"БСТ-БАНК" ЗАО 654041
г.Новокузнецк, ул.Кутузова, 31
т./ф. 77-88-88 www bstbank ru
e-mail: root@bstbank.ru

Лицензия ЦБ РФ №2883 от 31.08.12г.
ИНН 4218004258 КПП 422001001
БИК 043209706 к/с 30101810000000000706
в РКЦ г.Новокузнецка ОКПО 34777119

Приложение № 2

Договор об электронном обмене документами, подписанных электронной подписью (Интернет-банк) №_____

г. Новокузнецк « ____ » _____ **20 __ г.**

Акционерный коммерческий банк «Бизнес-Сервис-Траст» закрытое акционерное общество, именуемый в дальнейшем «Банк», в лице Заместителя Генерального директора **Задерга Максима Александровича** действующего на основании Устава и приказа № _____ от _____, с одной стороны,
и _____,
именуемое в дальнейшем «Клиент», в лице
_____,
действующего на основании Устава, с другой стороны, заключили настоящий договор (в дальнейшем упоминании по тексту «Договор») о нижеследующем:

1. Предмет договора

1.1.Настоящий договор регулирует отношения сторон, возникающие в процессе оказания Банком услуг по дистанционному банковскому обслуживанию Клиента с использованием Системы, в том числе порядок обмена электронными документами, подписанными электронной подписью, в соответствии с «Регламентом дистанционного банковского обслуживания с применением системы «Интернет-Банк», права, обязанности и ответственность сторон.

1.2. Банк и Клиент договариваются об обмене документами в электронной форме, подписанными электронной подписью, в соответствии с «Регламентом дистанционного банковского обслуживания с применением системы «Интернет-Банк» Акционерного коммерческого банка «Бизнес-Сервис-Траст» закрытого акционерного общества (далее – «Регламент» (Приложение № 7).

1.3. Настоящий Договор является неотъемлемой частью заключенного сторонами Договора "Об открытии счета и расчетно-кассовом обслуживании" № _____ от _____.

1.4. Стороны признают, что используемые во взаимоотношениях Сторон документы, заверенные электронной подписью, подготовленные и переданные одной Стороной другой Стороне с помощью программного обеспечения «Интернет-Банк» в соответствии со всеми процедурами защиты информации, предусмотренные настоящим Договором, эквивалентны документам на бумажном носителе и имеют юридическую силу наравне с документами, подписанными должностными лицами Сторон и скрепленными печатью.

1.5. Кодовый номер при обращении по телефону в банк, для блокировки работы в системе «Интернет-Банк», в случае недоверия (компрометации) ключевым носителям клиента устанавливается в приложении №3.

2. Права и обязанности Клиента

2.1. Права Клиента

2.1.1. На основании настоящего договора Клиент вправе с использованием Системы осуществлять:

2.1.1.1 расчетные операции по банковскому счету/счетам, открытым в Банке и указанным Клиентом в заявке на подключение Системы;

2.1.1.2. прием/передачу иных электронных документов и приложений к ним, определенных заключенными сторонами договорами или соглашениями (Перечень электронных документов (ЭД), используемых в Системе определен в Приложение 2);

2.1.2. Клиент вправе получить выписку о движении денежных средств по его счетам, как с помощью средств Системы, так и на бумажном носителе. Стоимость осуществление выписки по счету определяется тарифам Банка действующими на момент формирования выписки.

2.1.3. Клиент вправе обращаться в Банк за получением бесплатных консультаций, связанных с эксплуатацией Системы, к сотрудникам технической поддержки Банка и менеджеру счета в течение всего срока действия настоящего договора. Оказание технической помощи, в том числе, требующей выезда к Клиенту, осуществляется Банком на основании письменной заявки с обоснованием требования о предоставлении технической помощи и подтверждается актом приемки выполненных работ. Стоимость услуг по оказанию технической помощи определяется действующими тарифами Банка на момент оказания услуги.

2.1.4. В течение срока действия настоящего договора Клиент вправе в любое время прекратить передачу документов, а Банк обязан прекратить прием документов с момента поступления соответствующего требования от Клиента. Требование должно быть предоставлено в письменной форме, подписано уполномоченным лицом и заверено печатью Клиента.

2.1.5. Клиент (уполномоченный представитель Клиента) вправе инициировать замену ключей Электронной Подписи (ЭП) в любой момент до истечения срока их действия.

2.1.6.Для обеспечения более высокого уровня безопасности, Клиент вправе подключить сервис подтверждения платежей по своим счетам одноразовыми паролями через СМС уведомления – «Сервис одноразовых паролей».

2.2. Обязанности Клиента

2.2.1. Клиент обязан самостоятельно контролировать исполнение платежных документов, отправленных в Банк с использованием средств Системы, посредством контроля изменений состояния отправленного электронного документа.

2.2.2. Клиент обязан за свой счет поддерживать в рабочем состоянии принадлежащие ему аппаратные и программные средства, в том числе средства антивирусной защиты, используемые для функционирования Системы, а также обеспечить своевременное их обновление.

2.2.3. Клиент обязан соблюдать правила информационной безопасности при использовании Системы (Приложение 4):

2.2.3.1. обеспечить хранение материального носителя, содержащего закрытый ключ ЭПв месте, исключающем доступ неуполномоченных лиц и/или повреждение материального носителя (сейф, личная запираемая ячейка и т.п.);

2.2.3.2. хранить ключ ЭПна защищённом хранилище USB-ключ (смарт-карта, смарт-ключ);

2.2.3.3. исключить хранение закрытого ключа ЭПна жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах;

2.2.3.4. исключить передачу закрытого ключа ЭПи его копий третьим лицам, а так же передачу по телефону, электронной почте или публичным сетям;

2.2.3.5. в случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям, должна быть проведена смена ключей ЭП, к которым он имел доступ;

2.2.3.6. при подозрении несанкционированного доступа третьих лиц к счетам, программно-аппаратным средствам Клиента, копирования или подозрения в копировании ключей третьими лицами, с целью предотвращения финансовых потерь, незамедлительно любым доступным способом проинформировать об этом Банк и инициировать процедуру смены всех потенциально скомпрометированных ключей ЭП.

2.2.4. Клиент гарантирует Банку, что все проводимые им операции по счету с использованием средств Системы носят легитимный характер, не нарушают действующего законодательства РФ, и не связаны с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

2.2.5. В случае подключения сервиса подтверждения платежей по своим счетам одноразовыми паролями через СМС уведомления – «Сервис одноразовых паролей», Клиент при блокировании сим-карты, выхода из строя телефона, подозрений, что телефоном завладел злоумышленник, обязан немедленно любым доступным способом известить об этом Банк.

2.2.6. В случае невозможности доставки электронного документа, в том числе при неработоспособности контура интернет-банкинга в зоне ответственности Банка, Клиент обязан предпринять все меры по доставке документа на бумажном носителе.

2.2.7. Клиент обязан своевременно (в последний рабочий день месяца) оплачивать услуги Банка по обслуживанию Системы в соответствии с действующими тарифами.

3. Права и обязанности Банка

3.1. Права Банка

3.1.1. В течение всего срока действия настоящего договора Банк вправе в одностороннем внесудебном порядке изменять действующие тарифы. Информирование Клиента об изменении тарифов осуществляется путем размещения соответствующей информации на информационных стендах в операционных залах Банка, сайте Банка или посредством Системы.

3.1.2. Банк вправе отказать Клиенту в приеме от него распоряжения на проведение операции или приостановить совершение Клиентом операций по счету с использованием средств Системы в случаях и в порядке, установленных ФЗ РФ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» № 115-ФЗ от 07.08.2001г.

3.1.3. Банк, для исполнения действующего законодательства, а также внутрибанковских инструкций, вправе запрашивать у Клиента документы и сведения о проводимых/проведенных операций по счетам Клиента, осуществленных с использованием Системы. При этом обязательный срок для представления документов по запросам Банка составляет 7 (семь) рабочих дней со дня вручения запроса Банком Клиенту лично (при посещении Клиентом офиса Банка), заказным письмом с уведомлением либо с использованием средств Системы.

3.1.4. При непредставлении запрашиваемых Банком документов и сведений, либо предоставлении неполных или некорректных сведений, Банк вправе не исполнять электронный документ до предоставления Клиентом надлежащим образом оформленного платежного документа на бумажном носителе и запрошенных документов и сведений.

3.1.5. На время разрешения спорной ситуации, связанной с исполнением Банком электронного документа Клиента, Банк вправе в одностороннем внесудебном порядке приостановить обслуживание Клиента в Системе с последующим его уведомлением.

3.1.6. Банк вправе использовать инструменты контроля платежей Клиента на предмет компрометации ключей ЭП Клиента по своему усмотрению.

3.1.7. При обнаружении Банком признаков (фактов) нарушения требования безопасности, установленных настоящем договором, Банк в праве немедленно приостановить прием электронных документов Клиента, после чего должен любым доступным способом известить об этом Клиента.

3.1.8. Банк имеет право направлять Клиенту с использованием средств Системы рекламные материалы и информационные сообщения об услугах и продуктах Банка.

3.1.9. Банк имеет право приостанавливать работу Системы в случае образования задолженности по оплате комиссии более 10 дней. Повторное подключение к Системе производить с письменного распоряжения клиента при условии полного погашения образовавшейся задолженности и оплаты повторного подключения согласно тарифам Банка.

3.2. Обязанности Банка

3.2.1. Банк обязуется предоставлять Клиенту услуги с использованием Системы согласно п.2.1.1 настоящего договора.

3.2.2. Предоставлять Клиенту необходимые рекомендации и методическую помощь в работе с Системой.

3.2.3. По требованию Клиента блокировать в Системе активные открытые ключи ЭПКлиента, регистрировать новые открытые ключи ЭП, временно блокировать работу Клиента в Системе.

3.2.4. Банк производит подключение Клиента к Системе для совершения операций в рамках договоров, заключенных между Банком и Клиентом (Приложение №8).

3.3. Стороны взаимно обязуются

3.3.1. Не осуществлять действий, наносящих ущерб другой Стороне вследствие использования Системы.
3.3.2. Поддерживать системное время ПЭВМ своего абонентского пункта по местному времени с точностью до пяти минут. При обработке документов полученных по Системе определяющим временем является текущее время по системным часам аппаратных средств Банка.

3.3.3. Не осуществлять операцию по ЭД, заверенному ЭП, если программа проверки, используя действующий открытый ключ подписывающей Стороны, не подтвердила подлинность ЭПподписывающей Стороны под ЭД.
3.3.4. При осуществлении операций на основании полученных по Системе ЭД руководствоваться требованиями законодательства РФ и соглашений между Банком и Клиентом.
3.3.5. Обеспечивать целостность и сохранность программных средств, ЭД, защите секретных ключей ЭП, паролей доступа и другой информации, передаваемой и получаемой по Системе.
3.3.6. Вести архивы документов на магнитных и бумажных носителях, хранить их в соответствии с порядком и сроками установленными для хранения платежных документов.
3.3.7. Предоставлять по запросам другой Стороны подтверждения по ЭД, а также надлежащим образом оформленные бумажные копии ЭД.
3.3.8. За собственный счет поддерживать в рабочем состоянии и при необходимости самостоятельно модернизировать, свои помещения и технические средства обеспечения работоспособности вычислительной техники, средств связи, автоматизированного рабочего места, на котором установлено программное обеспечение Системы. Обеспечить техническую готовность компьютера и предоставить доступ уполномоченного сотрудника Банка для проведения работ по установке и настройке Системы, а также обеспечить присутствие технического специалиста Клиента на время проведения работ.
3.3.9. Исключить доступ к Системе лиц, не имеющих право на формирование, подпись и отправку Электронных документов.
3.3.10. Назначить лицо, ответственное за информационную безопасность при работе с системой.
3.3.11. Хранить Ключевой носитель в надежном месте, исключающем доступ к нему неуполномоченных лиц, а также его повреждение.
3.3.12. Ежедневно осуществлять связь с банком для просмотра почтовых сообщений, поступающих из Банка, касающихся взаимодействия Банка и Клиента (извещения, запросы на предоставление в Банк необходимой информации и другие). Фактом отправки электронного почтового сообщения из Банка считается запись в протоколе электронной почты банка.
3.3.13. В случае истечения срока действия полномочий лиц, наделенных правом первой и/или второй подписи, действующих в соответствии с учредительными, распорядительными документами юридического лица, своевременно предоставить в Банк документы о продлении сроков действия полномочий указанных лиц.

4. Ответственность сторон

4.1. Стороны обязуются обеспечивать конфиденциальность сведений о технологии Системы.

4.2. Стороны обязуются формировать и хранить не менее трех лет (а в случае возникновения споров – до их разрешения) архивы:

4.2.1. всех своих открытых ключей ЭП;

4.2.2. всех входящих электронных документов в принятом виде с электронной подписью;

4.2.3. всех исходящих электронных документов в исходном виде с электронной подписью;

4.2.4. извещений (в электронном виде с электронной подписью) о приеме электронных документов;

4.2.5. сообщений свободного формата, подписанных электронной подписью;

4.2.6. электронных протоколов сеансов обмена информацией.

4.3. Стороны несут ответственность за целостность и достоверность этих архивов.

4.4. Сроки хранения электронных расчетных документов должны соответствовать срокам хранения, установленным для расчетных документов на бумажных носителях.

4.5. Архивы подлежат защите от несанкционированного доступа непреднамеренного или преднамеренного уничтожения и/или искажения.

4.6. Банк не несёт ответственности за ущерб, возникший вследствие:

4.6.1. некорректного оформления Клиентом электронных документов;

4.6.2. ошибочно переданных электронных документов Клиентом в Банк;

4.6.3. несанкционированного доступа посторонних лиц к программно-аппаратным средствам, закрытого ключа ЭП, используемых Клиентом для осуществления обмена электронными документами;

4.6.4. воздействия вредоносного программного обеспечения на программно-аппаратные средства, используемые Клиентом для осуществления обмена электронными документами;

4.6.5. срывов и помех на линии связи, используемой Клиентом при работе с Системой.

4.7. В случае несоблюдения требований настоящего договора, ответственность за негативные последствия несет сторона, допустившая эти нарушения в размере прямого ущерба.

4.8. Ни одна из Сторон не будет нести ответственность за полное или частичное неисполнение своих обязательств по настоящему договору, если неисполнение будет являться следствием таких обстоятельств, как: пожар, наводнение, землетрясение, любые другие стихийные бедствия, войны, военные операции любого характера, блокады, акты государственных органов, а также изменение действующего законодательства и иные ограничения экономического и политического характера.

4.9. Если любое из вышеуказанных обстоятельств непосредственно повлияло на исполнение обязательств в сроки, установленные настоящим договором, то эти сроки соразмерно отодвигаются на время действия соответствующего форс-мажорного обстоятельства.

4.10. Сторона, для которой создались условия, при которых исполнение ее обязательств стало невозможным, обязана не позднее 1 (одного) дня направить другой стороне уведомление посредством Системы и/или в письменной форме о наступлении таких условий. Не уведомление или несвоевременное уведомление лишает сторону права ссылаться на любое из перечисленных выше обстоятельств.

4.11. Банк несет ответственность, предусмотренную законодательством, за задержки, сбои и другие недостатки в исполнении обязательств по договору, связанные с неработоспособностью системы в зоне ответственности Банка при условии, что время неработоспособности системы превышает время, указанное в п. 3.10.6 Приложения №8 и клиент предпринял меры предусмотренные п. 2.2.6 настоящего договора.

4.12. Стороны ограничивают размер возмещения убытков по настоящему договору размером реального ущерба. Упущенная выгода не возмещается, ни при каких обстоятельствах.

5. Порядок расчетов

5.1. Стоимость услуг по подключению к Системе, ее использованию, предоставлению технической помощи и порядок оплаты определяются тарифами Банка, действующими на момент оказания услуг.

5.2. Оплата стоимости банковских услуг, услуг по подключению к Системе, ее использованию, предоставлению технической помощи осуществляется путем списания денежных средств банковским ордером с любого расчетного счета, открытого в Банке в рублях, либо в порядке, установленном соответствующими договорами, соглашениями, а так же иными способами, не запрещенными законодательством РФ.

5.3. Использование Системы в течение неполного календарного месяца оплачивается Клиентом как за использование Системы в течение полного календарного месяца.

5.4. Неиспользование Системы, не освобождает Клиента от обязанности по оплате Банку комиссионного вознаграждения за предоставление прав дистанционного доступа к банковскому счету Клиента.

5.5. Стоимость услуг третьих лиц, обеспечивающих подключение Клиента к сети Интернет и обслуживание его в сети, оплачивается Клиентом самостоятельно и не входит в стоимость банковских услуг.

6. Урегулирование споров

6.1. При возникновении разногласий и споров, связанных с исполнением настоящего договора, стороны обязуются решать их путем переговоров.

6.2. При возникновении споров, связанных с принятием (неприятием) и/или с исполнением (неисполнением) электронных документов, стороны обязаны соблюсти порядок разрешения спорных ситуаций, изложенный в Приложении №1 к настоящему договору.

6.3. Если одна из сторон предъявляет другой стороне претензию по документу, а также подтверждение другой стороны о получении такого документа, а другая сторона не может представить архивную копию спорного документа вследствие ненадлежащего хранения архива, виновной признается сторона, не представившая архивную копию спорного документа.

6.4.Споры, по которым не достигнуто соглашение сторон, разрешаются в Арбитражном суде Кемеровской области.

7. Срок действия договора

7.1.Настоящий договор вступает в силу с даты его подписания Сторонами и действует до 31 декабря текущего года.

7.2. По окончании срока его действия, настоящий договор автоматически пролонгируется на следующий календарный год на тех же условиях, если не менее чем за 5 (пять) календарных дней до

окончания срока его действия ни одна из сторон не заявит о своем отказе от пролонгации настоящего договора или необходимости пересмотра его условий.

Если какая-либо сторона заявила о необходимости пересмотра условий настоящего договора, стороны должны провести переговоры и согласовать новые условия до окончания срока действия настоящего договора, после чего его перезаключить на вновь согласованных условиях. В противном случае действие договора прекращается.

7.3. Любая сторона вправе расторгнуть настоящий договор в одностороннем порядке досрочно, предупредив другую сторону в письменной форме не менее чем за 10 дней до предполагаемой даты расторжения.

Досрочное расторжение настоящего договора возможно при условии выполнения сторонами обязательств, предусмотренных настоящим договором, дополнениями, приложениями к нему.

7.4. Договор считается расторгнутым:

7.4.1. по истечении 30 календарных дней с даты окончания срока действия Сертификата Клиента, если Клиент не обратился в Банк за оформлением нового Сертификата;

7.4.2. отсутствие денежных средств на счете Клиента более 3 (трех) месяцев подряд;

7.4.3. окончания действия или расторжения всех договоров между Банком и Клиентом, предусматривающих обмен электронными документами.

8. Заключительные положения

8.1. Настоящий договор составлен в двух подлинных экземплярах на русском языке, имеющих равную юридическую силу, из которых один находится в Банке, второй - у Клиента.

8.2. *(данный пункт применяется при заключении договора с клиентами, переведенными с системы «Клиент-Банк»)* Договор_____ от «____» _____г. № _____ считается расторгнутым по истечению календарного месяца с момента подписания настоящего договора. Соответствующее число месяца, следующего за месяцем, в котором был подписан настоящий договор, является последним днем работы системы «Клиент-Банк».

8.3. Любая информация (в том числе уведомления, извещения) может быть доведена до клиента посредством размещения ее на официальном сайте Банка в сети интернет. При необходимости, такая информация может быть доведена до клиента посредством телефонной связи, смс-сообщения, электронного сообщения, почтового сообщения по реквизитам, указанным в разделе 9 настоящего договора.

9. Юридические адреса сторон и иные реквизиты

Банк:	**Клиент:**
«БСТ-БАНК» ЗАО ИНН/КПП 4218004258/422001001 к/с 30101810000000000706 в РКЦ г. Новокузнецка БИК 043209706 Адрес, почтовый индекс: 654041, Кемеровская обл., г. Новокузнецк, ул. Кутузова, 31	
_____Задерг М.А..	_____
М.П.	М.П.

Приложение 1
к Договору об электронном обмене документами, подписанных
электронной подписью (Интернет-банк) №_____

ПОЛОЖЕНИЕ
по разбору споров, связанных с подлинностью
электронных документов.

1. Общие положения

В данном Положении описан порядок разрешения споров между Банком и Клиентом, связи с осуществлением электронного документооборота между Банком и Клиентом возможно возникновение спорных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронных документов, а также использованием в данных документах электронной цифровой подписи. Спорные ситуации могут возникать в следующих случаях:

1.1. неподтверждение подлинности электронных документов средствами проверки ЭП принимающей Стороны;

1.2. оспаривание факта формирования электронного документа;

1.3. оспаривание факта идентификации владельца сертификата ключа подписи, подписавшего документ;

1.4. заявление Банка об искажении электронного документа;

1.5. оспаривание факта отправления и/или доставки электронного документа;

1.6. оспаривание времени отправления и/или доставки электронного документа;

1.7. оспаривание соответствия экземпляров электронного документа и/или подлинника и копии электронного документа на бумажном носителе;

1.8. иные случаи возникновения спорных ситуаций, связанных с функционированием Системы.

В рамках настоящего положения стороны договорились о следующем: Электронный документ считается подлинным, если он был с одной стороны надлежащим образом оформлен, подписан и отправлен, а с другой - получен, проверен и принят.

2. Спорная ситуация возникает также в случае, если Банк высказывает недоверие к программному обеспечению, функционирующему на рабочем месте Клиента.

3. Уведомление о спорной ситуации:

3.1. В случае возникновения спорной ситуации сторона, предполагающая возникновение этой ситуации, должна не позднее чем в течение трех рабочих дней после ее возникновения, направить письменную претензию (в виде электронного документа либо заказного письма с уведомлением о вручении) с изложением сути протеста и детальным описанием спорной операции и материалы, имеющие отношения к предмету спора второй стороне.

3.2. Претензия должна содержать реквизиты электронного документа, а также фамилию, имя, отчество, должность и координаты лица или лиц, уполномоченных вести переговоры по урегулированию данной ситуации.

3.3. Сторона, которой направлена претензия, обязана не позднее чем в течение следующего рабочего дня проверить наличие обстоятельств, свидетельствующих о возникновении спорной ситуации, и направить лицу, уполномоченному вести переговоры, информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей этой ситуации.

4. Любые споры разрешаются между участниками путем проведения переговоров.

5. При невозможности разрешения спора путем переговоров, Стороны вправе обращаться к оператору Системы, имеющему эталон программного обеспечения Системы (далее - Оператор), с письменным заявлением о создании конфликтной комиссии для разрешения спора.

Оператор принимает участие в урегулировании разногласий между участниками при условии заблаговременного предоставления Оператору всех документов, касающихся возникших разногласий, документов, подтверждающих полномочия сторон, государственную регистрацию сторон, а также иных документов, дополнительно затребованных Оператором.

Если стороны не договорятся об ином, в состав конфликтной комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих сторон и представитель Оператора. Не предоставление одной из Сторон со своей стороны членов комиссии не является основанием для отложения или не рассмотрения заявления. В таком случае заключение об авторстве и/или подлинности электронного документа делается только представителями Оператора.

6. Право представлять в комиссии соответствующую Сторону, а также Оператора, должно подтверждаться доверенностью, выданной каждому представителю на срок работы комиссии.

7. Конфликтная комиссия создается и приступает к работе в двухнедельный срок с момента поступления письменного заявления от заинтересованного участника. Конфликтная комиссия осуществляет свою работу на территории Оператора и должна вынести свое заключение, оформленное соответствующим актом, в месячный срок с момента начала работы. Акт комиссии признается имеющим силу в случае согласия с содержащимся в нем решении большинства членов комиссии. В случае несогласия с решением комиссии, член комиссии вправе указать в решении своё мотивированное особое мнение.

8. Компетенция и полномочия Конфликтной комиссии:

8.1. Сформированная комиссия при рассмотрении спорной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки электронного документа, его подлинности, а также о подписании электронного документа конкретной ЭП, идентичности отправленного и полученного электронного документа.

8.2. Комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению комиссии, для выяснения причин и последствий возникновения спорной ситуации.

8.3. Комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.

9. Для разрешения спора о подлинности документа, подписанного закрытым ключом ЭП, заинтересованный участник предоставляет Оператору для передачи экспертной комиссии:

9.1. спорный документ в электронном виде;

9.2. спорный документ на бумажном носителе;

9.3. акт о передаче Клиенту Сертификата, подписанный участниками, с указанием идентификатора Сертификата (DN) участника.

9.4. иные документы, имеющие значение, по мнению непосредственных участников обмена электронными документами или Оператора.

10. Для проверки подлинности документа, подписанного закрытым ключом ЭП, и достоверной идентификации Сертификата используется Эталонный Модуль Проверки подписи документа, хранящийся у Оператора. Результатом работы такого Эталонного Модуля Проверки является:

10.1. установление факта создания спорного документа с использованием Системы;

10.2. установление факта подписи спорного документа в соответствии с технологией Системы;

10.3. установление факта целостности спорного документа;

10.4. раскрытие информации об идентификаторе Сертификата (DN), соответствующего закрытому ключу ЭП, использованному для подписи спорного документа.

11. Конфликтная комиссия сравнивает данные идентификатора Сертификата (DN), содержащиеся в акте о передаче Сертификата и полученные в результате работы Эталонного Модуля Проверки подписи документа.

12. Подтверждением подлинности электронного документа является единовременное наличие следующих условий:

12.1. подтверждена подлинность закрытого ключа ЭП, использованного для подписи спорного документа;

12.2. подтверждена целостность спорного документа;

12.3. идентификатор Сертификата (DN), содержащийся в акте о передаче Сертификата, и идентификатор Сертификата (DN), полученный в результате работы Эталонного Модуля Проверки подписи документа, совпадают;

12.4. получен положительный результат проверки спорного документа на соответствие технологии Системы.

12.5. в указанном случае конфликтной комиссией составляется акт о признании подлинности документа, подписанного закрытым ключом ЭП.

13. При отсутствии одного или нескольких из вышеперечисленных условий (п.12), конфликтной комиссией составляется акт о не признании подлинности документа, подписанного закрытым ключом ЭП. Акты, составленные конфликтной комиссией, являются доказательством при дальнейшем разбирательстве спора.

14. Подтверждение конфликтной комиссией подлинности документа, подписанного закрытым ключом ЭП, принятого по Системе, означает, что этот документ имеет юридическую силу.

15. Не подтверждение конфликтной комиссией подлинности документа, подписанного закрытым ключом ЭП, принятого по Системе, означает, что этот документ не имеет юридической силы.

16. Если по результатам работы конфликтной комиссии Стороны не достигли договоренности, либо одна из Сторон не согласна с выводами конфликтной комиссии, дальнейшее разбирательство спора продолжается в установленном действующим законодательством порядке в Арбитражном суде Кемеровской области.

Банк:
«БСТ-БАНК» ЗАО
ИНН/КПП 4218004258/422001001
к/с 30101810000000000706
в РКЦ г. Новокузнецка
БИК 043209706
Адрес, почтовый индекс:
654041, Кемеровская обл.,
г. Новокузнецк, ул. Кутузова, 31

_____Задерг М.А.
М.П.

Клиент:

_____

М.П.

Приложение 2
к Договору об электронном обмене документами, подписанных
электронной подписью (Интернет-банк) №_____

Перечень электронных документов (ЭД), используемых в Системе

Расчетные документы:

- Платежные поручения по перечислению рублевых средств;
- Распоряжение на списание средств в иностранной валюте с транзитного валютного счета;
- Поручения на продажу иностранной валюты за рубли;
- Поручения на покупку иностранной валюты за рубли;
- Поручения на конвертацию иностранной валюты (покупка одной валюты за другую).

Иные документы:

- Справка о валютных операциях;
- Справка о подтверждающих документах;
- Справка о поступлении валюты РФ;
- Паспорт сделки по контракту;
- Паспорт сделки по кредитному договору;
- Заявления на перевод средств в иностранной валюте;
- Заявление на закрытие паспорт сделки;
- Заявления на открытие импортного аккредитива;
- Заявление об акцепте, отказе от акцепта
- Заявления на досрочное расторжение/изъятие части /пролонгацию депозита
- Заявление на заключение договора бронирования денежных средств
- Заявление на подключение услуги Мобильный банк
- Заявление на открытие корпоративного карточного счета
- Заявление на подключение дополнительного сервиса по системе «Интернет-Банк»
- Заявление на открытие аккредитива
- Запросы, письма, сообщения в свободном формате.
- Реестр на зачисление заработной платы и иных выплат работникам
- Депозитные договоры и соглашения к ним
- Дополнительные соглашения к договору банковского счета
- Оферты
- Заявки к Договору о выдаче собственных векселей по заявкам
- Акт приема-передачи сертификата для системы «Интернет-Банк»
- Акт приемки выполненных работ
- Распоряжение на изменение условий аккредитива
- Распоряжение на отмену аккредитива
- Прочие документы и приложения к ним, определенные заключенными сторонами договорами или соглашениями.

Подписи сторон:

Банк:
«БСТ-БАНК» ЗАО
ИНН/КПП 4218004258/422001001
к/с 30101810000000000706
в РКЦ г. Новокузнецка
БИК 043209706
Адрес, почтовый индекс:
654041, Кемеровская обл.,
г. Новокузнецк, ул. Кутузова, 31

_____Задерг М.А.
М.П.

Клиент:

_____
М.П.

Приложение 3
к Договору об электронном обмене документами, подписанных электронной подписью (Интернет-банк) №_____

ПАМЯТКА
КЛИЕНТУ «БСТ-БАНК» ЗАО
ПО СОБЛЮДЕНИЮ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В целях повышения безопасности при общении с Банком обращаем Ваше внимание на необходимость соблюдения следующих мер предосторожности:

При заключении договоров на расчетно-кассовое и дистанционное банковское обслуживание, передает Клиенту памятку по формированию кодового номера. Кодовый номер используется Клиентом при обращении в Банк посредством телефонной связи для получения информации о текущем состоянии счетов Клиента и для блокировки криптографических ключей в случае их компрометации. Клиент обеспечивает сохранность конфиденциальности памятки и кодового номера.

Кодовый номер состоит из семи цифр и формируется следующим образом:

		–			–			

1. Позиции с 1 по 3 – последние две цифры ИНН Клиента;
2. Позиции с 4 по 5 – последние две цифры КПП Клиента.
3. Позиции с 6 по 7 – последние три цифры расчётного счёта Клиента;

Клиент также обязан определить круг лиц, допущенных к получению информации из Банка (как по договорам РКО, так и по договорам ДБО).

1 _____

2 _____

3 _____

При телефонном обращении в Банк Клиент обязан назвать наименование организации, должность фамилию (из списка лиц, допущенных к получению информации) и кодовый номер Клиента, в течение 24 часов, с момента сообщения о факте компрометации, необходимо направлять в Банк «Уведомление о компрометации секретного ключа ЭП» на бумажном носителе (Приложение 5), заверив его рукописной подписью владельца ключа, **иначе работа в системе БК будет возобновлена.**

В случае несовпадения одного из параметров (фамилии или кодового номера) сотрудник Банка вправе отказать звонящему в получении информации.

Телефон _____, время приема обращений, рабочие дни с 8:30 до 17:00.

С содержанием Памятки ознакомлен.

_____

(Должность, ФИО представителя Клиента)

« __ » _____ 20 __ г.

МП

Приложение 4
к Договору об электронном обмене документами, подписанных
электронной подписью (Интернет-банк) №_____

Требования и рекомендации
по обеспечению информационной безопасности
при работе в системе Интернет-Банк.

1. Требования по обеспечению информационной безопасности.

1.1. Организационные меры.

- доступ к рабочему месту (РМ) должен предоставляться лицам, наделенным соответствующими полномочиями;
- руководством Клиента должен быть утвержден список пользователей и администраторов, допускаемых к работе на РМ, с закреплением за каждым пользователем конкретных функций и полномочий;
- Пользователи РМ должны быть в обязательном порядке проинструктированы по вопросам соблюдения требований безопасности.

1.2. Требования по защите РМ.

- на РМ должно быть установлено только лицензионное ПО;
- установленное на РМ ПО должно своевременно обновляться;
- на РМ в обязательном порядке должно быть установлено лицензионное антивирусное ПО с ежедневным обновлением;
- на РМ должен быть активирован персональный сетевой экран, разрешающий доступ с РМ только к доверенным ресурсам сети. Сетевой доступ к ресурсам РМ (в том числе и удаленный вход) с других станций сети из внешних сетей;
- на РМ не должно быть установлено ПО для разработки и отладки программ;
- пользователи РМ, работающие с системой не должны иметь прав администратора. Доступ к файловым ресурсам компьютера должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.
- на РМ должна быть установлена только одна операционная система;
- на РМ должен быть исключен режим автоматического входа пользователя в операционную систему при ее загрузке;
- средствами BIOS должна быть исключена возможность загрузки операционной системы, отличной от установленной на жестком диске (должны быть отключены загрузка с дискет, CD/DVD приводов, USB flash дисков, сетевая загрузка и т.д.);
- доступ к BIOS должен быть защищен паролем;
- в случае обнаружения на РМ незарегистрированных программ, вирусов, нарушений целостности операционной системы, работа должна быть прекращена, а в Банк направлено уведомление о компрометации ключей для их блокировки.

1.3. Требования к эксплуатации РМ.

- на РМ еженедельно должна выполняться полная антивирусная проверка;
- при возникновении подозрения на вирусную активность или при обнаружении вирусов на РМ откажитесь от работы на РМ до полного восстановления его работоспособности;
- при подключение к РМ отчуждаемые носители (дискеты, компакт-диски, USB-накопители, мобильные телефоны и тд.) обязательно должна быть проведена антивирусная проверка ;
- при работе с электронной почтой не открывайте письма от неизвестных отправителей;
- никогда не отвечайте на письма, в которых от имени Банка или иных адресатов вас просят предоставить какую-либо информацию, связанную с работой в системе Банк-Клиент. Никогда не следуйте по ссылкам в таких письмах, т.к. скорее всего вы попадете на сайт мошенников.
- в случае обнаружения ложного Web-сайта Банка, или получения от имени Банка подозрительного электронного сообщения, незамедлительно сообщите об этом персоналу Банка;
- при работе в Интернете никогда не давайте согласия на установку каких-либо дополнительных программ;
- не оставляйте ключевые носители в компьютере после окончания работы в системе Банк-Клиент.

1.4. Требования по использованию и хранению ключевой информации.

- клиент должен самостоятельно генерировать криптографические ключи;
- носители ключевой информации должны хранится у тех лиц, которым они принадлежат;
- порядок хранения и использования носителей ключевой информации с секретными ключами должен исключать возможность несанкционированного доступа к ним;
- категорически запрещается сохранять ключевые файлы (файлы ключей ЭП) на жестком диске компьютера;
- во время работы с носителями ключевой информации доступ посторонних к ним должен быт исключен;
- по окончании рабочего дня, а также вне времени сеансов с Банком, носители ключевой информации должны храниться в металлических сейфах;
- не разрешается:

* передавать носители ключевой информации лицам, к ним не допущенным;
* выводить секретные ключи на печать или экран монитора;
* подключать носители ключевой информации к другим компьютерам и устройствам;
* записывать на носители ключевой информации посторонние файлы.

2. Рекомендации по обеспечению информационной безопасности.

2.1. Регулярно проверять РМ на наличие вирусов.

2.2. При кратковременном отсутствии на рабочем месте необходимо блокировать РМ (средствами операционной системы) и убирать ключевые носители в сейф.

2.3. Избегать подключений к сомнительным сайтам, а также ресурсам, маскирующимся под известные кредитные организации.

2.4. В работе использовать надежные, сложные пароли, содержащие различные буквы, цифры и спецсимволы (например, знаки препинания), а также сочетания заглавных и строчных букв. Не записывать и никому не сообщать свои пароли.

2.5. В случае, если РМ вышло из строя (не включается, виден «синий экран») – незамедлительно связаться с Банком и выполнить блокировку ключей – возможно выход из строя РМ является следствием вирусной атаки, цель которой – лишить вас возможности оперативно отслеживать состояние вашего счета.

3. Меры, направленные на защиту ключевой и парольной информации:

Нельзя оставлять носители с ключами ЭПподключёнными к ПК после подписания платёжных документов. Носители секретных ключей ЭП нужно подключать к ПК только в момент подписания документов, после подписания носители сразу отключать и убирать в место хранения (сейф, и т.п.).

В случае компрометации ключей ЭП клиент обязан немедленно по телефонным каналам связи с использованием кодового номера информировать сотрудника операционно-кассового отдела Банка, отвечающего за обслуживание счёта Клиента, о факте компрометации используемых закрытых (секретных) ключей. Прекратить обмен электронными документами с использованием скомпрометированных ключей.

В кратчайшие сроки с момента определения компрометации ключей Клиент обязан предоставить в банк на имя руководителя Банка письменное «Уведомление о компрометации криптографических ключей», подписанное руководителем организации и заверенное печатью Клиента (Приложение5).

Необходимо заменять ключи ЭП во всех случаях увольнения или смены руководителей юридического лица, подписывавших распоряжения (доверенности) о предоставлении сотрудникам организации полномочий подписания ЭП электронных документов.

При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбами сообщить или передать конфиденциальную информацию (ключи, пароли и пр.) ни при каких обстоятельствах не сообщать данную информацию.

Клиент несёт ответственность за достоверность сведений указанных в Заявке, а также обязан сообщать обо всех изменениях этих сведений.

Клиент несёт ответственность за сохранность СКЗИ и секретных ключей шифрования и ЭП.

В случае если Клиент допустил компрометацию секретных криптографических ключей и немедленно не уведомил об этом Банк, то всю ответственность за возможные при этом последствия несёт Клиент.

С содержанием ознакомлен.

_____

(Должность, ФИО представителя Клиента)

« __ » _____ 20 __ г.

МП

Приложение 5
к Договору об электронном обмене документами, подписанных электронной подписью (Интернет-банк) №_____

Зам. Генерального
директора «БСТ-БАНК»
ЗАО
_____

Уведомление о компрометации криптографических ключей

№ _____ « __ » _____ 20 __ г.

Настоящим уведомляю о компрометации криптографических ключей, идентифицируемых перечисленными ниже параметрами:

_____

(полное наименование организации Участника СЭД)

владельцем сертификата ключа электронной подписи

_____

(фамилия, имя, отчество полномочного представителя Участника СЭД)

Данные криптографические ключи прошу считать скомпрометированными и выведенными из действия с « __ » _____ 20 __ г.

Руководитель _____ _____
(подпись) *(Ф.И.О.)*

Главный бухгалтер _____ _____
(подпись) *(Ф.И.О.)*

М.П.

Примечание:

1. Дата вывода криптографических ключей из действия, указываемая в настоящем Уведомлении, не может быть ранее даты получения данного Уведомления Банком.
2. В случае если Участник СЭД, формирующий настоящее Уведомление, ранее сообщил в Банк о компрометации данных криптографических ключей по телефону, то в настоящем Уведомлении дата вывода криптографических ключей из действия определяется датой соответствующего сообщения по телефону.

Приложение 6
к Договору об электронном обмене документами, подписанных
электронной подписью (Интернет-банк) №_____

ТЕРМИНЫ, ИХ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В ДОГОВОРЕ

Термины их понятия и определения в смысле настоящего Договора следует понимать и трактовать следующим образом:

1.1. Дистанционное банковское обслуживание (ДБО) – предоставление Банком Клиенту предусмотренных настоящим договором банковских и информационных услуг с использованием системы «Интернет-Банк».

1.2. Система «Интернет-Банк»/Система – совокупность программного, информационного и аппаратного обеспечения, позволяющая производить электронный документооборот между ее участниками в соответствии с установленными действующим законодательством РФ нормами и правилами Системы.

1.3. Участники Системы – Банк и Клиент, осуществляющие электронный документооборот посредством Системы в рамках заключенных между Банком и Клиентом договоров.

1.4. Электронная цифровая подпись (ЭП) – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, позволяющий идентифицировать участника Системы, подписавшего документ, а также установить отсутствие искажения информации в электронном документе.

1.5. Электронный документ (ЭД) – документ, согласно Приложению №2 к настоящему договору, в котором информация представлена в электронно-цифровой форме и соответствует установленному оператором формату.

1.6. Ключ ЭП - совокупность закрытого и соответствующего ему открытого ключей ЭП.

1.7. Открытый ключ ЭП – уникальная последовательность символов, соответствующая закрытому ключу ЭП, доступная другому пользователю Системы и предназначенная для подтверждения подлинности ЭП в электронном документе.

1.8. Закрытый ключ ЭП – уникальная последовательность символов, известная сотруднику Клиента (владельца сертификата ключа подписи) и предназначенная для создания в электронных документах электронной цифровой подписи.

1.9. Сертификат ключа подписи (Сертификат) – электронный документ, служащий для идентификации и проверки подлинности ЭП Клиента.

1.10. Расчетный документ – оформленное, в виде документа на бумажном носителе или электронного платежного документа, распоряжение Клиента на перечисление денежных средств в безналичном порядке за отпущенные товарно-материальные ценности, выполненные работы и оказанные услуги.

1.11. Банковский счет – счет (счета) Клиента в рублях и/или в иностранной валюте, открытый (ые) Банком на имя Клиента на основании Договора банковского счета.

1.12. Компрометация ключа ЭП – констатация обстоятельств или наступление обстоятельств, при которых возможно несанкционированное использование закрытого ключа ЭП неуполномоченными лицами.

1.13. Оператор – владелец системы «Интернет-Банк», осуществляющий информационное и технологическое обслуживание Банка в системе «Интернет-Банк».

1.14. Удостоверяющий центр – юридическое лицо, осуществляющее изготовление сертификатов ключей подписи и действующее в соответствии с требованиями Федерального закона «Об электронной цифровой подписи» от 10.01.2002 № 1-ФЗ. Удостоверяющий центр обладает полномочиями по удостоверению сертификатов ключей подписи для осуществления обмена документами в электронно-цифровой форме.

Банк:	**Клиент:**
_____ **Задерг М.А.**	_____
м.п.	м.п.

Приложение 7
к Договору об электронном обмене документами, подписанных
электронной подписью (Интернет-банк) №_____

РЕГЛАМЕНТ
БАНКОВСКОГО ОБСЛУЖИВАНИЯ С ПРИМЕНЕНИЕМ
ЭЛЕКТРОННОЙ СИСТЕМЫ “Интернет-Банк”
«БСТ-БАНК» ЗАО

1. ОБЩИЕ ПОЛОЖЕНИЯ

Электронные платежные документы, применяемые в системе “Интеренет- Банк”, юридически эквивалентны бумажным платежным документам, используемым в соответствии с нормативными актами Центрального Банка Российской Федерации, и являются основанием для осуществления операции по счету Клиента.

Стороны признают, что используемая по настоящему Договору система телекоммуникации, обработки и хранения информации является достаточной для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а система защиты информации, обеспечивающая разграничение доступа, шифрование, контроль целостности и электронную цифровую подпись, является достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, и для разрешения спорных ситуаций.

Электронный документ (ЭД) порождает обязательства Сторон по настоящему Договору, если он передающей Стороной должным образом оформлен, заверен электронной цифровой подписью и передан, а принимающей Стороной получен, проверен и принят. Свидетельством того, что ЭД получен и принят, являются должным образом оформленные и заверенные электронной цифровой подписью электронные квитанции о получении и принятии в обработку ЭД.

Готовность Сторон к работе по системе «Интернет-Банк» оформляется подписанием Акта ввода в эксплуатацию клиентского модуля по форме Банка.

2. Порядок подключения к Системе

1.1. Обязательным условием подключения Клиента к Системе является наличие у него доступа в сеть Интернет, а также наличие собственного комплекта технического оборудования, удовлетворяющего требованиям Системы:

1.1.1. Персональный компьютер.

1.1.2. Программное обеспечение:

- Операционная система Windows XP или выше;
- Брандмауэр, который не должен запрещать работу браузера Internet Explorer по порту 443;
- Web - браузер Internet Explorer не ниже версии 5.5 (со стойкостью шифра 128-бит);
- Средства антивирусной защиты, не блокирующие работу компонентов Системы.

1.2. Действия сторон после заключения настоящего договора:

1.2.1. Клиент предоставляет письменную заявку о подключении Системы в Банк в 1-ом экземпляре по установленной форме Банка;

1.2.2. Банк в течение 5 рабочих дней после получения заявки передает Клиенту по акту приема-передачи USB-ключ (Приложение 8);

1.2.3. Клиент самостоятельно формирует закрытый ключ ЭП и передаёт в банк заявление на выдачу Сертификата ключа;

1.2.4. Банк подтверждает выдачу Сертификата ключа по положительному результату проверки сведений, указанных в заявлении на выдачу Сертификата ключа и в заявке на подключение ИБ;

1.2.5. Клиент самостоятельно записывает выданную ЭП на USB-ключ, подписывает и передаёт в банк акт приёма-передачи Сертификата ключа подписи.

1.2.6. Банк предоставляет Клиенту необходимую документацию о порядке работы Системы и осуществления операций с ее помощью, при необходимости, консультирует представителя Клиента о порядке работы с Системой.

1.3. С момента подписания акта приема-передачи USB-ключа риск его утраты лежит на Клиенте.

1.4. Создание закрытого и открытого ключей ЭП, PIN-кодов и паролей доступа осуществляется в порядке, предусмотренном Системой и требований, установленных действующим законодательством.

1.5. Подключение к Системе подтверждается Сертификатом ключа подписи электронного документа, формируемым Удостоверяющим центром в соответствии с требованиями Системы и действующего законодательства для подтверждения подлинности электронной цифровой подписи и идентификации участника Системы. Факт выдачи Клиенту Сертификата, оформляется актом приема–передачи, с момента подписания которого Клиент вправе осуществлять операции с использованием Системы.

1.6. С момента подписания акта приема-передачи Сертификата ключа, риск компрометации закрытого ключа третьими лицами лежит на Клиенте, за возможные убытки Клиента, возникшие вследствие этого, Банк ответственности не несет.

1.7. Информация о Сертификатах содержится в реестре Сертификатов ключей подписей Удостоверяющего центра, который обеспечивает актуальность реестра.

2. Общие условия и порядок электронного документооборота

2.1. Электронные документы передаются Клиентом с использованием средств Системы, при этом обмен документами на бумажных носителях сторонами не производится, кроме случаев, предусмотренных настоящим договором, в частности при возникновении обстоятельств непреодолимой силы или возможных нарушениях работы Системы, а также в иных случаях, предусмотренных соглашениями между Банком и Клиентом.

2.2. Банк осуществляет платежи на основании расчетных документов в электронной форме при условии соответствия этих документов требованиям законодательства РФ, Договора банковского счета, форматам, установленным Системой, а также наличия корректной ЭП.

2.3. Стороны признают, что полученные с помощью Системы электронные документы, заверенные ЭП, юридически эквивалентны документам, составленным на бумажном носителе, подписанным уполномоченными лицами и удостоверенным печатью Клиента и являются основанием проведения операций по счету Клиента.

2.4. В случае несоответствия электронного документа требованиям п.2.3. настоящего договора, положений заключенных между сторонами договоров, соглашений, а также в случае выявления угрозы несанкционированного доступа к программно-аппаратным средствам Клиента или его счетам, Банк отказывает в исполнении документа, уведомив Клиента посредством Системы о причинах отказа.

2.5. Прием электронных документов производится Банком круглосуточно. Исполнение документов осуществляется в операционное время. Документы, поступившие во внеоперационное время, отражаются по счетам на следующий рабочий день. Банк самостоятельно определяет продолжительность операционного дня. Информация о времени начала, и окончания операционного дня помещается у входа в операционный зал.

Сроки обработки платежей

Работа Системы обеспечивается Банком по рабочим дням по местному времени:

с 9:00 до 14:00 по межрегиональным платежам.

с 9:00 до 15:00 по остальным платежам.

В предпраздничные дни:

с 9:00 до 14:00 по всем платежам.

Обработка ЭД Банком в другое время возможна, но не гарантируется.

Списание средств со счета Клиента производится в соответствии с условиями заключенного с клиентом «Договора банковского счёта» на основании ЭД Клиента, переданных им по каналам связи в Банк.

2.6. Клиент имеет право отозвать ранее переданный ЭД, защищенный ЭП, при условии, что банк к моменту получения уведомления Клиента ещё не приступил к исполнению ранее полученного от Клиента ЭД.

2.7. Аварийный режим работы

2.7.1. При возникновении неисправности технических или программных средств Клиента, или других нештатных ситуаций, Клиент до 14 часов местного времени, того же дня, должен предупредить

уполномоченных сотрудников Банка, и осуществить действия для доставки в Банк, надлежащим образом оформленных бумажных платежных документов.

2.8. Прием электронных документов подтверждается электронным извещением Банка с указанием времени приема документа. При возникновении разногласий в правильности указания времени приема документов, Стороны признают, что временем приема документов является текущее время по системным часам аппаратных средств Банка.

2.9. Стороны признают, что способы защиты и обеспечения целостности информации, средства аутентификации и авторизации, применяемые Системой при передаче электронных документов, достаточны для подтверждения авторства и подлинности документов, и обязуются выполнять режим обеспечения безопасности, установленный правилами Системы. К исполнению документы принимаются только после проверки подлинности всех ЭП электронных документов.

2.10. Стороны признают, что срок действия Сертификата составляет один календарный год с даты его выдачи. Продление срока действия Сертификата осуществляется путем обновления Сертификата с обязательной сменой закрытого ключа ЭП. Обновление Сертификата производится по инициативе Клиента не позднее 15 календарных дней до момента окончания срока действия действующего Сертификата.

2.11. Исполнение сторонами обязательств по настоящему договору приостанавливается с момента окончания срока действия Сертификата и до момента оформления Клиенту нового Сертификата. В течение этого срока стороны не вправе проводить в Системе какие-либо операции, а Банк прекращает прием электронных документов

2.12. Стороны также признают, что:

2.12.1. при любом изменении электронного документа, совершенном после его подписания электронной цифровой подписью одной из сторон, электронная цифровая подпись становится некорректной;

2.12.2. знание информации, которая передается между сторонами по каналу связи Системы, не приводит к компрометации закрытых ключей ЭП сторон;

2.12.3. подделка электронной цифровой подписи участника Системы, т.е. создание корректной электронной цифровой подписи, невозможна без знания закрытого ключа ЭП;

2.12.4. созданный в единственном экземпляре в рамках настоящего договора закрытый ключ ЭП Клиента уникален, создание дубликата закрытого ключа ЭП возможно только Клиентом или при нарушении Клиентом условий хранения и/или использования закрытого ключа ЭП, предусмотренных настоящим договором;

2.12.5. каждый участник Системы несет ответственность за сохранение в тайне своих закрытых ключей ЭП, паролей, за правильность заполнения и оформления электронных документов и за действия своего персонала при работе с Системой. Правильность оформления и заполнения полей электронного документа проверяется ответственным должностным лицом Клиента. Ответственность за передачу ошибочного электронного документа несет Клиент.

2.12.6. заключая настоящий договор и проводя с использованием Системы операции настоящего договора, Клиент соглашается с тем, что привлечение Банком оператора и использование удостоверяющего центра для осуществления операций с использованием Системы (в частности, при формировании и передаче документов через процессинговый центр оператора) не является нарушением Банком банковской тайны.

2.12.7. Стороны определили, что в течение срока действия настоящего договора допускается временное приостановление Банком/Оператором работы Системы по техническим причинам, но не более чем на четыре часа в сутки.

3. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

3.1. Общие положения

3.1.1. Защита информации в Системе является многоуровневой и задействует возможности операционной системы, прикладного программного обеспечения и специализированных программных и технических средств и организационных мер (наличие соответствующих администраторов), организации хранения ПО задействованного в Системе.

3.1.2. Система комплексной защиты информации, состоящая из набора аппаратно-программных средств и административных мер, обеспечивает:

- создание ключей шифрования и электронно-цифровой подписи;
- электронно-цифровую подпись под документами;
- шифрование передаваемой информации;
- идентификацию и авторизацию Клиентов и разграничение их прав;
- достоверность факта получения документа получателем;
- подтверждение авторства и целостность электронных документов;
- выявление ошибок, сбоев и несанкционированных действий обслуживающего персонала;
- разбор конфликтных ситуаций.

3.1.3. Для разрешения возможных споров в Банке ведутся контрольные архивы ЭД подписанных ЭП, а также архивы открытых ключей электронно-цифровой подписи. Хранение контрольных архивов ЭД осуществляется в течение трех лет с момента проведения операции.
3.1.4. При проверке подписи под файлом (при расшифровке файла) используется соответствующий ключ подписи (шифрования) абонента, подписавшего (зашифровавшего) электронный файл.

3.2. Порядок хранения ключей ЭП и шифрования

3.2.1. Надежность закрытия и подлинности передаваемой по каналам связи информации обеспечивается только при условии сохранности от компрометации (утрата, копирование и т.п.) действующих ключей.
3.2.2. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение своих ключей. В случае потери, кражи, несанкционированного копирования или любого подозрения о компрометации ключей Клиент обязан немедленно оповестить Банк, прислав в дальнейшем подтверждение в письменной форме.
3.2.3. Банк и Клиент обеспечивают сохранность ключей. При этом выведенные из употребления открытые ключи хранятся те же сроки, что и документы, подписанные и зашифрованные этими ключами.

3.3. Порядок смены ключей

3.3.1. Смена ключей производится при:

- смене уполномоченных лиц по счету;
- истечении срока действия ключей.;
- компрометации ключей;
- заявлении одной из Сторон.

3.3.2. Срок действия ключей устанавливается в 365 дней с момента оформления Сертификата ключа электронно-цифровой подписи.
3.3.3. Смена ключей уполномоченных лиц Клиента производится при их личной явке.
3.3.4. ЭД, подписанный ЭП с использованием новых ключей принимается Банком только после получения Сертификата ключа электронно-цифровой подписи и проведения регистрации ключей в Системе.

3.4. Порядок блокировки ключей ЭП и шифрования

3.4.1. Банк блокирует (приостанавливает действия) ключа, с момента получения уполномоченными службами Банка письменного заявления Клиента о блокировке ключа (содержащего причину блокировки), подписанного руководителем и главным бухгалтером Клиента. В экстренных случаях, блокировка может быть произведена по устному заявлению Клиента, или иным способом (по телефону, по электронной почте, факсу и т.п.) с последующим предоставлением письменного заявления в течении 24 часов. Блокируемый ключ временно исключается из каталога открытых ключей, прием и обработка документов, подписанных данным ключом, прекращается.
3.4.2. Банк может блокировать ключ Клиента самостоятельно, в случае возникновения подозрений в компрометации ключа. В этом случае Банк немедленно извещает Клиента о принятом решении и о приостановлении обработки ЭД, подписанных этим ключом.
3.4.3. Снятие блокировки производится на основании заявления Клиента, подписанного руководителем и главным бухгалтером, об устранении причин, приведших к блокированию ключа. В случае блокировки ключа по инициативе Банка, снятие блокировки с ключа Клиента производится по согласованию с Клиентом и с его письменного разрешения.

3.5. Порядок исключения ключей ЭП и шифрования

3.5.1. Банк исключает (удаляет) ключ из каталога открытых ключей, с момента получения уполномоченными службами Банка письменного заявления Клиента, подписанного руководителем и главным бухгалтером. Ключ исключается из каталога открытых ключей, прием и обработка ЭД, подписанных данным ключом прекращается.

3.5.2. Банк и Клиент обеспечивают сохранность исключенных открытых ключей. При этом исключенные ключи хранятся те же сроки, что и документы, подписанные и зашифрованные этими ключами.

3.6. Порядок действий в случае компрометации секретных ключей

3.6.1. В случае компрометации или подозрения на компрометацию ключа, Клиент должен незамедлительно известить уполномоченных сотрудников Банка для блокировки соответствующего ключа (Приложение 3).

3.6.2. В случае не подтверждения компрометации ключа, Банк производит снятие блокировки сертификата ключа.

3.6.3. В случае подтверждения компрометации ключа Банк отключает сертификат скомпрометированного ключа из Системы.

3.6.4. ЭД, подписанные скомпрометированным ключом, и открытая часть ключа хранятся в соответствии с п.п.4.3.3.

3.7. При регенерации новых ключей по заявлению Клиента, одновременно производится отключение имеющихся ключей, с указанием причины отключения сертификата ключа.

3.8. Банк блокирует исполнение Электронных документов со счетов Клиента с использованием старого Секретного ключа.

3.9. Банк и Клиент проверяют, что все Электронные документы, принятые и проведенные Банком с использованием «старой» ЭП верны и не вызывают сомнений. По результатам проверки составляется акт, подписываемый сторонами.

Банк:	**Клиент:**
_____ **Задерг М.А.**	_____
м.п.	м.п.

Приложение 8
к Договору об электронном обмене документами, подписанных
электронной подписью (Интернет-банк) №_____

АКТ ПРИЕМА – ПЕРЕДАЧИ
USB-ключей

г._____ «___» _____ 20__г.

Ключевого носителя: USB-ключи
Серийный номер: №
Серийный номер: №

Количество:

Представитель ООО «БАНК»
передал:

(Должность)	*(Подпись)*	*(Ф.И.О.)*

Представитель:

(Наименование Клиента)
принял:

(Должность)	*(Подпись)*	*(Ф.И.О.)*

Приложение № 9

Вводная инструкция по работе с интернет банк Фактура

Для работы в системе Фактура Клиент получает смарт-ключ. Смарт-ключ - это не флеш накопитель, это защищенный носитель, который содержит только один закрытый ключ и сертификат, больше ничего невозможно записать на смарт-ключ.

При первой генерации ключа Клиент устанавливает два пароля. Первый пароль PIN (ПИН) для повседневной работы, второй пароль (код разблокировки администратора) на случай, если необходимо сменить первый пароль.

Банк не хранит пароли, в случае утери (блокировки) обоих паролей, смарт-ключ полностью и безвозвратно блокируется. Кол-во попыток для ввода пароля ограниченно смарт-ключом и составляет 10.

Смена заводских паролей обязательно производиться при первичной генерации обоих паролей

Банк рекомендует ставить сложные пароли содержащие 8 знаков, цифры, символы, заглавные и строчные.

В заявке на Интернет банк в поле уполномоченного сотрудника указанны данные:

- Email. На электронный адрес будут приходить уведомления об окончание сертификата (за 14 дней. до окончания срока) и ссылка на новый (процесс по продлению сертификата описан в инструкциях, который содержаться в самом интернет банке, на главной странице личного кабинете). Сертификат выдается на 1 год.
- Сотовый телефон. На телефон будут приходить СМС, в случае осуществления платежа от вашего имени. В случае, если Клиент не осуществлял платеж в договоре прописан порядок действий по дистанционному блокированию платежа.

Требования к обеспечению безопасности:

При смене должностного лица незамедлительно необходимо поменять сертификат и документы в банке (Смарт-ключ приобретается организацией один раз, при повторной выдаче сертификата приобретать не нужно)

В случае утери ключа, не корректной работы или выхода из строя необходимо обратиться в банк (предварительно заблокировав ключ по телефону, порядок прописан в договоре)

При смене Email и сотового телефона, необходимо обратиться в банк или направить средствами интернет-Банка письмо в свободной форме, содержащее наименование организации, дату, подпись и расшифровку ФИО руководителя. Описание причины, и какие данные нужно изменить.

Банк рекомендует не передавать смарт-ключ третьим лицам, своевременно уведомлять о проблемах работы в системе, об изменениях Email и сотового телефона, соблюдать требовании договора по обеспечению информационной безопасности, в противном случае банк не несет ответственности за неправомерные операции или задержки в совершение операций.

«_____»_____ 20___г.

_____

наименование организации

_____/_____

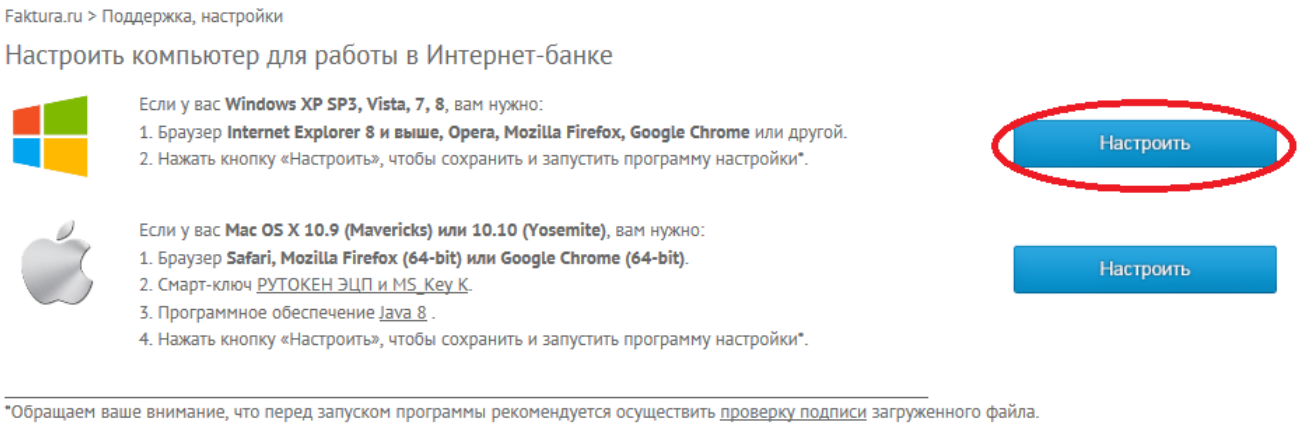
подпись/ расшифровка

Приложение № 10

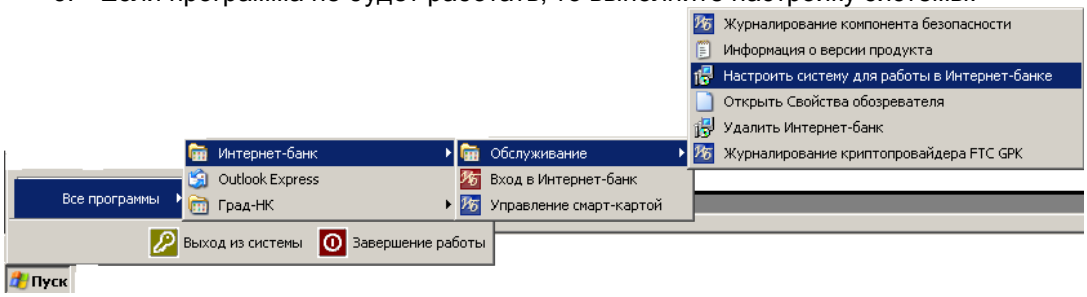
Инструкция по настройке компьютера для работы в Интернет-банке:

(Если вы уже используете другой Интернет-банк, то ничего настраивать не нужно, просто меняете смарт-карты. Не должно быть подключено больше одной смарт-карты за раз!)

1. Зайдите на сайт www.faktura.ru
2. Нажмите кнопку «Настройка и поддержка»
3. Далее перейдите по ссылке «1. Настроить компьютер для работы в системе»
4. Находим операционную систему, стоящую на вашем компьютере. (Чтобы узнать какая у вас операционная система, нажмите «Пуск – Правой кнопкой мыши по «Мой компьютер» - свойства). Далее нажимаем кнопку настроить, как на картинке.



5. После установки программы на рабочем столе появится ярлык «Вход в Интерент-банк». Чтобы зайти в Интернет-банк, вставьте смарт-карту в компьютер и запустите созданный ярлык.
6. Если программа не будет работать, то выполните настройку системы:



7. ПО умолчанию на смарт картах рутокен установлен пароль 12345678 (ПИН), при первом запуске интернет банка его необходимо сменить (устанавливаемый вами пароль должен содержать 8 знаков (рекомендуем использовать в пароле цифры, символы, заглавные и строчные буквы)).

8. Для смены пароля заходим в «Пуск – Все программы – Интернет-банк – Обслуживание – Управление смарт-картой», выбираем смену пароля, вводим сначала первичный пароль затем дважды вводим устанавливаемый пароль и нажимаем ОК.

9. В случае, если вы забыли пароль от своего ключа, вы можете ввести код разблокировки администратора (базовый пароль администратора 87654321), при первом запуске интернет банка его необходимо сменить (устанавливаемый вами пароль не должен содержать 8 знаков (рекомендуем использовать в пароле цифры, символы, заглавные и строчные буквы)). После чего вам будет предложено ввести свой ПИН заново. В случае если вы введете его не верно карта заблокируется после 10 попыток.
   По всем вопросам связанным с паролями, рекомендуем обратиться по номеру: +7(495)925-77-90 (поддержка смарт картах RuToken)

10. Скачать краткие инструкции пользователя можно на сайте www.faktura.ru в разделе «Настройка и поддержка» - «4. Скачать инструкции пользователя». Нужные инструкции «Интернет-банк для корпоративных клиентов» и «Инструкция по экспорту/импорту данных в 1С», если вы пользуетесь 1С. Или на главной странице интернет банка фактура.

Смарт карт РУТОКЕН

Телефон технической поддержки банка 777-448 (с 9-00 до 17-00)
Телефон технической поддержки системы интернет банк указан на главной странице сайта www.faktura.ru