

Оглавление

Термины и определения.....	4
1. Общие положения	6
2. Права и обязанности сторон.....	8
3. Финансовые взаимоотношения сторон	12
4. Конфиденциальность	12
5. Ответственность сторон.....	12
6. Порядок разрешения споров.....	13
7. Срок действия Договора ДБО, порядок его изменения и расторжения.....	13
8. Прочие условия.....	14
Приложение 1.....	15
Приложение 2.....	16
Приложение 4.....	18
Приложение 5.....	19
Приложение 6.....	24
Приложение 7.....	25
Приложение 8.....	26
Приложение 9.....	28

Термины и определения

Автоматизированное рабочее место (АРМ) – программно-технический комплекс, оборудованный в соответствии с требованиями настоящих Правил, представляющий Клиенту возможность для взаимодействия с системой «КТБ-Онлайн» и получения услуг.

Аналог собственноручной подписи (АСП) – Персональный идентификатор Клиента, являющийся контрольным параметром правильности заполнения обязательных полей электронных документов.

Аутентификация - процедура подтверждения предъявителем Псевдонима того, что Псевдоним действительно принадлежит ему.

Банк – Акционерное общество коммерческий банк «Кубанский торговый банк», ИНН 2309023960, ОГРН 1022300000502. Местонахождение: 350075, Краснодарский край, г. Краснодар, ул. им. Стасова, 176. Банковские реквизиты: корреспондентский счет 30101810900000000718 в Южном ГУ Банка России, БИК 040349718. Контактные телефоны: +7(861)212-60-80, адрес электронной почты info@kubantorgbank.ru, официальный сайт: bktb.ru.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом «Об электронной подписи» (№ 63-ФЗ от 6 апреля 2011 года) порядке выдан сертификат ключа проверки электронной подписи, и которое указанное в карточке с образцами подписей и оттиска печати Клиента, принятой Банком, либо действующее на основании распорядительного акта Клиента или доверенности, выданной в порядке, установленном законодательством Российской Федерации.

Идентификация – определение Банком Уполномоченного лица Клиента по предъявленному псевдониму.

Клиент – юридическое лицо (за исключением кредитных организаций), индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации (далее – РФ) порядке частной практикой.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключевой носитель – физический носитель определенной структуры, предназначенный для безопасного хранения ключа электронной подписи и ключа проверки.

Компрометация ключа электронной подписи – событие, определенное владельцем сертификата ключа проверки электронной подписи, как ознакомление неуполномоченным лицом с его ключом электронной подписи, утеря носителя ключа, копирование или другие причины появления у владельца сертификата ключа проверки электронной подписи сомнений в конфиденциальности ключа электронной подписи.

Подтверждение подлинности ЭП – процедура проверки принадлежности электронной подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Порядок обмена электронными документами – средство и (или) способ, позволяющие Клиенту составлять, удостоверить и передавать распоряжения в целях осуществления перевода денежных средств в рамках системы «КТБ-Онлайн», на условиях, указанных в настоящих Правилах.

Сертификат ключа проверки электронной подписи (СКПЭП) – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Согласительная комиссия – комиссия, создаваемая Сторонами для разрешения разногласий, возникающих при обмене электронными документами.

Средства электронной подписи – средства криптографической защиты информации, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средство криптографической защиты информации (СКЗИ) – программные, аппаратные и программно-аппаратные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и/или для защиты информации от несанкционированного доступа при ее обработке и хранении, имеющие сертификат, подтверждающий соответствие стандартам системы шифрования и электронной подписи, принятым в РФ, которые заданы соответствующим ГОСТ.

Стороны – Банк и Клиент.

Тарифы – перечень предоставляемых Клиенту в Банке услуг и размеры комиссионного вознаграждения.

Удостоверяющий центр – юридическое лицо, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей (Банк).

Уполномоченное лицо Клиента – лицо, наделенное Клиентом правом действовать от его имени и в его интересах (в том числе, с правом подписания документов аналогом собственноручной подписи), полномочия которого подтверждены надлежащим образом (например, доверенностью).

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с этой информацией и которая используется для определения лица, подписывающего информацию.

Электронный документ (ЭД) – это информация в электронной форме, подписанная усиленной неквалифицированной электронной подписью Владельца СКПЭП, и равнозначная документу на бумажном носителе, подписанному его собственноручной подписью.

Электронный платежный документ (ЭПД) – Электронный документ, являющийся распоряжением по Счету Клиента, подписанный электронной подписью Клиента.

Электронный информационный документ (ЭИД) – Электронный документ, не являющийся Электронным платежным документом (информационные сообщения, в том числе рекламного характера и т.п.).

Любые другие термины и определения, используемые в настоящих Правилах, применяются в том значении, в котором они определены действующим законодательством Российской Федерации, в том числе Гражданским кодексом Российской Федерации и Федеральным законом от 06.04.2011 г. № 63–ФЗ «Об электронной подписи».

1. Общие положения

1.1. Настоящие Правила дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, и физических лиц, занимающихся в установленном законом порядке частной практикой (система «КТБ-Онлайн») (далее по тексту – настоящие Правила) действуют совместно с регламентом Удостоверяющего центра АО «Кубаньторгбанк» и Заявлением об открытии расчетного счета в АО «Кубаньторгбанк»/подключении услуг, и регулирует обмен электронными документами, подписанными электронной подписью, между Банком и Клиентом при осуществлении расчетов с использованием системы «КТБ-Онлайн», а также устанавливает обязательства Сторон по обеспечению информационной безопасности при обмене ЭД.

1.2. Банк осуществляет обслуживание Клиента в системе «КТБ-Онлайн» в соответствии с действующим законодательством Российской Федерации, настоящими Правилами и приложениями к ним, с которыми Клиент ознакомлен, согласен и принимает на себя обязательства неукоснительно их выполнять.

1.3. Настоящие Правила размещаются на сайте Банка в сети Интернет www.bktb.ru. По письменному запросу настоящие Правила могут быть переданы Клиенту на бумажном носителе, высланы в электронной форме по адресу электронной почты, указанному в запросе.

1.4. Заключение Договора дистанционного банковского обслуживания (далее по тексту «Договор ДБО») осуществляется в соответствии со ст. 428 Гражданского кодекса РФ, в порядке присоединения Клиента к настоящим Правилам, путем предоставления в Банк подписанного и скрепленного в установленных законом случаях оттиском печати Клиента Заявления об открытии расчетного счета либо заявления о подключении к системе «КТБ-Онлайн» (в двух экземплярах, по одному для Банка и Клиента), и его акцепта Банком, в котором Клиент указал о своем намерении подключить услугу «КТБ-Онлайн» либо заявления на подключение услуги «КТБ-Онлайн».

1.5. Настоящие Правила распространяются на все счета Клиента в Банке, как открытые на дату присоединения к настоящим Правилам, так и на счета, которые будут открыты Клиентом в последующем.

1.6. Настоящим Клиент подтверждает, что до присоединения к настоящим Правилам ознакомился и проинформирован об условиях использования электронного средства платежа, в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования электронного средства платежа.

1.7. Обслуживание Клиента осуществляется Банком с использованием принадлежащего Банку программного обеспечения и аппаратно-программного средства криптографической защиты информации (СКЗИ) (далее по тексту «Система «КТБ-Онлайн» или «Система»).

1.8. Стороны осуществляют обмен по системе «КТБ-Онлайн» электронными документами, согласно функционалу, определенному в «Инструкции клиента системы дистанционного банковского обслуживания «КТБ-Онлайн», размещенной на сайте Банка, и требованиям, определенным в Приложении 3 настоящих правил, являющимся неотъемлемой частью Договора ДБО.

1.9. Расчетные операции по счету Клиента осуществляются на основании ЭПД, подписанных ЭП и осуществляются Банком в соответствии с законодательством Российской Федерации и Договором комплексного банковского обслуживания с учетом особенностей, установленных Договором ДБО.

1.10. Банк предоставляет в пользование Клиенту программное обеспечение системы «КТБ-Онлайн» и средства ЭП на срок действия Договора ДБО. Клиент не вправе передавать, продавать, копировать или иным способом делать доступным третьим лицам полученное от Банка программное обеспечение, средства ЭП либо иную информацию или сведения, связанные с Договором ДБО.

1.11. Стороны признают, что:

1.11.1. Средства, используемые для криптографической защиты информации при ее обработке, хранении и передаче между Банком и Клиентом, а также для генерации ключей ЭП и формирования ЭП, достаточны для подтверждения подлинности ЭД.

1.11.2. Внесение изменений в ЭПД, после их подписания ЭП, дает отрицательный результат проверки ЭП.

1.11.3. Подделка ЭП невозможна без использования ключа ЭП.

1.11.4. Каждая Сторона несет ответственность за сохранность своих ключей ЭП и действий своего персонала при использовании ЭП для обмена ЭД.

1.12. ЭПД Клиента приравнивается к расчетному (платежному) документу на бумажном носителе, подписанному уполномоченными лицами Клиента, указанными в карточке образцов подписей и оттиска печати Клиента, имеющейся в Банке, и имеющим оттиск печати Клиента, при одновременном соблюдении следующих условий:

1.12.1. ЭПД создан Клиентом в системе «КТБ-Онлайн», подписан ЭП Клиента и отправлен в Банк для исполнения в порядке, установленном Договором ДБО.

1.12.2. Содержит в себе все реквизиты, предусмотренные действующим законодательством для расчетных документов на бумажном носителе с учетом особенностей форм и порядка осуществления безналичных расчетов на территории Российской Федерации.

1.12.3. Подтверждена подлинность ЭП в ЭД.

1.12.4. Сертификат ключа подписи, относящийся к этой ЭП, не утратил силу (действует) на момент проверки или на момент подписания ЭД при наличии доказательств, определяющих момент подписания.

1.13. ЭП в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

1.13.1. Сертификат ключа подписи, относящийся к этой ЭП, не утратил силу (действует) на момент проверки или на момент подписания ЭД при наличии доказательств, определяющих момент подписания.

1.13.2. Подтверждена подлинность ЭП в ЭД.

1.13.3. ЭП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

1.14. Расчетная операция, совершенная Банком на основании ЭПД, подписанного ЭП Клиента (при положительном результате проверки ЭП), не может быть оспорена только на том основании, что она совершена на основании платежных документов, представленных в виде электронных документов.

1.15. Порядок действий Сторон в обмене ЭД определены в Приложениях 1-9 к настоящим Правилам, являющихся неотъемлемой частью настоящих Правил.

1.16. Смена ключей ЭП производится в случае их компрометации по инициативе любой из Сторон, а также в иных предусмотренных настоящими Правилами случаях. После ввода в действие новых ключей ЭП недействительные ключи ЭП уничтожаются, а ключи проверки ЭП хранятся Сторонами в течение всего срока хранения ЭД для подтверждения подлинности, которых они могут быть использованы. Уничтожение открытых ключей ЭП после истечения срока их хранения осуществляется Сторонами самостоятельно.

1.17. В целях повышения безопасности работы Клиента в системе «КТБ-Онлайн», проведение банковских операций в том числе, списание (перевод) денежных средств со счетов Клиента производится на основании распоряжения Клиента, полученного Банком в ответ на SMS-сообщение для подтверждения операции в виде SMS-сообщения/USSD-команды, направленных с номера мобильного телефона, зарегистрированного для доступа к системе «КТБ-Онлайн» (Приложение 4 к настоящим Правилам).

1.18. Обеспечение информационной безопасности защищенного электронного документооборота между Сторонами осуществляется в соответствии с Приложением 5.

2. Права и обязанности сторон

2.1. Стороны обязаны:

2.1.1. Самостоятельно поддерживать в рабочем состоянии свои и полученные от другой стороны программно-технические средства, используемые для электронного документооборота в соответствии с настоящими Правилами.

2.1.2. Не разглашать третьим лицам (за исключением случаев, прямо установленных действующим законодательством РФ или Договором ДБО) способы защиты информации и обеспечения безопасности при работе в системе «КТБ-Онлайн», сохранять в тайне ключи ЭП.

2.1.3. Немедленно информировать другую сторону обо всех случаях компрометации известных ей ключей ЭП Клиента и ЭП Банка, их утраты, хищения, несанкционированного использования, а также повреждения программно-технических средств, используемых для электронного документооборота в соответствии с Договором ДБО.

2.1.4. Соблюдать порядок и регламент обмена ЭД, использовать при обмене ЭД, соответствующие перечню, предусмотренному настоящими Правилами, вести архивы входящих и исходящих ЭД, а также направленных Клиенту и полученных от Клиента уведомлений в соответствии с требованиями действующего законодательства и Договора ДБО.

2.1.5. Основанием для прекращения участия Клиента в обмене ЭД является расторжение Договора ДБО или отключение услуги «КТБ-Онлайн» в случаях, предусмотренных п.7.4, 7.5. настоящих Правил.

2.2. Банк вправе:

2.2.1. Не принимать от Клиента к исполнению ЭПД в случаях, предусмотренных Договором ДБО и действующим законодательством Российской Федерации, в частности отказать Клиенту в приеме распоряжения на проведение операции по банковскому счету (вкладу), подписанному аналогом собственноручной подписи.

2.2.2. В одностороннем порядке вносить в настоящие Правила и Договор ДБО, изменения и дополнения, в том числе: изменять порядок обмена ЭД, перечень ЭД и их форматы, требования к обеспечению безопасности электронного документооборота, порядок исполнения ЭПД и т.д., с уведомлением Клиента не менее чем за 14 календарных дней до вступления изменений в силу с указанием даты вступления указанных изменений в силу, путем размещения соответствующей информации в офисах Банка, на сайте Банка в сети Интернет, www.bktb.ru, или путем отправки Клиенту по системе «КТБ-Онлайн» уведомления об изменении/дополнении, содержащее дату изменения, рассчитанную с учетом указанного срока. Начиная с даты, указанной в уведомлении Банка, подлежащие изменению положения Правил, утрачивают для Сторон юридическую силу.

2.2.3. В одностороннем порядке пересматривать действующие и вводить новые Тарифы, уведомляя об этом Клиента не позднее, чем за 14 календарных дней до даты введения таких изменений. Уведомление Клиента об изменении Тарифов осуществляется путем размещения соответствующей информации в офисах Банка, на сайте Банка в сети Интернет, www.bktb.ru, отправки Клиенту по системе «КТБ-Онлайн» уведомления об изменении/дополнении, содержащее дату изменения, рассчитанную с учетом указанного срока.

2.2.4. В одностороннем порядке приостановить с Клиентом обмен ЭД в следующих случаях:

- несоблюдение Клиентом предусмотренных Договором ДБО требований к обмену ЭД и обеспечению информационной безопасности при обмене ЭД;
- компрометация ключей ЭП Клиента;
- иные основания, предусмотренные действующим законодательством РФ, в частности ФЗ от 28.06.2014 г. №173 – ФЗ «Об особенностях осуществления финансовых

операций с иностранными гражданами и юридическими лицами, о внесении изменений в Кодекс об административных правонарушениях и признании утратившими силу отдельных положений законодательных актов Российской Федерации», ФЗ от 07.08.2001 г. № 115 – ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

2.2.5. О приостановлении участия в обмене ЭД Банк письменно уведомляет Клиента не позднее рабочего дня, следующего за днем приостановления обмена ЭД, с указанием причин и даты начала приостановления участия в обмене ЭД. В случае компрометации ключей ЭП Клиента обмен ЭД с Клиентом приостанавливается с момента установления Банком факта компрометации ключей ЭП Клиента. Участие Клиента в обмене ЭД возобновляется после устранения причин его приостановления на основании решения Банка. О решении возобновить участие Клиента в обмене ЭД Банк письменно уведомляет Клиента.

2.2.6. Изменить порядок передачи информации по движению денежных средств Клиента, установленный Договором ДБО. При этом изменения вступают в силу с момента получения Клиентом соответствующего уведомления Банка.

2.2.7. В соответствии с действующими Тарифами Банка, списывать без распоряжения Клиента сумму комиссионного вознаграждения за обслуживание с применением системы «КТБ-Онлайн» с расчетного счета/счетов Клиента в Банке. Указанное условие о списании рассматривается, как заранее данный акцепт Клиента на полное или частичное списание денежных средств Банком.

2.2.8. Запросить, в случае необходимости, копии ЭД на бумажном носителе.

2.3. Банк обязан:

2.3.1. Предоставить Клиенту необходимые программное обеспечение Системы и средства ЭП на время действия Договора ДБО.

2.3.2. Оказывать консультации по установке программного обеспечения и по вопросам приема/передачи информации, технологии ее обработки в Системе и использования средств ЭП.

2.3.3. На основании заявления Клиента производить выпуск сертификата для клиента.

2.3.4. Исполнять текущим операционным днем принятые до 16-30 по московскому времени ЭПД (до 15-30 – в предвыходные и предпраздничные дни, если иное не будет установлено внутренним распоряжением Банка), а документы, принятые после 16-30 (после 15-30 – в предвыходные и предпраздничные дни, если иное не будет установлено внутренним распоряжением Банка), – следующим операционным днем.

2.3.5. В срок, не позднее следующего рабочего дня с даты совершения операции, передавать в электронном виде Клиенту банковские выписки по его счету, создаваемые на основе стандартных банковских выписок, и любую другую информацию, согласованную сторонами.

2.3.6. Соблюдать порядок обмена ЭД, перечень используемых при обмене ЭД и их форматы, порядок осуществления контроля ЭД.

2.3.7. Уведомлять Клиента о совершении каждой операции с использованием ЭПД путем направления Клиенту соответствующего уведомления, одним из следующих способов:

- посредством отправки электронных сообщений на адрес электронной почты Клиента, указанный в заявлении об открытии расчетного счета/ подключении услуг;
- посредством отправки SMS – сообщений на номера телефонов уполномоченных лиц Клиента, указанных в заявлении на открытие расчетного счета/заявлении на подключении услуг.

2.3.8. Обязанность Банка по уведомлению Клиента о совершении каждой операции с использованием ЭПД считается выполненной надлежащим образом, с момента направления Клиенту уведомления.

2.3.9. Уведомление о совершении операции считается полученным Клиентом по истечении трех часов с момента его направления Банком. Банк не несет ответственности за отсутствие у Клиента доступа к средствам, с использованием которых Клиент может получить уведомление, либо несвоевременное получение уведомления, в том числе за сбои в работе Интернета, сетей связи, возникшие по независящим от Банка причинам и повлекшие за собой несвоевременное получение или неполучение Клиентом уведомлений о совершении операции.

2.3.10. В случае подключения Клиентом услуги «SMS – Инфо» Клиенту на платной основе предоставляется дополнительная информация в соответствии с выбранным тарифным планом. Комиссионное вознаграждение за услугу «SMS – Инфо» взимается Банком в соответствии с действующими Тарифами Банка.

2.3.11. Предоставить Клиенту возможность направления уведомлений об утрате электронного средства платежа и/или использования его без согласия Клиента (далее - Уведомление об утрате ЭСП).

2.4. Клиент вправе:

2.4.1. Составлять и направлять в Банк ЭД по системе «КТБ-Онлайн» в соответствии с Договором ДБО.

2.4.2. Обращаться в Банк по вопросам обмена ЭД и функционирования системы «КТБ-Онлайн».

2.4.3. Обращаться в Банк с заявлением о предоставлении копий ЭД, находящихся в Банке.

2.4.4. Обращаться в Банк для блокировки работы в системе «КТБ-Онлайн».

2.4.5. Обращаться в Банк с целью ограничения максимальной суммы платежа за операцию или периода времени проведения операций, ограничения перечня возможных получателей денежных средств.

2.4.6. В случае несогласия с новыми тарифами, Клиент вправе расторгнуть Договор ДБО в одностороннем порядке, при этом, Стороны установили, что при расторжении Клиентом Договора ДБО по истечении 14 (четырнадцати) дней с даты извещения Банком о дополнении/изменении тарифов, в отношении Клиента действуют тарифы в дополненной/измененной редакции.

2.4.7. Отключить услугу системы «КТБ-Онлайн».

2.5. Клиент обязан:

2.5.1. Предоставлять представителям Банка доступ в помещение, где размещается АРМ Клиента, на котором осуществляется работа в системе «КТБ-Онлайн», для разрешения возникших разногласий при обмене ЭД.

2.5.2. Использовать полученные от Банка программно-технические средства только в целях, установленных настоящими Правилами, без права передачи, продажи или передачи иным образом третьим лицам, а также копирования. В случае нарушения установленных в отношении использования программного обеспечения запретов и ограничений Клиент несет перед Банком и правообладателем программно-технических средств ответственность, предусмотренную действующим законодательством Российской Федерации.

2.5.3. Соблюдать порядок обмена ЭД, перечень используемых при обмене ЭД и их форматы, порядок осуществления контроля ЭД.

2.5.4. Информировать Банк обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих обмену ЭД.

2.5.5. В случае компрометации ключей, утрате электронного средства платежа и/или использования его без согласия Клиента ЭП незамедлительно обратиться в Банк для принятия необходимых мер, с уведомлением об утрате электронного средства платежа

и/или использования его без согласия Клиента (далее - Уведомление об утрате ЭСП), Уведомление об утрате ЭСП направляется Клиентом в Банк на бумажном носителе, за подписями лиц, указанных в карточке с образцами подписей и оттиском печати с подробным описанием ситуации и указанием одного из следующих действий, необходимых выполнению Банком:

- аннулирование (отзыв) СКПЭП уполномоченного лица Клиента (одного или всех) и смена криптографических ключей;

- блокировка учетной записи Клиента в системе «КТБ-Онлайн».

2.5.6. Уведомление об утрате ЭСП должно быть направлено Банку незамедлительно после обнаружения факта утраты ЭСП и/или его использования без согласия Клиента, но не позднее дня следующего за днем получения от Банка уведомления о совершенной операции.

2.5.7. Клиент считается просрочившим обязанность по незамедлительному уведомлению, по истечении дня следующего за днем получения от Банка уведомления о совершенной операции.

2.5.8. Инициировать изменение всех (некоторых) ЭП в случаях, предусмотренных настоящими Правилами.

2.5.9. Осуществлять в течение операционного дня не менее двух сеансов связи с Банком для получения возможных экстренных сообщений либо другой актуальной информации, своевременно реагировать на все сообщения Банка. Инициатором сеансов связи с Банком всегда является Клиент.

2.5.10. Поддерживать актуальными системные дату и время на АРМ, на которых осуществляется работа в системе «КТБ-Онлайн».

2.5.11. Оплачивать Банку комиссионное вознаграждение за услуги по электронному документообороту, осуществляемому с использованием Системы, в порядке, установленном разделом 3 настоящих Правил, в соответствии с Тарифами Банка.

2.5.12. По требованию Банка в соответствии с п.2.2.8. предоставить Банку платежный документ, оформленный на бумажном носителе в соответствии с требованиями Банка России.

2.5.13. Не передавать третьим лицам программное обеспечение, ключевые носители, средства ЭП, а также прочие сведения, относящиеся к Договору ДБО.

2.5.14. В случае расторжения Договора ДБО или отключения услуги «КТБ-Онлайн», не позднее 3 (трех) календарных дней осуществить возврат средств ЭП Банку, полученных от Банка в соответствии с п.2.3.1. данных Правил, по акту в произвольной форме.

2.5.15. Клиент обязан в течение 5 (пяти) рабочих дней уведомить Банк обо всех изменениях, связанных с полномочиями по распоряжению счетом, об изменениях наименования Клиента, его юридического и почтового адреса, номеров контактных телефонов, изменения права подписи и содержания доверенности, внесении изменений в учредительные документы, получении Клиентом лицензий на осуществляемые основные виды деятельности, подлежащие лицензированию, с обязательным предоставлением в Банк надлежащим образом заверенных копий указанных документов.

2.5.16. Клиент обязан выполнять требования по обеспечению информационной безопасности, указанных в Приложении 5.

2.5.17. Клиент обязан соблюдать Регламент Удостоверяющего Центра АО «Кубаньторгбанк» и его приложений.

2.5.18. Клиент подтверждает, что полученное Банком в соответствии с п.1.13 настоящих Правил распоряжение Клиента имеет юридическую силу равную документу на бумажном носителе, заверенному собственноручной подписью Клиента, оформленному в соответствии с требованиями законодательства Российской Федерации.

3. Финансовые взаимоотношения сторон

3.1. За обслуживание системы «КТБ-Онлайн» и оказание услуг по осуществлению электронного документооборота в рамках системы, проведение расчетных операций по счету Клиента на основании ЭПД, Клиент выплачивает Банку комиссионное вознаграждение согласно установленным в Банке тарифам. На момент присоединения к настоящим Правилам Клиент с тарифами Банка ознакомлен, согласен и обязуется их выполнять.

3.2. Клиент предоставляет Банку право без дополнительного распоряжения списывать сумму комиссионного вознаграждения, подлежащую выплате Клиентом Банку по Договору ДБО, со своего банковского счета, открытого в Банке. В случае невозможности оплаты услуг Банка по причине отсутствия (недостаточности) денежных средств на банковском счете Клиента, ареста денежных средств на банковском счете Клиента, приостановления операций по счету Клиента, либо по иным основаниям, Банк вправе приостановить оказание услуг в системе «КТБ-Онлайн», данное условие понимается Сторонами, как нарушение Клиентом установленного порядка обмена электронными документами. При наличии причин, препятствующих списанию денежных средств в размере и порядке, предусмотренных Договором ДБО, Клиент вправе оплатить комиссионное вознаграждение за услуги Банка путем перечисления денежных средств с иных счетов Клиента как открытых в Банке, так и в иных кредитных организациях. Банк возобновляет оказание услуг после оплаты Клиентом денежных средств не позднее дня, следующего за днем получения Банком оплаты, предусмотренной п.3.1 настоящих Правил.

4. Конфиденциальность

4.1. Сведения о счете Клиента и операциях по счету Клиента, о ключевой информации и средствах шифрования, материалах работы Согласительной комиссии, персональных данных Клиента не подлежат передаче третьим лицам, за исключением случаев, прямо установленных законом и Договором ДБО.

4.2. Стороны согласны с тем, что обязательства по Договору ДБО в части конфиденциальности, паролей и ключей остаются в силе и исполняются Сторонами в течение двух календарных лет после прекращения действия Договора ДБО.

5. Ответственность сторон

5.1. За неисполнение или ненадлежащее исполнение обязательств, предусмотренных настоящими Правилами Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

5.2. Клиент несет ответственность за содержание любого ЭД, подписанного ЭП Клиента.

5.3. Сторона, несвоевременно сообщившая о случаях утраты ключей ЭП, прекращения действия ЭП, несет связанные с этим убытки.

5.4. Банк не несет ответственности в случае невозможности осуществления обмена ЭД с Клиентом, если это вызвано неисправностями используемых программно-аппаратных средств и каналов связи, а также электросетей.

5.5. Банк не несет ответственности за убытки, понесенные Клиентом в результате исполнения Банком ЭПД, подписанных ЭП Клиента (при положительном результате проверки ЭП), и/или платежных документов на бумажном носителе, подписанных оригиналами подписей уполномоченных лиц Клиента и заверенных печатью Клиента, если они отправлены Клиентом ошибочно или повторно.

5.6. Банк не несет ответственности за убытки, понесенные Клиентом в результате исполнения Банком ЭПД, подписанных ЭП Клиента (при положительном результате проверки ЭП), и при несанкционированном использовании ЭП Клиента, которой подписан ЭПД, за исключением случая, когда Клиент надлежащим образом уведомил Банк о том, что ЭП утратила силу.

5.7. Банк не несет ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к АРМ Клиента, на котором осуществляется работа в системе «КТБ-Онлайн», включая удаленный сетевой доступ, и ключам ЭП Клиента.

5.8. Ответственность за ущерб, возникший вследствие нарушения конфиденциальности, несет Сторона, допустившая нарушение.

5.9. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств согласно данных Правил, если таковое явилось следствием обстоятельств непреодолимой силы (стихийные бедствия, технические сбои, а также иные обстоятельства), возникших после присоединения Клиента к данным Правилам, в результате событий чрезвычайного характера, которые не могли быть предвидены и предотвращены разумными мерами.

5.10. Клиент осведомлен о рисках сопутствующих при проведении операций посредством незащищенной сети передачи данных «Интернет».

6. Порядок разрешения споров

6.1. Все разногласия Сторон, касающиеся подлинности ЭД и принадлежности ЭП, разрешаются Согласительной комиссией Сторон с использованием согласительной процедуры. Создание согласительной комиссии и рассмотрение споров осуществляется в соответствии с Регламентом Удостоверяющего Центра АО «Кубаньторгбанк» и Приложением 8 к настоящим правилам.

6.2. Стороны признают решения согласительной комиссии, оформленные Актом в соответствии с Регламентом Удостоверяющего Центра АО «Кубаньторгбанк», обязательными и обязуются добровольно исполнить их в сроки, установленные этим актом.

6.3. Все иные разногласия, которые могут возникнуть при исполнении Договора ДБО и обмене ЭД, разрешаются путем переговоров. При этом Сторона, получившая претензию другой Стороны, обязана рассмотреть ее, подготовить и направить ответ в течение десяти рабочих дней с момента получения такой претензии.

6.4. В случае невозможности разрешения существующих разногласий путем переговоров, не достижения соглашения в рамках действия согласительной комиссии все споры между Сторонами подлежат рассмотрению в Арбитражном суде Краснодарского края в порядке, установленном законодательством Российской Федерации.

7. Срок действия Договора ДБО, порядок его изменения и расторжения

7.1. Клиент считается присоединившимся к настоящим Правилам, а Договор ДБО заключенным с момента акцепта Банком заявления Клиента о подключении к системе «КТБ-Онлайн» на неопределенный срок.

7.2. Клиент вправе в любое время отключить услугу «КТБ-Онлайн» в одностороннем порядке путем подачи заявления на отключение услуги по форме, установленной Банком.

7.3. Уведомления и любая другая переписка в рамках данных Правил считаются направленными надлежащим образом, если они доставлены адресату курьером, отправлены по почте заказным письмом, направлены по системе «КТБ-Онлайн» в виде ЭИД свободного формата, подписанного ЭП стороны-отправителя, или посредством иной связи по реквизитам Сторон.

7.4. Банк вправе отключить услугу «КТБ-Онлайн» в одностороннем порядке в следующих случаях:

7.4.1. При закрытии всех Счетов, обслуживание которых осуществлялось с использованием системы «КТБ-Онлайн».

7.4.2. В случае несогласия Клиента с изменениями данных Правил, вносимыми Банком в порядке, предусмотренном п.2.2.2. настоящих Правил.

7.4.3. В случае нарушения Клиентом требований к обмену ЭД и обеспечению безопасности при обмене ЭД, предусмотренных действующим законодательством, и

условий настоящих Правил или в случае неоднократного нарушения указанных требований и условий, независимо от последствий нарушения.

7.4.4. В случае неуплаты Клиентом комиссионного вознаграждения за услуги Банка в соответствии с действующими тарифами Банка и настоящих Правил более трех месяцев подряд.

7.4.5. При неактивности Клиента, отсутствии входа, в системе «КТБ-Онлайн» более трех месяцев подряд.

7.4.6. Иных случаях, предусмотренных действующим законодательством РФ.

7.5. Сторона вправе расторгнуть Договор ДБО или отключить услугу «КТБ-Онлайн», в одностороннем порядке в случаях, предусмотренных настоящими Правилами, после направления другой стороне соответствующего уведомления не менее чем за 10 (десять) рабочих дней до даты расторжения Договора ДБО. С момента получения такого уведомления обмен ЭПД прекращается. При этом Договор ДБО считается расторгнутым, услуга «КТБ-Онлайн» отключенной, с момента надлежащего исполнения сторонами всех принятых на себя обязательств. Ежемесячная плата, осуществленная Клиентом Банку в соответствии с тарифами до расторжения Договора ДБО, возврату не подлежит.

7.6. В случае расторжения Договора ДБО, отключения услуги «КТБ-Онлайн» по инициативе Клиента, последний обязан передать в Банк письменное уведомление. Датой расторжения считается дата получения Банком указанного заявления при условии отсутствия у Клиента обязательств по погашению перед Банком задолженности по Договору ДБО. При наличии указанных обязательств по погашению задолженности перед Банком Договор ДБО считается расторгнутым с момента исполнения Клиентом обязанности по оплате указанной задолженности.

7.7. В случае расторжения Договора ДБО Клиент обязуется сдать в Банк все программно-технические средства, предоставленные ему Банком.

8. Прочие условия

8.1. Стороны обязуются уведомлять друг друга об изменении своего места нахождения, а также об изменении иных реквизитов, имеющих существенное значение для определения юридического статуса и идентификации Сторон не позднее 5 (пяти) рабочих дней с момента вступления таких изменений в силу.

8.2. Права и обязанности Сторон по Договору ДБО не могут быть переуступлены или переданы третьим лицам без получения предварительного согласия другой стороны.

8.3. По неурегулированным настоящими Правилами вопросам Стороны руководствуются действующим законодательством РФ.

8.4. К настоящим Правилам прилагаются и являются их неотъемлемой частью следующие приложения:

8.4.1. Порядок подключения к системе «КТБ-Онлайн» (Приложение 1).

8.4.2. Требования к организации рабочего места Клиента, необходимые для работы в системе «КТБ-Онлайн» (Приложение 2).

8.4.3. Список основных функций, выполняемых в системе «КТБ-Онлайн» (Приложение 3).

8.4.4. Заявление о присоединении к системе «КТБ-Онлайн» или изменение параметров подключения (Приложение 4).

8.4.5. Обеспечение информационной безопасности (Приложение 5).

8.4.6. Акт приема-передачи СКЗИ (Приложение 6).

8.4.7. Запрос на регистрацию и выпуск сертификата (Приложение 7).

8.4.8. Порядок проведения технической экспертизы при возникновении спорных ситуаций (Приложение 8).

8.4.9. Протокол проверки электронной подписи (Приложение 9).

Порядок подключения к системе «КТБ-Онлайн»

1. Для подключения к системе «КТБ-Онлайн», Клиент предоставляет в Банк:
 - 1.1. Подписанное и скрепленное в установленных законом случаях оттиском печати Клиента Заявление об открытии расчетного счета в АО «Кубаньторгбанк»/подключении услуг (в двух экземплярах, по одному для Банка и Клиента), и его акцепта Банком, в разделе 3 которого Клиент указал о своем намерении подключить услугу «КТБ-Онлайн».
 - 1.2. Заявление о присоединении к системе «КТБ-Онлайн» (Приложение 4 к настоящим Правилам).
 - 1.3. Доверенность полномочного представителя Клиента (Приложение 1 к регламенту Удостоверяющего центра АО «Кубаньторгбанк»).
2. Порядок формирования ключей ЭП, регистрации в Удостоверяющем Центре АО «Кубаньторгбанк» и установки программного обеспечения, изложен в Регламенте Удостоверяющем Центре АО «Кубаньторгбанк». Регламент в электронном виде размещен на сайте Банка в сети Интернет по адресу: www.bktb.ru.

Требования к организации рабочего места Клиента

1. На рабочем месте Уполномоченного лица Клиента должна быть установлена лицензионная ОС MS Windows 10 или 11.
2. Запрещено использовать различные редакции ОС не предназначенных для коммерческого использования.
3. Доступ в сеть общего пользования «Интернет».
4. При наличии в организации межсетевого экрана должна быть обеспечена возможность устанавливать TCP-соединения через порт 443.
5. На компьютере должен быть установлен интернет обозреватель актуальной версии (Google Chrome, Mozilla Firefox, Microsoft Edge).
6. В интернет обозревателе должно быть отключено блокирование всплывающих окон.
7. Сайт b2b.bktb.ru должен быть доступен с рабочего места Уполномоченного лица Клиента.

Список основных функции, выполняемых в системе «КТБ-Онлайн»

1. Просмотр остатков и оборотов выбранного счета за текущий или произвольный период.
2. Просмотр и печать платежных документов, проведенных по счету.
3. Печать выписок по счету за день и за произвольный период.
4. Ввод платежных документов, просмотр и коррекция, подпись и отправка в банковскую систему.
5. Загрузка и выгрузка документов.
6. Просмотр отправленных в банк документов и их текущего состояния.
7. Ведение списка получателей, контрагентов и назначений платежа.
8. Изменение собственного пароля.

Обеспечение информационной безопасности

1. Общие требования по информационной безопасности

1.1. Клиентом самостоятельно организовать антивирусную защиту на АРМ обмена электронными документами и обеспечить использование телекоммуникационных каналов связи общего пользования.

1.2. Обеспечивать конфиденциальность ключей электронных подписей своих Уполномоченных лиц, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия.

1.3. Не использовать ключ электронной подписи своего Уполномоченного лица при наличии оснований полагать, что произошла компрометация данного ключа электронной подписи.

1.4. Уведомлять Банк официальным электронным письмом о нарушении конфиденциальности (компрометации) ключа электронной подписи своего Уполномоченного лица, в течение не более чем одного рабочего дня, со дня получения информации о таком нарушении, на почтовый ящик sib@kubantorgbank.ru или телефону +7(861)212-60-80.

1.5. Выполнять процедуру аутентификации Уполномоченного лица (пользователя УЦ) и процедуру смены его Сертификата и ключа электронной подписи в случае компрометации последнего, в соответствии с порядком, установленным Регламентом УЦ.

1.6. Своевременно производить плановую и внеплановую смену Сертификатов и ключей электронной подписи Уполномоченных лиц в соответствии с порядком, установленным Регламентом УЦ.

1.7. Обеспечить хранение архивов, переданных и принятых ЭД и ключей проверки электронной подписи Уполномоченных лиц в течение 5 (пяти) лет, если иное не предусмотрено Договором ДБО.

2. Требования к эксплуатации сертифицированных СКЗИ и средств ЭП

2.1. Клиентом, эксплуатирующим СКЗИ, для осуществления мероприятий по обеспечению функционирования и безопасности СКЗИ, в соответствии с действующими в Российской Федерации нормативными правовыми актами, назначается ответственное должностное лицо (администратор безопасности).

2.2. На администратора безопасности Клиента возлагаются задачи работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контроль над соблюдением описанных ниже требований.

2.3. Правом доступа к пользованию СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку.

2.4. Администратор безопасности Клиента, эксплуатирующей СКЗИ должен обеспечить ознакомление с эксплуатационной документацией разработчика на СКЗИ и данными требованиями всех уполномоченных и ответственных лиц, допущенных к работе с СКЗИ на автоматизированном рабочем месте.

2.5. Установку (инсталляцию) и настройку СКЗИ на автоматизированное рабочее место Клиента, эксплуатирующего СКЗИ, может производить только при наличии штатного работника, отвечающего квалификационным требованиям законодательства Российской Федерации в области информационной безопасности.

2.6. Клиентом, эксплуатирующим СКЗИ, создаются условия, обеспечивающие сохранность конфиденциальной информации, обрабатываемой с помощью СКЗИ.

2.7. Клиентом, эксплуатирующим СКЗИ, обеспечивается контроль используемых для работы с СКЗИ операционных систем на наличие обновлений по безопасности и производится их своевременная установка.

2.8. Клиентом, эксплуатирующим СКЗИ, исключается возможность неконтролируемого проникновения или пребывания в помещении, где эксплуатируется автоматизированное рабочее место, посторонних лиц посредством использования специального оборудования и Клиента режима охраны.

2.9. Клиентом, эксплуатирующим СКЗИ, обеспечивается наличие на автоматизированном рабочем месте средств антивирусной защиты и межсетевого экранирования, а также производится своевременное их обновление.

2.10. Владельцы сертификатов ключей проверки ЭП обеспечивают конфиденциальность своих ключевых документов и не допускать использование принадлежащих им ключей электронных подписей без их согласия.

2.11. Клиентом, эксплуатирующим СКЗИ, регламентируется поэкземплярный учет и хранение ключевых документов, непосредственная работа с ними, а также персональная ответственность за их сохранность.

2.12. Клиентом, эксплуатирующим СКЗИ, хранение ключевых документов и ключевых носителей допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение и несанкционированное использование.

2.13. Клиентом, эксплуатирующим СКЗИ, ключевые документы должны храниться в металлических шкафах (сейфах), оборудованных внутренними замками с двумя экземплярами ключей. Дубликаты ключей от металлических шкафов (сейфов) должны находиться у ответственного лица.

2.14. Владельцы сертификатов ключей проверки ЭП не должны использовать ключевые документы, в отношении которых возникло подозрение в компрометации.

2.15. При первоначальной эксплуатации ключевых документов Уполномоченные лица должны сменить код доступа (пин-код) к ключевому носителю на известный только им.

2.16. Владельцам сертификатов ключей проверки ЭП запрещается:

2.16.1. Раскрывать содержание ключевых документов и передавать их неуполномоченным лицам.

2.16.2. Использовать ключевые документы после окончания срока их действия.

2.16.3. Использовать ключевые документы и СКЗИ в целях непредусмотренных Условиями.

2.16.4. Самостоятельно вносить изменения в настройки программного обеспечения и СКЗИ используемого в Условиях.

2.17. Клиентом, эксплуатирующим СКЗИ, должна осуществляться процедура резервного копирования автоматизированного рабочего места, чтобы обеспечить непрерывность функционирования СКЗИ, в случае выхода из строя оборудования.

3. Порядок приема-передачи электронных документов в системе

3.1. В соответствии с Условиями Стороны при осуществлении обмена ЭД могут являться отправляющей (далее – Отправитель) или получающей (далее – Получатель) стороной.

3.2. Уполномоченное лицо Отправителя готовит документ в соответствии с требованиями к форматам, формирует электронный документ, путем подписания созданного документа личной электронной подписью.

3.3. Отправка ЭД осуществляется по открытым каналам связи, с использованием сертифицированных средств криптографической защиты информации.

3.4. Основанием для принятия Получателем ЭД Отправителя является наличие и подлинность электронной подписи Уполномоченного лица Отправителя, а также соответствие ЭД требованиям к форматам.

3.5. При возникновении разногласий и споров, связанных с ведением ЗЭДО в рамках настоящих Условий, с целью установления фактических обстоятельств, послуживших основанием для их возникновения, а также для проверки подлинности и подтверждения авторства ЭД, Стороны проводят техническую экспертизу в соответствии с данным Приложением.

3.6. В случае невозможности ведения ЗЭДО, Клиент имеет право предоставить в Банк документы, оформленные в соответствии с Договором ДБО на бумажном носителе.

4. Меры обеспечения конфиденциальности ключей ЭП

4.1. Стороны обеспечивают конфиденциальность личных ключей ЭП и выполнение требований по информационной безопасности при пользовании СКЗИ в соответствии с эксплуатационной документацией разработчика (формулярами СКЗИ) и Руководства по обеспечению безопасности использования ЭП и средств ЭП (Приложение 4 к регламенту УЦ АО «Кубаньторгбанк»).

4.2. Ключи ЭП Пользователей УЦ записываются при их генерации на отчуждаемые ключевые носители. В качестве ключевых носителей используются только носители, указанные в формуляре используемого средства ЭП и СКЗИ УЦ.

4.3. Обязательно используется защита ключа ЭП на ключевом носителе ПИН-кодом. К ПИН-коду предъявляются следующие требования:

4.3.1. Длина ПИН-кода не должна быть меньше 8 символов.

4.3.2. В ПИН-коде должны присутствовать символы из следующих категорий: строчные буквы английского алфавита от "a" до "z"; прописные буквы английского алфавита от "A" до "Z"; десятичные цифры от "0" до "9"; символы, не принадлежащие к алфавитно-цифровому набору; - использование трех и более символов, набранных в одном регистре, идущих подряд на клавиатуре, недопустимо.

4.3.3. Использование трех и более символов, набранных в одном регистре, идущих подряд в алфавитном порядке, недопустимо.

4.3.4. Использование двух и более одинаковых символов, набранных в одном регистре, идущих подряд, недопустимо.

4.3.5. Задание ПИН-кода, совпадающего с одним из трех последних ПИН-кодов, недопустимо.

4.3.6. ПИН-код не должен содержать букв русского алфавита.

4.3.7. Установленный по умолчанию на новых ключевых носителях ПИН-код пользователя должен быть изменен перед началом эксплуатации.

4.3.8. ПИН-коды должны быть случайны, насколько это возможно, и не связаны каким-либо образом с конкретным пользователем.

4.3.9. Ответственность за сохранение ПИН-кода в тайне возлагается на Владельца ключа ЭП.

4.3.10. Использование одного и того же значения ПИН-кода для защиты нескольких ключей ЭП недопустимо.

4.4. Все изготавливаемые УЦ ключи ЭП защищены от экспорта (некопируемые).

4.5. По требованиям Бизнес-процесса Банка могут использоваться ключевые носители с аппаратным СКЗИ, которые обеспечивают неизвлекаемость ключа ЭП.

4.6. Работники УЦ, являющиеся Владельцами ключей ЭП, также выполняют указанные в разделе меры защиты ключей ЭП.

5. Действия при компрометации ключа электронной подписи (КЭП)

5.1. К событиям, связанным с компрометацией КЭП, относятся следующие:

5.1.1. Утрата (в том числе хищение) ключевого документа.

5.1.2. Утрата ключевого документа с последующим обнаружением.

5.1.3. Увольнение сотрудников, имевших доступ к ключевому документу.

5.1.4. Передача КЭП по каналу связи в открытом виде.

5.1.5. Нарушение правил хранения (нарушение печатей на сейфе и т.п.) и уничтожения ключевого документа.

5.1.6. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.

5.1.7. Несанкционированное копирование КЭП.

5.1.8. Случаи, когда нельзя достоверно установить, что произошло с ключевым документом, содержащими ключевую информацию (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

5.2. Уведомлять Банк официальным электронным письмом о нарушении конфиденциальности (компрометации) ключа электронной подписи своего Уполномоченного лица, в течение не более чем одного рабочего дня, со дня получения информации о таком нарушении, на почтовый ящик sib@kubantorgbank.ru или телефону +7 (861)212-60-80.

6. Требования к обеспечению защиты персональных данных

6.1. Стороны обязаны выполнять требования Федерального Закона №152-ФЗ «О персональных данных» при обмене ЭД.

6.2. Клиент гарантирует, что персональные данные получены законными способами, цели сбора персональных данных совместимы с целями, указанными в настоящих Условиях.

6.3. Стороны гарантируют ограничение обработки персональных данных достижением целей, определенных настоящими Условиями, и недопущение обработки персональных данных, несовместимой с целями сбора персональных данных.

6.4. Стороны обязаны обеспечивать конфиденциальность и целостность конфиденциальной информации (персональные данные и банковская тайна) при передаче их стороне.

6.5. Клиент обязан иметь согласие Работника на передачу персональных данных в Банк.

6.6. Для обеспечения защиты конфиденциальной информации, при передаче по открытым каналам связи (сеть Интернет), стороны применяют сертифицированные средства криптографической защиты информации.

6.7. Запрещено передавать/пересылать/ознакомлять третьих лиц с конфиденциальной информацией.

7. Порядок проведения технической экспертизы при возникновении спорных ситуаций

7.1. В случае возникновения спорной ситуации, Сторона, являющаяся инициатором (далее по тексту Инициатор) рассмотрения спорной ситуации, представляет противоположной Стороне (далее Ответчик) письменную претензию, содержащую существо претензии с указанием на документы с ЭП, явившиеся источником претензии (далее по тексту - спорные документы). Претензия и все прилагаемые к ней документы направляются нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату. Сторона, в адрес которой направлена претензия, обязана не позднее чем в течение 30 (тридцати) дней, а в случае трансграничного перевода денежных средств в течение 60 (шестидесяти) дней рассмотреть претензию. Непредставление ответа на претензию в течение установленного срока является нарушением установленного настоящими Правилами претензионного порядка и может рассматриваться лицом, направившим претензию, в качестве отказа в удовлетворении претензии.

7.2. Сторона - ответчик обязана в течение установленного сторонами срока от даты подачи претензии сформировать разрешительную комиссию для рассмотрения претензии. В состав комиссии включаются представители Стороны - инициатора, представители Стороны - ответчика, и при необходимости - независимые эксперты. В

состав членов комиссии может включать представители компании-разработчика средств ЭП. Выбор членов комиссии осуществляется по согласованию всеми Сторонами. При невозможности согласованного выбора, последний проводится случайно (по жребию). Все расходы, связанные с Клиентом деятельности согласительной комиссии несет сторона - инициатор. В случаях, установленных сторонами в дополнительных соглашениях, расходы, связанные с деятельностью согласительной комиссии, могут возлагаться и на сторону - ответчика.

7.3. Согласительная комиссия (далее - комиссия) создается с целью разрешения разногласий при обмене электронными документами (ЭД), установления фактических обстоятельств, послуживших основанием их возникновения, а также для проверки целостности и подтверждения подлинности ЭД. Бремя доказывания лежит на стороне, заявившей о нарушении своих прав.

7.4. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение Стороны, несущей ответственность согласно выводу об истинности ЭП под приложенными документами.

7.5. Разрешительная комиссия в течение установленного срока проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:

7.5.1. Разрешительная комиссия проводит техническую экспертизу электронных документов, заверенных электронной цифровой подписью и являющихся основаниями для рассматриваемой претензии.

7.5.2. Разрешительная комиссия проводит техническую экспертизу ключей ЭП, которыми были подписаны спорные документы, период действия и статус этих открытых ключей, и установление их принадлежности той или иной Стороне. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых для обмена ЭД (в пределах отношений, устанавливаемых Соглашением об использовании документов в электронной форме и признании ЭП сторон).

7.5.3. Разрешительная комиссия проводит техническую экспертизу корректности электронной цифровой подписи в спорных документах.

7.5.4. На основании данных технической экспертизы разрешительная комиссия составляет акт.

7.5.5. Решение комиссии и сопутствующие материалы по данному делу предоставляются каждой из Сторон и могут использоваться Сторонами при рассмотрении споров в Арбитражном суде Краснодарского края.

7.6. Сторона несет ответственность перед другой в случае, когда имело место хотя бы одна из следующих ситуаций:

7.6.1. Сторона не предъявляет своей копии спорного электронного документа.

7.6.2. ЭП Стороны в спорном документе оказалась некорректной (или отсутствует).

7.6.3. Противоположная Сторона предоставляет документ, отменяющий рассмотрение электронных документов с данной ЭП и имеющий отметку о приеме ранее даты спорного документа.

7.7. В случае, когда Сторона предъявляет электронный документ, корректность ЭП противоположной Стороны под которым признана разрешительной комиссией, принадлежность ключа ЭП противоположной Стороне подтверждена, эта Сторона по выполненным операциям перед противоположной Стороной ответственности не несет.

**Акт № _____ / _____
приема-передачи СКЗИ**

г. Краснодар

_____ 20____

АО «Кубаньторгбанк», именуемое далее Банк, в лице _____

с одной стороны, и _____
*наименование юридического лица, ИНН/Ф.И.О. индивидуального предпринимателя или физического лица,
занимающегося в установленном законодательством Российской Федерации порядке частной практикой*

именуемый далее Клиент, в лице _____
должность, Фамилия, Имя и Отчество представителя Клиента (полностью)

действующего на основании _____
Устав; доверенность №, дата. ЕГРИП

с другой стороны, составили настоящий Акт о нижеследующем:
Банк передал, а Клиент принял:

Номер сейф-пакета	Наименование СКЗИ	Регистрационный номер СКЗИ	ФИО УЛК, для которого предназначено СКЗИ

СКЗИ переданы в сейф-пакетах, обеспечивающих защиту от несанкционированного доступа и предназначены для использования УЛК.

Клиент:

Банк:

должность

должность

подпись

расшифровка подписи

подпись

расшифровка подписи

Отметки Органа криптографической защиты информации Банка:
Компоненты системы «КТБ-Онлайн» выдал:

должность

ФИО

дата

Порядок проведения технической экспертизы при возникновении спорных ситуаций

1. В случае возникновения спорной ситуации, Сторона, являющаяся инициатором (далее по тексту Инициатор) рассмотрения спорной ситуации, представляет противоположной Стороне (далее Ответчик) письменную претензию, содержащую существо претензии с указанием на документы с ЭП, явившиеся источником претензии (далее по тексту - спорные документы).

2. Претензия и все прилагаемые к ней документы направляются нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

3. Сторона, в адрес которой направлена претензия, обязана не позднее чем в течение 30 (тридцати) дней, а в случае трансграничного перевода денежных средств в течение 60 (шестидесяти) дней рассмотреть претензию. Непредставление ответа на претензию в течение установленного срока является нарушением установленного настоящими Правилами претензионного порядка и может рассматриваться лицом, направившим претензию, в качестве отказа в удовлетворении претензии.

4. Сторона - ответчик обязана в течение установленного сторонами срока от даты подачи претензии сформировать согласительную комиссию для рассмотрения претензии. В состав комиссии включаются представители Стороны - инициатора, представители Стороны - ответчика, и при необходимости - независимые эксперты. Выбор членов комиссии осуществляется по согласованию всеми Сторонами. При невозможности согласованного выбора, последний проводится случайно (по жребию). Все расходы, связанные с организацией деятельности согласительной комиссии несет сторона - инициатор. В случаях, установленных сторонами в дополнительных соглашениях, расходы, связанные с деятельностью согласительной комиссии, могут возлагаться и на сторону - ответчика.

5. Согласительная комиссия (далее - комиссия) создается с целью разрешения разногласий при обмене электронными документами (ЭД), установления фактических обстоятельств, послуживших основанием их возникновения, а также для проверки целостности и подтверждения подлинности ЭД.

6. Бремя доказывания лежит на стороне, заявившей о нарушении своих прав.

7. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение Стороны, несущей ответственность согласно выводу об истинности ЭП под приложенными документами.

8. Разрешительная комиссия в течение установленного срока проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:

8.1. Разрешительная комиссия проводит техническую экспертизу электронных документов, заверенных электронной цифровой подписью и являющихся основаниями для рассматриваемой претензии.

8.2. Разрешительная комиссия проводит техническую экспертизу ключей ЭП, которыми были подписаны спорные документы, период действия и статус этих открытых ключей, и установление их принадлежности той или иной Стороне.

8.2.1. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых для обмена ЭД (в пределах отношений, устанавливаемых Соглашением об использовании документов в электронной форме и признании ЭП сторон).

8.3. Разрешительная комиссия проводит техническую экспертизу корректности электронной цифровой подписи в спорных документах.

8.4. Технические экспертизы проводятся согласительной комиссией в соответствии с Регламентом УЦ АО «Кубаньторгбанк» и технической документацией на средства ЭП, используемых согласно данных Правил.

8.5. На основании данных технической экспертизы разрешительная комиссия составляет Протокол проверки электронной подписи (Приложение 9).

9. Решение комиссии и сопутствующие материалы по данному делу предоставляются каждой из Сторон и могут использоваться Сторонами при рассмотрении споров в Арбитражном суде Краснодарского края.

10. Сторона несет ответственность перед другой в случае, когда имело место хотя бы одна из следующих ситуаций:

10.1. Сторона не предъявляет своей копии спорного электронного документа.

10.2. ЭП Стороны в спорном документе оказалась некорректной (или отсутствует).

10.3. Противоположная Сторона предоставляет документ, отменяющий рассмотрение электронных документов с данной ЭП и имеющий отметку о приеме ранее даты спорного документа.

11. В случае, когда Сторона предъявляет электронный документ, корректность ЭП противоположной Стороны под которым признана согласительной комиссией, принадлежность ключа ЭП противоположной Стороне подтверждена, эта Сторона по выполненным операциям перед противоположной Стороной ответственности не несёт.

Протокол проверки электронной подписи

Время создания отчета: 14 Январь 2010 г. 16:36:15

Время, на которое проводилась проверка: <по штампу времени>

Проверен файл: H:\Экспертиза\Пакет 1\Документы\Подписанный документ.sig созданный 10 Декабрь 2009 г. 19:10:12 , размер (в байтах) 3966 , размер преобразованного из base64 (в байтах) 2896

Размер обработанного криптографического сообщения (в байтах): 2896

Количество проверенных ЭП: 1

Результат подтверждения подлинности ЭП номер 1

ЭП - ВЕРНА

ЭП была создана: не определено

В проверенном атрибуте подписи (1.2.840.113549.1.9.5) указано время подписания 10 Декабрь 2009 г. 19:10:12

Время, на которое проводилась проверка ЭП: 14 Январь 2010 г. 16:05:00
Время проверки определено по указанному времени при отсутствии действительных штампов времени

Информация об ЭП:

Алгоритм хеширования:

Название: ГОСТ Р 34.11-94 Идентификатор:

1.2.643.2.2.9

Алгоритм открытого ключа:

Название:

ГОСТ Р 34.10-2001 Идентификатор: 1.2.643.2.2.19

Значение:

809F F2A2 F1D5 675B 3E80 2741 2ADB EB8F D004
C24E 9928 393F EB8B 0940 ADFE 6422 866E F3FA
77DC 89DE 984B BAAB F5B9 C4EB EC73 212C A6B2
6DA8 C41D BCDC BA55 B0D1

Серийный номер: 07

Субъект: Mock Test CA TBSCert, ООО Crypto-Pro, RU

ЭП уполномоченных лиц удостоверяющих центров в цепочке сертификатов - ВЕРНА

Статус сертификата подписи - ДЕЙСТВИТЕЛЕН

Количество штампов времени на подпись: 0

Результат установления статуса цепочки сертификатов

Сертификаты, использованные при подтверждении подлинности ЭП Сертификат X.509:

Сведения о сертификате:

Кому выдан: Mock Test CA TBSCert

Кем выдан: Mock Test CA

Действителен с 6 июня 2008 г. 0:00:00 UTC по 1 января 2013 г. 0:00:00 UTC

Версия: 3 (0x2)

Серийный номер: 07

Издатель:

CN = Mock Test CA

SN = Сидоров

G = Сидор Сидорович

O = ООО Crypto-Pro

C = RU

Срок действия:

Действителен с: 6 июня 2008 г. 0:00:00 UTC

Действителен по: 1 января 2013 г. 0:00:00 UTC

Субъект:

CN = Mock Test CA TBSCert

O = ООО Crypto-Pro

C = RU

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.19

Параметры: 30 12 06 07 2a 85 03 02 02 23 01 06 07 2a 85 03 02 02 1e 01

Значение:

0440 6053 66A4 4333 CB62 59A7 C50E 3A03 3E72
8754 F950 DDB8 70DE C3C7 2070 1D1A 6CA1 BD87
606F A83A B8E0 B730 F705 297E E5C6 58C2 D1A6
AC65 6687 48A1 6B6D 3046 1EF6

Расширения X.509

1. Расширение 2.5.29.16

Название: Период использования закрытого ключа

Значение: 30 22 80 0f 32 30 30 38 30 36 30 36 30 30 30 30 30 5a 81 0f 32 30 31 33 30 31 30 31 30 30 30 30 30 30 5a

2. Расширение 2.5.29.15

Название: Использование ключа

Значение: Цифровая подпись (80)

3. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение: Идентификатор ключа=6b f9 35 da ee b0 4d c4 30 d5 21 29 42 ea 53 51 75 11 5e f8

4. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: 1f fc b1 0b d4 c5 97 fe d3 11 1a be 86 f6 f2 3e 3b b6 a1 7f

ЭП:

Алгоритм ЭП:

Название: ГОСТ Р 34.11/34.10-2001 Идентификатор: 1.2.643.2.2.3

Значение:

CA0D D3E8 3409 1F0D B99F 9F86 C72E 8A08 7050
44FA 0D3B 4003 F013 BDAD 513F 740A 45C4 C1AB
8A65 DE51 626D 699F 5912 DD57 3CAB 4DC0 B177 6771 3FB7 34BD A84F A9AC

Сертификат X.509:

Сведения о сертификате:

Кому выдан: Mock Test CA

Кем выдан: Mock Test Root CA

Действителен с 5 мая 2008 г. 0:00:00 UTC по 1 января 2014 г. 0:00:00 UTC

Версия: 3 (0x2)

Серийный номер: 01

Издатель:

CN = Mock Test Root CA

SN = Иванов

G = Иван Иванович

O = ООО Crypto-Pro

C = RU

Срок действия:

Действителен с: 5 мая 2008 г. 0:00:00 UTC

Действителен по: 1 января 2014 г. 0:00:00 UTC

Субъект:

CN = Mock Test CA

SN = Сидоров

G = Сидор Сидорович

O = ООО Crypto-Pro

C = RU

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.19

Параметры: 30 12 06 07 2a 85 03 02 02 23 01 06 07 2a 85 03 02 02 1e 01

Значение:

0440 17EE 1684 5D16 B46E 158A 2BAB 8CE8 D7DE
847A E964 ADAD 6D46 C8F0 5D86 0319 E94C 7B2E
100C 3F1C 2A02 9D5C 0036 F3EC 95B0 2A25 D7F4
AAE4 598E 35C3 4E1F F298 A3FC

Расширения X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Подписывание сертификатов,

Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (e6)

1. Расширение 2.5.29.19 (критическое)

Название: Основные ограничения

Значение:

Тип субъекта=ЦС

Ограничение на длину пути=Отсутствует

3. Расширение 2.5.29.16

Название: Период использования закрытого ключа

Значение: 30 22 80 0f 32 30 30 38 30 35 30 35 30 30 30 30 30 5a 81 0f 32 30 31 34 30 31 30 31 30 30 30 30 30 30 5a

4. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение:

Идентификатор ключа=4e ca 97 a2 2c 2f d7 4e d3 db e2 5b 28 4e e8 ba 00 61 8d 1d

5. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: 6b f9 35 da ee b0 4d c4 30 d5 21 29 42 ea 53 51 75 11 5e f8

ЭП:

Алгоритм ЭП:

Название: ГОСТ Р 34.11/34.10-2001

Идентификатор: 1.2.643.2.2.3

Значение:

EE90 2977 E94A F67A BA9D C059 34E9 6CF5 C825

3048 5FB1 93C2 A4E0 4561 8DA4 7849 C018 39F7

A745 81AC 23B9 EF05 D2A0 84DE DB30 1A3C 02DE 36C3 34B0 32CF 2EA8 94EB

Сертификат X.509:

Сведения о сертификате:

Кому выдан: Mock Test Root CA

Кем выдан: Mock Test Root CA

Действителен с 1 января 2003 г. 0:00:00 UTC по 1 января 2018 г. 0:00:00 UTC

Версия: 3 (0x2)

Серийный номер: 53A9 BBF8 A39B 1FF4 3613 381D 0A5C 6B7C

Издатель:

CN = Mock Test Root CA

SN = Иванов

G = Иван Иванович

O = ООО Crypto-Pro

C = RU

Срок действия:

Действителен с: 1 января 2003 г. 0:00:00 UTC

Действителен по: 1 января 2018 г. 0:00:00 UTC

Субъект:

CN = Mock Test Root CA

SN = Иванов

G = Иван Иванович

O = ООО Crypto-Pro

C = RU

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.19

Параметры: 30 12 06 07 2a 85 03 02 02 23 01 06 07 2a 85 03 02 02 1e 01

Значение:

0440 C4C4 D6FA 092D B548 7300 C380 7753 255E

3F3A 5712 02D6 AF37 BA41 20CB 15BA C889 D40F

446D 9390 C3B5 3245 E70A 3F8D 0DFA 7685 D670

DD6C 2D72 0A0E 3BFC 6332 F341

Расширения X.509

1. Расширение 2.5.29.16

Название: Период использования закрытого ключа

Значение: 30 22 80 0f 32 30 30 35 30 31 30 31 30 30 30 30 30 31 5a 81 0f 32 30 31 39 30 31 30 31 30 30 30 30 31 5a

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа
 Значение: Подписывание сертификатов, Автономное подписание списка отзыва (CRL),
 Подписывание списка отзыва (CRL) (06)
 2. Расширение 2.5.29.19 (критическое)
 Название: Основные ограничения
 Значение:
 Тип субъекта=ЦС
 Ограничение на длину пути=Отсутствует
 4. Расширение 2.5.29.14
 Название: Идентификатор ключа субъекта
 Значение: 4e ca 97 a2 2c 2f d7 4e d3 db e2 5b 28 4e e8 ba 00 61 8d 1d
ЭП:
 Алгоритм ЭП:
 Название: ГОСТ Р 34.11/34.10-2001
 Идентификатор: 1.2.643.2.2.3
 Значение:
 FF48 D11E FF91 E7F1 6E76 CC15 615E 2140 B205
 BFB7 2F41 433B 8961 1D2F 7308 E9B4 4286 63D7
 D240 C9F6 CC86 5821 C860 DE21 22C9 FB79 F7D4 B0EC B19F 741E 169F A006

Согласительная комиссия:

_____	_____	_____	_____
Организация	ФИО	подпись	дата
_____	_____	_____	_____
Организация	ФИО	подпись	дата
_____	_____	_____	_____
Организация	ФИО	подпись	дата
_____	_____	_____	_____
Организация	ФИО	подпись	дата