ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ БАНК «ИТУРУП»

УТВЕРЖДЕНО
Правлением Банк «ИТУРУП» (ООО)
(протокол от «__» ____ 2019 г. № __)

Регламент обмена электронными документами по телекоммуникационным каналам связи с использованием технологий дистанционного банковского обслуживания юридических лиц на базе системы ДБО.

Настоящий Регламент обмена электронными документами по телекоммуникационным каналам связи с использованием технологий дистанционного банковского обслуживания (далее – «Регламент») разработан на основании действующего законодательства Российской Федерации и определяет порядок и условия:

- подключения и предоставления клиентам Банка «ИТУРУП» (ООО) (кроме кредитных организаций) услуг по обмену электронными документами с электронной подписью по телекоммуникационным каналам связи с использованием системы ДБО;
- электронного документооборота в системе ДБО;
- организации защиты информации в системе ДБО;
- рассмотрения конфликтных ситуаций, связанных с подлинностью электронных документов.

Термины и определения, используемые в Регламенте

Для целей Регламента и Договора оказания услуг дистанционного банковского обслуживания юридических лиц используются следующие термины и определения:

Автоматизированное рабочее место системы ДБО (АРМ «Клиент»/АРМ «Банк») – составная часть системы Дистанционного Банковского Обслуживания (ДБО), устанавливаемая на территории Клиента/Банка, используемая Клиентом/Банком для предоставления и получения ЭД.

Авторство ЭД - принадлежность ЭД создавшей его Стороне.

Администратор АРМ Банка / АРМ Клиента – уполномоченный сотрудник Банка/Клиента, отвечающий за функционирование и работоспособность системы ДБО.

Банк – Общество с ограниченной ответственностью Банк «ИТУРУП».

Владелец сертификата ключа проверки электронной подписи – участник системы ДБО, который в установленном порядке сгенерировал ключ и получил сертификат ключа проверки электронной подписи;

Действительная электронная подпись – электронная подпись, прошедшая процедуру признания, сертификат ключа проверки которой не прекратил свое действие и не был аннулирован на момент подписания электронного документа;

Договор оказания услуг дистанционного банковского обслуживания юридических лиц (Договор) – в силу Договора Клиент присоединяется к системе ДБО, организованной Банком в соответствии с настоящим Регламентом;

Клиент – лицо (юридическое лицо; индивидуальный предприниматель;), присоединившееся к Регламенту и Договору оказания услуг дистанционного банковского обслуживания юридических лиц;

Ключевой носитель - отчуждаемый носитель (USB Token), предназначенный для хранения криптографических ключей;

Ключ электронной подписи (секретный ключ, ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи и имеющаяся только у его владельца;

Ключ проверки электронной подписи (открытый ключ) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;

Конфликтная ситуация - ситуация, при которой у Участников Системы возникает необходимость разрешить вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных средствами криптографической защиты информации;

Компрометация ключа ЭП - утрата доверия к тому, что используемые секретные ключи недоступны посторонним лицам и обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства). К таким событиям относятся, включая, но не ограничиваясь, следующие:

- утрата или порча носителя ключевой информации;
- утрата носителя ключевой информации с последующим обнаружением;
- временный доступ посторонних лиц к носителям ключевой информации либо
- подозрение, что такой доступ имел место;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к носителям ключевой информации посторонних лиц;

Корректная электронная подпись - электронная подпись, дающая положительный результат при ее проверке программно-аппаратными средствами системы ДБО, с использованием действующего на момент создания ЭП для ЭД, сертификата ключа проверки электронной подписи;

Криптографический профиль – техническая учетная запись, содержащая совокупность сведений о сертификате проверки ключа ЭП, его владельце, праве подписи владельца и количестве подписей на ЭД в рамках системы ДБО;

Криптографический ключ – ключ электронной подписи или ключ проверки электронной подписи;

НЗН – не защищённый носитель (флэш карта, дискета);

Обезличенный дистрибутив - дистрибутив программного обеспечения клиентской части Системы, подготовленный Банком без привязки к конкретной организации и\или физическому лицу и предназначенный для оптимизации подключения Клиентов к системе ДБО;

Право подписи ключа – роль, предоставляемая криптографическому ключу в системе ДБО в соответствии с карточкой образцов подписей и оттиска печати Клиента. А в случае отсутствия представителя Клиента в карточке образцов подписей и оттиска печати – ключу может быть дана роль создания документов без права их подписи;

Проверка электронной подписи - процедура признания электронной подписи, которую проходят подписанные электронной подписью электронные документы, передаваемые участниками электронного обмена системы ДБО друг другу;

Псевдоним владельца сертификата ключа проверки ЭП – вымышленное или обезличенное имя владельца сертификата ключа подписи, присваивается в случае отсутствия представителя клиента в карточке подписей и только по заявлению Клиента. Владелец такого обезличенного сертификата не может создавать ЭП на ЭД, вместе с тем имеет право входа в систему ДБО, создания документов и обработки входящих документов из Банка;

Система обмена электронными документами с ЭП - сервис системы ДБО, обеспечивающий работу Клиента посредством сайта Банка https://www.iturupbank.ru (либо https://biz.iturupbank.ru) и позволяющий осуществлять переводы денежных средств, получать выписки по счетам, принимать и отправлять иные электронные документы, в рамках текущей версии системы, а также совокупность нормативных и организационно-методических документов, регламентирующих взаимоотношения Участников Системы, организованной в соответствии с настоящим Регламентом;

Сертификат ключа проверки электронной подписи (сертификат ключа проверки ЭП) - электронный документ и/или документ на бумажном носителе, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи, бумажный вариант удостоверяется соб-

ственноручной подписью владельца и печатью организации (при наличии), в случае электронного документа удостоверяется усиленной квалифицированной электронной подписью выданной, аккредитованным Минкомсвязью РФ, удостоверяющим центром, при этом необходимо предварительное согласование с Банком;

Средства криптографической защиты информации (СКЗИ) - сертифицированные в порядке, установленном законодательством Российской Федерации, аппаратные и (или) программные средства, обеспечивающие шифрование, контроль целостности и применение ЭП при обмене электронными документами в Системе ДБО и совместимые с СКЗИ, используемыми Банком;

Статус электронного документа (статус ЭД) – стадия (этапы) обработки Банком ЭД;

Счет – счет Клиента, открытый в Банке на основании Договора банковского счета;

Технологический ключ – последовательность бит, создаваемая Банком, применяемая при первоначальной регистрации Клиента в системе ДБО. Технологический ключ не участвует при создании ЭП на ЭПД и служит только для создания Клиентом секретного ключа ЭП и регистрации открытого ключа ЭП;

Участники системы ДБО – Банк и его Клиенты, осуществляющие обмен электронными документами с ЭП в системе ДБО, а также организации, предоставляющие услуги по обеспечению и обслуживанию осуществляемого обмена;

Электронный платежный документ (ЭПД) - документ в электронной форме, являющийся основанием для совершения операций по счету (счетам) Клиента, подписанный (защищенный) соответствующими электронными подписями и имеющий равную юридическую силу с расчетными (платежными) документами на бумажных носителях, подписанными уполномоченными лицами Клиента и заверенными оттиском печати Клиента (при наличии);

Электронный информационный документ (ЭИД) - документ в электронной форме, подписанный (защищенный) ЭП участника Системы и обеспечивающий обмен информацией при совершении расчетов и проведении операций по счету Клиента (запросы, отчеты, выписки из счетов, квитанции и т.п.);

Электронный документ (ЭД) – ЭПД или ЭИД;

Электронная подпись (ЭП) - информация в электронной форме, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяющая определить лицо, подписавшее электронный документ и обнаружить факт внесения изменений в электронный документ после момента его подписания;

ЭП Клиента - ЭП, владельцем сертификата ключа проверки электронной подписи которой является Клиент (уполномоченное лицо Клиента), использующий средства ЭП в рамках системы ДБО;

ЭП Банка - ЭП, владельцем сертификата ключа проверки электронной подписи которого является Банк;

USB-токен- «MS_KEY K» - «АНГАРА» Исп.8.1.1 (сертификат ФСБ РФ № СФ/124-3072 от 20.02.2017), персональное средство аутентификации и идентификации пользователя, безопасного хранения ключей ЭП в виде USB-брелока, в котором реализованы криптоалгоритмы в соответствии с стандартами Российской Федерации (ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 28147-89, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015), генерирует ключи ЭП внутри себя, обеспечивает их защищенное не извлекаемое хранение и формирует ЭП под электронными документами внутри устройства.

Прочие используемые термины и сокращения соответствуют законодательству Российской Федерации, нормативным актам Банка России, а также заключенным между Сторонами договору банковского счета и Договору оказания услуг дистанционного банковского обслуживания юридических лиц .

1. Общие положения

Регламент является общедоступным документом, обязательным для исполнения всеми участниками системы ДБО.

Регламент содержит процедурные вопросы и правила работы в системе ДБО, определяет порядок защиты информации и разбора конфликтных ситуаций при обмене электронными документами. Регламент начинает действовать между Банком и Клиентом с момента присоединения к Договору оказания услуг дистанционного банковского обслуживания юридических лиц, размещенного на сайте http://www.iturupbank.ru и получения Банком от Клиента Заявления о присоединении к Договору.

При обмене электронными документами в системе ДБО Клиенты должны руководствоваться положениями настоящего Регламента. Клиент принимает порядок и условия электронного документооборота путем присоединения к Договору в целом.

2. Процесс работы в системе ДБО

2.1. Для осуществления информационного обмена в рамках системы ДБО Клиенту необходимо:

- подписать и представить в Банк Заявление (Приложение 1 к договору) на подключение к системе ДБО;
- ознакомиться с настоящим Регламентом;
- обеспечить соответствие аппаратного обеспечения требованиям Регламента
- (Приложение №1 Регламента);
- сгенерировать ЭП, распечатать и подписать сертификат ЭП или подготовить аналогичный электронный документ.

2.2 Информационный обмен в рамках системы ДБО осуществляется по открытым каналам связи, в том числе с использованием сети Интернет.

2.3 Банк выполняет работы по подключению Клиента к системе ДБО только на основании его Заявления.

2.4. Если у Банка нет замечаний по оформлению и комплектности документов, представленных Клиентом, и получен сертификат ключа проверки ЭП, Банк регистрирует сертификат в системе ДБО.

2.5. Дата регистрации сертификата является датой подключения Клиента к системе ДБО в режиме исполнения ЭД.

2.6 В процессе эксплуатации системы ДБО Стороны самостоятельно выполняют необходимые мероприятия, обеспечивающие на своей территории: работоспособность своих программно-технических средств, каналов связи, защиту ключей электронной подписи (секретных ключей), паролей и других ресурсов от несанкционированного доступа.

2.7 Работа Клиента в Системе ДБО состоит из следующих основных этапов:

1) вход свою учетную запись для получения выписок, для отправки электронных документов;

2) ежедневный контроль остатка по счету и состояния документов, обработанных Банком;

3) заполнение электронных бланков документов, подпись платежных документов уполномоченными лицами, обладающими правом подписи электронных документов;

4) получение в течение операционного дня отрицательных финансовых квитанций, отправленных Банком, в случае обнаружения ошибок;

5) анализ сообщений с причинами отказа, получение телефонных консультаций при возникновении сомнений в правомерности возврата документов;

6) создание новых электронных документов с учетом замечаний (обнаруженных ошибок);

7) отправка электронных документов в Банк в соответствии с графиком приема электронных документов;

8) отзыв направленного в Банк ЭД. Осуществляется путем отправки в Банк заявки на отзыв документа. Исполнение Банком заявки Клиента на отзыв документа производится в соответствии п.5.10 регламента.

2.8 График приёма и обработки электронных документов.

Система ДБО принимает ЭД от Клиента круглосуточно, без выходных дней (за исключением возможных технических перерывов). Исполняются принятые документы в операционное время работы Банка (9-30 – 17-00, Пн-Пт). Документы, принятые после текущего операционного времени, исполняются на следующий операционный день. Контрольным временем при приеме документов является время на сервере Банка. Банк производит исполнение документов в соответствии с Договором банковского счета.

2.9. Обмен электронными документами включает:

- формирование ЭД;
- отправку и доставку ЭД;
- проверку ЭД;
- подтверждение получения ЭД;
- отзыв ЭД;
- хранение электронных документов (ведение архивов ЭД);
- создание дополнительных экземпляров ЭД;
- создание бумажных копий ЭД.

2.10 ЭД порождает права и обязанности Сторон по договору(ам) банковского счета, Договору оказания услуг дистанционного банковского обслуживания юридических лиц, другим договорам, в рамках которых происходит взаимодействие с использованием системы ДБО, если ЭД передающей Стороной оформлен надлежащим образом, заверен корректными ЭП в необходимом количестве и передан, а принимающей Стороной – получен, обработан, ЭП проверены и их проверка дала положительный результат.

2.11 Условия использования ЭП

2.11.1. Все документы, исходящие от Участников Системы, подписываются ЭП Участников. За неправомерное подписание электронного документа ЭП ответственность несет Участник Системы, допустивший это нарушение.

2.11.2. Банк использует программные и технические средства генерации ключевой информации в неизменном виде по отношению к сертифицированному эталону и гарантирует отсутствие привнесенных нерегламентированных процедур скрытого копирования индивидуальной секретной ключевой информации в используемых программных и технических средствах.

2.11.3. Выдача USB-токена, указанному в Заявлении на подключение к системе ДБО, осуществляется при предъявлении документа, удостоверяющего личность.

Если USB-токен получает представитель, он должен предъявить доверенность от владельца ключа ЭП.

2.11.4. Открытый ключ\СКПЭП считается действующим, если на момент получения адресатом электронного документа, подписанного ЭП, не было заявлено о его недействительности.

2.11.5. Участники Системы должны обеспечить сохранность открытых ключей ЭП и их сертификатов в течение всего периода хранения электронных документов в архивном хранилище.

2.11.6. Плановая замена сертификатов проверки ключей ЭП Клиентов производится не реже одного раза в 2 года, а также при смене уполномоченных лиц.

За 30 дней до окончания установленного срока действия сертификата проверки ключа ЭП система начнет оповещать Клиента при каждом подключении о необходимости проведения плановой смены (перегенерации) ключа.

Плановую смену (перегенерацию) ключа можно провести в любое время, но не позднее 5 рабочих дней до истечения указанного в оповещении срока.

2.11.7. В случае компрометации закрытого ключа проверки ЭП, Клиент должен немедленно известить об этом Банки произвести внеплановую замену ключа проверки ЭП и сертификата.

2.11.8. При проведении операций по счету Клиента, ЭД подписываются ЭП уполномоченных лиц Клиента, указанных в карточке с образцами подписей, хранящейся в Банке, и зарегистрированными в системе ДБО.

2.11.9. ЭП уполномоченного лица Клиента на ЭД является аналогом первой/второй или единственной подписи в карточке с образцами подписей Клиента.

2.12. Стороны признают, что:

каждая Сторона несет полную ответственность за обеспечение безопасности и сохранность своих секретных ключей ЭП, а также за действия уполномоченных лиц;

2.13. Клиент самостоятельно:

- выбирает организацию – провайдера, обеспечивающую доступ к сети Интернет, и осуществляет подключение к сети Интернет за счет собственных средств;

- обеспечивает необходимую настройку телекоммуникационного и другого оборудования в своей локальной сети;

- обеспечивает защиту собственных программно-технических средств и криптографических ключей от несанкционированного доступа и вирусных атак из сети Интернет и полностью несет все риски, связанные с подключением его вычислительных средств к сети Интернет.

- обеспечивает восстановление работоспособности собственных вычислительных средств в случае выхода их из строя.

2.14. Клиент должен ежедневно сверять поступившую из Банка информацию с собственными данными и незамедлительно информировать Банк о любых обнаруженных расхождениях.

3. Перечень используемых в системе ДБО электронных документов

3.1. Электронные Платежные Документы (ЭПД):

- платежные поручения;
- заявления на перевод в иностранной валюте;
- поручения на покупку иностранной валюты за валюту Российской Федерации;
- поручения на продажу иностранной валюты за валюту Российской Федерации;
- распоряжения на списание средств с транзитного валютного счета (распоряжения на перечисление средств без осуществления продажи иностранной валюты).

3.2. Электронные Информационные Документы (ЭИД):

- заявление о постановке на учет контрактов (кредитных договоров);
- заявление о внесении изменений в раздел 1 Ведомости банковского контроля;
- заявление о снятии с учета контрактов (кредитных договоров);
- информация о валютных операциях;
- справка о подтверждающих документах;
- запросы на выписки;
- запросы на отзыв документа;
- произвольные документы в Банк (иные документы или письма, составленные в произвольной форме);
- выписки, содержащие информацию о движении средств по счетам;
- сообщения о статусе обработки ЭД (например: «Доставлен», «На обработке», «Исполнен», «Удален», «Отозван», «Отвергнут» и другие).

3.3. Любые документы в электронной форме, предоставляемые в Банк по системе ДБО, в том числе для осуществления валютных операций и обмена ЭД между Банком и Клиентом в целях валютного контроля, в том числе, взаимосвязанные документы, предоставляемые пакетом ЭД, присоединенным к сообщениям свободного формата, а также к формам учета и отчетности, заверяются ЭП.

При подписании ЭП клиента сообщения свободного формата, а также указанных выше документов, являющихся формами учета и отчетности, каждый из присоединенных электронных документов (пакета присоединенных взаимосвязанных электронных

документов), считается подписанным электронной подписью, которой подписано сообщение свободного формата или документы, являющиеся формами учета и отчетности.

3.4. Клиенту предоставляется право направлять в Банк подписанные ЭП сообщения свободного формата, формы учета и отчетности по валютным операциям, документы, полученные с использованием сканирующих устройств изображения документов (сканы), оформленные первоначально на бумажных носителях.

3.5. Предоставляемые Клиентом документы с применением электронных образов (сканированные изображения документов, оформленных первоначально на бумажных носителях) должны быть доступны для чтения без использования специальных устройств. Банк принимает к исполнению документы только при надлежащем качестве предоставляемых в Банк копий оригинальных документов (отражение без искажений всех элементов документа) и доступности для прочтения текста в предоставляемых документах с применением электронных образов, присоединенных к сообщениям свободного формата, а также к формам учета и отчетности, подписанных ЭП.

4. Порядок подключения к системе ДБО

4.1. Клиент обращается в Банк к сотруднику, ответственному за обслуживание клиентов (далее – Клиентский менеджер). Клиентский менеджер передает Клиенту для заполнения форму заявления о присоединении, по форме Приложения №1 к Договору оказания услуг дистанционного банковского обслуживания юридических лиц, проверяет правильность заполнения заявления, наличие подписи и печати (как в карточке образцов подписей Клиента), заполняет отметки Банка на заявлении.

Форма заявления о присоединении также размещена на сайте Банка и доступна для самостоятельного скачивания клиентами.

4.2. Клиентский менеджер передаёт USB-токен клиенту (представителю клиента) и подписывает с ним акт приема-передачи USB-токенов (Приложение №3 к договору). Один экземпляр акта отдается клиенту, другой помещается в досье клиента.

4.3. Заполненное заявление, в случае, если расчетный счет клиенту открыт, передается Клиентским менеджером сотруднику Отдела программирования и автоматизации банковских процессов (ОПиАБП) в бумажном виде.

В случае, если расчетный счет не открыт, то заполненное заявление передается Клиентским менеджером сотруднику ОПиАБП после его открытия.

На основании полученного заявления, сотрудник ОПиАБП, производит необходимую настройку системы ДБО.

4.4. Клиент самостоятельно (допускается консультирование сотрудником ОПиАБП) генерирует необходимый(е) криптографический(е) ключ(и), передает клиентскому менеджеру распечатанные сертификаты на бумажном носителе, подписанные уполномоченным лицом и заверенные печатью (при наличии). Клиентский менеджер проверяет наличие подписи и печати (как в карточке образцов подписей Клиента).

По предварительному согласованию с сотрудником ОПиАБП допускается передача сертификата в электронном виде[1].

После получения Банком сертификата на бумажном носителе или в виде электронного документа и открытия расчетного счета клиенту, сотрудник ОПиАБП сверяет предоставленные данные и регистрирует сертификат в системе ДБО с подключением Клиента к системе ДБО в режиме исполнения ЭД, или отказывает в регистрации, в случае несовпадения данных, после чего ставит соответствующую отметку в заявлении клиента, подписывает заявление и передает его вместе с сертификатом Клиентскому менеджеру. Клиентский менеджер помещает заявление и сертификат в досье клиента.

4.5. Клиент получает ответ из Банка от Клиентского менеджера по телефону (или другому виду связи) о том, что сертификат(ы) принят(ы) или не приняты.

---

[1] Порядок определяется регламентом обмена электронных документов.

4.6. В случае изменения реквизитов Клиент незамедлительно и в обязательном порядке оформляет в произвольной форме заявление и направляет его в Банк на бумажном носителе или с использованием системы ДБО в виде текстового файла, вложенного в ЭД.

4.7. В Системе ДБО возможно предоставление Клиенту услуги по разграничению права доступа, с предоставлением сотрудникам Клиента права доступа только в режиме «Просмотр», который позволяет получать информацию о состоянии его счета(ов), указанных в Заявлении, в том числе в виде выписки из лицевого счета, без права подачи распоряжений на совершение операций.

4.8. Изменение параметров подключения к системе ДБО.

4.8.1. При изменении параметров подключения к системе ДБО (подключение дополнительных счетов, отключении от системы ДБО счетов, перегенерации сертификатов ключей проверки ЭП на новых уполномоченных лиц, отзыв криптографических ключей\сертификатов ключей проверки ЭП, добавлении/отключении сервисов, изменении полномочий представителей) Клиент направляет в Банк на бумажном носителе (либо через систему ДБО) соответствующее Уведомление в произвольной форме.

4.8.2. При изменении полномочий представителей Клиента, определяемых доверенностью, Клиент одновременно с Уведомлением направляет в Банк новую доверенность. При этом Клиент одновременно с предоставлением новой доверенности может отменить ранее выданную доверенность.

4.8.3. В дату согласованного ввода в действие новых параметров подключения администраторы системы ДБО Банка и Клиента производят перенастройку Системы, в том числе (при необходимости) системы криптографической защиты информации.

4.8.4. При изменении полномочий сотрудников Клиента, имеющих право доступа только в режиме «Просмотр», Клиент должен направить в Банк уведомление, сформированную в виде документа свободного формата - текстовое сообщение, визируемое и шифруемое отправителем, подписанное ЭП.

5. Порядок электронного документооборота

5.1. Для передачи в Банк ЭД/приема из Банка ЭД Клиенту необходимо войти в свою учетную запись системы ДБО через сайт Банка.

5.2. Клиент производит подготовку ЭД, руководствуясь правилами, изложенными в соответствующей инструкции (размещена на сайте Банка), а также законодательством РФ и нормативными актами Банка России, и сохраняет подготовленные ЭД в базе данных Системы ДБО.

5.3. Если ЭД подписан необходимым количеством ЭП, документ отправляется в Банк на обработку.

5.4. Система ДБО автоматически отображает стадию обработки ЭД. Текущая стадия обработки ЭД в системе ДБО отражается статусом документа.

Документам могут быть присвоены следующие статусы:

- «Доставлен» - получение Банком электронного документа;
- «На обработке» - осуществление проверки документа ответственным сотрудником Банка;
- «Исполнен» - прием к исполнению документа со стороны Банка;
- «Отвергнут» - отказ в исполнении документа со стороны Банка, сопровождается комментариями о причинах возврата и срока для исправления;
- «Отозван» - документ отозван клиентом до обработки.

5.5. Система ДБО последовательно проводит автоматический контроль корректности ЭП и реквизитов каждого ЭД. ЭД, успешно прошедший проверку, принимается Банком в обработку. Время присвоения ЭД статуса «Доставлен» считается временем поступления документа в Банк. Присвоение ЭД статуса «Доставлен» не означает при-

нятия Банком обязательства исполнить ЭД, т.к. документ к этому времени еще не прошел все виды банковского контроля.

5.6. ЭД с некорректными ЭП и/или с ошибками реквизитов и/или неверно оформленные не принимаются Банком в обработку и получают согласно документации к текущей версии системы ДБО статус «Отвергнут». При этом у Клиента отображается сообщение с расшифровкой ошибок.

5.7. Поступившие ЭПД, прошедшие все виды контролей, исполняются в сроки, установленные Договором банковского счета, соглашениями и договорами, заключенными между Сторонами.

5.8. Статус «Исполнен» присваивается документу после приема к исполнению документа со стороны Банка.

5.9. Клиент самостоятельно контролирует (отслеживает) этапы и результаты обработки отправленных в Банк ЭД в соответствующих разделах Системы ДБО.

5.10. При необходимости отозвать документ, Клиент может направить в Банк запрос на отзыв документа, используя предназначенный для этого функционал системы ДБО. Отправленный в Банк запрос на отзыв может быть обработан автоматически (без участия сотрудника Банка). Отозваны могут быть только ЭПД, которые еще не проведены по счету Клиента или не включены Банком в реестр платежей, направленных в платежную систему Банка России. В случае невозможности исполнения, запрос на отзыв получит отрицательный статус. В случае, когда невозможно отозвать ЭД в автоматическом режиме, Клиент может обратиться в Банк для решения этого вопроса при помощи ЭД произвольного формата, в котором указывает ЭД, который требуется отозвать. После этого с целью сократить время реакции, обращается в Банк по телефону.

5.11. Банк формирует и передаёт Клиенту по системе ДБО следующие ЭД: выписки по счетам, обслуживаемым в системе ДБО, справочную и иную информацию, уведомления, извещения, в том числе направление которых в соответствии с действующим законодательством Российской Федерации является обязательным.

Информирование Клиента, предусмотренное настоящим пунктом, осуществляется Банком в сроки, установленные действующим законодательством Российской Федерации и договором банковского счета.

6. Порядок разрешения спорных ситуаций

6.1. Споры и разногласия, связанные с электронным документооборотом, решаются между Банком и Клиентом в процессе переговоров. При возникновении разногласий, возникающих при обмене ЭД с использованием Системы ДБО, обмен ЭД между Сторонами немедленно прекращается.

6.2. Порядок рассмотрения споров и разногласий между участниками Системы ДБО, связанных с авторством и/или подлинностью ЭД:

Несогласная Сторона (Сторона-заявитель) должна не позднее третьего рабочего дня после обнаружения причины, повлекшей несогласие, направить другой Стороне письменное заявление (претензию) в произвольной форме, в котором должны быть изложены причины несогласия.

Заявление (претензия) должно содержать информацию с указанием фамилий, имен, отчеств, должностей и контактной информации лиц Стороны-заявителя, уполномоченных в разрешении конфликтной ситуации, адрес электронной почты для получения уведомления о созыве Комиссии.

Не позднее 5 рабочих дней со дня получения Участником системы письменного заявления (претензии) Банк созывает Комиссию и направляет Участнику системы уведомление о дате и времени сбора Комиссии, ее составе, контактной информации (телефон, факс, электронная почта). Уведомление составляется и направляется по электронной почте, указанной в заявлении (претензии).

Состав Комиссии формируется минимум из двух представителей от каждой Стороны. Для участия в составе Комиссии в качестве независимой экспертной стороны

возможно привлечение представителя разработчика системы ДБО и/или используемого СКЗИ. Полномочия представителей Банка и Клиента на участие в работе Комиссии должны быть подтверждены соответствующими доверенностями.

Комиссия работает в помещении Банка и на его компьютерном оборудовании, конфигурация которого соответствует требованиям разработчика, используемого СКЗИ.

Комиссия организует экспертизу на основании архивных копий документов, предъявленных сторонами, и/или архивных файлов подтверждений отправки, подписанных ЭП Банка и/или Клиента.

Экспертиза осуществляется в три этапа:

1) подготовка оборудования и программного обеспечения, тестирование их работоспособности;

2) контроль целостности оспариваемого электронного документа путем проверки электронной подписи при помощи сертификата проверки ключа электронной подписи. При этом предварительно сверяется текст открытого ключа в сертификате ключа проверки ЭП и Запросе на выпуск сертификата проверки ключа ЭП, который Клиент предоставляет в Банк на бумажном носителе для выпуска сертификата.

3) аутентификация отправителя оспариваемого электронного документа путем проверки принадлежности, актуальности и целостности сертификата открытого ключа, использованного Комиссией для проверки электронной подписи.

6.3. Подтверждением подлинности оспариваемого электронного документа является единовременное наличие следующих условий:

1) проверка электронной подписи оспариваемого электронного документа с использованием сертификата ключа проверки ЭП, выпущенного для Клиента на основании Запроса на выпуск сертификата ключа проверки ЭП, дала положительный результат;

2) подтверждена принадлежность, актуальность сертификата проверки ключа ЭП Стороны - заявителя, с помощью которого проводится проверка электронной подписи оспариваемого электронного документа, при этом Банк предъявляет оригинал запроса на выпуск этого сертификата проверки ключа ЭП подписанный владельцем сертификата и печатью юридического лица(если имеется), текст открытого ключа которого совпадает с текстом открытого ключа в сертификате проверки ключа ЭП используемого для проверки ЭП для спорного ЭД.

6.4. Комиссия имеет право:

- получать доступ к необходимым для проведения ее работы документальным материалам, на бумажных и электронных носителях;

- получать объяснения от должностных лиц Сторон, обеспечивающих обмен электронными документами;

- получать от Сторон любую иную информацию, относящуюся, по ее мнению, к рассматриваемой конфликтной ситуации.

6.5. Результаты экспертизы в течение 3 рабочих дней оформляются в виде письменного заключения - Акта Комиссии, подписываемого всеми членами Комиссии. Акт составляется в двух экземплярах - по одному для каждой Стороны. Акт является окончательным и пересмотру не подлежит.

Акт, составленный Комиссией, является доказательством при дальнейшем разбирательстве спора в суде (арбитражном суде).

6.6. Если в ходе работы Комиссии один или несколько ее членов не согласны с результатами экспертизы, либо одна из Сторон не согласна с выводами Комиссии, дальнейшее разбирательство спора продолжается в порядке, установленном действующим законодательством.

7. Общие принципы обеспечения безопасности при работе по Системе ДБО

7.1. Клиент обязан:

- соблюдать положения настоящего Регламента;

- немедленно требовать аннулирования сертификат ключа проверки ЭП (далее по тексту СКПЭП) в случае компрометации ключей ЭП, а также в случае изменений сведений, указанных в СКПЭП, либо в случае прекращения действия документа, на основании которого он оформлен;

- использовать программное обеспечение, позволяющее производить информационный обмен между Участниками Системы только в рамках Системы;

- руководствоваться положениями и инструкциями эксплуатационной документации программного обеспечения;

- применять СКЗИ в соответствии с требованиями законодательства Российской Федерации и только в рамках Системы;

- хранить в тайне закрытый ключ ЭП и принимать меры для предотвращения его компрометации;

- при уничтожении утративших силу ключей ЭП, обеспечивать расшифровывание зашифрованных этими ключами электронных документов и хранение их в расшифрованном виде в соответствии с требованиями, установленными законодательством Российской Федерации и настоящим Регламентом. Перед уничтожением ключей ЭП необходимо расшифровать все ЭД, зашифрованные с их использованием, иначе в дальнейшем прочитать эти документы будет невозможно.

7.2. Доступ к ПК с установленной Системой ДБО и ее использование должны быть регламентированы внутренними документами Клиента, включая список узлов (ip-адресов, сайтов в интернете), доступных для данного ПК. Список узлов (ip-адресов, сайтов) должен содержать только список адресов Банка или государственных служб.

7.3. Клиент принимает на себя все риски, связанные с несоблюдением правил хранения секретных ключей (необходимо подключать носители ЭП к компьютеру только на время работы в системе ДБО хранить в надежном, недоступном для третьих лиц месте (например, сейф)).

Совмещение ключевых носителей разных клиентов может повлечь множественную компрометацию или утерю криптографических ключей.

Ответственность за безопасное хранение и использование ключа ЭП лежит на Владельце сертификата ключа проверки ЭП.

7.4. Для обеспечения безопасности при работе с Системой ДБО необходимо:

- Выделить отдельный компьютер (далее – ПК) для работы с Системой ДБО и определить должностное лицо, ответственное за обеспечение безопасности информации и эксплуатации СКЗИ.

- Не использовать на ПК нелицензионное программное обеспечение (операционную систему, иное программное обеспечение) (далее – ПО). Клиент предупрежден, что оно может заведомо содержать вредоносный код.

- Установить на ПК антивирусную программу с актуальными базами, регулярно обновляемую.

- При первом входе в систему, а также регулярно (один раз в месяц) менять пароли на систему ДБО

- Использовать секретные ключи (подключение внешнего носителя с ключом) только в момент работы с системой ДБО. Извлекать ключевой носитель из ПК в другое время. Не оставлять внешний носитель с ключом, постоянно подключенным к ПК.

- Не оставлять секретные Ключи без присмотра. Клиент предупрежден, что в противном случае он рискует скомпрометировать секретные ключи. Никогда и никому не сообщать логины \ пароли систем ДБО и тем более не доверять секретные ключи, включая родственников и сотрудников Банка.

- Обеспечить соответствие пароля доступа к ключу ЭП требованиям сложности (пароль должен быть не менее 6 символов, состоять из прописных и\или строчных латинских букв с цифрами и\или символами);

- Избегать использования системы ДБО на чужих компьютерах или в интернет-кафе, на подобных ПК высок риск скомпрометировать свои ключи \ логин \ пароль.

- **Контролировать действия IT-специалистов, особенно внештатных, в момент технического обслуживания, установки программного обеспечения на компьютер с установленной системой ДБО, не сообщать IT-специалистам пароли для проверки работы Системы – делать это самостоятельно.**

- Осуществлять постоянный контроль за отправляемыми платежными документами при работе с системой ДБО, а также за состоянием своего банковского счета не реже 3 раз в операционный день.

- Проверять информацию об IP-адресе, с которого осуществлялся предыдущий вход в Систему.

- Не использовать ПК с установленной системой ДБО для работы с электронной почтой. Клиент предупрежден, что электронные письма — это самый популярный способ распространения вредоносного ПО.

- Перед открытием внешнего подключаемого носителя – обязательно проверить его содержимое на вирусы.

7.5. КЛИЕНТ ДОЛЖЕН НЕЗАМЕДЛИТЕЛЬНО СООБЩИТЬ В БАНК любым доступным способом (по электронной почте, телефону) в случае, если:

- Сломался ПК, на котором установлена система ДБО;
- Заблокировался логин;
- Невозможно войти в систему ДБО;
- Потерян контроль над носителем с секретными ключами;
- Возникли подозрения в несанкционированном доступе к системе ДБО.

7.6. Примерный сценарий реагирования Банка на инциденты в системе ДБО. При получении информации об инциденте, предусмотренной п.7.5. Регламента, сотрудник Банка:

- Фиксирует полученную информацию от Клиента об инциденте;
- Временно блокирует работу Клиента в системе ДБО;
- Идентифицирует пострадавшего клиента, информирует непосредственное руководство о получении от Клиента информации об инциденте;
- Дает Клиенту инструкции о совершении необходимых действий, сохранению доказательств;
- Информирует (при необходимости) официальным письмом банк – получатель денежных средств о факте инцидента и необходимости отменить операцию (транзакцию);
- Направляет (при необходимости) информационное письмо о факте совершения мошенничества в полицию;
- Собирает журналы работы с системой ДБО Клиента;
- Осуществляет (при необходимости) выезд к Клиенту с целью сбора дополнительной информации об инциденте;
- Направляет (при необходимости) данные по инциденту в ФинЦЕРТ Банка России.

7.7. По письменному заявлению Клиента, при наличии соответствующей технической возможности у Банка, Банк аннулирует ЭД принятые к исполнению до получения информации о компрометации ключа ЭП.

7.8. Банк вправе блокировать работу Клиента в системе ДБО при возникновении подозрений в компрометации ключа ЭП. При этом Банк связывается с клиентом любыми доступными способами для прояснения ситуации.

РИСКИ, СВЯЗАННЫЕ С НЕСВОЕВРЕМЕННЫМ СООБЩЕНИЕМ В БАНК О СЛУЧАЯХ УТРАТЫ ИЛИ КОМПРОМЕТАЦИИ СЕКРЕТНЫХ КЛЮЧЕЙ ЭП, НЕСЕТ КЛИЕНТ.

8. Порядок уведомления о внесении изменений в настоящий Регламент

8.1 Изменения и дополнения в настоящий Регламент и Приложения к нему, а также сроки и порядок вступления в силу вносимых в настоящий Регламент изменений и дополнений публикуются на официальном сайте Банка в сети Интернет (http://www.iturupbank.ru/) и считаются доведенными до сведения Клиентов в течении трех дней со дня публикации.

Изменения и дополнения, вносимые в настоящий Регламент, становятся обязательными для Банка и Клиента с даты введения их в действие и размещения на официальном сайте Банка в сети Интернет (http://www.iturupbank.ru/).

8.2 Клиент имеет право запрашивать копии текстов настоящего Регламента и всех изменений и дополнений к нему на бумажном носителе. Указанные в настоящем пункте документы должны быть предоставлены Банком в течение 10 (Десяти) дней с даты получения письменного запроса от Клиента.

Приложение № 1 к Регламенту обмена электронными документами по телекоммуникационным каналам связи с использованием технологий дистанционного банковского обслуживания

Требования
к программно-техническим средствам Клиента
(приобретаются и настраиваются Клиентом за собственный счет):

Персональный компьютер: в конфигурации не ниже достаточной для нормального функционирования Операционной системы.

Операционная система не ниже: MSWindows7;

Интернет-браузер - MS Internet Explorer, Google Chrome, Firefox актуальных версий;

Доступный для использования в операционной системе USB порт;

Выход в сеть «Интернет» с возможностью перехода на адрес Банка: http://www.iturupbank.ru (https://biz.iturupbank.ru по порту 443).

Рекомендуемая, гарантированная, минимальная скорость соединения не ниже 256кбит/сек.