

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ «КЛИЕНТ-БАНК» К ДОГОВОРУ НА РАСЧЕТНО-КАССОВОЕ ОБСЛУЖИВАНИЕ

1. Термины и определения

1.1. Термины «Электронная подпись» (ЭП), «Ключ электронной подписи», «Ключ проверки электронной подписи», «Сертификат ключа проверки электронной подписи», «Владелец сертификата ключа проверки электронной подписи» (Владелец сертификата), «Удостоверяющий центр» применяются в настоящем Соглашении в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

1.2. Специальные термины, применяемые в тексте настоящего Соглашения, используются в следующем значении:

Автоматизированная система Дистанционного Банковского Обслуживания «Клиент-Банк» (Система ДБО) – корпоративная информационная система «Клиент-Банк» ООО «Банк «Элита», включающая в себя совокупность программно-аппаратных средств, устанавливаемых у Клиента и Банка с целью обеспечения подготовки, защиты, отправки, приема, проверки и обработки документов в электронном виде.

Система ДБО состоит из:

- программных и аппаратных средств, соответствующих требованиям Банка, комплектуемых и эксплуатируемых Клиентом за свой счет;
- аппаратных средств Банка, эксплуатируемых Банком за свой счет;
- программных средств Системы ДБО, устанавливаемых в соответствующих частях на аппаратных средствах Клиента и Банка и самостоятельно эксплуатируемых Сторонами;
- программных и аппаратных средств связи, обеспечивающих обмен электронными документами между Сторонами.

Автоматизированное рабочее место «Клиент-Банк» (АРМ «Клиент») (Клиентская часть Системы ДБО) – составная часть Системы ДБО, устанавливаемая на территории Клиента, используемая Клиентом для предоставления в Банк и получения от Банка электронных документов. АРМ «Клиент» является основным рабочим местом Клиента в Системе ДБО.

Авторство ЭД – принадлежность ЭД создавшей его Стороне.

СКЗИ Рутокен ЭЦП 2.0 (СКЗИ) – средство криптографической защиты информации, используемое для генерации и хранения ключей ЭП и ключей проверки ЭП, формирования и проверки ЭП.

Дополнительное рабочее место «Клиент-Банк» - составная часть Системы ДБО, устанавливаемая на программно-аппаратных средствах Клиента, используемая Клиентом для предоставления в Банк и получения от Банка электронных документов.

Ключи шифрования – ключи, изготавливаемые Банком с использованием средств Системы ДБО и предназначенные для защиты ЭД Сторон при их передаче по каналам связи. Передача ключей шифрования Банком Клиенту отражается в Акте приема-передачи программного обеспечения и средств защиты автоматизированной Системы ДБО «Клиент-Банк», который подписывается Сторонами.

Корректная электронная подпись – электронная подпись, дающая положительный результат ее проверки программно-аппаратными средствами Системы ДБО, с использованием действующего на момент подписания ключа проверки электронной подписи его владельца.

Пароль СКЗИ Рутокен ЭЦП 2.0 – пароль, необходимый для получения доступа к функциям СКЗИ Рутокен ЭЦП 2.0.

Уполномоченное лицо Клиента – сотрудник Клиента, уполномоченный распоряжаться денежными средствами, находящимися на счете, и совершать иные действия, предусмотренные разделом 1 настоящего Соглашения, используя электронную подпись.

Уполномоченное лицо Банка – физическое лицо Банка, уполномоченное предоставлять Клиенту информацию об операциях, совершенных по счету(-ам), и остатках средств по счету(-ам) Клиента, и совершать иные действия, предусмотренные разделом 1 настоящего Соглашения, используя электронную подпись.

Хэш-функция – однонаправленное отображение (свертка) содержимого файла или блока данных произвольного размера в блок данных фиксированного размера, обладающее заданными математическими свойствами; используется при формировании и проверке ЭП, а также для контроля целостности программного обеспечения и данных.

ЭП Стороны (ЭП Банка или Клиента) – ЭП любого уполномоченного лица Стороны.

Электронный документ (ЭД) – электронный образ документа (платежного или иного), представленный в согласованном Сторонами формате, определяемом программными средствами создания документа. ЭД передается между Сторонами в составе файла, подписанного ЭП. В состав файла может входить несколько ЭД. Если файл имеет корректную ЭП, то каждый электронный документ, входящий в файл, считается подписанным ЭП.

Электронный платежный документ (ЭПД) – электронный документ (платежное поручение Клиента), являющийся основанием для совершения Банком операций по банковскому счету Клиента. ЭПД, защищенные корректной ЭП, имеют равную юридическую силу с расчетными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.

Электронный служебно-информационный документ – электронный документ, защищенный корректной ЭП и обеспечивающий обмен информацией между Банком и Клиентом при совершении расчетов и проведении операций по счету Клиента.

Arbiter-РКИ – программное обеспечение ЗАО Сигнал-КОМ, предназначенное для подтверждения авторства и целостности электронных документов, подписанных ЭП.

2. Общие положения

2.1. Настоящие Условия регулирует отношения Сторон, возникшие в процессе оказания Банком услуг по дистанционному банковскому обслуживанию Клиента с использованием Системы Дистанционного Банковского Обслуживания «Клиент-Банк» (далее – Система ДБО «Клиент-Банк» или Система ДБО).

2.2. Обслуживание Клиентов в Системе ДБО осуществляется Банком на основании данного Соглашения, состоящего из Заявлений о присоединении к Дополнительному соглашению (Приложение 11 к настоящему Дополнительному соглашению).

2.3. Клиент в соответствии со статьей 428 Гражданского кодекса Российской Федерации, полностью и безусловно присоединяется к Условиям Дополнительного Соглашения дистанционного банковского обслуживания «Клиент-Банк» к Договору на расчетно-кассовое обслуживание путем подписания Заявления о присоединении к Дополнительному соглашению.

2.4. Стороны признают, что используемая для обработки и хранения информации по Дополнительному соглашению дистанционного банковского обслуживания Система ДБО, является достаточной для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а используемые средства защиты информации,

обеспечивающие разграничение доступа, шифрование, контроль целостности и формирование ЭП, являются достаточными для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых ЭД, обеспечения целостности информации, условий неотказуемости, неизменности, достоверности, отсутствия искажений, а также разрешения спорных ситуаций при условии соблюдения Сторонами мер безопасности, в том числе обеспечения Клиентом надлежащей защиты Клиентского модуля Системы ДБО от несанкционированного доступа.

Клиент понимает повышенный риск несанкционированного использования Системы ДБО, включая компрометацию ключей ЭП и несанкционированное удаленное управление Клиентским модулем Системы ДБО, при ненадлежащем соблюдении Клиентом мер безопасности.

2.5. Конфиденциальными сведениями признаются сведения, содержащиеся в документах, переданных Сторонами друг другу по Системе ДБО, персональные электронные адреса, идентификационные параметры, регистрационные номера, пароли и ключи ЭП Сторон, используемые для разграничения доступа, передачи и защиты передаваемой информации, а также материалы работы комиссии по разбору спорных ситуаций. Передача конфиденциальных сведений третьим лицам подлежит только в случаях и в порядке, установленных действующим законодательством Российской Федерации.

2.6. Стороны обязуются обеспечить доступ к работе в Системе ДБО только Уполномоченным лицам Клиента в соответствии с Заявлением о присоединении к Дополнительному соглашению дистанционного банковского обслуживания «Клиент-Банк» и запросами на выдачу сертификатов ключей проверки ЭП.

2.7. Для получения доступа к работе в Системе ДБО Клиент предоставляет ответственному работнику Банка Акт признания открытого ключа ЭП (сертификат) для обмена сообщениями. Количество Актов должно соответствовать количеству Уполномоченных лиц Клиента, указанных в Заявлении о присоединении к Дополнительному соглашению дистанционного банковского обслуживания «Клиент-Банк».

2.8. В соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» ЭД признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случае соблюдения следующих условий:

- ЭД передан одной Стороной другой Стороне с использованием программного обеспечения Системы ДБО, СКЗИ;
- для ЭД пройдена проверка ЭП в соответствии с настоящим Дополнительным соглашением с использованием СКЗИ;
- для ЭД, переданных Клиентом в Банк, пройдена проверка в соответствии со всеми процедурами защиты информации.

2.9. При возникновении у Банка подозрений о нарушении требований по защите информации при проведении Банком проверки ЭД на соответствие всем процедурам защиты информации Клиент должен подтвердить Банку исполнение требований по защите информации в порядке, предусмотренном пунктом 3.2.8 настоящего Дополнительного соглашения.

2.10. Подлинность ЭП осуществляется автоматически в Системе ДБО с использованием СКЗИ.

2.11. Свидетельством того, что ЭД получен, проверен и принят, а также проверена подлинность ЭП указанного ЭД, является соответствующий статус, присваиваемый ЭД в Системе ДБО.

2.12. Система ДБО присваивает следующие статусы ЭД:

- «Создан», «Импортирован», «Доставлен», «Исполнен», «Отвергнут Банком», «Отложен», «Отозван», «Ошибка контроля», «Подписан», «Частично подписан», «ЭП/АСП неверна», «Принят», «Приостановлен».

2.13. В случае выставления инкассового поручения к счету плательщика, необходимо предоставить в Банк или Банк плательщика документы, подтверждающие данное право на бумажном носителе.

2.14. На момент подписания Заявления о присоединении к Дополнительному соглашению дистанционного банковского обслуживания «Клиент-Банк» Клиент признает факт ознакомления со всеми условиями Дополнительного соглашения и соответствующих Приложений к нему.

2.15. Подтверждающим фактом совершения операций по счету с использованием Системы ДБО является получение на электронных и/или бумажных носителях соответствующего уведомления.

3. Права и обязанности Банка

3.1. Банк обязуется:

3.1.1. Передавать пакет программных средств и документов Клиенту, либо Представителю Клиента на основании доверенности, оформленной в соответствии с Приложением 3 к настоящему Дополнительному соглашению.

Фактом передачи Клиенту, либо Представителю Клиента ключевой информации для подключения Клиента к Системе ДБО подтверждается подписанием Сторонами Актов приема-передачи по форме Приложения 1 к настоящему Дополнительному соглашению.

Фактом передачи Клиенту, либо Представителю Клиента ключевого носителя является фиксирование в соответствующем журнале учета.

3.1.2. Принимать к исполнению, осуществлять обработку и исполнение ЭД, полученных по Системе ДБО, признанные равнозначными документу на бумажном носителе, подписанному собственноручной подписью, оформленные и подписанные (заверенные) Клиентом в соответствии с карточкой с образцами подписей и оттиском печати, действующей на дату подписания ЭД.

3.1.3. Предоставлять Клиенту по Системе ДБО следующие виды сообщений: выписки по счетам, сертификат ключа проверки электронной подписи, письма из банка прочие сообщения.

3.1.4. Осуществлять консультирование клиентов по использованию Системы ДБО при обращении по контактному телефону 8 (4842) 27-74-20 (пн.-чт. с 9.00 до 17.45, пт. с 9.00 до 16.30).

3.1.5. Обеспечить конфиденциальность информации по счетам Клиента.

3.1.6. Обеспечить защиту Системы ДБО от несанкционированного доступа.

3.1.7. Незамедлительно сообщать Клиенту об обнаружении попытки несанкционированного доступа к Системе ДБО любым доступным Банком способом.

3.1.8. В случае приостановления операций по переводу денежных средств для проведения контроля в целях предотвращения осуществления перевода денежных средств без согласия Клиента:

- незамедлительно информировать Клиента любым доступным способом о приостановлении операции по переводу денежных средств, а также о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без согласия;

- запрашивать у Клиента подтверждение возобновления исполнения распоряжения о переводе денежных средств.

3.1.9. При получении уведомления от Клиента об утрате/компрометации, либо подозрении на компрометацию ключа ЭП или о совершении операции с использованием Системы ДБО без согласия клиента, отзывается/приостанавливается действие сертификата ключа.

3.1.10. Формировать и направлять Клиенту выписки по счету о совершении каждой операции с использованием Системы ДБО не позднее 10.00 рабочего дня, следующего за днем совершения операции.

3.1.11. Хранить направленные Клиенту уведомления о совершенных операциях, а также о полученных от Клиента уведомлениях об утрате/компрометации, либо подозрении на компрометацию ключа ЭП или о совершении операции с использованием Системы ДБО без согласия Клиента, не менее 5 (пяти) лет со дня прекращения деловых отношений с клиентом.

Предоставление Клиенту необходимой информации осуществляется на основании соответствующего запроса Клиента, оформленного в письменной форме, либо направленного в Банк в электронном виде с использованием Системы ДБО.

3.1.12. В случае внесения изменений в программное обеспечение Системы ДБО не менее чем за 7 (семь) рабочих дней до введения в действие изменений уведомить Клиента путем направления информации через Систему ДБО.

3.2. Банк имеет право:

3.2.1. На основании заранее данного акцепта списывать плату за осуществление дистанционного банковского обслуживания Клиента в соответствии с действующими Тарифами Банка.

3.2.2. Если на момент оказания услуги у Клиента отсутствуют открытые в Банке счета, оплата производится безналичным переводом со счета Клиента, открытого в другом Банке в соответствии с действующими Тарифами Банка.

3.2.3. При недостаточности денежных средств на счете Клиента, ЭД помещаются в очередь неисполненных в срок распоряжений, после чего списание денежных средств осуществляется в соответствии со ст. 855 ГК РФ.

3.2.4. В случае необходимости связаться с Клиентом по контактными номерами телефонов для получения подтверждения подлинности ЭД, поступившего по Системе ДБО.

3.2.5. Требовать от Клиента оформления платежного документа на бумажном носителе, о чем Банк обязан сообщить Клиенту не позднее следующего рабочего дня с момента получения ЭД по Системе ДБО.

3.2.6. В одностороннем порядке вносить изменения в программное обеспечение Системы ДБО или данное дополнительное соглашение с обязательным уведомлением Клиента согласно п. 3.1.12 настоящего Соглашения.

3.2.7. В одностороннем порядке вносить изменения в действующие Тарифы Банка, предварительно уведомив Клиента за 14 (четырнадцать) рабочих дней, путем размещения информации в помещении Банка и на официальном сайте Банка: www.bankelita.ru.

3.2.8. После предварительного предупреждения, отказать Клиенту в приеме от него распоряжений на проведение операции по банковскому счету, подписанного корректной ЭП, при наличии у Банка подозрений о том, что целью такого распоряжения является совершение сомнительных операций в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма. В данном случае Клиент предоставляет в Банк оформленные надлежащим образом расчетные документы на бумажном носителе.

3.2.9. Приостановить использование Системы ДБО в случае не предоставления Клиентом обновленных идентификационных сведений (документов) о Клиенте, Представителе Клиента, Бенефициарных владельцах, а также иной информации в соответствии с требованиями Положения Банка России от 15.10.2015 №499-П «Об идентификации кредитными организациями клиентов, представителей клиентов, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

3.2.10. Приостановить использование Системы ДБО на срок не более 2 (двух) рабочих дней в целях предотвращения осуществления перевода денежных средств без согласия

Клиента до получения от Клиента подтверждения авторства распоряжения. При получении от Клиента подтверждения, Банк незамедлительно возобновляет исполнение распоряжения и возобновляется доступ к Системе ДБО.

В случае неполучения по истечении 2 (двух) рабочих дней от Клиента подтверждения, доступ к Системе ДБО возобновляется, и исполнение Банком ЭД осуществляется в соответствии с требованиями Федерального закона от 27.06.2011 №161-ФЗ «О национальной платежной системе».

3.2.11. В одностороннем порядке расторгнуть Дополнительное соглашение о использовании Системы ДБО, в любое время, в том числе, если в течение 6 (шести) месяцев Клиентом не уплачивалось комиссионное вознаграждение.

Банк уведомляет Клиента о предстоящем расторжении Дополнительного соглашения за 30 (тридцати) календарных дней путем направления письма Клиенту по адресу, указанному в Заявлении о присоединении к Дополнительному соглашению.

3.3. Клиент обязуется:

3.3.1. Выполнять требования настоящего Дополнительного соглашения.

3.3.2. Обеспечить защиту клиентской части Системы ДБО от несанкционированного доступа и заражения вредоносным кодом. В случае обнаружения неработоспособности Системы ДБО, признаков несанкционированного доступа, признаков заражения вредоносным кодом, не позднее дня, следующего за днем обнаружения, известить Банк любым доступным способом.

3.3.3. Не разглашать и не передавать другим лицам (обеспечить конфиденциальность) информацию, связанную с использованием Системы ДБО, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и условиями настоящего Соглашения.

3.3.4. Подписывать электронные платежные документы ЭП уполномоченных лиц в соответствии с требованиями действующего законодательства Российской Федерации¹ и Банка России.

3.3.5. При подключении к Системе ДБО после получения Клиентом ключевого носителя создать запрос на соответствующий им сертификат ключа проверки ЭП, направив в Банк в электронном виде и на бумажном носителе Акт признания открытого ключа ЭП (сертификата) для обмена сообщениями в двух экземплярах, подписанных со стороны Клиента и заверенный печатью (при наличии).

3.3.6. Оплачивать комиссионное вознаграждение Банка в соответствии с действующими Тарифами. Данное условие также является заранее данным акцептом Клиента Банку на списание причитающегося ему вознаграждения.

3.3.7. При получении от Банка уведомления о смене программного обеспечения осуществлять необходимые действия для своевременного получения и установки новой версии программного обеспечения Системы ДБО.

3.3.8. В установленные Банком сроки осуществлять необходимые мероприятия по плановой смене действующих ключей ЭП и соответствующих им сертификатов ключей проверки ЭП.

3.3.9. В случае компрометации ключа ЭП/логина/пароля от Системы ДБО незамедлительно, но не позднее чем за 1 (один) час до завершения работы по обслуживанию Клиентов, уведомить Банк о случившемся.

3.3.10. В случае перевода на другую работу/увольнением лица, имеющего право подписи, незамедлительно предоставить в Банк новую карточку с образцами подписей и оттиском печати и Соглашение о количестве и сочетании подписей к карточке, а также осуществить мероприятия по аннулированию действующего сертификата ключа проверки ЭП.

¹ Федеральный закон «О бухгалтерском учете» от 06.12.2011 N 402-ФЗ

Вместе с карточкой с образцами подписей и оттиском печати представить в Банк документ, удостоверяющий личность уполномоченного лица Клиента, а также передать в Банк документы, подтверждающие права уполномоченного лица Клиента по распоряжению денежными средствами, находящимися на счете, используя ЭП или копии указанных документов, заверенные установленным порядком.

3.3.11. Обеспечить согласие физических лиц, персональные данные которых содержатся в представляемых Клиентом Банку документах в рамках настоящего Соглашения, на проверку и обработку (включая автоматизированную обработку) их персональных данных Банком в соответствии с требованиями действующего законодательства Российской Федерации, в том числе Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Рекомендуемая форма заявления о согласии размещается на сайте ООО банк «Элита».

3.3.12. Не позднее следующего рабочего дня после совершения операций по счету без согласия Клиента с использованием Системы ДБО, не позднее чем за 1 (один) час до завершения работы по обслуживанию Клиентов, уведомить Банк о случившемся путем подачи заявления на бумажном носителе, подписанного уполномоченным лицом Клиента, либо путем обращения в Банк по контактному телефону, указанному в Заявлении о присоединении к Дополнительному соглашению дистанционного банковского обслуживания Системы «Клиент-Банк».

3.3.13. В случае приостановления Банком операции в целях предотвращения осуществления перевода денежных средств без согласия Клиента, подтверждать авторство ЭД в течение 2 (двух) рабочих дней со дня приостановления операции.

3.4. Клиент имеет право:

3.4.1. Обращаться в Банк за консультациями по вопросам эксплуатации Системы ДБО, а также получать из Банка справочную информацию.

3.4.2. Отозвать ранее переданный ЭД, имеющий корректную ЭП Клиента, путем направления в Банк по Системе ДБО соответствующего уведомления в виде электронного служебно-информационного документа, защищенного ЭП, при условии, что Банк к моменту получения уведомления Клиента не произвел списание со счета Клиента денежных средств во исполнение ранее полученного от Клиента электронного платежного документа.

3.4.3. Приостановить предоставление услуг по настоящему Соглашению, путем направления не менее, чем за 7 (семь) дней письменного уведомления с указанием даты начала и даты окончания приостановки предоставления услуг, заверенного руководителем Клиента или лицом, наделенного правом подписывать Договор(ы) финансово-банковских услуг, а также оттиском печати Клиента.

3.4.4. В любое время производить замену ключей ЭП Клиента.

3.4.5. Обращаться в Банк с заявлением об использовании фиксированного IP-адреса, а также об установлении:

- максимальной суммы перевода денежных средств с использованием Системы ДБО за одну операцию и (или) за определенный период времени (например, один день, один месяц);
- перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием Системы ДБО;
- временного периода, в который могут быть совершены переводы денежных средств с использованием Системы ДБО.

3.4.6. В случае несогласия с изменениями условий настоящего Дополнительного соглашения и/или Тарифов Банка, а также в любых иных случаях Клиент имеет право расторгнуть настоящее Дополнительное соглашение в одностороннем порядке путем направления в Банк письменного уведомления.

4. Ответственность сторон

4.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Дополнительному соглашению виновная Сторона несет ответственность в соответствии с действующим законодательством Российской Федерации.

4.2. Стороны несут ответственность за содержание ЭД, подписанных ЭП их уполномоченных лиц, и не отвечают за правильность заполнения и оформления ЭД другой Стороной.

4.3. В случае неоплаты Банку предоставленных услуг (в том числе по причине отсутствия достаточной суммы средств на счете Клиента или невозможности списания средств в связи с приостановлением расходных операций по счету или наложением ареста на денежные средства, находящиеся на счете), Банк имеет право приостановить на срок до одного месяца предоставление услуг по настоящему Соглашению, а в случае неоплаты по истечении 6 (шести) месяцев – расторгнуть Соглашение в одностороннем порядке без соблюдения срока, установленного настоящим Соглашением. При этом Клиенту направляется письменное уведомление о расторжении данного Соглашения.

4.4. Банк несет ответственность за неизменность и конфиденциальность ЭД на всем цикле его обращения в расчетной сети Банка с момента приема ЭД по Системе ДБО.

4.5. Клиент несет ответственность за целостность и конфиденциальность ЭД на всем цикле его создания и обращения до момента ввода его в Систему ДБО. Ввод считается завершенным после положительного результата проверки в Банке ЭД электронным ключом.

4.6. Клиент несет ответственность за достоверность сведений, предоставляемых в Банк.

4.7. Банк не несет ответственность за ошибочное списание средств со счета по ошибочным ЭД, составленным и подписанным Клиентом.

4.8. Банк не несет ответственности в случае не уведомления или несвоевременного уведомления Клиентом обо всех случаях утраты или раскрытия (компрометации) электронного ключа, иных сведений необходимых для подтверждения достоверности электронного платежного документа.

4.9. Банк не несет ответственности за ущерб, возникший вследствие разглашения уполномоченными лицами Клиента собственного ключа ЭП, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.

4.10. Банк не несет ответственности за последствия исполнения электронного платежного документа, защищенного корректной ЭП Клиента, в т. ч. в случае использования ключей ЭП и программно-аппаратных средств клиентской части Системы ДБО неуполномоченным лицом.

4.11. Банк не несет ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к части Системы ДБО, установленной у Клиента, и криптографическим ключам Клиента, включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи.

4.12. Банк не несет ответственности за неработоспособность оборудования и программных средств Клиента, и третьих лиц, повлекшую за собой невозможность доступа Клиента к банковской части Системы ДБО и возникшие в результате задержки в осуществлении платежей Клиента, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах Клиента, подключенных к сети Интернет для обеспечения предоставления услуг по настоящему Соглашению.

4.13. Убытки, возникшие в результате невыполнения какой-либо стороной условий настоящего Соглашения, направленных на обеспечение безопасности электронных расчетов, несет сторона, допустившая данные нарушения.

4.14. Если несанкционированный доступ происходит, несмотря на надлежащее исполнение Сторонами требований безопасности, риск убытков несет Сторона направившая ЭД.

4.15. В случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих или препятствующих осуществлению Сторонами своих функций по Соглашению и иных обстоятельств, не зависящих от волеизъявления Сторон, Стороны по настоящему Соглашению освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.

При наступлении обстоятельств непреодолимой силы Сторона должна в течении 3 рабочих дней известить о них другую Сторону. Извещение должно содержать данные о характере обстоятельств, а также оценку их влияния на возможность исполнения Стороной обязательств по настоящему Соглашению.

По прекращении указанных выше обстоятельств Сторона должна в течении трёх рабочих дней известить об этом другую Сторону. В извещении должен быть указан срок, в течение которого предполагается исполнить обязательства по настоящему Соглашению.

5. Порядок разрешения споров

5.1. В случае возникновения споров по настоящему Дополнительному соглашению стороны примут все меры к их разрешению на взаимоприемлемой основе путем переговоров.

5.2. Для разрешения спорной ситуации, связанной с отказом Клиента от авторства или содержания электронного документа или связанной с отказом Банка от факта приема или проводки электронного документа, переданного Клиентом по Системе ДБО, стороны создают совместную комиссию (Приложение 8 к настоящему Дополнительному соглашению).

5.3. На время разрешения спорной ситуации, связанной с исполнением Банком платежного поручения Клиента, Банк имеет право приостановить действие настоящего Дополнительного соглашения в одностороннем порядке с последующим письменным уведомлением Клиента.

5.4. Принятие споров к рассмотрению и урегулированию производится в течение 1 (одного) дня следующего за днем совершения Банком операций по поступившему через Систему ДБО электронному документу.

5.5. При невозможности разрешения споров и разногласий путем переговоров они разрешаются в арбитражном суде Калужской области в соответствии с действующим законодательством РФ.

6. Срок действия дополнительного соглашения, порядок его изменения и расторжения

6.1. Настоящее соглашение вступает в силу с момента подписания Банком подписанного Клиентом Заявления о присоединении к данному Дополнительному соглашению и заключается на неопределенный срок.

6.2. Настоящее Дополнительное соглашение утрачивает силу автоматически при окончании срока действия или досрочном расторжении соответствующего Договора на расчетно-кассовое обслуживание.

6.3. Все изменения и дополнения к настоящему Дополнительному соглашению дистанционного банковского обслуживания «Клиент-Банк» оформляются в письменном виде по обоюдному согласию сторон в виде соглашения и вступают в силу с момента их подписания полномочными представителями обеих Сторон.

6.4. В случае расторжения настоящего Дополнительного соглашения или прекращения его действия, Клиент имеет право вернуть Банку носитель электронной

цифровой подписи Рутокен ЭЦП 2.0, о чем составляется соответствующий акт приёма-передачи.

6.5. В случае наступления условий, изложенных в п. 6.4. настоящего Дополнительного соглашения, стороны обязаны выполнить все взаимные обязательства, вытекающие из настоящего Дополнительного соглашения.

6.6. Все приложения к настоящему Дополнительному соглашению являются его неотъемлемой частью.

7. Приложения

7.1. Приложение 1 «Акт приема-передачи Клиентской части Системы ДБО «Клиент-Банк» по дополнительному соглашению ДБО «Клиент-Банк» в ООО банк «Элита» №__ от «__» __ 20__ г. к договору на расчетно-кассовое обслуживание №__ от «__» __ 20__ г.

7.2. Приложение 2 «Форма Анкеты для технической работы и поддержки Системы ДБО «Клиент-Банк» к дополнительному соглашению ДБО «Клиент-Банк» в ООО банк «Элита» №__ от «__» __ 20__ г.

7.3. Приложение 3 «Доверенность на получение средств криптографической защиты информации и электронной цифровой подписи».

7.4. Приложение 4 «Правила безопасности Клиента при использовании Системы ДБО «Клиент-Банк».

7.5. Приложение 5 «Уведомление об изменении параметров подключения к Системе ДБО «Клиент-Банк».

7.6. Приложение 6 «Порядок ввода в действие Системы ДБО и общие условия предоставления услуг и обслуживания Системы ДБО».

7.7. Приложение 7 «Заявление на приостановление / отключение Системы ДБО «Клиент-Банк».

7.8. Приложение 8 «Процедура проведения технической экспертизы спорных ситуаций, связанных с принятием или непринятием, исполнением или неисполнением Банком электронного документа Клиента».

7.9. Приложение 9 «Заявление о смене логина и пароля при их компрометации для Системы ДБО «Клиент-Банк».

7.10. Приложение 10 «Акт признания открытого ключа ЭП (Сертификата) для обмена сообщениями».

7.11. Приложение 11 «Заявление о присоединении к Дополнительному Соглашению дистанционного банковского обслуживания «Клиент-Банк» в ООО банк «Элита» №_____».

**«Акт приема-передачи Клиентской части Системы ДБО «Клиент-Банк»
к дополнительному соглашению ДБО «Клиент-Банк» в ООО банк «Элита»
№ _____ от « ____ » _____ 20 ____ г.**

г. _____ « ____ » _____ 20 ____ г.

Общество с ограниченной ответственностью банк «Элита», именуемое в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____ (указывается организационно-правовая форма и наименование юридического лица/ Ф.И.О. индивидуального предпринимателя)

в лице _____, действующего на основании _____, именуемый в дальнейшем «Клиент», с другой стороны, вместе «Стороны», а индивидуально «Сторона», составили настоящий Акт о нижеследующем.

1. Банк передал, а Клиент принял дистрибутивные копии программных средств Системы ДБО «Клиент-Банк» и СКЗИ в следующем составе:

- Утилита Панель управления Рутокен для управления Носителем Ключевой Информации Рутокен ЭЦП 2.0 (в электронном виде);
- Анкеты, Заявления, Акты, Памятки, Требования, Правила для работы по Соглашению;
- Запечатанный конверт с паролем для входа в систему.
- СКЗИ Рутокен ЭЦП 2.0 в количестве _____ штук.

2. Настоящий Акт составлен в 2-х экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон и является неотъемлемой частью Дополнительного соглашения дистанционного банковского обслуживания «Клиент-Банк».

Банк:

_____/_____
(подпись) (Фамилия И.О.)

М.П.

Клиент:

_____/_____
(подпись) (Фамилия И.О.)

М.П.

Форма Анкеты
для технической работы и поддержки Системы ДБО «Клиент-Банк»
к дополнительному соглашению ДБО «Клиент-Банк» в ООО банк «Элита»
№ _____ от « ____ » _____ 20 ____ г.

Обеспечить функционирование Системы ДБО со следующих IP – адресов / фиксированных сетей Клиента:

№ п/п	IP-адрес / фиксированная сеть
1	
2	
3	

Номера мобильных и стационарных телефонов Клиента для службы технической поддержки системы ДБО «Клиент-Банк»:

№ п/п	Номер мобильного телефона	ФИО пользователя
1	+7 (____) _____	
2	+7 (____) _____	
3	+7 (____) _____	
4	8 _____	
5	8 _____	

E-Mail Клиента для службы технической поддержки системы ДБО «Клиент-Банк»:

№ п/п	E-Mail	ФИО пользователя
1		
2		
3		
4		
5		

Кодовое слово для обращения в службу технической поддержки:

№ п/п	Кодовое слово	ФИО пользователя
1		
2		
3		

(Должность)

(подпись)

(Фамилия И.О.)

М.П.

« ____ » _____ 20 ____ г.

ДОВЕРЕННОСТЬ № _____
на получение средств криптографической защиты информации
и электронной цифровой подписи

« _____ » _____ 20 ____ г.

Настоящим Заявлением _____ ,
(указывается организационно-правовая форма и наименование юридического лица/ Ф.И.О. индивидуального предпринимателя)

в лице _____ ,
действующего на основании _____ ,
(Устав; доверенность №, дата; свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя; лицензия, приказ о назначении на должность нотариуса)

настоящей доверенностью уполномочивает _____
(Должность)

(Фамилия, Имя, Отчество полностью)

Паспорт серия _____ № _____ , выдан « _____ » _____ 20 ____ г.

(кем выдан)

код подразделения _____ - _____ .
получить средства криптографической защиты информации (СКЗИ) и электронной цифровой подписи (ЭЦП) и выполнить все необходимые действия, связанные с исполнением настоящего поручения.

Доверенность действительна до « _____ » _____ 20 ____ г.

Подпись лица, получившего доверенность _____ , удостоверяем.
(подпись)

(Должность)

(подпись)

(Фамилия И.О.)

М.П.

Правила безопасности Клиента при использовании Системы ДБО «Клиент-Банк»

- Для работы с Системой ДБО необходимо иметь персональный компьютер (далее - ПК).
- Операционная система и необходимое программное обеспечение (далее - ПО) данного ПК должны быть только лицензионными.
- Используемый ПК должен быть оснащен антивирусным ПО.
- При первом входе в систему, а также регулярно, каждый месяц меняйте пароли на систему ДБО.
- Ежегодно производите регенерацию криптографических ключей.

Доступ к данному ПК и его использование внутри организации Клиента должен быть регламентирован, в том числе список хостов, доступных для данного ПК. Список должен исключать хосты, содержащие рекламный, новостной и развлекательный контент, и содержать только список IP-адресов Банковских Систем ДБО или подобных государственных служб.

- Очень опасно хранить секретные ключи на жестком диске в каком-либо виде и создавать копии. Необходимо хранить секретные ключи на съемном носителе Рутокен и держать их в надежном, недоступном для третьих лиц месте (например, сейф).
- Использование секретных Ключей должно производиться в момент работы с Системой ДБО и контролироваться Вами как Владельцем данного Ключа. Используя нелицензионное ПО и оставляя секретные Ключи без присмотра, Вы рискуете их скомпрометировать и сделать доступными для третьих лиц, т.к. такое ПО может заведомо содержать вредоносный код.
- Никогда и никому не сообщайте логины \ пароли Систем ДБО и тем более не доверяйте секретные ключи. Даже если этого попросит сотрудник Банка.
- В случае, если Вы, как Владелец секретного Ключа, доверяете управление своим банковским счетом посредством ДБО другому лицу, такая передача управления должна быть зафиксирована юридически, с обязательным письменным уведомлением Банка и предоставлением заверенной нотариально копии доверенности.
- Избегайте использования Системы ДБО на чужих компьютерах или в интернет-кафе.

В случае, если у Вас:

- Неожиданно сломался компьютер, на котором у Вас установлена Система ДБО;
- Зabloкировался логин;
- Невозможно зайти в Систему ДБО;
- Потерян контроль над носителем с секретными ключами;
- Потерян контроль над программой «Клиент-Банк»;
- Возникли подозрения в несанкционированном доступе к Системе ДБО:
 - появляются \ *исчезают* \ документы, контрагенты;
 - остатки на счетах Клиента в Системе ДБО не соответствуют Вашим расчетам;
 - любое другое подозрение.

Вы должны немедленно обратиться в Банк с тем, чтобы решить все возникшие вопросы.

С правилами безопасности эксплуатации Системы ДБО ознакомлены:

(наименование юридического лица/ Ф.И.О. индивидуального предпринимателя)

(Должность)

(подпись)

(Фамилия И.О.)

М.П.



**Уведомление
об изменении параметров подключения к Системе ДБО «Клиент-Банк»**

г. _____

« ____ » _____ 20 ____ г.

Настоящим Заявлением _____,
(указывается организационно-правовая форма и наименование юридического лица/ Ф.И.О. индивидуального предпринимателя)

в лице _____,
действующего на основании _____,
(Устав; доверенность №, дата; свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя; лицензия, приказ о назначении на должность нотариуса)

в рамках Дополнительного соглашения дистанционного банковского обслуживания «Клиент-Банк» № _____ от « ____ » _____ 20 ____ г. просит:

1. Включить в число владельцев криптографических ключей и предоставить им права:

№ п/п	Ф.И.О. уполномоченного лица Клиента (полностью)	Должность	Полномочия уполномоченных лиц Клиента	
			Право подписи (первая/вторая/единственная)	Без права подписи

2. Изменить права владельца криптографических ключей:

№ п/п	Ф.И.О. уполномоченного лица Клиента (полностью)	Должность	Полномочия уполномоченных лиц Клиента	
			Право подписи (первая/вторая/единственная)	Без права подписи

3. Отозвать сертификаты владельцев криптографических ключей:

№ п/п	Ф.И.О. уполномоченного лица Клиента (полностью)	Должность	Полномочия уполномоченных лиц Клиента	
			Право подписи (первая/вторая/единственная)	Без права подписи

ПОРЯДОК ВВОДА В ДЕЙСТВИЕ СИСТЕМЫ ДБО И ОБЩИЕ УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ И ОБСЛУЖИВАНИЯ СИСТЕМЫ ДБО

1. Банк предоставляет Клиенту Программное обеспечение, Ключи проверки ЭП Банка и Сопроводительную документацию, перечисленные в п. 3.1.1, настоящего Соглашения.

2. Клиент самостоятельно проводит установку, переустановку и настройку переданного Банком программного обеспечения, в соответствии с предоставленными инструкциями, на своих аппаратных средствах, отвечающих требованиям спецификации (СПЕЦИФИКАЦИЯ аппаратных и программных средств для установки АРМ «Клиент» для настройки доступа Клиентской части Системы ДБО в Сопроводительной документации).

3. Для регистрации программного обеспечения на каждую процедуру установки, переустановки или переноса АРМ «Клиент» на иные аппаратные средства, а также в случаях, когда производятся действия, связанные с изменениями конфигурации программно-аппаратных средств, Клиент предоставляет в Банк кодовое слово (Приложение 5) не позднее рабочего дня, предшествующего дню проведения работ.

4. По окончании работ по настройке программного обеспечения для доступа к Системе ДБО Клиент или Уполномоченные лица Клиента самостоятельно формируют ключи ЭП и ключи проверки ЭП и производят распечатку сертификатов ключа проверки электронной подписи на бумажном носителе.

5. По окончании работ в соответствии с пунктами 2 – 4 настоящего Приложения Клиент одновременно передает Банку:

– Распечатки проектов сертификатов ключей проверки электронной подписи, заверенные собственноручной подписью владельца сертификата, руководителя или лица, наделенного правом подписывать Договор(ы) финансово-банковских услуг и оттиском печати Клиента (по два экземпляра для каждого ключа проверки ЭП);

6. При замене ключей ЭП в соответствии с условиями настоящего Договора Клиент предоставляет в Банк распечатки проектов сертификатов ключей проверки электронной подписи и документ(-ы) подтверждающий(-ие) полномочия указанного в сертификате лица на право распоряжения денежными средствами на счете с использованием ЭП.

7. Все документы, предоставляемые Клиентом Банку или подписываемые Сторонами по итогам проведения работ в соответствии с пунктами 2 – 4. настоящего Приложения, должны быть составлены по формам, приведенным в Сопроводительной Документации к настоящему Соглашению.

8. При выходе из строя аппаратных или программных средств Системы ДБО или их элементов, а также в иных случаях невозможности предоставления (получения) услуг, указанных в разделе 1. Соглашения и, соответственно, приостановлении использования Системы ДБО, обмен документами между Сторонами осуществляется на бумажных носителях или с использованием иных, предусмотренных Договором банковского счета, систем и средств связи.

9. Стороны признают, что программные средства, обеспечивающие шифрование, изготовление ключей ЭП и ключей проверки ЭП, а также формирование и проверку ЭП, реализуют алгоритмы в соответствии с *ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи*.

10. Клиент признает, что получение Банком электронных документов, подписанных корректной ЭП Клиента, равнозначно получению документов на бумажном носителе, подписанных собственноручной подписью уполномоченных(-ого) лиц(-а) и заверенных оттиском печати Клиента.

11. Банк признает, что получение Клиентом электронных документов, подписанных корректной ЭП Банка, равнозначно получению документов на бумажном носителе, подписанных собственноручной подписью уполномоченных(-ого) лиц(-а) и заверенных оттиском штампа Банка.

12. Стороны признают, что:

– в соответствии с настоящим Соглашением Сторонами используется усиленная неквалифицированная электронная подпись в терминах Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи».

– используемая Сторонами в соответствии с настоящим Соглашением система защиты информации, которая реализует подписание ЭП и шифрование электронных документов, при условии выполнения «Требований безопасности в процессе эксплуатации АС «Клиент-Банк» достаточна для обеспечения конфиденциальности, а также подтверждения авторства и контроля целостности электронных документов;

– после подписания электронного документа ЭП любое изменение, добавление или удаление символов документа делает ЭП некорректной, т.е. проверка подписи с ключом проверки ЭП Стороны, подписавшей электронный документ, дает отрицательный результат;

– создание корректной ЭП электронного документа возможно исключительно с использованием ключа ЭП;

– по содержанию электронных документов, подписанных ЭП, и ключей ЭП невозможно определить ключи ЭП;

– каждая Сторона несет полную ответственность за обеспечение безопасности и сохранность своих ключей ЭП, а также за действия своего персонала;

– предоставление в Банк распечатки проекта сертификата ключа проверки электронной подписи на бумажном носителе, сформированной на АРМ «Клиент» и заверенной собственноручной подписью владельца сертификата, руководителя или лица, наделенного правом подписывать Договор(ы) финансово-банковских услуг, и оттиском печати Клиента, эквивалентно подаче в Удостоверяющий центр заявления на выдачу сертификата ключа проверки электронной подписи уполномоченного лица Клиента.

13. Порядок применения средств Системы ДБО предусматривает, что:

– функции Удостоверяющего центра по настоящему Соглашению выполняет Банк;

– каждая Сторона может иметь несколько ключей ЭП, каждому ключу ЭП соответствует собственный ключ проверки ЭП;

– каждая Сторона самостоятельно формирует (изготавливает) свои ключи ЭП и ключи проверки ЭП;

– Клиент предоставляет Банку каждый собственный ключ проверки электронной подписи одновременно в виде электронного файла и в виде распечатки проекта сертификата на бумажном носителе, заверенной собственноручной подписью владельца сертификата, руководителя или лица, наделенного правом подписывать Договор(ы) финансово-банковских услуг, и оттиском печати Клиента, в трех экземплярах. В случае, когда уполномоченное лицо Клиента является руководителем или лицом, наделенным правом подписывать Договор(ы) финансово-банковских услуг, проект сертификата ключа проверки электронной подписи на бумажном носителе заверяется одной подписью уполномоченного лица Клиента и оттиском печати Клиента;

– Удостоверяющий центр не позднее трех рабочих дней осуществляет проверку уникальности идентификатора ключа электронной подписи, корректности и соответствия ключа проверки электронной подписи в распечатке проекта сертификата электронному файлу и оформляет сертификаты ключа электронной подписи на бумажном носителе с указанием сроков действия ключа электронной подписи. Один экземпляр сертификата передается Клиенту;

– Клиент предоставляет Банку документы (доверенность или распоряжение), подтверждающие права уполномоченных лиц на распоряжение денежными средствами,

находящимися на счетах Клиента и передачу иных документов по счетам Клиента с использованием ЭП. В случае изменения в составе уполномоченных лиц Клиент обязан представить соответствующие документы, подтверждающие изменения.

Банк устанавливает личности уполномоченных лиц Клиента на основании документов, удостоверяющих их личность;

– Стороны предоставляют друг другу собственные ключи проверки электронной подписи в виде электронного файла и в виде сертификата на бумажном носителе, заверенном подписью уполномоченного лица и оттиском печати Удостоверяющего центра;

– представленный Клиентом ключ электронной подписи вводится в действие с даты, указанной в его сертификате;

– предоставленный Клиентом ключ электронной подписи может быть временно заблокирован Банком в случае окончания полномочий Владельца сертификата до предоставления Клиентом в Банк документов, подтверждающих пролонгацию полномочий Владельца сертификата;

– при компрометации или подозрении на компрометацию ключа ЭП или ключа шифрования одной из Сторон (т.е. при ознакомлении или подозрении на ознакомление неуполномоченного лица с ключом ЭП или с ключом шифрования, а также при несанкционированном использовании или подозрении на несанкционированное использование ключа ЭП или ключа шифрования) другая Сторона извещается передачей электронного служебно-информационного документа по Системе ДБО или иным доступным способом о прекращении действия соответствующего ключа ЭП. С момента уведомления Стороны прекращают передачу электронных документов с использованием указанного ключа ЭП, и выводят из действия соответствующий ключ проверки ЭП. Скомпрометированные ключи уничтожаются Сторонами самостоятельно;

– Сторона, получившая по Системе сообщение о компрометации и/или замене ключа ЭП, выводит соответствующий ключ проверки ЭП из действия в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о компрометации;

– Количество различных ключей ЭП, используемых Клиентом для подписания передаваемых Банку электронных платежных документов, определяется действующим законодательством Российской Федерации и требованиями Банка России и указывается в Акте готовности к эксплуатации автоматизированной Системы ДБО «Клиент-Банк». При использовании 2-х ЭП электронный документ признается имеющим корректную ЭП, если корректны и принадлежат разным лицам, имеющим право первой и второй подписи, обе ЭП, которыми он подписан;

– Клиент самостоятельно выбирает организацию – провайдера, обеспечивающую доступ к сети Интернет, и осуществляет подключение к сети Интернет за счет собственных средств. Все расходы, связанные с подключением к сети Интернет, эксплуатацией и обменом данными по Системе ДБО через сеть Интернет, осуществляются Клиентом за счет собственных средств;

– Клиент по предоставленным Банком спецификациям для обеспечения защищенной связи по сети Интернет самостоятельно обеспечивает необходимую настройку телекоммуникационного и другого оборудования (коммутаторы, маршрутизаторы, прокси-сервера, сетевые экраны и пр.) в своей локальной сети;

– Клиент полностью несет все риски, связанные с подключением его вычислительных средств к сети Интернет. Клиент самостоятельно обеспечивает защиту собственных вычислительных средств и криптографических ключей от несанкционированного доступа, и вирусных атак из сети Интернет. Стороны также признают, что потеря доступа к Клиентской части Системы ДБО в результате вмешательства из сети Интернет рассматривается как выход из строя по вине Клиента и восстановление доступа к Системе ДБО осуществляется в соответствии с действующими тарифами Банка.

14. Исходя из изложенного в пунктах 12 – 16 настоящего Приложения Стороны признают аутентификационные свойства средств ЭП, применяемых ими. Электронный документ, подписанный корректной ЭП одной из Сторон, признается другой Стороной как эквивалентный документу на бумажном носителе, составленному и оформленному в соответствии с законодательством Российской Федерации, а также нормативными документами Банка России, и порождает права и обязанности Сторон при выполнении взаимных обязательств по настоящему Соглашению, дополнительным соглашениям и всем приложениям к ним по счету(-ам) Клиента.

15. Контрольным является время системных часов аппаратных средств Банка.

16. Стороны установили, что моментом получения электронного документа принимающей Стороной в Системе является текущее время по системным часам принимающей Стороны в момент помещения информации в архив входящих сообщений принимающей Стороны.

17. Банк исполняет поступившие от Клиента в пределах операционного времени Банка по месту ведения счета электронные платежные документы, имеющие корректную ЭП, на совершение операций по счету Клиента, указанным в настоящем Соглашении, текущим рабочим днем, а поступившие в послеоперационное время – следующим рабочим днем.

18. На дату заключения настоящего Соглашения Банком установлено следующее операционное время:

- для электронных платежных документов в валюте Российской Федерации:

в рабочие дни – с ____ ч. ____ мин. до ____ ч. ____ мин.,

в предвыходные и предпраздничные дни – с ____ ч. ____ мин. до ____ ч. ____ мин.

ПРОЦЕДУРА ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ СПОРНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПРИНЯТИЕМ ИЛИ НЕПРИНЯТИЕМ, ИСПОЛНЕНИЕМ ИЛИ НЕИСПОЛНЕНИЕМ БАНКОМ ЭЛЕКТРОННОГО ДОКУМЕНТА КЛИЕНТА

1. При возникновении разногласий Сторон в связи с обменом документами в электронном виде с помощью Системы ДБО «Клиент-Банк», а также в иных случаях возникновения спорных ситуаций в связи с эксплуатацией Системы ДБО, обмен документами в электронном виде с использованием Системы ДБО «Клиент-Банк» между Сторонами немедленно прекращается.

2. Сторона, заявляющая разногласие, (инициатор спора) обязана направить другой Стороне заявление о разногласиях, подписанное руководителем или лицом Стороны, наделенным правом подписывать Договор(ы) финансово-банковских услуг, с предложением создать согласительную комиссию и изложением причин разногласий, в объеме, необходимом для исполнения настоящей Процедуры. Заявление должно содержать фамилии, имена, отчества и иные сведения о представителях Стороны – инициатора спора, которые будут участвовать в работе комиссии, место, время и дату сбора комиссии. Дата сбора комиссии должна быть не позднее _____ дней со дня получения другой Стороной заявления.

3. В состав комиссии должно входить равное количество представителей от Клиента и Банка (не менее двух представителей, от каждой из Сторон), полномочия которых удостоверяются доверенностями, оформленными в соответствии с действующим законодательством Российской Федерации. При необходимости, с письменного согласия обеих Сторон, в состав комиссии могут быть дополнительно введены эксперты третьей стороны. Состав комиссии должен быть зафиксирован в акте, который является итоговым документом, отражающим результаты работы комиссии.

Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке. Срок работы комиссии - не более пяти рабочих дней.

В исключительных ситуациях этот срок может быть увеличен по взаимной договоренности Сторон.

4. Стороны должны способствовать работе комиссии и не допускать отказа от предоставления необходимых документов. При необходимости Стороны обязаны предоставить комиссии возможность ознакомиться с условиями и порядком работы Системы ДБО.

5. При возникновении у Клиента претензий к Банку по поводу корректности действий, совершенных в рамках выполнения обязательств подпунктов 3.1.5. – 3.1.6. Соглашения, комиссия должна:

- проверить авторство предъявляемого Банком полученного им от Клиента электронного документа, в соответствии с которым совершены действия;

- проверить, что совершенные Банком действия соответствуют содержанию электронного документа.

6. При возникновении у Клиента претензий к Банку по поводу неисполнения направленных электронных платежных документов, в рамках выполнения обязательств в соответствии с подпунктом 3.1.2. Дополнительного соглашения, комиссия должна:

- проверить авторство предъявляемого Клиентом полученного им от Банка электронного документа, подтверждающего прием или проводку ЭПД, по которому не совершены необходимые действия;

- при необходимости проверить авторство предъявляемого Банком документа, содержащего поручение.

7. Для проверки авторства электронного документа выполняются следующие действия:

7.1. Определяется файл, содержащий электронный документ, авторство которого должно быть проверено в связи со спорной ситуацией на основе проверки корректности ЭП файла, содержащего оспариваемый документ.

7.2. Из электронного архива Стороны, получившей электронный документ, комиссии предъявляется файл с ЭП, содержащий оспариваемый электронный документ.

7.3. Сторона, получившая оспариваемый документ, предъявляет комиссии действующую на момент подписания базу сертификатов ключей проверки электронной подписи, либо сертификат ключа проверки электронной подписи, либо ключ проверки ЭП, переданный ей противоположной Стороной и предназначенный для проверки корректности ЭП файла, содержащего оспариваемый документ.

7.4. Проверяется целостность программного модуля Arbiter-PKI, предъявляемого любой из Сторон. Проверка целостности осуществляется путем вычисления значения хэш-функции и сравнения его со значением, соответствующим версии предъявленного модуля Arbiter-PKI опубликованным на сайте ЗАО Сигнал-КОМ.

7.5. Проверяется корректность электронной подписи файла, содержащего оспариваемый электронный документ, с помощью программного модуля Arbiter-PKI.

7.6. По требованию Стороны, ключ проверки ЭП которой предъявлен второй Стороной, может быть проверена принадлежность предъявленного ключа проверки ЭП первой Стороне. Ключ проверки ЭП признается принадлежащим первой Стороне, если ключ проверки ЭП, представленный комиссии в виде файла, соответствует ключу проверки ЭП, содержащемуся в сертификате на бумажном носителе, выданном Удостоверяющим центром в соответствии с условиями Соглашения. Если предъявленный в виде файла ключ не соответствует ключу проверки ЭП, содержащемуся в сертификате на бумажном носителе, либо период действия предъявленного ключа не соответствует времени получения оспариваемого документа, то комиссия признает, что ключ проверки ЭП не был представлен Стороной, получившей оспариваемый документ.

8. Если в результате проведенной проверки корректности ЭП файла, содержащего оспариваемый документ, по ключу проверки ЭП, предъявленному Стороной, получившей оспариваемый документ, ЭП признана корректной, то авторство оспариваемого электронного документа признается комиссией установленным. Если авторство оспариваемого электронного документа признано комиссией установленным и действия Стороны, к которой предъявляются претензии, соответствуют содержанию оспариваемого документа, то претензии инициатора спора признаются необоснованными.

Если авторство оспариваемого электронного документа признано комиссией установленным, а действия Стороны, к которой предъявляются претензии, не соответствуют содержанию оспариваемого документа, то претензии инициатора спора признаются обоснованными.

9. Если в результате проведенной проверки корректности ЭП файла, содержащего оспариваемый документ, по ключу проверки ЭП, предъявленному Стороной, получившей оспариваемый документ, ЭП признана некорректной, то предъявленный для проверки авторства электронный документ признается комиссией ложным.

Если Сторона, представившая ложный электронный документ, является инициатором спора, то претензии данной Стороны к другой Стороне признаются необоснованными.

Если Сторона, к которой предъявляются претензии, представила ложный электронный документ, то претензии к данной Стороне признаются обоснованными.

10. Претензии инициатора спора к противоположной Стороне признаются необоснованными, если инициатор спора был обязан в соответствии с п. 7.2. настоящей Процедуры предъявить, но не предъявил комиссии полученный им файл, содержащий

оспариваемый документ, или не предъявил в соответствии с п. 7.3. настоящей Процедуры ключ проверки электронной подписи противоположной Стороны.

11. С целью выяснения причин и обстоятельств возникновения спорной ситуации комиссией при необходимости проводится исследование внутренних архивов, протоколов и системных журналов рабочего места Клиента.

12. Отсутствие на клиентском рабочем месте Системы ДБО признаков отправки электронного документа, принятого Банком с корректной ЭП данного Клиента, не является основанием для отказа Клиента от авторства данного документа.

13. По итогам работы комиссии составляется акт, в котором в обязательном порядке отражаются:

- состав комиссии;
- действия членов комиссии;
- установленные обстоятельства;
- основания, которые послужили для формирования выводов;
- выводы, влияющие на возможность установления подлинности оспариваемого документа.

В этом случае акт признается Сторонами надлежащим.

14. В случае, если предложение о создании комиссии оставлено другой Стороной без ответа, либо Сторона отказывается от участия в комиссии или препятствует работе комиссии, а также отказывается от подписания акта, заинтересованная Сторона самостоятельно составляет акт, в котором указываются сведения о причинах его составления в одностороннем порядке. В данном акте фиксируются обстоятельства, позволяющие сделать вывод о том, что оспариваемый электронный документ является корректным, либо формулируется вывод об обратном.

Указанный акт направляется другой Стороне для сведения.

При рассмотрении в суде споров о наличии документа, исполненного с помощью Системы ДБО или подписанного электронной подписью, заинтересованная Сторона обязана предоставить суду акт, составленный в соответствии с настоящей Процедурой.

15. Составленный комиссией акт является основанием для выработки Сторонами окончательного решения комиссии. Данное решение должно быть подписано Сторонами не позднее 10 дней с момента окончания работы комиссии. В случае, если решение не будет подписано в указанный срок, заинтересованная Сторона вправе обратиться в Арбитражный суд и без выработанного Сторонами решения, а в качестве доказательства представить акт, составленный в соответствии с настоящей Процедурой.



ЗАЯВЛЕНИЕ

о смене логина и пароля при их компрометации для Системы ДБО «Клиент-Банк»

г. _____ « ____ » _____ 20 ____ г.

Настоящим Заявлением _____,
(указывается организационно-правовая форма и наименование юридического лица/ Ф.И.О. индивидуального предпринимателя)

в лице _____,

действующего на основании _____
(Устав; доверенность №, дата; свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя; лицензия, приказ о назначении на должность нотариуса)

в рамках Дополнительного соглашения дистанционного банковского обслуживания «Клиент-Банк» № _____ от « ____ » _____ 20 ____ г. просит заменить логин и пароль.

(Должность)

(подпись)

(Фамилия И.О.)

М.П.

Отметка Банка

Работник Банка, принявший заявление:

(Должность)

(подпись)

(Фамилия И.О.)

« ____ » _____ 20 ____ г.

**АКТ
ПРИЗНАНИЯ ОТКРЫТОГО КЛЮЧА ЭП (СЕРТИФИКАТА)
ДЛЯ ОБМЕНА СООБЩЕНИЯМИ**

Настоящим Актом признается ключ шифрования, принадлежащий уполномоченному представителю:

ФИО владельца сертификата: **Иванов Иван Иванович**

Организация: **ООО «Тестовая организация»**

Дата начала срока действия сертификата: **xx.xx.xxxx xx:xx:xx**

Дата окончания срока действия сертификата: **xx.xx.xxxx xx:xx:xx**

Ключ ЭП создан с использованием СКЗИ: **Рутокен ЭЦП**

Идентификатор ключа: **xx**

Местонахождение: **RU**

Хранилище ключевой информации: **xxxxxxxx:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx**

Момент генерации ключа: **xx.xx.xxxx xx:xx:xx**

Открытый ключ клиента:

xx xx xx
--

Достоверность приведенных данных подтверждаем

Владелец сертификата

_____/ /

Руководитель компании

(первая подпись согласно карточке образцов подписей)

_____/ /

М.П.

От Банка

_____/ /

М.П.

--	--	--	--	--

Сведения об администраторе Системы ДБО «Клиент-Банк»	
номер контактного телефона:	8 (4842) 27-74-20 доб. 122
адрес электронной почты:	support@bankelita.ru

Клиент:

_____ (Должность) _____ (подпись) _____ (Фамилия И.О.)

Клиент:

_____ (Должность) _____ (подпись) _____ (Фамилия И.О.)

М.П.

Заполняется Банком:

Заявление зарегистрировано в Банке « ____ » _____ 20 ____ г. за № _____ .

Уполномоченное лицо Банка:

_____ (Должность) _____ (подпись) _____ (Фамилия И.О.)

действующее на основании _____

М.П.

Вместе с настоящим Заявлением Клиент предоставляет в Банк подписанные и скрепленные печатью документы, указанные в Приложениях 1, 2, 4 к Дополнительному Соглашению ДБО «Клиент-Банк».

Настоящее Заявление составлено в двух экземплярах: первый экземпляр передается Клиенту, второй хранится в Банке. Все экземпляры идентичны и имеют одинаковую юридическую силу.

Клиент _____

Банк _____