП Клиента в Банке.

9.6. С даты начала действия первого Ключа проверки ЭП Клиента в Банке Клиент ежемесячно оплачивает обслуживание по настоящему Договору согласно действующим Тарифам Банка.

9.7. С даты начала действия первого Ключа проверки ЭП Клиента в Банке расчет абонентской платы за пользование системой «iBank2» производится за полный календарный месяц.

9.8. В случае если настоящий договор будет расторгнут по инициативе Клиента в период, за который Клиент произвел оплату услуг Банка в виде абонентской платы за очередной месяц, возврат Банком перечисленных сумм не производится.

9.9. Услуга(и) «SMS информирование», «Одноразовый SMS пароль на вход в «iBank2», «Дополнительное подтверждение платежных документов» доступна(ы) Клиентам по активным счетам подключенным к системе «iBank2».

9.10. При подключении услуги «SMS информирование» в системе «iBank2» Клиент самостоятельно производит настройку рассылки SMS/email сообщений согласно инструкции, а также выбор и детализацию событий, о которых хочет получать сообщения. Одно SMS уведомление может состоять из нескольких SMS сообщений.

9.11. Сообщения направляются Клиенту в виде SMS сообщений на мобильный номер телефона оператора связи, действующего на территории РФ, либо на адрес электронной почты.

9.12 Банк не несет ответственности за время доставки SMS, ответственность лежит на операторе, предоставляющем услугу.

9.13 Услуги «SMS информирование», «Одноразовый SMS пароль на вход в «iBank2», «Дополнительное подтверждение платежных документов» предоставляются круглосуточно, 7 дней в неделю.

9.14 Если система «iBank2» заблокирована по какой-либо причине, но при этом услуга «SMS информирование» активна (при условии, что у пользователя подключено событие «О движении по счету»), пользователю будут поступать соответствующие SMS/email уведомления**.**

10. РАЗРЕШЕНИЕ СПОРОВ

10.1. Споры и разногласия, возникающие в связи с настоящим Договором, разрешаются Сторонами путем переговоров, результаты которых оформляются Протоколом согласований.

10.2. Если Стороны не достигли соглашения путем переговоров, споры по настоящему Договору передаются на разрешение в Арбитражный суд Приморского края.

11. СРОКИ И УСЛОВИЯ ДЕЙСТВИЯ ДОГОВОРА

11.1. Настоящий Договор вступает в силу с момента подписания Сторонами Заявления о присоединении (Приложение №1 к настоящему Договору) установленной формы и заключается на неопределенный срок.

11.2. Договор может быть расторгнут по требованию любой из Сторон.

11.3. В случае расторжения Договора по инициативе Банка, последний направляет письменное уведомление Клиенту (при возможности по системе «iBank2»), прекращает прием и исполнение электронных документов, передаваемых от имени Клиента при помощи системы. Договор считается расторгнутым с даты и времени, указанных в уведомлении.

11.4. В случае расторжения Договора по инициативе Клиента последний передает в Банк письменное уведомление о расторжении Договора составленное в произвольной форме либо по форме согласно Приложения № 6 к настоящему Договору. Договор считается расторгнутым по инициативе Клиента с даты, указанной в уведомлении, а при ее отсутствии – с момента регистрации в Банке уведомления Клиента о расторжении Договора.

11.5. Настоящий договор прекращает свое действие без каких-либо дополнительных уведомлений и/или извещений между Сторонами в следующих случаях:

- в случае расторжения Клиентом последнего «Договора банковского счета в валюте РФ/иностранной валюте» или иного договора, предусматривающего использование системы «iBank2»;
- в случае неоплаты или неполной оплаты услуг Банка до окончания текущего месяца.

11.6. При расторжении Договора Клиент обязуется уничтожить или передать в Банк все принадлежащие ему конфиденциальные документы, ключи ЭП, относящиеся к настоящему Договору, и не передавать их третьим лицам.

12. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

12.1. Все возникшие вопросы при реализации настоящего Договору решаются путем переговоров с учетом взаимных интересов в соответствии с «Процедурой проведения технической экспертизы при возникновении спорных ситуаций» (Приложение №3 настоящего Договора), а при не достижении соглашения - в судебном порядке.

12.2. При изменении реквизитов Стороны обязуются своевременно уведомлять об этом друг друга путем направления по системе «iBank2» соответствующего уведомления в виде информационного документа (письма), защищенного ЭП.

12.3. Ни одна из Сторон не может передавать свои права и обязательства по Договору третьей Стороне без письменного согласия на то другой Стороны.

12.4. Банк вправе в одностороннем порядке вносить изменения в настоящий Договор.

12.5. Для вступления в силу изменений, внесенных в договор, Банк обязан опубликовать информацию об изменениях на информационных стендах в помещениях Банка и сайте ПАО КБ “САММИТ БАНК” по адресу www.kbsammit.ru).

12.6. Изменения Договора вступают в силу по истечении 10 календарных дней с даты опубликования Банком информации, либо с даты вступления изменений в силу, если такая дата указана в опубликованной информации, но не ранее 10 календарных дней с даты опубликования информации.

12.7. Клиент обязан не реже одного раза в 10 дней знакомиться с информацией, публикуемой Банком.

12.8. Банк не несет ответственности, если с информацией об изменении условий Договора, опубликованной в порядке и в сроки, установленные настоящими Договором, не был ознакомлен Клиент.

ЮРИДИЧЕСКИЙ АДРЕС И РЕКВИЗИТЫ БАНКА

ПАО КБ «САММИТ БАНК»

Адрес местонахождения Банка: 690106, г. Владивосток, проспект Красного Знамени, 3
ИНН 2503001251 КПП 254001001 ОГРН 1022500001930
Платежные реквизиты: БИК 040507840,
кор.счет № 30101810905070000840 в Дальневосточном ГУ Банка России
Телефон / факс 8(423) 246-83-12, 246-83-10

Приложение № 1
к Договору на использование
электронного средства платежа в системе «iBank2»
№____- ib от «___» _____ 201__ года

От:_____
_____
(полное / сокращенное наименование Клиента,
ФИО индивидуального предпринимателя, адвоката, нотариуса)

ЗАЯВЛЕНИЕ О ПРИСОЕДИНЕНИИ
к Договору на использование электронного средства платежа в системе «iBank2»

Настоящим заявляем о присоединении к Договору на использование электронного средства платежа в системе «iBank2», в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, условий Договора на использование электронного средства платежа в системе «iBank2», являющегося Договором присоединения, принимаем на себя обязательства следовать положениям и условиям Договора на использование электронного средства платежа в системе «iBank2», подтверждаем, что все положения (условия) действующей в ПАО КБ "САММИТ БАНК" редакции Договора на использование электронного средства платежа в системе «iBank2», размещенного на веб-сайте ПАО КБ "САММИТ БАНК" по адресу: www.kbsammit.ru, ему известны и разъяснены в полном объеме (включая все приложения и дополнения к нему, порядок внесения изменений и дополнений, порядок опубликования информации, ответственность и Тарифы Банка).

Банк осуществляет обслуживание счета (счетов) с использованием системы «iBank2», позволяющей осуществлять платежи, отправлять информационные сообщения и получать выписки.

Банк информирует Клиента о совершении каждой операции с использованием ЭСП путем предоставления:

- уведомления в виде SMS сообщения на телефонный номер +7 | | | | | | | | | | | и/или
- сообщения электронной почты _____.

Настоящее заявление о присоединении является приложением к Договору на использование электронного средства платежа в системе «iBank2» заключенному Сторонами.

Ответственными представителями Сторон для контроля и решения организационно-технических вопросов по настоящему Договору являются:

от Банка:

специалисты Отдела автоматизации - **8 (423) 246-83-12**
специалисты Учетно-операционного отдела - **8 (423) 246-83-04**

от Клиента: _____
(ФИО, контактный телефон, e-mail)

Руководитель: _____ _____ «____» _____ 201_ г.
Подпись *Ф.И.О*

М.П.

Заполняется Банком
Отметка сотрудника Банка, принявшего заявление:_____/_____
Подпись *Ф.И.О.*
«____» _____ 201_ г.

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО**:** _____ /_____
Подпись *Ф.И.О.*
«____» _____ 201__ г.

Договор на использование электронного средства платежа в системе «iBank2»

№ _____-ib от «_____» _____ 201__ г.

Уполномоченный представитель
ПАО КБ «САММИТ БАНК»: _____ _____
Подпись *Ф.И.О*

М.П.

Форма сертификата. Распечатывается при формировании ключа ЭП сотрудника клиента в двух экземплярах

Приложение N 2
к Договору на использование электронного средства платежа в системе "iBank2"
N_____ от "____"_____20___г.

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА
В СИСТЕМЕ "iBank 2"
ПАО КБ "САММИТ БАНК"

1. Наименование организации ООО "ТЕСТОВЫЙ"

2. Место нахождения юр. лица 690001 Приморский край, г. Владивосток, ул. Первая, 1

3. ОГРН* 1022500123456 дата внесения в ЕГРЮЛ (ЕГРИП)* "____" _____ года
4. Тел. +7 999 888 77 66 5. ИНН (КИО) 2543111251 6. КПП* 254301001
7. Факс* +7 999 888 77 66 8. E-mail* abcde@xxxxx.ru
9. Сведения о владельце ключа
Фамилия, имя, отчество Иванов Иван Иванович
Должность Генеральный директор
Документ, удостоверяющий личность Паспорт гражданина РФ
серия 0500 номер 123456 дата выдачи "05" апреля 2001 года
кем выдан ОВД г. Артем Приморского края
10. Примечания*

* необязательно для заполнения

Настоящим подтверждаю согласие на обработку банком моих персональных данных _____
подпись

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа проверки ЭП 14062487683623469 Идентификатор устройства 86F5431A681177
Наименование криптосредств USB-токен "iBank 2 Key" (СКЗИ "Криптомодуль С")
Алгоритм ГОСТ Р 34.10-2001 ID набора параметров алгоритма 1.2.643.2.2.35.1
Дата начала действия "____" _____ 201__ г. (заполняется банком)
Дата окончания действия "____" _____ 201__ г. (заполняется банком)
Представление ключа проверки ЭП в шестнадцатеричном виде

```
7D 2E 8B 76 2F A3 77 ED 6A 28 61 99 C5 D5 36 CD
E2 E9 A8 10 EA D5 88 B1 A1 9D 7C 10 84 65 BE 6D
B6 65 20 71 31 1E EE 51 2B EB 39 76 07 ED FA 77
9C 49 25 36 97 D8 EC 46 18 DD 2E 3A ED 15 E9 33
```

Личная подпись владельца ключа проверки ЭП

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках договора на обслуживание по системе "iBank 2" N _____ от "_____" _____ 20__ г.

Достоверность приведенных данных подтверждаю

Руководитель организации
_____ / Иванов И.И. /
подпись Ф.И.О.

Оттиск печати

Уполномоченный представитель банка
_____ / _____ /
подпись Ф.И.О.

Оттиск печати Банка

Дата приема сертификата ключа проверки ЭП
"___" _____ 20___ г.

Администратор безопасности системы
_____ / _____ /
подпись Ф.И.О.

Оттиск печати

Дата регистрации сертификата ключа проверки ЭП
"___" _____ 20___ г.

Приложение № 3
к Договору на использование электронного
средства платежа в системе «iBank2»

ПРОЦЕДУРА ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ ВОЗНИКНОВЕНИИ СПОРНЫХ СИТУАЦИЙ

1. В настоящем Разделе под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть установлена только по результату проверки электронных подписей Клиента под электронным документом.
2. Клиент представляет Банку заявление, содержащее существо претензии со ссылкой на электронный документ, на основании которого Банк выполнил операции по счёту Клиента.
3. Банк обязан в течение пяти рабочих дней от даты подачи заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии должно входить равное количество представителей от Клиента и Банка. При необходимости, с письменного согласия обеих Сторон, в состав комиссии могут дополнительно введены независимые эксперты. Выбор членов комиссии осуществляется по согласованию Сторон.
4. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение истинности электронных подписей Клиента под спорным документом.
5. Разрешительная комиссия в срок не более пяти рабочих дней проводит рассмотрение заявления. В исключительных ситуациях этот срок может быть увеличен по взаимной договоренности Сторон. Рассмотрение заявления включает следующие этапы:
   5.1. Разрешительная комиссия проводит техническую экспертизу электронного документа, на основании которого Банком выполнены оспариваемые Клиентом действия с его счетом.
   5.2. Разрешительная комиссия проводит техническую экспертизу ключей проверки ЭП Клиента:
   - С использованием штатного программного обеспечения Системы «iBank» АРМ «Операционист» выполняется распечатка Сертификата ключа проверки ЭП Клиента. По согласованию сторон печатная форма сертификата может быть получена с использованием ПО АРМ «Администратор».
   - Распечатанный сертификат сверяется с Сертификатом ключа проверки ЭП Клиента, заверенным подписью уполномоченного лица Клиента и являющимся приложением к договору. Сверяются ID ключа и его шестнадцатеричное представление.
6. Разрешительная комиссия проводит техническую экспертизу подлинности ЭП Клиента в Электронном документе:
   6.1. С использованием штатного программного обеспечения Системы «iBank2» АРМ «Операционист» выбирается документ и выполняется операция «Проверить ЭП». При необходимости, комиссией также могут использоваться специализированные утилиты разработчика Системы «iBank2» для выгрузки документа из Базы данных Системы «iBank2» и автономной проверки.
   6.2. На основании данных технической экспертизы разрешительная комиссия составляет акт, содержащий**:**
   - обстоятельства, послужившие основанием возникновения разногласий;
   - порядок работы членов комиссии;
   - вывод о подлинности ЭП в оспариваемом Электронном документе и его обоснование.
7. Банк несет ответственность перед Клиентом в случае, когда имело место хотя бы одна из следующих ситуаций:
   - Банк не предъявляет электронного документа, переданного Клиентом, на основании которого Банк выполнил операции по счёту Клиента;
   - ID ключа и/или шестнадцатеричное представление распечатанного сертификата ключа проверки ЭП Клиента, который хранится в Банке, отличается от сертификата ключа проверки ЭП Клиента, заверенным подписью уполномоченного лица Клиента и являющимся приложением к договору;
   - Хотя бы одна электронная подпись Клиента в электронном документе оказалась некорректной;
   - Клиент предоставляет «Уведомление об отмене действия Пары ключей ЭП Клиента», подписанное должностным лицом Банка и имеющим оттиск печати Банка. При этом указанная в Уведомлении дата блокировки действия ключа проверки ЭП Клиента раньше даты, указанной в рассматриваемом электронном документе.
8. Банк не несет ответственность перед Клиентом в случае, если Банк предъявляет электронный документ с корректными электронными подписями Клиента и принадлежность ключей проверки ЭП Клиента подтверждена.

Руководитель: _____ _____ «____» _____ 201_ г.
Подпись *Ф.И.О*

М.П.

Приложение № 4
к Договору на использование электронного
средства платежа в системе «iBank2»

Правила хранения и использования ключевых носителей

1. Правила хранения и использования ключевых носителей (далее – электронного ключа) должны исключать возможность несанкционированного доступа.

2. Ключевой носитель для применения в системе «iBank2» руководитель Клиента лично или его представитель по доверенности получает в Банке.

3. По окончании рабочего дня, а так же вне времени сеансов связи электронный ключ должен храниться в сейфе или другом хранилище, исключающем несанкционированный доступ.

4. Во время работы должен быть исключен доступ к электронному ключу неуполномоченных лиц.

5. Хранение USB-токена, содержащего электронный ключ, допускается в одном хранилище с другими документами, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц.

6. Не допускается:
- изготавливать несанкционированные копии с электронного ключа;
- знакомить или передавать электронный ключ лицам, к ним не допущенным;
- вставлять ключ в компьютер в режимах, не предусмотренных функционированием системы;
- разбирать электронный ключ.

7. Необходимо оберегать USB-токен, содержащий электронный ключ, от механических воздействий (ударов, падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения сильных магнитных, электрических или радиационных полей — все это может привести к его поломке.

8. Важно не прилагать излишних усилий при подсоединении USB-токена к порту компьютера, не допускать попадания на USB-токен (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема нужно принять меры для их очистки. Для очистки корпуса и разъема устройства необходимо использовать сухую безворсовую ткань. Использование растворителей и моющих средств недопустимо.

9. Не допустимо разбирать устройство! Помимо того, что при этом будет утрачена гарантия на устройство, такие действия могут привести к поломке корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие — к ненадежной работе или выходу из строя самого USB-токена.

10. Разрешается подключать USB-токен только к исправному оборудованию. Параметры USB-порта должны соответствовать спецификации для USB.

11. Не рекомендуется использовать длинные переходники или USB-хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для USB-токена или считывателя смарт-карт, может подаваться несоответствующее напряжение.

12. Запрещается извлекать USB-токен из порта компьютера, если на нем мигает индикатор, поскольку это обозначает работу с данными, и прерывание работы может негативно сказаться как на данных, так и на работоспособности устройства (ЗА ИСКЛЮЧЕНИМ СЛУЧАЕВ ПОДОЗРЕНИЯ НА КОМПРОМЕТАЦИЮ КЛЮЧА).

13. Запрещается оставлять устройство подключенным к компьютеру во время включения, выключения, перезагрузки, перехода в «ждущий» или «спящий» режимы, поскольку в это время возможны перепады напряжения на USB-порте и, как следствие, выход устройства из строя.

14. Не рекомендуется оставлять устройство подключенным к компьютеру, когда он не используется.

Руководитель: _____ _____ «____» _____ 201_ г.
Подпись *Ф.И.О*

М.П.

Приложение № 5
к Договору на использование электронного
средства платежа в системе «iBank2»

УВЕДОМЛЕНИЕ
об отмене действия пары ключей ЭП Клиента

Настоящим_____
_____(КЛИЕНТ)
уведомляет ПАО КБ «САММИТ БАНК» о том, что с «____» _____ 201_ г. считать недействительным ключ ЭП Клиента в связи с _____:

ФИО Владельца ключа ЭП _____
Идентификатор ключа проверки ЭП _____
Дата начала действия сертификата ключа проверки ЭП "____"_____ 201___г.
Дата окончания действия сертификата ключа проверки ЭП "____"_____ 201___г.

Соответствующий ему ключ проверки ЭП Клиента утрачивает силу для дальнейшего применения.

Руководитель: _____ _____ «____» _____ 201_ г.
Подпись *Ф.И.О*

М.П.

Заполняется Банком

Отметка сотрудника Банка, принявшего заявление: _____/_____
Подпись *Ф.И.О.*

«____» _____ 201_ г. в _____час. ____ мин.

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО:

«____» _____ 201_ г. в _____ час. ____ мин. _____/_____
Подпись *Ф.И.О.*

Ключ проверки ЭП Клиента блокирован в системе «iBank2» с «____» _____ 201_ г. . в _____час. ____ мин.

Администратор безопасности системы _____/_____
Подпись *Ф.И.О.*

«____» _____ 201_ г. в _____час. ____ мин.

Уполномоченный представитель
ПАО КБ «САММИТ БАНК»: _____ _____
Подпись *Ф.И.О*

М.П.

Приложение № 6
к Договору на использование электронного
средства платежа в системе «iBank2»

Уведомление
о расторжении Договора на использование электронного средства платежа в системе «iBank2»

Настоящим_____
_____
_____(КЛИЕНТ)

уведомляет ПАО КБ «САММИТ БАНК» о расторжении Клиентом Договора на использование электронного средства платежа в системе «iBank2»
№ ____ ib от «___» _____ 201_ г. с «___» _____ 201_ г.

Руководитель: _____ _____ «____» _____ 201_ г.
Подпись *Ф.И.О*

М.П.

Заполняется Банком

Отметка сотрудника Банка, принявшего заявление: _____/_____
Подпись Ф.И.О.

«____» _____ 201_ г.

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО:

«____» _____ 201_ г. в _____час. ____ мин. _____/_____
Подпись *Ф.И.О.*

Ключ (и) проверки ЭП Клиента блокирован (ы) в системе «iBank2», Клиент переведен в «архивные»

Администратор безопасности системы _____/_____.
Подпись *Ф.И.О.*

«____» _____ 201_ г

Уполномоченный представитель
ПАО КБ «САММИТ БАНК»: _____ _____
Подпись *Ф.И.О*

М.П.

Приложение № 7
к Договору на использование электронного
средства платежа в системе «iBank2»

Заявление о подключении Услуг(и)
«SMS информирование», «Одноразовый SMS пароль на вход в «iBank2», «Дополнительное подтверждение платежных документов в системе «iBank2», «Фильтрация IP адресов»

_____
(Юридическое лицо, индивидуальный предприниматель, адвокат, нотариус)

_____(КЛИЕНТ)

просит ПАО КБ «САММИТ БАНК» подключить Услугу(и):
(отметьте нужное)
☐ ***«SMS информирование»***
☐ ***«Одноразовый SMS пароль на вход в систему «iBank2»***
Указать номер мобильного телефона для получения одноразового пароля:

+7									
+7									

☐ ***«Дополнительное подтверждение платежных документов» на сумму более***

								рублей

Указать номер мобильного телефона для получения одноразового пароля:

+7									
+7									

☐ ***«Фильтрация IP адресов»*** **- список адресов, с которых разрешена работа с системой «iBank2»**
Указать IP адрес или диапазон IP адресов, с которых разрешена работа в системе «iBank2»

			.				.				.			
			.				.				.			
			.				.				.			
			.				.				.			
			.				.				.			
			.				.				.			
			.				.				.			

Ознакомлены и согласны с условиями оказания услуг «SMS информирование», «Одноразовый SMS пароль на вход в «iBank2», Дополнительное подтверждение платежных документов», «Фильтрация IP адресов»

Руководитель: _____ _____ «____» _____ 201_ г.
Подпись *Ф.И.О*

М.П.

Заполняется Банком

Отметка сотрудника Банка, принявшего заявление: _____/_____
Подпись Ф.И.О.
«____» _____ 201__ г.

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО**:** _____/_____
Подпись *Ф.И.О.*
«____» _____ 201__ г.

1.Договор на использование электронного средства платежа в системе «iBank2»
№ ____ ib от «____» _____ 20__г.

Администратор безопасности системы _____ / _____
Подпись *Ф.И.О.*

Уполномоченный представитель
ПАО КБ «САММИТ БАНК»: _____ _____
Подпись *Ф.И.О*

М.П.

Приложение № 8
к Договору на использование электронного
средства платежа в системе «iBank2»

УТВЕРЖДАЮ
Уполномоченный представитель
ПАО КБ «САММИТ БАНК»
_____ /_____ /

М.П.

АКТ
приема-передачи средства криптографической защиты документооборота системы «iBank2».

г. Владивосток

Мы, нижеподписавшиеся: _____ ПАО КБ «САММИТ БАНК»
Должность

_____ с одной стороны
ФИО

и _____
Должность представителя Клиента

_____
Организация Клиента

_____, с другой стороны,
ФИО

составили настоящий акт о том, что ПАО КБ «САММИТ БАНК» передало,

а _____ приняло средство
Организация Клиента

криптографической защиты информации USB-токен «iBank2Key»/TrustScreen для применения в системе «iBank2»

(*нужное подчеркнуть*).

№пп	Средство криптографической защиты информации	Серийный номер
1	USB-токен «iBank2 Key»	
2	TrustScreen	
3		

От клиента

_____ / _____ /
подпись *Ф.И.О.*

«___» _____ 201__ г.

От Банка

_____ / _____ /
подпись *Ф.И.О.*

«___» _____ 201__ г.

Приложение № 9
к Договору на использование электронного
средства платежа в системе «iBank2»

Распоряжение на расторжение Договора на использование электронного средства платежа в системе «iBank2» по инициативе Банка

С «___» _____ 201__ года расторгнуть Договор № ____- ib от «___» _____ 201_ года, на использование электронного средства платежа в системе «iBnank2», заключенный между Банком и _____
_____
_____
(наименование юридического лица, индивидуального предпринимателя)
в соответствие с _____
_____
_____
_____
(причина расторжения Договора)

Уполномоченный представитель
ПАО КБ «САММИТ БАНК»: _____ _____
Подпись *Ф.И.О*

«____» _____ 201_ г. М.П.

Заполняется Банком

Отметка сотрудника Банка, отправившего уведомление Клиенту _____/_____
Подпись *Ф.И.О.*
«____» _____ 201__ г.

Ключ(и) проверки ЭП Клиента блокирован(ы) в системе «iBank2», Клиент переведен в «архивные»
Администратор безопасности системы _____/_____.
Подпись *Ф.И.О.*

«____» _____ 201_ г.