

**АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК
«БАЛТИЙСКИЙ БАНК РАЗВИТИЯ»
(закрытое акционерное общество)**

СОГЛАШЕНИЕ

от «__»__20__г.№_____

(по обслуживанию клиентов - физических лиц по системе «Клиент-Банк»)

г. Санкт-Петербург

«__»__20__г

Акционерный коммерческий банк «Балтийский Банк Развития» (закрытое акционерное общество), именуемый в дальнейшем «Банк», в лице Управляющего Филиалом Акционерного коммерческого банка «Балтийский Банк Развития» (закрытое акционерное общество) в г. Санкт-Петербурге Горцевского Александра Юрьевича, действующего на основании доверенности № 1.1-10-1/226 от 24.07.2009 г, с одной стороны и _____, именуемый в дальнейшем «Клиент», с другой стороны, вместе именуемые Стороны, заключили настоящее Соглашение о нижеследующем

1. Понятия, используемые в настоящем Соглашении

1.1. **Система** – комплекс программных и технических средств, с помощью которых осуществляется формирование, заверение электронно-цифровой подписью (ЭЦП), отправка, прием и проверка на подлинность электронных документов.

1.2. **Электронный документ** – один из следующих документов, которые сформированы в электронном виде с помощью Системы:

- Платежное поручение,
- Документ свободного формата (письмо),
- Иные документы, связанные с проведением валютных операций Клиентом.

Все электронные документы, подписанные ЭЦП, полученные и направленные Сторонами друг другу, хранятся в Системе в течение установленных сроков хранения документов. Просмотр электронного документа и проверка ЭЦП возможны в любое время с терминала Банка. Ни Банк, ни какие-либо третьи лица не имеют возможность вносить изменения в электронный документ, хранящийся в Системе.

1.3. **Электронно-цифровая подпись (ЭЦП)** – аналог собственноручной подписи уполномоченного лица Банка или Клиента, и/или уполномоченного им лица под электронным документом, полученный с использованием секретного (закрытого) ключа ЭЦП, позволяющий идентифицировать владельца сертификата ключа подписи и подтверждающий отсутствие искажения информации в электронном документе. Наличие ЭЦП в электронном документе, полученном по системе Клиент-Банк, является необходимым и достаточным условием, позволяющим установить, что электронный документ исходит от Стороны по Соглашению.

1.4. **Владелец сертификата ключа подписи** – физическое лицо, на имя которого выдан сертификат ключа подписи в соответствии с правилами настоящего соглашения.

1.5. **Технические средства** – IBM-совместимый персональный компьютер, необходимые телекоммуникационные средства для передачи электронных документов.

1.6. **Программные средства** – программное обеспечение, с помощью которого выполняются установленные настоящим Соглашением процедуры формирования, отправки и приема электронных документов, а также формирование и проверка ЭЦП (экземпляр модуля *Inter-PRO Client*). Банк обладает правом на передачу экземпляра программного обеспечения на основании Договора №СО-292-04 от 22.12.2004 с ЗАО «Сигнал-КОМ». По окончании действия настоящего соглашения у Клиента прекращается право пользования программными средствами).

1.7. **Ключи ЭЦП** – пара ключей (открытый и секретный (закрытый)), с помощью которых осуществляется формирование и проверка ЭЦП. Секретный ключ должен храниться только у владельца сертификата ключа подписи и используется для формирования ЭЦП, а открытый ключ служит для проверки ЭЦП и передается Стороне, получающей электронные документы, заверенные ЭЦП. Клиент и Банк обеспечивают хранение в тайне владельцами сертификатов ключей подписи своих секретных ключей и обмениваются друг с другом открытыми ключами ЭЦП лиц, уполномоченных подписывать электронные документы от имени каждой из Сторон настоящего Соглашения. По известному открытому ключу невозможно восстановить парный ему секретный ключ.

1.8. **Сертификат ключа подписи** - электронный файл содержащий заверенные ЭЦП уполномоченного лица Банка идентификационные данные и открытый ключ владельца сертификата открытого ключа подписи – Клиента и/или уполномоченного им лица. Сертификат ключа создается на основании Запроса на Сертификат и Заявления на Сертификат по форме Приложения № 2 к настоящему Соглашению, предоставляемого Клиентом в Банк. Сертификат ключа Клиента необходим для проверки его ЭЦП и должен находиться в Банке. Сертификаты (в том числе утратившие силу) хранятся в Системе в период действия Договоров, указанных в Приложении № 4 к настоящему Соглашению, а также в течение не менее чем трех лет после прекращения указанных Договоров. При изготовлении Банком Сертификата ключа подписи в виде электронного файла Банком также оформляется два экземпляра сертификата ключа подписи на бумажных носителях по форме Приложения № 3 к настоящему Договору, которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица Банка. Один экземпляр выдается владельцу сертификата ключа подписи, второй – остается в Банке.

1.9. **Запрос на Сертификат** - электронный файл, создаваемый в процессе генерации ключей ЭЦП и содержащий «открытый» ключ ЭЦП Клиента и/или его уполномоченного лица и полные идентификационные данные этого лица (ФИО, должность, данные документа, удостоверяющего личность Клиента или уполномоченного им лица).

1.10. **Заявление на Сертификат** – документ на бумажном носителе, подписанный Клиентом и/или уполномоченным им лицом, составленный по форме Приложения № 2 к настоящему Соглашению содержащий сведения, необходимые для идентификации владельца сертификата ключа подписи, к Заявлению в обязательном порядке, если не было представлено ранее, должна быть приложена копия доверенность на распоряжение счетом Клиента с указанием срока полномочий, если таковой имеется, заверенная в установленном законом порядке, а также запрос на Сертификат в электронном виде.

1.11. **Договор(ы)** – договор(ы) банковского счета (вклада), к которым применяются правила настоящего Соглашения, указанные в Приложении № 4 к настоящему Соглашению.

1.12. **USB-ключ MS_key (USB-ключ)** – специализированное аппаратное устройство с интерфейсом Universal Serial Bus (USB), предназначенное для хранения сгенерированных секретных ключей ЭЦП и формирования ЭЦП под документами при осуществлении электронного документооборота между Клиентом и Банком в системе «Клиент-Банк». Выдается Клиенту (лицу, уполномоченному Клиентом) с взиманием с Клиента платы в соответствии с действующими на дату оказания услуг тарифами Банка. Применяемая в USB-ключе технология генерации и хранения секретного ключа ЭЦП и формирования ЭЦП под документом полностью исключает возможность получения прямого доступа к секретному ключу ЭЦП с целью его копирования, переноса на внешний носитель или использования для формирования ЭЦП вне USB-ключа. Использование USB-ключа принципиально исключает возможность хищения секретного ключа ЭЦП отдельно от хищения самого USB-ключа.

1.13. **PIN-код** – пароль доступа к USB-ключу.

2. Предмет Соглашения

2.1. Настоящее Соглашение устанавливает процедуру использования электронных документов в процессе отношений, возникающих между Сторонами при исполнении договора(ов) банковского счета (вклада), указанного(ых) в Приложении № 4 к настоящему Соглашению (далее – Договоры).

2.2. Обязанность Сторон осуществлять прием и исполнение электронных документов наравне с аналогичными документами, переданными на бумажном носителе, возникает с момента подписания Акта по форме Приложения № 7.

2.3. Возможность направления Клиентом распоряжений в электронной форме в порядке, установленном настоящим Соглашением, не исключает обязанности Банка по приему распоряжений Клиента на бумажном носителе.

2.4. Стороны признают юридическую силу ЭД, подписанных ЭЦП (при положительном результате проверки ЭЦП) и оформленных в соответствии с требованиями действующего законодательства Российской Федерации, равной юридической силе документов на бумажном носителе, оформленных в соответствии с требованиями действующего законодательства Российской Федерации.

2.5. Система используется для работы со счетами Клиента указанными в Приложении № 4.

3. Порядок формирования и обмена электронными документами

3.1. Формирование ключей ЭЦП и Сертификата ключа подписи.

Банк передает Клиенту инструкцию по формированию ключей ЭЦП, программное обеспечение для формирования ключей ЭЦП и обмена документами, а также, в соответствии с п.1.12. Соглашения, USB-ключ, инструкцию по работе с USB-ключом. Передача осуществляется на электронном носителе

либо по электронным каналам связи, доступным для Клиента. USB-ключ выдается в Банке непосредственно Клиенту или его представителю при предъявлении в Банк оформленной надлежащим образом доверенности, составленной по форме Приложения № 5 к настоящему Соглашению. Для каждой ЭЦП рекомендуется использовать отдельный USB-ключ. В подтверждение передачи инструкции по формированию ключей ЭЦП, программного обеспечения для формирования ключей ЭЦП и обмена документами, USB-ключей, инструкции по работе с USB-ключом и Стороны подписывают Акт передачи программных средств по форме Приложения № 1 к настоящему Соглашению.

Клиент, посредством переданного ему программного обеспечения, формирует ключи ЭЦП (секретный и открытый) и Запрос на Сертификат. Не позднее рабочего дня, следующего за днем формирования Клиентом ключей и Запроса на Сертификат, Клиент передает в Банк Запрос на Сертификат. Передача Запроса на Сертификат осуществляется на электронном носителе с одновременной передачей на бумажном носителе Заявления на Сертификат, заверенного подписью Клиента и/или уполномоченного им лица.

Банк в течение двух рабочих дней с момента получения Запроса на Сертификат и Заявления на сертификат, при условии наличия на расчетном счете Клиента достаточного количества денежных средств для оплаты предоставляемых услуг, согласно Тарифам Банка, осуществляет регистрацию владельца сертификата ключа в Системе, обрабатывает Запрос на Сертификат, создавая, таким образом, Сертификат ключа подписи. В результате создания Сертификата ключа подписи Банк получает возможность использовать открытый ключ для проверки подлинности ЭЦП Клиента и/или уполномоченного им лица – владельца Сертификата ключа подписи. Два экземпляра Сертификата ключа подписи на бумажном носителе заверяются собственноручными подписями владельца Сертификата ключа подписи – Клиента и/или уполномоченного им лица, уполномоченного лица Банка и банковской печатью. Один экземпляр выдается владельцу Сертификата ключа подписи, второй – остается в Банке.

В подтверждение обмена открытыми ключами подписей Стороны подписывают Акт обмена электронными ключами по форме Приложения № 7 к настоящему Соглашению.

3.2. Формирование ЭЦП и проверка подлинности ЭЦП.

Клиент, сформировавший электронный документ, подписывает его с помощью своей ЭЦП и/или ЭЦП уполномоченного им лица, используя программу формирования/проверки ЭЦП и секретные ключи владельцев (владельца) ключей подписи.

При получении подписанных электронных документов Банк проверяет подлинность ЭЦП при помощи программы формирования/проверки ЭЦП и «открытого» ключа Клиента.

3.3. Поступившие в Банк электронные документы Клиента, принимаются Банком к исполнению (или к сведению, если документ не является распоряжением Клиента) в сроки, установленные Договорами, при условии, что проверка на подлинность ЭЦП дала положительный результат, документ оформлен правильно, не противоречит действующему законодательству Российской Федерации и нормативным актам Банка России.

Все исполненные Банком электронные документы Клиента распечатываются, на них проставляются отметки Банка, и после проведения операций по счету Клиента помещаются в документы дня Банка, снабженные штампом Банка, выполненным программным путем и личной подписью сотрудника Банка.

Банк по требованию Клиента предоставляет последнему копии проведенных платежных документов со штампом Банка, выполненным программным путем и заверенных личной подписью сотрудника Банка.

3.4. Поступившие в Банк распоряжения Клиента, проверка подлинности ЭЦП в которых не дала положительного результата, оформленные ненадлежащим образом (не соответствуют действующему законодательству Российской Федерации, нормативным документам Банка России), либо требующие предоставления дополнительных документов для исполнения распоряжения Клиента, не подлежат исполнению Банком, и в течение текущего рабочего дня Клиенту направляется соответствующее сообщение с указанием причины не исполнения.

3.5. Смена ключей ЭЦП.

Клиент обязуется незамедлительно в письменном виде уведомлять Банк о факте утраты владельцами сертификатов ключей подписи ключей ЭЦП. В случае получения такого уведомления, а так же по истечении срока действия сертификата и/или если Банку стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи, в иных случаях установленных нормативно-правовыми актами - Банк аннулирует действие сертификата ключа подписи конкретного владельца сертификата ключа и не принимает электронные документы, подписанные ЭЦП данного конкретного лица от имени Клиента. Производится замена ключей в соответствии с п. 3.1. Соглашения.

4. Порядок формирования и направления электронных документов, исходящих от Банка

4.1. Банк формирует и направляет Клиенту в электронной форме по Системе ежедневные выписки по счетам Клиента и все приложения к ним.

4.2. Документы, указанные в п.4.1 подписываются ЭЦП Банка.

4.3. Формирование открытого и закрытого ключа ЭЦП Банка осуществляется Банком без участия Клиента.

4.4. Проверка подлинности ЭЦП Банка в отношении исходящих от Банка документов осуществляется Клиентом самостоятельно с использованием открытого ключа ЭЦП Банка Сертификат ключа ЭЦП Банка, содержится в направляемых Клиенту сообщениях.

4.5. Повторное получение Клиентом на бумажных носителях ежедневных выписок по счетам Клиента и приложений к ним, а также иных документов, ранее направленных Клиенту Банком в электронной форме по Системе, производится на основании заявления Клиента и подлежит оплате в соответствии с Тарифами Банка

5. Права и обязанности сторон

5.1. При установке и использовании Системы Клиент:

- обязан обеспечить наличие оборудования, программного обеспечения и телекоммуникаций, необходимых для организации автоматизированного рабочего места Клиента и подключения к Системе, в том числе:

- персональный компьютер, совместимый с IBM PC с параметрами: Pentium 133 или выше, объем ОЗУ 32 Мб или выше, объем свободной памяти на жестком диске 80 Мб или выше; операционная система Windows XP/Vista/2000/2003; интернет-браузер Explorer 4.0 или выше;
- наличие USB порта для использования USB-ключа;
- канал Интернет;
- русифицированный принтер;

- обязан соблюдать правила пользования предоставленными ему программными средствами;

- обязан соблюдать инструкцию по работе с USB-ключом;

- обязан подписать Акт по форме Приложения № 1 к настоящему Соглашению;

- получает от Банка посредством Системы выписки по счетам, открытым на его имя в Банке на основании Договоров, и кредитовые приложения, поступающие в Банк в электронном виде;

- обязан знакомиться с выписками, направляемыми ему Банком, в день их предоставления;

- признает, что получение Банком зашифрованных электронных документов, подписанных ЭЦП Клиента и/или ЭЦП уполномоченного им лица, в порядке, установленном настоящим Соглашением, эквивалентно получению документов на бумажном носителе, заверенных подписями Клиента и/или уполномоченного им лица;

- несет риск убытков, связанных с получением третьими лицами несанкционированного доступа к ключам ЭЦП, до момента получения Банком уведомления от Клиента об указанном факте;

- несет риск убытков, связанных с невозможностью передачи электронных документов (неисправности электронной техники, сбой в передаче информации по сети, нарушение программ шифрования электронных документов и т.д.);

- несет риск убытков, связанных с неисполнением электронных документов содержащих распоряжения, в случае несоблюдения правил пользования предоставленными ему программными средствами;

- отвечает за сохранность программного обеспечения, ключей ЭЦП;

- обязан оплачивать Банку повторную установку программного обеспечения, вышедшего из строя из-за не обеспечения Клиентом его сохранности;

- гарантирует оплату услуг Банка, оказываемых в соответствии с настоящим Соглашением в соответствии с действующими на дату оказания услуг тарифами Банка;

- обязан не передавать третьим лицам предоставленное ему Банком программное обеспечение и не оказывать с его использованием услуги в области шифрования третьим лицам.

- обязан хранить полученные в Банке USB-ключи в недоступном для неуполномоченных и посторонних лиц месте и отдельно от PIN-кода;

- обязан не передавать полученные в Банке USB-ключ и PIN-код третьим лицам;
- обязан немедленно информировать Банк о компрометации USB-ключа и/или PIN-кода, в т.ч. их утраты, хищения, несанкционированного использования;
- обязан прекратить использование полученного USB-ключа по требованию Банка, в случае прекращения действия сертификата на встроенные в USB-ключ средств шифрования.

5.2. После предоставления Клиенту пакета программы «Клиент-Банк» Банк:

- обязан передать Клиенту в течение 3-х рабочих дней программное обеспечение, спецификации на оборудование, спецификации на системное программное обеспечение и спецификации на телекоммуникации, необходимые для установки, настройки и функционирования программных средств;
- предоставляет Клиенту в начале каждого операционного дня выписки по его счетам по операциям, совершенным за предыдущий день;
- хранит программное обеспечение в запечатанном конверте на электронных носителях в качестве эталонного образца;
- осуществляет бесплатное обновление программных средств в связи с модернизацией разработчиками их версий;
- не принимает к исполнению документы Клиента в случае их ненадлежащего оформления и/или в случае, если проверка на подлинность ЭЦП дала отрицательный результат;
- имеет право приостанавливать доступ уполномоченных лиц Клиента к Системе в случае не соблюдения ими правил настоящего Соглашения, компрометации USB-ключа и/или PIN-кода, в т.ч. их утраты, хищения, несанкционированного использования до момента обмена новыми открытыми ключами.

5.3. В целях исключения несанкционированного доступа к секретным ключам Стороны обеспечивают сохранение в секрете своих Ключей подписи и Ключей подписи уполномоченных ими лиц.

6. Действия сторон в случае восприятия аналога собственноручной подписи как фальшивой

6.1. В случае если Банк отказывается от приема и исполнения документа, полученного от Клиента, на основании того, что ЭЦП под документом воспринимается как фальшивая, либо при невозможности проверки ЭЦП данного документа, то Банк направляет Клиенту по модему, Интернету, электронной почтой или любым другим способом соответствующее уведомление. Клиент вновь создает электронный документ, подписывает его ЭЦП и направляет Банку.

6.2. Если подпись под вновь предоставленным документом также признается Банком фальшивой (недействительной), либо проверка ЭЦП данного документа невозможна, то, следовательно, нарушена сохранность ключей ЭЦП и/или программных средств, и Стороны осуществляют повторную установку программного обеспечения в порядке, установленном в п.3.1 настоящего Соглашения.

6.3. До восстановления программного обеспечения стороны переходят на расчетное обслуживание в обычном порядке, т.е. путем обмена документами на бумажных носителях.

7. Действия Сторон в случае возникновения разногласий по поводу исполнения /неисполнения электронных документов (досудебный порядок урегулирования споров)

7.1. В случае возникновения разногласий у Сторон по поводу исполнения Банком электронных документов, подпись под которыми была воспринята Банком как подлинная ЭЦП Клиента и/или уполномоченного им лица, а также в случае неисполнения Банком электронных документов, ЭЦП под которыми была воспринята Банком как фальшивая, Стороны урегулируют возникшие разногласия следующим образом.

7.2. Не позднее чем через 10 рабочих дней с момента возникновения разногласий Сторонами создается Согласительная комиссия, в которую входят:

- 2 представителя от Банка, которых Банк обязан назначить в течение 10 рабочих дней с момента возникновения разногласий;
- Клиент и/или его представитель, которого Клиент обязуется назначить в тот же 10-дневный срок;
- эксперт - представитель фирмы-разработчика программы формирования/проверки ЭЦП.

В случае если Клиент уклоняется от принятия участия или не направит своего представителя для участия в работе Согласительной комиссии, то он обязан оплатить услуги эксперта, и лишается права предъявления каких-либо возражений по выводам Согласительной комиссии.

7.3. Согласительная комиссия проверяет идентичность открытого ключа Клиента и/или уполномоченного им лица, хранящегося в Системе, открытому ключу, который хранится в Банке на бумажном носителе, а также осуществляет оценку хранящегося в Системе электронного документа, по поводу исполнения/неисполнения которого возникли разногласия, путем проверки электронного документа в установленном порядке.

7.4. По результатам работы Согласительной комиссией принимается решение простым большинством голосов членов комиссии. Решение комиссии фиксируется в Акте, который составляется и подписывается экспертом. Указанный Акт признается Сторонами в качестве окончательного документа, разрешающего возникшие разногласия.

7.5. Услуги эксперта оплачиваются Сторонами в равных долях. Клиент обязан возместить Банку расходы, связанные с оплатой услуг эксперта в полном объеме в том случае, если Клиент уклонился от участия в Согласительной комиссии или не направил своего представителя для участия в работе Согласительной комиссии.

8. Ответственность сторон

8.1. За неисполнение или ненадлежащее исполнение обязательств, принятых на себя в соответствии с настоящим Соглашением стороны несут ответственность, предусмотренную действующим законодательством Российской Федерации.

8.2. Каждая сторона имеет право требовать от другой стороны возмещения убытков, возникших у нее в связи с несоблюдением другой стороной условий настоящего Соглашения.

8.3. Банк освобождается от ответственности в случаях, если:

- Клиентом допущено несвоевременное оповещение об утрате или раскрытии ключей ЭЦП;
- Клиентом не была обеспечена конфиденциальность хранения ключей, а также программы формирования (проверки) аналогов собственноручных подписей;
- если Клиент не обеспечил сохранность программных средств в процессе их использования, если владелец сертификата ключа подписи нарушил обязательства по хранению и использованию сертификата ключа подписи, установленные законом (ст. 12 Закона РФ «Об электронной цифровой подписи») и принятые им на себя при подписании Заявления на Сертификат ключа подписи (в процессе исполнении настоящего соглашения).

9. Действие, изменение и расторжение Соглашения

9.1. Настоящее Соглашение вступает в действие с момента его подписания сторонами и прекращается одновременно с прекращением действия Договоров банковского счета.

Все ранее подписанные Сторонами Соглашения или любые другие документы, касающиеся предмета настоящего Соглашения, с момента заключения настоящего Соглашения становятся недействительными.

9.2. Права и обязанности по электронным документам, подписанным ЭЦП, возникают при условии наличия на расчетном счете Клиента достаточного количества денежных средств для оплаты предоставляемых услуг, согласно Тарифам Банка и после подписания сторонами Акта по форме Приложения № 7

9.3. Настоящее Соглашение может быть также расторгнуто:

9.3.1. в одностороннем порядке любой из сторон в связи с отказом от использования Системы «Клиент-Банк» в отношениях с другой стороной с письменным предупреждением другой стороны не менее, чем за 10 рабочих дней до даты расторжения.

9.3.2. в одностороннем порядке Банком в случае нарушения Клиентом правил обмена электронными документами и обеспечения безопасности, предусмотренных настоящим Соглашением и законодательством Российской Федерации.

- при наличии задолженности Клиента по ежемесячной абонентской плате за пользование более трех месяцев;

9.3.3. по соглашению Сторон.

9.4. В случае расторжения настоящего Соглашения без расторжения Договоров, платежные документы Клиента принимаются Банком на бумажных носителях на общих основаниях.

9.5. Банк вправе отказать в исполнении электронных платежных документов (приостановить обслуживание Клиента по Системе «Клиент-Банк») без расторжения настоящего Соглашения при проведении Клиентом сомнительных операций либо при наличии оснований полагать, что система «Клиент-Банк» используется неуполномоченными (неизвестными) лицами.

9.5.1. Решение о приостановлении операций принимается Банком по его внутренним правилам, которые Клиенту не сообщаются.

9.5.2. О приостановлении обслуживания по Системе «Клиент-Банк» Банк немедленно уведомляет Клиента по телефону, по Системе «Клиент-Банк», а также направляет в адрес Клиента уведомление заказным письмом.

9.5.3. В случае предоставления Клиентом информации и документов либо совершения иных действий (включая прибытие в Банк), которые позволят устранить сомнения, послужившие основаниями для приостановления обслуживания, Банк возобновляет обслуживание Клиента по Системе "Клиент-Банк".

9.5.4. Банк не несет перед Клиентом ответственности за приостановление обслуживания по системе «Клиент-Банк», предусмотренное настоящим пунктом, поскольку такое приостановление не исключает для Клиента возможности проведения операций по его счетам на основании документов на бумажных носителях.

9.6. Не позднее 3 (трех) рабочих дней с момента прекращения действия настоящего Соглашения Клиент обязан самостоятельно удалить установленные у него программное обеспечение «Клиент-Банк».

9.7. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для Банка и Клиента.

9.8. Все изменения и дополнения к настоящему Соглашению совершаются в письменной форме.

10. Порядок расчетов по Соглашению

10.1. Оплата услуг Банка за предоставление программных средств, USB-ключей, установку системы «Клиент-Банк», оформление дополнительных сертификатов ключей подписи (дополнительным считается оформление более чем одного сертификата ключей подписи на Клиента) и абонентское обслуживание осуществляется согласно действующим Тарифам Банка. Банк имеет право осуществить взимание комиссии путем безакцептного списания комиссии с расчетного счета Клиента по курсу Банка России, установленному на дату списания комиссии.

10.2. Банк имеет право осуществить в безакцептном порядке взимание с Клиента сумм, причитающихся Банку по оплате услуг эксперта, участвующего в Согласительной комиссии.

11. Порядок рассмотрения споров

11.1. Не урегулированные Сторонами споры и разногласия, возникающие при исполнении настоящего Соглашения, а также при исполнении всех сделок, совершенных в связи и в соответствии с настоящим Соглашением, включая споры о возмещении убытков, причиненных сторонам в связи с использованием аналога собственноручной подписи, разрешаются в суде г. Москвы по местонахождению Банка, после обязательного выполнения досудебного порядка разрешения споров в соответствии с п.7 настоящего Соглашения. Применимым правом является материальное право Российской Федерации.

Подписи Сторон:

Банк: Акционерный коммерческий банк «Балтийский Банк Развития» (закрытое акционерное общество) Местонахождение: Банк: 121099, г.Москва, 1-ый Николощеповский переулок, д. 6, стр. 1 к/с 3010181050000000769 в Отделении № 1 Московского ГТУ Банка России, БИК 044583769, ИНН 3900001002	Клиент:

Филиал Банка: Филиал Акционерного коммерческого банка «Балтийский Банк Развития» (закрытое акционерное общество) в г. Санкт-Петербурге.

Местонахождение: 191119, Санкт-Петербург, ул. Звенигородская., д. 12/17, лит. А, пом.16-Н

ИНН 3900001002, БИК 044030785

к/с № 30101810300000000785 в ГРКЦ ГУ Банка России по Санкт-Петербургу.

Тел/факс: (812) 447-98-94

Руководитель _____ **А.Ю. Горцевский**

Клиент _____

Главный бухгалтер _____ **Ж.О. Полякова**

Контактные телефоны: (812) 447-98-94 (96), Факс 447-98-95

Начальник отдела информационных технологий

_____ **В.Н. Некрасов**

АКТ
передачи программных средств

"__" _____ 20__ года

Мы, нижеподписавшиеся, от лица Банка: Начальник отдела информационных технологий Филиала Акционерного коммерческого банка «Балтийский Банк Развития» (закрытое акционерное общество) в г. Санкт-Петербурге Некрасов Владимир Николаевич и Клиент:

составили настоящий Акт о следующем.

В соответствии с условиями Соглашения (по обслуживанию клиентов - физических лиц по системе «Клиент-Банк») от «__» _____ 20__ г. № _____ Банком переданы, а Клиентом получены:

- инструкция по формированию ключей ЭЦП;
- программное обеспечение для формирования ключей ЭЦП «Admin- PKI»;
- программное обеспечение для обмена документами «Inter-PRO»;
- инструкция по работе с USB-ключом;
- USB-ключи MS_key в количестве _____ шт.

От Банка

Клиент

(подпись)

МП

(подпись)

Заявление на Сертификат ключа подписи

На основании Соглашения № _____ от _____ между Ф-ом АКБ «Балтийский Банк Развития» (ЗАО),
Спб и _____ (наименование Клиента)

прошу выдать сертификат ключа подписи _____
(фамилия имя отчество)

(дата рождения),

(место жительства)

(паспортные данные)

(далее – Владелец сертификата ключа подписи), уполномоченному подписывать документы.

Открытый ключ ЭЦП Владельца сертификата ключа подписи следующий (одновременно предоставляется в электронном виде в Запросе на сертификат):



Владелец сертификата ключа подписи настоящим принимает на себя обязательство хранить в тайне закрытый ключ подписи и возместить Клиенту возможные убытки, причиненные ненадлежащим исполнением данного обязательства.

Приложения:

- 1) Доверенность на распоряжение счетом(ами) Клиента, удостоверенная в установленном законом порядке, подтверждающая предоставление полномочий Владельцу сертификата ключа подписи действовать от имени Клиента при подписании электронных документов.
- 2) Запрос на сертификат на электронном носителе.

Владелец сертификата ключа подписи: _____ (ФИО, подпись) _____

Клиент

(подпись) _____

АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК

«БАЛТИЙСКИЙ БАНК РАЗВИТИЯ»

(закрытое акционерное общество)

рег. № 2929

адрес: Российская Федерация, 121099, г. Москва, 1-ый Николощеповский пер., д.6 стр.1

С Е Р Т И Ф И К А Т

ключа подписи

уникальный регистрационный № _____

Открытый ключ ЭЦП

Открытый ключ используется с программным обеспечением NOTARY-PRO, Inter-PRO, разработчик ЗАО «Сигнал Ком»

Владелец _____

(ФИО владельца сертификата подписи)

Дата начала действия сертификата _____.20__

Дата окончания срока действия сертификата _____.20__

Юридическое значение будет иметь электронный документ, подписанный ЭЦП указанного выше владельца сертификата ключа подписи при осуществлении отношений между Банком и _____

(указать Клиента _____), который является _____ владельцем Сертификата ключа подписи _____ (указать Клиента).

Владелец сертификата ключа подписи настоящим принимает на себя обязательство хранить в тайне секретный (закрытый) ключ подписи и возместить Банку возможные убытки, причиненные ненадлежащим исполнением данного обязательства.

От Банка:

(Подпись)

М.П.

Сертификат ключа подписи получил: _____ (подпись, ФИО)_____

Приложение № 4
к Соглашению
по обслуживанию клиентов - физических лиц

г. Санкт-Петербург

« » 20 г.

Настоящим Акционерный коммерческий банк «Балтийский Банк Развития» (закрытое акционерное общество), именуемый в дальнейшем «Банк», в лице Начальника отдела информационных технологий Филиала Акционерного коммерческого банка «Балтийский Банк Развития» (закрытое акционерное общество) в г. Санкт-Петербурге Некрасова Владимира Николаевича, действующего на основании Доверенности от 15.07.2009 № 1.1-10-2/227, с одной стороны и _____, именуемый в дальнейшем «Клиент», с другой стороны, вместе именуемые Стороны согласились, что Система «Клиент-Банк» используется для работы со следующими счетами Клиента:

№ _____ (договор банковского счета № _____ от _____)
№ _____ (договор банковского счета № _____ от _____)
№ _____ (договор банковского счета № _____ от _____)
№ _____ (договор банковского счета № _____ от _____)
№ _____ (договор банковского счета № _____ от _____)

доступ к Системе предоставляется с любого IP-адреса, если не указано иное:

(указываются конкретные IP-адреса)

От Банка

Клиент

(подпись)

М.П.

(подпись)

Приложение № 5
к Соглашению по обслуживанию клиентов – физических лиц
по системе «Клиент-Банк»

№ _____ от _____ 20__ г.

Банк _____

Клиент _____ 12

ПАМЯТКА ПО БЕЗОПАСНОЙ РАБОТЕ В СИСТЕМЕ "КЛИЕНТ-БАНК"

Уважаемые Клиенты!

«Хакерские» атаки на системы "Клиент-Банк", приводящие к хищениям денежных средств клиентов банков в РФ фиксируются все чаще и чаще.

При этом "хакерами" взламываются не серверы банков, а похищаются клиентские ключи подписи и пароли доступа, как путем прямого доступа, так и с помощью вредоносных программ. Завладев ключами и паролями, злоумышленники осуществляют платежи от имени клиентов.

Поэтому очень важны меры безопасности при работе в системе «Клиент-Банк».

1. Выделите отдельный компьютер, подключаемый к сети Интернет только для работы с системой «Клиент-Банк».

Максимально ограничьте к нему доступ сотрудников. Запретите сотрудникам использовать на этом компьютере какие-либо съемные устройства, за исключением ключевых носителей.

Установленное программное обеспечение должно быть лицензированным и регулярно обновляться.

Установите на этот компьютер антивирусную программу и поддерживайте ее актуальность.

По возможности ограничьте (наши специалисты помогут вам в этом) количество ваших ip-адресов с которых разрешён доступ в систему "Клиент-Банк".

2. Необходимо обеспечить хранение ключей электронной подписи и пароля доступа к системе «Клиент-Банк» в тайне и только уполномоченными сотрудниками.

Ключ электронной подписи храните только на съёмном носителе.

Пароль доступа в систему желательно помнить и вводить вручную. Ни в коем случае не используйте функцию "запомнить пароль". Пароль, записанный на листе бумаги, обязательно храните отдельно от ключевого носителя.

Меняйте пароль доступа не реже одного раза в 3 месяца, и обязательно при компрометации или смене ключей подписи.

3. Не используйте для работы с системой "Клиент-Банк" общедоступные или чужие компьютеры.

4. Для хранения сгенерированных секретных ключей ЭЦП и формирования ЭЦП под документами используется USB-ключ «MS_key».

При использовании этого устройства секретный ключ электронно-цифровой подписи формируется в защищенной области памяти, встроенной в USB-ключ. В отличие от других носителей, с USB-ключа невозможно извлечь, считать или скопировать информацию ни при каких обстоятельствах. USB-ключ – неуязвим в отношении хакерских атак, которые нацелены на похищение секретных ключей не только со съемных носителей, но и из памяти компьютера. USB-ключ может содержать в себе до 64 секретных ключей!

Соблюдение перечисленных мер позволяет Вам существенно снизить риски, связанные с использованием систем "Клиент-Банк" и предотвратить хищение денежных средств.

Если у Вас появились подозрения, что Ваши данные (электронные ключи, пароли) могли быть скомпрометированы, свяжитесь со службой тех. поддержки Банка -

(812) 447-98-96, доб.252

Приложение №7
к Соглашению
по обслуживанию клиентов – физических лиц
по системе «Клиент-Банк»
№ _____ от _____ 20__ г. »

Банк _____

Клиент _____ 14

АКТ

Обмена электронными ключами

"__" _____ 20__ года

Мы, нижеподписавшиеся, от лица Банка: Начальник отдела информационных технологий Филиала Акционерного коммерческого банка «Балтийский Банк Развития» (закрытое акционерное общество) в г. Санкт-Петербурге Некрасов Владимир Николаевич и от лица Клиента:

составили настоящий Акт о следующем.

В соответствии с условиями Соглашения (*по обслуживанию клиентов – юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой, по системе «Клиент-Банк»*) от «__» _____ 20__ г. № _____ Осуществлен обмен «открытыми» ключами ЭЦП лиц, уполномоченных от имени Клиента подписывать электронные документы, и лиц, уполномоченных от имени Банка подписывать сертификат ключей подписи и лиц, уполномоченных от имени Банка подписывать электронные документы. С тарифами Банка Клиент ознакомлен и согласен на безакцептное списание суммы комиссии со счета № _____.

Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу.

От Банка

От Клиента

М.П. (подпись)

М.П. (подпись)