

Приложение № 2 к Условиям расчетно-кассового обслуживания юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в АО «Банк Русский Стандарт»

Условия дистанционного банковского обслуживания корпоративных клиентов

1. Настоящие Условия дистанционного банковского обслуживания корпоративных клиентов (далее – **Условия ДБО**) являются неотъемлемой частью Условий расчетно-кассового обслуживания юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в АО «Банк Русский Стандарт» (далее – **Условия**) и определяют отношения между Банком и Клиентом в рамках Договора, возникающие в связи с предоставлением Клиенту удаленного доступа к Системе «Интернет-Банк» и дистанционным обслуживанием Клиента.

2. ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе указанные ниже термины и определения, написанные с заглавной буквы, будут иметь следующие значения:

2.1. **Владелец ЭП** – уполномоченное лицо Клиента, которому в установленном действующим законодательством Российской Федерации и Договором порядке выдан Сертификат ключа проверки ЭП или Ключ eToken PASS;

2.2. **Дистанционное банковское обслуживание (ДБО)** – предоставление Банком Клиенту предусмотренных Условиями ДБО банковских и информационных услуг с использованием Системы «Интернет-Банк»;

2.3. **Документы валютного контроля** – паспорта сделок, справки о валютных операциях (корректирующие справки о валютных операциях), справки о подтверждающих документах (корректирующие справки о подтверждающих документах), ведомости банковского контроля, заявления о переоформлении паспортов сделок, заявления о закрытии паспортов сделок, документы, являющиеся основанием для проведения валютной операции, предусмотренные Инструкцией Банка России от 04.06.2012 № 138-И «О порядке представления резидентами и нерезидентами уполномоченным банкам документов и информации, связанных с проведением валютных операций, порядке оформления паспортов сделок, а также порядке учета уполномоченными банками валютных операций и контроля за их проведением» (далее – **Инструкция № 138-И**), в том числе документы валютного контроля, представляемые Клиентом в соответствии с п.4 ст.23 Федерального закона от 12.10.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»;

2.4. **Ключ проверки ЭП** – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП;

2.5. **Ключ ЭП** – уникальная последовательность символов, предназначенная для создания ЭП;

2.6. **Ключ eToken PASS** – автономное устройство, предназначенное для генерации Одноразовых паролей, используемых для дополнительной авторизации в Системе, а также подтверждения и отправки ЭД;

2.7. **Ключевая информация** – обобщенное понятие информации, содержащей Логин, Пароль, Одноразовый пароль, Ключи, Ключ eToken PASS, используемые для аутентификации ЭД;

2.8. **Ключи** – совокупность Ключа ЭП и соответствующего ему Ключа проверки ЭП;

2.9. **Компрометация ключевой информации** – ситуация, при которой Логин, Пароль, Ключи, Ключ eToken PASS, Одноразовый пароль стали доступны постороннему лицу независимо от того, нанесен или нет ущерб Банку и/или Клиенту. Под Компрометацией ключевой информации подразумеваются произошедшие события: утрата, утрата с последующим обнаружением, несанкционированное копирование или подозрение на копирование, любые другие ситуации, при которых достоверно неизвестно, что произошло с носителем Ключевой информации;

2.10. **Корпоративный удостоверяющий центр Банка** (далее – **Удостоверяющий центр**) – уполномоченное подразделение Банка, осуществляющее функции по созданию и выдаче Сертификатов ключей проверки ЭП, а также иные функции, предусмотренные действующим законодательством Российской Федерации;

2.11. **Логин** – уникальная последовательность алфавитно-цифровых символов, присваиваемая каждому уполномоченному лицу Клиента при регистрации в Системе;

2.12. **Неквалифицированная электронная подпись** – усиленная неквалифицированная электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием Ключа ЭП;
- позволяет определить лицо, подписавшее ЭД;
- позволяет обнаружить факт внесения изменений в ЭД после момента его подписания;
- создается с использованием Средств электронной подписи;

2.13. **Одноразовый пароль** – пароль, генерируемый Ключом eToken PASS для дополнительной авторизации в Системе и подписи ЭД, не является статичным и действует только на одноразовое подтверждение действий в Системе;

2.14. **Ответственный сотрудник Банка** – уполномоченный сотрудник Банка, который на основании распорядительного акта Банка уполномочен осуществлять от имени Банка предусмотренные Инструкцией №138-И действия по валютному контролю, в том числе подписывать ЭП Документы валютного контроля/уполномоченный сотрудник Банка, который уполномочен на основании распорядительного акта Банка на подписание ЭП иных ЭД (кроме Документов валютного контроля), в рамках настоящих Условий ДБО;

- 2.15. **Пароль** – последовательность алфавитно-цифровых символов, связанная в Системе с соответствующим Логинном;
- 2.16. **Простая электронная подпись** (далее – **Простая ЭП**) – электронная подпись, которая посредством использования Одноразового пароля подтверждает подпись уполномоченного лица Клиента;
- 2.17. **Сертификат ключа проверки ЭП/Сертификат** – документ на бумажном носителе или ЭД, выданные Удостоверяющим центром и подтверждающие принадлежность Ключа проверки ЭП Владельцу ЭП;
- 2.18. **Средства Удостоверяющего центра** – программные и (или) аппаратные средства, используемые для реализации функций Удостоверяющего центра;
- 2.19. **Средства электронной подписи** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание Ключа ЭП и Ключа проверки ЭП;
- 2.20. **Статус документа** – информация о текущем состоянии ЭД в Системе;
- 2.21. **Удаленное рабочее место Системы** (далее – **Рабочее место**) – составная часть Системы, используемая Клиентом для направления Банку и получения от Банка ЭД;
- 2.22. **Участники Системы** – Банк и Клиент, осуществляющие электронный документооборот посредством Системы в рамках заключенных между ними договоров;
- 2.23. **Электронная подпись** (ранее и далее – **ЭП**) – реквизит ЭД, информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Под ЭП в рамках настоящих Условий ДБО понимается Неквалифицированная электронная подпись и Простая ЭП;
- 2.24. **Электронный документ** (ранее и далее – **ЭД**) – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах; В настоящих Условиях ДБО термины и определения, обозначающие единственное число, включают в себя, как единственное, так множественное число.
- Иные термины и определения (не перечисленные в настоящем разделе Условий ДБО), используемые в настоящем документе и написанные с заглавной буквы, имеют то же значение, что и в Условиях.

3. ОБЩИЕ УСЛОВИЯ

- 3.1. Настоящие Условия ДБО регулируют отношения между Банком и Клиентом (далее при совместном упоминании Стороны, а по отдельности – Сторона) по предоставлению Банком услуг по Дистанционному банковскому обслуживанию Клиента с использованием Системы, в том числе порядок обмена ЭД, права, обязанности и ответственность Сторон.
- 3.2. Для целей обмена ЭД с использованием Системы Банк передает Клиенту на срок действия Договора право доступа к Системе и право использования Рабочего места для получения услуг по Дистанционному банковскому обслуживанию, а Клиент оплачивает Банку такие услуги в соответствии с Тарифами. Стоимость услуг третьих лиц, обеспечивающих подключение Клиента к сети Интернет и обслуживание его в сети Интернет, оплачивается Клиентом самостоятельно и не входит в стоимость услуг Банка.
- 3.3. Настоящим Банк и Клиент пришли к соглашению об использовании Системы для защищенного обмена между Сторонами следующими ЭД:
- 3.3.1. документами для осуществления расчетных и иных Операций по Счету Клиента, открытому в Банке, получения Клиентом информации в электронной форме о состоянии Счета, а также реестрами перечислений согласно договору об обслуживании организации по выплате заработной платы с использованием банковских карт, заключенному между Сторонами;
- 3.3.2. Документами валютного контроля (в случае если оригинал документов оформлен на бумажном носителе и содержит все необходимые для данного вида документа отметки, включая подписи уполномоченных лиц и печать Клиента (при наличии). Для представления Документа валютного контроля в Банк с использованием Системы оригинал документа должен быть преобразован в электронную копию посредством электронного сканирования. Электронные копии Документов валютного контроля представляются в Банк в виде вложенного файла в составе сообщения свободного формата;
- 3.3.3. иными документами, сообщениями и информацией, обмен которыми предусмотрен Договором, а также иными договорами и соглашениями, заключенными между Банком и Клиентом.
- 3.4. Каждый ЭД, направляемый с использованием Системы одной Стороной другой Стороне, должен быть подписан ЭП Владельца ЭП или ЭП Ответственного сотрудника Банка соответственно.
- 3.5. Стороны признают, что получение Банком ЭД с использованием Системы, подписанного ЭП Владельца ЭП, направленного от Клиента, юридически эквивалентно (равнозначно) получению соответствующего документа на бумажном носителе, подписанного от имени Клиента уполномоченным лицом Клиента и заверенного оттиском печати Клиента (при наличии) с учетом требований действующего законодательства Российской Федерации. При этом документы, указанные в п.п. 3.3.1, 3.3.2 Условий ДБО, должны быть подписаны ЭП Владельцев ЭП, имеющих право подписи расчетных документов Клиента, каждому из которых выдан Сертификат или Ключ eToken PASS в соответствии с Условиями ДБО и Договором в целом.
- 3.6. Стороны признают, что получение Клиентом ЭД с использованием Системы, подписанного ЭП Ответственного сотрудника Банка направленного от Банка, юридически эквивалентно (равнозначно) получению соответствующего документа на бумажном носителе, подписанного от имени Банка уполномоченным лицом Банка, и заверенного оттиском печати Банка с учетом требований действующего законодательства Российской Федерации.

- 3.7. Настоящим Стороны подтверждают и соглашаются с тем, что:
- 3.7.1. Сторона, получившая ЭД с использованием Системы, не несет ответственности за правильность содержания и/или оформления такого ЭД Стороной его направившей;
- 3.7.2. используемые Сторонами ЭП реализуют подлинность и авторство ЭД и являются достаточными для обеспечения безопасности, конфиденциальности, а также авторства и подлинности направляемых/принимаемых с использованием Системы ЭД. Проверка ЭП осуществляется в соответствии с порядком, изложенным в Приложении № 3 к Условиям ДБО.
- 3.8. В качестве уполномоченных лиц Сторон имеют право выступать лица, имеющие полномочия на подписание документов и сообщений, указанных в п. 3.3 Условий ДБО от имени соответствующей Стороны.
- 3.9. Исключительные права на программное обеспечение «Correpts», используемое Сторонами при эксплуатации Системы, принадлежат ООО «БСС» (ОГРН 1087746170181).

4. ОБЩИЕ УСЛОВИЯ И ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

- 4.1. ЭД передаются Клиентом в Банк с использованием Системы. При невозможности поступления в Банк ЭД с использованием Системы Клиент передает документы на бумажных носителях.
- 4.2. Банк осуществляет переводы на основании распоряжений в электронной форме при условии соответствия таких документов требованиям законодательства Российской Федерации, Договору, форматам, установленным Системой, а также при условии положительного результата проверки подлинности ЭП в ЭД.
- 4.3. В случае несоответствия ЭД требованиям законодательства Российской Федерации, Договора, положениям заключенных между Сторонами договоров, соглашений, а также в случае выявления угрозы несанкционированного доступа к программно-аппаратным средствам Клиента или его Счету, Банк отказывает в исполнении ЭД Клиента, уведомив Клиента посредством Системы о причинах отказа.
- 4.4. Порядок электронного документооборота установлен в Приложении № 3 к настоящим Условиям ДБО.
- 4.5. Стороны признают, что способы защиты и обеспечения целостности информации, средства аутентификации и авторизации, применяемые Системой при передаче ЭД, достаточны для подтверждения авторства, целостности и подлинности документов, и обязуются выполнять режим обеспечения безопасности, установленный «Инструкцией по обеспечению безопасности» (Приложение № 4 к Условиям ДБО).
- 4.6. Стороны также признают, что:
- 4.6.1. при любом изменении ЭД, совершенном после его подписания ЭП одной из Сторон, ЭП становится некорректной;
- 4.6.2. знание информации, которая передается между Сторонами по каналу связи Системы, не приводит к компрометации Ключевой информации;
- 4.6.3. подделка ЭП Участника Системы, т.е. создание корректной ЭП, невозможна без знания Ключа ЭП или Одноразового пароля;
- 4.6.4. созданный в единственном экземпляре в рамках Условий ДБО Ключ ЭП Клиента уникален, создание дубликата Ключа ЭП возможно только Клиентом или иными лицами при нарушении Клиентом условий хранения и/или использования Ключа ЭП, предусмотренных Условиями ДБО;
- 4.6.5. переданный Клиенту в соответствии с Условиями ДБО Ключ eToken PASS уникален;
- 4.6.6. каждый Участник Системы несет ответственность за сохранение в тайне своих Логина, Пароля, Ключей, Ключа eToken PASS, Одноразовых паролей, за правильность заполнения и оформления ЭД и за действия своего персонала при работе с Системой;
- 4.6.7. Правильность оформления и заполнения полей ЭД Клиента проверяется ответственным должностным лицом Клиента. Ответственность за передачу ошибочного ЭД Клиента несет Клиент.
- 4.7. Если иное в отношении документов на бумажном носителе, выдаваемых Банком Клиенту, не предусмотрено действующим законодательством Российской Федерации и нормативными актами Банка России, ЭД, переданные Клиенту в соответствии с Условиями ДБО, не представляются впоследствии Банком Клиенту на бумажном носителе.
- 4.8. По заявлению Клиента Банк предоставляет дубликат выписки по Счету на бумажном носителе. Данная услуга оплачивается Клиентом в соответствии с Тарифами, действующими на момент оказания соответствующей услуги.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

- 5.1. При эксплуатации Системы Стороны обязаны:
- руководствоваться Положением Банка России «О правилах осуществления перевода денежных средств» от 19.06.2012 №383-П, Федеральным законом «О национальной платежной системе» от 27.06.2011 №161-ФЗ, Федеральным законом «Об электронной подписи» от 06.04.2011 №63-ФЗ, Инструкцией № 138-И, Договором, иными договорами и соглашениями, заключенными между Банком и Клиентом, а также иными нормативно-правовыми актами, действующими в Российской Федерации;
 - за свой счет поддерживать в рабочем состоянии свои технические средства и оборудование, используемые для функционирования Системы, требования к которым указаны в Приложении № 1 к Условиям ДБО;
 - сохранять конфиденциальность информации относительно применяемых в Системе систем ограничения доступа к коммуникационному оборудованию Банка, обеспечения конфиденциальности, подлинности и авторства информации;
 - своевременно и добросовестно выполнять условия Договора.
- 5.2. Права и обязанности Клиента.
- 5.2.1. Клиент вправе:
- 5.2.1.1. Осуществлять с использованием Системы:

- расчетные Операции по Счету;
- прием/передачу ЭД, указанных в п. 3.3 Условий ДБО;
- 5.2.1.2. Получать с помощью Системы выписки о движении денежных средств по Счету;
- 5.2.1.3. Обращаться к сотрудникам технической поддержки Банка за получением консультаций, связанных с эксплуатацией Системы, в течение срока действия Договора;
- 5.2.1.4. В течение срока действия Договора в любое время прекратить передачу ЭД путем направления в Банк соответствующего уведомления. Уведомление должно быть предоставлено в письменной форме, подписано уполномоченным лицом Клиента и заверено печатью Клиента (при наличии);
- 5.2.1.5. Инициировать замену Ключей, Ключа eToken PASS в любой момент до истечения срока их действия.
- 5.2.2. Клиент обязан:
 - 5.2.2.1. Самостоятельно контролировать исполнение расчетных ЭД, отправленных в Банк с использованием Системы, посредством контроля изменений Статуса документа;
 - 5.2.2.2. За свой счет поддерживать в рабочем состоянии принадлежащие Клиенту аппаратные и программные средства, в том числе средства антивирусной защиты, используемые для функционирования Системы, а также обеспечить своевременное их обновление;
 - 5.2.2.3. Соблюдать инструкцию по обеспечению безопасности при использовании Системы (Приложение №4 к Условиям ДБО);
 - 5.2.2.4. Обеспечить хранение материального носителя, содержащего Ключ ЭП или Ключ eToken PASS в месте, исключающем доступ неуполномоченных лиц и/или повреждение материального носителя;
 - 5.2.2.5. Хранить Ключ ЭП на сменном носителе (flash-карта, диск) в месте, исключающем несанкционированный доступ к данному носителю;
 - 5.2.2.6. Исключить хранение Ключа ЭП на жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах;
 - 5.2.2.7. Исключить передачу Логина, Пароля, Ключа eToken PASS, Одноразовых паролей, Ключей и их копий третьим лицам, а так же их передачу по телефону, электронной почте или иным способом;
 - 5.2.2.8. При подозрении несанкционированного доступа третьих лиц к Счету, программно-аппаратным средствам Клиента, Ключу eToken PASS, а также копирования или подозрения в копировании Ключей третьими лицами или иной ситуации, которая приводит к Компрометации ключевой информации, с целью предотвращения финансовых потерь, незамедлительно любым доступным способом проинформировать об этом Банк (продублировав сообщение по электронной почте) и инициировать процедуру смены потенциально скомпрометированной ключевой информации. По требованию Банка в случае подозрения у Банка в Компрометации ключевой информации осуществить смену Ключей в срок 14 (четырнадцать) календарных дней с момента получения соответствующего уведомления от Банка;
 - 5.2.2.9. По требованию Банка в течение 2 (двух) рабочих дней представить оригиналы документов, являющихся основанием для проведения валютной операции, либо копии указанных документов, заверенные лицом, имеющим право подписи расчетных документов, и печатью Клиента (при ее наличии);
 - 5.2.2.10. В случае прекращения действия Договора произвести удаление с аппаратных средств программного обеспечения и пользовательской документации, используемых при эксплуатации Системы.
- 5.2.3. Клиент гарантирует Банку, что все проводимые им Операции по Счету с использованием Системы носят легитимный характер, не нарушают действующего законодательства Российской Федерации, и не связаны с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.
- 5.3. Права и обязанности Банка.
 - 5.3.1. Банк вправе:
 - 5.3.1.1. Приостановить совершение Клиентом Операций по Счету с использованием Системы в случаях и в порядке, установленных Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
 - 5.3.1.2. В случаях, предусмотренных действующим законодательством Российской Федерации, запрашивать у Клиента документы и сведения о проводимых/проведенных Операциях по Счету Клиента, осуществленных с использованием Системы. При этом обязательный срок для представления документов по запросам Банка составляет 3 (три) рабочих дня со дня получения Клиентом запроса Банка;
 - 5.3.1.3. Использовать инструменты контроля переводов Клиента на предмет компрометации Ключей, Ключа eToken PASS Клиента по своему усмотрению;
 - 5.3.1.4. При обнаружении Банком признаков (фактов) нарушения требований безопасности, установленных Условиями ДБО, немедленно приостановить прием ЭД Клиента, после чего любым доступным способом известить об этом Клиента;
 - 5.3.1.5. В случае подозрения Компрометации ключевой информации по своему усмотрению заблокировать Ключи ЭП, Ключ eToken PASS Клиента и требовать от Клиента смены Ключей, Пароля, Ключа eToken PASS;
 - 5.3.1.6. Направлять Клиенту с использованием Системы рекламные материалы и информационные сообщения об услугах и продуктах Банка.
 - 5.3.2. Банк обязан (при наличии технической возможности у Клиента):
 - 5.3.2.1. Предоставлять Клиенту услуги с использованием Системы согласно Условиям ДБО;

- 5.3.2.2. Произвести подключение и предоставление права доступа Клиента к Системе для совершения Операций и обмена документами в рамках Договора и иных договоров, заключенных между Банком и Клиентом, в соответствии с порядком, установленным в Приложении № 3 к Условиям ДБО. Факт предоставления права доступа Клиента к Системе оформляется Актом о предоставлении права доступа и введении в действие Системы «Интернет-Банк» (Приложение № 6 к Условиям ДБО), с момента подписания которого Клиент вправе осуществлять Операции и обмен документами с использованием Системы;
- 5.3.2.3. Предоставлять Клиенту необходимые рекомендации и методическую помощь в работе с Системой;
- 5.3.2.4. По требованию Клиента блокировать в Системе Пароль, активные Ключи проверки ЭП Клиента, активные Ключи eToken PASS, регистрировать новые Ключи, выдать новый Ключ eToken PASS, временно блокировать работу Клиента в Системе.

6. ОТВЕТСТВЕННОСТЬ СТОРОН, РИСКИ

- 6.1. Стороны обязуются обеспечивать конфиденциальность сведений о технологии Системы и программного обеспечения Системы.
- 6.2. Клиент несет ответственность за все Операции, проводимые Клиентом при использовании Системы.
- 6.3. Банк не несёт ответственности за ущерб, возникший вследствие:
 - 6.3.1. некорректного оформления Клиентом ЭД;
 - 6.3.2. ошибочно переданных ЭД Клиентом в Банк;
 - 6.3.3. несанкционированного доступа посторонних лиц к программно-аппаратным средствам, Паролю, Одноразовому паролю, Ключу ЭП, Ключу eToken PASS и другой Ключевой информации, используемых Клиентом для осуществления обмена ЭД;
 - 6.3.4. воздействия вредоносного программного обеспечения на программно-аппаратные средства, используемые Клиентом для осуществления обмена ЭД;
 - 6.3.5. срывов и помех на линии связи, используемой Клиентом при работе с Системой.
- 6.4. В случае несоблюдения требований Договора, ответственность за негативные последствия несет Сторона, допустившая эти нарушения, в размере прямого ущерба, за исключением случаев прямо предусмотренных Условиями ДБО.
- 6.5. Банк не несет ответственности за убытки, возникшие в результате неознакомления или несвоевременного ознакомления Клиентом со Статусами документа в Системе в порядке и сроки, установленные настоящими Условиями ДБО, а также за несоблюдение Клиентом мер по обеспечению защиты от несанкционированного доступа к информации.
- 6.6. Урегулирование споров и конфликтов между Сторонами, возникших в отношении получения/обмена/исполнения ЭД осуществляется в порядке, предусмотренном Приложением № 9.
- 6.7. По всем вопросам, не урегулированным Условиями ДБО, Стороны руководствуются законодательством Российской Федерации и Договором.
- 6.8. Составной и неотъемлемой частью Условий ДБО являются:
 - 6.8.1. Приложение № 1 - Требования к техническим средствам и оборудованию Клиента;
 - 6.8.2. Приложение № 2 - Порядок работы с Ключами, Сертификатом ключа проверки ЭП, Ключом eToken PASS;
 - 6.8.3. Приложение № 3 - Порядок подключения и использования Системы «Интернет-банк»;
 - 6.8.4. Приложение № 4 - Инструкция по обеспечению безопасности;
 - 6.8.5. Приложение № 5 - Образец Сертификата ключа проверки ЭП;
 - 6.8.6. Приложение № 6 - Акт о предоставлении права доступа и введении в действие Системы «Интернет-Банк» (форма);
 - 6.8.7. Приложение № 7 - Заявление на регистрацию Ключа eToken PASS для использования в Системе (форма);
 - 6.8.8. Приложение № 8 - Письмо о смене Логина и Пароля (форма);
 - 6.8.9. Приложение № 9 - Порядок урегулирования споров.

ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ СРЕДСТВАМ И ОБОРУДОВАНИЮ КЛИЕНТА

1. Для установки Системы необходимо обеспечить минимальные требования, предъявляемые к программно-аппаратному обеспечению Клиента для установки и работы Системы (клиентская часть):

Локальный персональный компьютер следующей конфигурации:

- цветной дисплей и видео-адаптер с минимальной разрешающей способностью 1024x600 точек на дюйм;
- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или выше;
- оперативная память 1 ГБ (для 32-разрядного процессора) или 2 ГБ (для 64-разрядного процессора);
- 16 ГБ (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) свободного места на жестком диске;
- графическое устройство DirectX 9 с драйвером WDDM 1.0 или более поздней версии;
- операционная система не позднее чем Windows 7 x86/x64;
- наличие браузера Internet Explorer версии 8 и выше, или Mozilla FireFox, Google Chrome, Opera;
- доступ к сети Интернет;
- средства антивирусной защиты.

Оснащение Клиента вышеуказанными и иными требующимися программами и техническими средствами осуществляется силами Клиента и за счет его средств.

2. Все перечисленное в п. 1. настоящего Приложения к Условиям ДБО оборудование Клиента должно иметь соответствующую техническую документацию.

ПОРЯДОК РАБОТЫ С КЛЮЧАМИ, СЕРТИФИКАТОМ КЛЮЧА ПРОВЕРКИ ЭП, КЛЮЧОМ eToken PASS

1. Порядок работы с Ключами и Сертификатом ключа проверки ЭП

- 1.1. Банк предоставляет уполномоченному лицу Клиента доступ в Систему исключительно для генерации Ключа ЭП, а также документацию на Средства электронной подписи. Все работы со Средствами электронной подписи Стороны проводят в соответствии с документацией, содержащей описание процедур генерации Ключей, создания и контроля правильности Ключей и других предусмотренных Системой операций.
- 1.2. Клиент самостоятельно производит генерацию своей пары Ключей: Ключа ЭП и Ключа проверки ЭП. Запрос на Сертификат ключа проверки ЭП в электронном виде передается в Банк посредством Системы.
- 1.3. Банк, получив запрос на Сертификат ключа проверки ЭП от Клиента (в электронном виде), проводит сертификацию (регистрацию) Ключа проверки ЭП Клиента в Удостоверяющем центре.
- 1.4. После проведения сертификации (регистрации) Ключа проверки ЭП Клиенту направляется Сертификат ключа проверки ЭП в двух экземплярах на бумажном носителе, оформленный в соответствии с Приложением № 5 к Условиям ДБО.
- 1.5. Клиент, получив от Банка свой Сертификат ключа проверки ЭП, должен убедиться, что Ключ проверки ЭП в Сертификате ключа проверки ЭП и в запросе на Сертификат ключа проверки ЭП совпадают.
- 1.6. Подписанные уполномоченным лицом и заверенные оттиском печати Клиента (при наличии) оригиналы Сертификата ключа проверки ЭП на бумажном носителе передаются в Банк (по почте либо курьером).
- 1.7. Экземпляр Сертификата ключа проверки ЭП, подписанный уполномоченным лицом и заверенный оттиском печати Удостоверяющего центра Банка, передается Клиенту (по почте либо курьером).
- 1.8. Ввод в действие Ключей производится с даты подписания Банком и Клиентом Акта о предоставлении права доступа и введении в действие Системы «Интернет-Банк» в соответствии с Приложением № 6 к Условиям ДБО.

2. Порядок хранения, использования Ключевой информации и смена Ключей

- 2.1. Режим хранения и использования Ключевой информации должен исключать возможность доступа к ней кого-либо, кроме уполномоченных лиц Сторон.
- 2.2. Сторона, допустившая возможность Компрометации ключевой информации, обязана немедленно сообщить об этом другой Стороне в порядке и в сроки, указанные в Условиях ДБО. Скомпрометированные Ключи не подлежат дальнейшему использованию и Стороны производят экстренную смену Ключей.
- 2.3. Экстренная, внеочередная и плановая смена Ключей производится Сторонами со следующей периодичностью:
 - 2.3.1. плановая смена Ключей производится один раз в два года;
 - 2.3.2. экстренная смена Ключей Банка – при Компрометации ключевой информации Банка по решению Банка;
 - 2.3.3. экстренная смена Ключей Клиента – при Компрометации ключевой информации Клиента;
 - 2.3.4. внеочередная смена Ключей Банка – по желанию Банка;
 - 2.3.5. внеочередная смена Ключей Клиента – по желанию Клиента.
- 2.4. В случае смены уполномоченных лиц Клиента Клиенту необходимо произвести смену Паролей, Ключей, к которым такие уполномоченные лица имели доступ.

3. Порядок работы с Ключами eToken PASS

- 3.1. Использование Клиентом Ключа eToken PASS в Системе осуществляется на основании заявления, составленного по форме Приложения № 7 к Условиям ДБО.
- 3.2. Ключ eToken PASS вводится в эксплуатацию с даты подписания Банком и Клиентом Акта о предоставлении права доступа и введении в действие Системы «Интернет-Банк» в соответствии с Приложения № 6 к Условиям ДБО.
- 3.3. Авторизация Клиента в Системе происходит по Логину и Паролю, дополнительная авторизация осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS.
- 3.4. Подпись ЭД в Системе осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS.
- 3.5. Отправка ЭД в Банк осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS.

4. Порядок хранения и использования Ключей eToken PASS

- 4.1. Режим хранения и использования Ключа eToken PASS должен исключать возможность доступа к Ключу eToken PASS кого-либо, кроме уполномоченных лиц Клиента.
- 4.2. В случае Компрометации ключевой информации Клиент обязан немедленно сообщить об этом в Банк в порядке и в сроки, указанные в Условиях ДБО.
- 4.3. В случае потери/выхода из строя Ключа eToken PASS Клиент обязуется оплатить за свой счет услуги Банка по возобновлению Дистанционного банковского обслуживания Клиента с использованием Ключа eToken PASS в соответствии с Тарифами.

4.4. В случае смены уполномоченных лиц Клиента Клиенту необходимо направить в Банк заявление на регистрацию Ключа eToken PASS для использования в Системе на новых уполномоченных Клиентом лиц по форме Приложения № 7 к Условиям ДБО.

ПОРЯДОК ПОДКЛЮЧЕНИЯ И ИСПОЛЬЗОВАНИЯ СИСТЕМЫ «ИНТЕРНЕТ-БАНК»

1. Подключение к Системе

- 1.1. Клиент обеспечивает наличие Рабочего места, отвечающего требованиям, изложенным в Приложении № 1 к Условиям ДБО.
- 1.2. Банк производит необходимые настройки Системы. Действие указанных настроек будет распространяться на все операции Клиента в Системе, если Клиент дополнительно не представит в Банк заявление на ограничение указанных настроек в Системе.
- 1.3. Подключение к Системе производится Клиентом самостоятельно, с использованием инструкций по установке и настройке Системы, предоставленных ему Банком.
- 1.4. В течение 3 (трех) рабочих дней с даты заключения Договора Банк:
 - 1.4.1. формирует для Клиента уникальное сочетание Логина и Пароля, зарегистрированное в Системе на имя уполномоченного лица Клиента, обеспечивающее доступ этого лица в Систему в сочетании с Ключом ЭП либо Ключом eToken PASS;
 - 1.4.2. передает Ключ eToken PASS на основании заявления Клиента (Приложение № 7 к Условиям ДБО) либо передает документацию, содержащую описание процедур формирования Ключа ЭП, либо передает и Ключ eToken PASS на основании заявления Клиента (Приложение № 7 к Условиям ДБО) и документацию, содержащую описание процедур формирования Ключа ЭП, в зависимости от выбранного режима работы в соответствии с п. 1.5. настоящего Приложения.
- 1.5. В Системе возможны следующие режимы работы:
 - 1.5.1. вход в Систему осуществляется по Логину и Паролю и обязательной авторизацией с помощью Ключа ЭП, подпись и отправка ЭД осуществляется с помощью Ключа ЭП;
 - 1.5.2. вход в Систему осуществляется по Логину и Паролю и обязательной авторизацией с помощью Ключа ЭП, подпись ЭД осуществляется с помощью Ключа ЭП, отправка ЭД в Банк осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS;
 - 1.5.3. вход в Систему осуществляется по Логину и Паролю и обязательной авторизацией путем ввода Одноразового пароля, сформированного Ключом eToken PASS, подпись и отправка ЭД осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS.
 - 1.5.4. вход в Систему осуществляется по Логину и Паролю и обязательной авторизацией с помощью Ключа ЭП без права подписи ЭД.
- 1.6. В случае намерения ограничить режим работы отдельных уполномоченных лиц Клиента возможностью подписания ЭД Клиент письменно информирует об этом Банк.
- 1.7. При необходимости Клиент вправе направить в Банк уведомление в произвольной форме с указанием списка IP-адресов, с которых Клиенту будет разрешен доступ в Систему, тем самым ограничивая доступ в Систему с других IP-адресов.
- 1.8. В случае прекращения действия Договора доступ Клиента к Системе аннулируется.

2. Электронный документооборот

- 2.1. Все документы в Системе «Интернет-Банк» представлены в электронном виде.
- 2.2. Ввод, обработка, прием и передача ЭД по Системе производится на специально оборудованных Рабочих местах Клиента и Банка.
- 2.3. Электронный документооборот между Клиентом и Банком осуществляется по открытым каналам передачи данных, в том числе с использованием сети Интернет.
- 2.4. Электронный документооборот осуществляется ежедневно 24 часа в сутки. Банк обязуется обеспечить функционирование своих технических средств и оборудования Системы в режиме ожидания взаимодействия с Клиентом.
- 2.5. Любые ЭД Клиента должны быть подписаны от имени Клиента Владелец ЭП. Для ЭД Клиента в Системе предусмотрены следующие операции:
 - а) формирование и подписание;
 - б) отправка Банку с подтверждением получения;
 - в) возможность отзыва;
 - г) учет и хранение.
- 2.6. Исполнение расчетных ЭД, поступивших и принятых к исполнению Банком, осуществляется в тот же день, если ЭД поступил в Банк:
 - до 16-00 часов МСК (в пятницу до 15-00) – при осуществлении переводов в рублях и долларах США;
 - до 13-00 МСК – при осуществлении переводов в Евро и других иностранных валютах.Исполнение расчетных ЭД, поступивших и принятых Банком позже указанного времени осуществляется Банком не позднее следующего рабочего дня.
- 2.7. Датой получения Банком Документа валютного контроля считается текущий рабочий день (круглосуточно), в случае поступления Документа валютного контроля в выходной день – следующий рабочий день.

Датой принятия Документов валютного контроля Банком в целях исполнения валютного законодательства РФ является дата присвоения в Системе Статуса документа «Принят ВК».

Датой отказа в приеме Документов валютного контроля Банком является дата присвоения в Системе Статуса документа «Отказан ВК».

2.8. Информация о факте принятия на обслуживание/оформления/переоформления/закрытия паспорта сделки; отказа в принятии на обслуживание/оформлении/переоформлении/закрытии паспорта сделки, принятия/возврата справки о валютной операции/справки о подтверждающих документах доводится до Клиента путем изменения Статуса документа соответствующего ЭД в Системе. Порядок заполнения Документов валютного контроля уставлен Инструкцией 138-И.

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

2.10. Клиент обязан удостовериться в получении Банком отправленных Клиентом ЭД:

- ЭД считается принятым Банком в случае изменения Статуса документа на «Принят», «Принят в обработку» по результатам автоматизированной проверки полученных Банком от Клиента ЭД;
- ЭД считается не принятым Банком в случае изменения Статуса документа на «Ошибка реквизитов», «Отвергнут банком», «Отказан АБС», «ЭП/АСП не верна» по результатам автоматизированной проверки полученных Банком от Клиента ЭД.

2.11. Банк не несет ответственность за неисправность каналов связи, используемых для взаимодействия Банка с Клиентом по Системе. Тем не менее, Банк обязуется принимать все возможные меры для устранения неисправности линий связи в кратчайшие сроки с момента их возникновения.

2.12. Все ЭД, подлежащие отправке от одной Стороны другой Стороне, перед установлением очередного сеанса связи между Клиентом и Банком подписываются ЭП Стороны, направляющей ЭД. Во время сеанса связи подготовленные ЭД по Системе передаются другой Стороне.

2.13. Все ЭД Банка формируются в соответствующем формате и подписываются ЭП Ответственного сотрудника Банка.

2.14. ЭД Банка загружаются Банком в Систему и могут быть получены Клиентом только в процессе соединения Клиента с Банком с использованием Системы. Надлежащей отправкой Клиенту ЭД Банка считается загрузка ЭД Банка в Систему, а датой отправки – дата загрузки.

2.15. В Системе предусмотрена операция присвоения Банком ЭД Клиента статуса приема/исполнения/отказа в исполнении, при этом при присвоении или изменении Статуса документа Система извещает Клиента о новом Статусе документа, информируя таким образом о состоянии ЭД.

2.16. Стороны признают, что срок действия Сертификата составляет 2 (два) года с даты его выдачи. Продление срока действия Сертификата осуществляется путем выдачи нового Сертификата с обязательной сменой Ключей. Выдача нового Сертификата производится по инициативе Клиента.

2.17. Стороны признают, что срок действия Ключа eToken PASS ограничен сроком работы элемента питания Ключа eToken PASS. По окончании срока действия Ключа eToken PASS Дистанционное банковское обслуживание Клиента приостанавливается. Возобновление Банком Дистанционного банковского обслуживания Клиента с использованием Ключа eToken PASS осуществляется за счет Клиента в соответствии с Тарифами.

2.18. Исполнение Сторонами обязательств по Условиям ДБО приостанавливается с момента окончания срока действия Сертификата/Ключа eToken PASS и до момента оформления Клиенту нового Сертификата/нового Ключа eToken PASS. В течение этого срока Стороны не вправе проводить в Системе какие-либо операции, а Банк прекращает прием ЭД.

2.19. Стороны определили, что в течение срока действия Договора допускается временное приостановление Банком работы Системы по техническим причинам, но не более чем на 3 (три) часа в сутки.

3. Формирование, подписание, отправка и отзыв ЭД

3.1. Порядок формирования, заполнения, подписания и представления в Банк ЭД Клиента должен, помимо требований установленных в Условиях ДБО, отвечать требованиям и условиям Договора, а также того договора, во исполнение которого ЭД Клиента представляется в Банк.

3.2. Переданные в Банк ЭД Клиента, в том числе составленные в свободном формате, не требуют представления Клиентом в Банк их версий на бумажном носителе.

3.3. Порядок заполнения встроенных бланков при формировании ЭД Клиента предусматривает контроль Системы за наличием и корректностью информации в полях соответствующей формы, при этом обязательному контролю подлежат те реквизиты, при отсутствии которых исполнение Банком ЭД Клиента является невозможным. При наличии в Системе встроенного бланка для определенного вида ЭД формирование этого вида ЭД в свободном формате не допускается. Встроенный бланк может не содержать визуального отображения всех реквизитов, заявлений, инструкций и информации, предусмотренных стандартным бланком, использование которого предписано соответствующим договором для оформления аналогичного документа на бумажном носителе. При этом, передача в Банк ЭД Клиента, оформленного путем заполнения встроенного бланка, безусловно означает, что все дополнительные реквизиты, заявления, инструкции и информация, содержащиеся в тексте документа, выданы Клиентом Банку надлежащим образом.

3.4. Отзыв ЭД Клиента производится с использованием ЭД «Запрос на отзыв документа», специально предусмотренного в Системе для этих целей. Отправка в Банк отзыва ЭД Клиента, оформленного в свободном формате, не гарантирует своевременного прекращения Банком процедуры исполнения соответствующего ЭД Клиента. Если отзыв ЭД от Клиента получен Банком после того, как Банк исполнил содержащееся в нем поручение по

распоряжению денежными средствами, Банк не несет ответственности за своевременно исполненное поручение Клиента, которое содержалось в полученном Банком ЭД.

3.5. При отсутствии в Системе встроенного бланка для ЭД какого-либо вида, ЭД формируется в свободном формате, а именно: а) в виде письма; б) в виде письма с прикрепленным файлом.

3.6. В случае если договором с Банком предусмотрено использование бланка, Клиент в обязательном порядке формирует ЭД в виде письма с прикрепленным файлом, при этом содержанием файла должен являться бланк, заполненный Клиентом в соответствии с требованиями соответствующего договора. Во всех остальных случаях вид ЭД свободного формата – просто письмо или просто с прикрепленным файлом – выбирается Клиентом по собственному усмотрению, если иное не предусмотрено соответствующим договором.

3.7. Сформированные ЭД Клиента подписываются уполномоченными лицами Клиента с использованием Ключей ЭП или Одноразового пароля Ключа eToken PASS.

3.8. Факт доставки в Банк ЭД Клиента подтверждается статусом «Доставлен», который присваивается ЭД Системой при одновременном соблюдении следующих условий:

- ЭД подписан действующими ЭП уполномоченных лиц Клиента;
- ЭД передан Банку с использованием Системы.

3.9. Факт приема Банком ЭД Клиента подтверждается статусом «Принят», «Принят в обработку», который присваивается ему Системой, если перечисленные ниже проверки дают положительный результат:

- проверка ЭП Клиента;
- проверка наличия информации и корректности ее значений в полях ЭД, обязательных к заполнению.

В случае если хотя бы одно из перечисленных в предыдущем пункте условий не выполнено, присвоение Системой ЭД статуса «Принят» не производится, о чем Клиент автоматически извещается Системой.

4. Проверка ЭП

4.1. Проверка ЭП в ЭД, передаваемых Сторонами друг другу в Системе, осуществляется в соответствии с процедурой, описанной в документации на Систему.

4.2. Исходными данными для процедуры проверки ЭП являются:

- ЭД, переданный одной из Сторон в формате Системы и подписанный ее ЭП;
- Сертификат ключа проверки ЭП или Ключ eToken PASS Стороны, подписавшей ЭД.

4.3. Электронная подпись в ЭД, передаваемых Сторонами в Системе, признается действительной при одновременном соблюдении следующих условий:

- Сертификат ключа проверки ЭП выпущен Удостоверяющим центром;
- Сертификат ключа проверки ЭП действителен на момент подписания ЭД;
- положительный результат проверки принадлежности Сертификата ЭП Участнику Системы;
- положительный результат проверки Одноразового кода, сформированного Ключа eToken PASS Уполномоченного лица Клиента;
- подтверждено отсутствие изменений, внесенных в ЭД после его подписания.

4.4. Проверка ЭП осуществляется Средством электронной подписи «Крипто-Ком», используемым в соответствии с Условиями ДБО.

4.5. Сертификат ключа проверки ЭП, используемый при проверке ЭП, должен соответствовать форме Сертификата по форме, установленной Приложением № 5 Условий ДБО.

5. Смена Пароля и Логина

5.1. Смена Пароля и/или Логина уполномоченного лица Клиента в случаях, установленных Условиями ДБО, осуществляется на основании письма о смене Логина и Пароля, составленного Клиентом по форме Приложения № 8 к Условиям ДБО и переданного в Банк.

6. Хранение ЭД

6.1. Стороны осуществляют хранение всех входящих и исходящих ЭД в Системе.

6.2. Клиент обязуется хранить не менее 5 (пяти) лет Ключи, Ключ eToken PASS используемые в рамках Условий ДБО. Сроки хранения ЭД должны соответствовать срокам хранения, установленным для документов на бумажных носителях. Архивы подлежат защите от несанкционированного доступа, непреднамеренного или преднамеренного уничтожения и/или искажения.

6.3. Банк формирует и хранит не менее 5 (пяти) лет (а в случае возникновения споров – до их разрешения) архивы:

- 6.3.1. всех входящих ЭД в принятом виде с ЭП;
- 6.3.2. всех исходящих ЭД в исходном виде с ЭП;
- 6.3.3. извещений (в электронном виде с ЭП) о приеме ЭД;
- 6.3.4. сообщений свободного формата, подписанных ЭП;
- 6.3.5. электронных протоколов сеансов обмена информацией.

6.4. Банк обязуется хранить не менее 5 (пяти) лет Ключи, используемые в рамках Условий ДБО. Сроки хранения ЭД должны соответствовать срокам хранения, установленным для документов на бумажных носителях. Архивы подлежат защите от несанкционированного доступа, непреднамеренного или преднамеренного уничтожения и/или искажения.

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

1. Системы ограничения доступа и защиты информации

- 1.1. Для обеспечения безопасности использования Системы каждой из Сторон должен быть определен и утвержден:
 - 1.1.1. порядок учета, хранения и использования носителей Ключевой информации, который должен полностью исключать возможность несанкционированного доступа к ним;
 - 1.1.2. порядок доступа и работы на персональном компьютере с Системой, который должен полностью исключать возможность несанкционированного доступа к Системе и носителю Ключевой информации; список лиц, имеющих доступ к Системе с разграничением прав доступа.
- 1.2. Ключи хранятся на сменных носителях у каждой из Сторон. Каждая из Сторон несет полную ответственность за сохранность, конфиденциальность и подлинность своего комплекта Ключей.
- 1.3. Ключ eToken PASS является автономным устройством и хранится в соответствии с п.4.2.2.4 Условий ДБО. Клиент несет полную ответственность за сохранность, конфиденциальность каждого Ключа eToken PASS.
- 1.4. Все работы по выработке и смене Ключей производятся в соответствии с порядком работы с Ключами и Сертификатом ключа проверки ЭП, указанным в Приложении № 2 к Условиям ДБО.
- 1.5. Все работы по регистрации и смене Ключа eToken PASS производятся в соответствии с порядком работы с Ключами eToken PASS, указанным в Приложении № 2 к Условиям ДБО.
- 1.6. Доступ неуполномоченных лиц к носителям Ключевой информации должен быть исключен.
- 1.7. По окончании рабочего дня, а также вне времени составления и обмена ЭД, носители секретных Ключей, Ключ eToken PASS должны храниться в недоступном для неуполномоченных лиц месте.
- 1.8. Не допускается:
 - 1.8.1. снимать несанкционированные копии с ключевых носителей;
 - 1.8.2. знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным;
 - 1.8.3. выводить секретные Ключи на дисплей (монитор) персонального компьютера или принтер;
 - 1.8.4. устанавливать носитель Ключевой информации в считывающее устройство (дисковод) локального персонального компьютера в режимах, не предусмотренных функционированием Системы, а также в другие персональные компьютеры;
 - 1.8.5. записывать на носитель Ключевой информации постороннюю информацию;
 - 1.8.6. передавать Одноразовый пароль Ключа eToken PASS неуполномоченным лицам.
- 1.9. Банк имеет право производить замену средств защиты информации и других программных или аппаратных средств, используемых при обмене ЭД, о чем уведомляет Клиента не менее чем за 30 (тридцать) дней. Клиент обязан в соответствующий срок приобрести за свой счет необходимые программно-технические средства и подготовить их ввод в действие в соответствии с рекомендациями Банка.

2. Процедура обмена информацией между Банком и Клиентом

- 2.1. Для обеспечения безопасности и конфиденциальности обмена ЭД в Системе используются специальные процедуры, включающие:
 - 2.1.1. формирование ЭП, предназначенной для обеспечения подтверждения подлинности ЭП в ЭД. ЭП жестко увязывает в одно целое содержание документа и Ключ ЭП или Ключ eToken PASS уполномоченных лиц Сторон и делает невозможным изменение ЭД без нарушения подлинности данной ЭП;
 - 2.1.2. использование Паролей/ Одноразовых паролей для ограничения доступа к Системе.
- 2.2. Процесс обмена ЭД происходит в следующем порядке:
 - 2.2.1. Сторона-отправитель формирует документы и ставит под ними ЭП Владельца ЭП/Ответственного сотрудника Банка;
 - 2.2.2. документы передаются по защищенному каналу связи Стороне-получателю;
 - 2.2.3. Сторона-получатель проверяет в принятых ЭД их ЭП. Если проверка ЭП под ЭД с применением Ключей проверки ЭП другой Стороны подтверждает их авторство и подлинность, то такие ЭД принимаются Стороной-получателем в качестве документов, поступивших от противоположной Стороны. В противном случае ЭД не принимаются Стороной-получателем в качестве документов, поступивших от противоположной Стороны, о чем Сторона-отправитель уведомляется посредством формирования соответствующего статуса о неприеме ЭД после автоматизированной обработки ЭД в Системе;
 - 2.2.4. Банк проверяет в принятых ЭД их ЭП, сформированную с использованием Ключа eToken PASS Клиента. Если проверка ЭП, сформированной с использованием Одноразового пароля Ключа eToken PASS, введенного Клиентом подтверждает авторство и подлинность, то такие ЭД принимаются Банком в качестве документов, поступивших от Клиента. В противном случае ЭД не принимаются Банком в качестве документов, поступивших от Клиента, о чем Банк уведомляется Клиента посредством формирования соответствующего статуса о неприеме ЭД после автоматизированной обработки ЭД в Системе.
- 2.3. Подлинность и авторство информации обеспечивается применением ЭП.
 - 2.3.1. Для формирования Неквалифицированной электронной подписи используется сертифицированное ФСБ РФ Средство электронной подписи «Крипто-Ком». Ключи ЭП Клиента генерируются в соответствии с порядком работы с Ключами и Сертификатом ключа проверки ЭП, указанным в Приложении № 2 к Условиям ДБО.

2.3.2. Для формирования Простой электронной подписи используются уникальные Одноразовые пароли, формируемые с помощью Ключа eToken PASS для подписи документов, генерируются в соответствии с индивидуальным алгоритмом каждого Ключа eToken PASS.

ФОРМА

АКТ

о предоставлении права доступа и введении в действие Системы «Интернет-Банк»

г. _____

«__» _____ 20__ г.

АО «Банк Русский Стандарт», именуемое в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, именуемые вместе в дальнейшем «Стороны», составили настоящий Акт о предоставлении права доступа и введении в действие Системы «Интернет-Банк» (далее – Акт) о нижеследующем:

1. Банком произведена регистрация Клиента в Системе.
2. Банк предоставил Клиенту Логин и Пароль для доступа к Системе «Интернет-Банк».
3. Банк передал, а Клиент принял:
 - Сертификат(-ы) ключа проверки ЭП.
 - Ключ(-и) eToken PASS, серийный № _____
4. Программное обеспечение Рабочего места признано Сторонами работоспособным и принято Клиентом в эксплуатацию с «__» _____ 20__ г. С указанной даты Стороны обязуются выполнять обязательства, предусмотренные Условиями ДБО.
5. Программное обеспечение Рабочего места Клиента считается принятым в эксплуатацию с момента подписания настоящего Акта Сторонами. Все корректно оформленные документы, переданные с использованием Системы «Интернет-Банк», начиная с даты подписания настоящего Акта, будут иметь юридическую силу.
6. Стороны претензий к друг другу не имеют.
7. Настоящий Акт составлен в 2 (Двух) экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон и является неотъемлемой частью Условий.

ПОДПИСИ СТОРОН

БАНК

КЛИЕНТ

_____/_____
подпись / *Ф.И.О.*

_____/_____
подпись / *Ф.И.О.*

М.П.

М.П.

ФОРМА

Заявление на регистрацию Ключа eToken PASS для использования в Системе

«__» _____ 20__ г.

Полное наименование Клиента: _____

Уполномоченное лицо Клиента: _____

Просим зарегистрировать Ключ eToken PASS уполномоченного лица Клиента для дополнительной авторизации в Системе и подтверждения Электронных документов в Системе с помощью Простой электронной подписи.

Обязуемся исключить доступ к Ключу eToken PASS неуполномоченных лиц и хранить Ключ eToken PASS в безопасном от хищения месте.

С Тарифами Банка ознакомлен.

Ключ eToken PASS серийный № _____ получен «__» _____ 20__ г.

_____/_____
подпись *Ф.И.О. уполномоченного лица Клиента*

КЛИЕНТ

_____/_____
подпись *Ф.И.О.*

М.П.

В АО «Банк Русский Стандарт»

От _____
(наименование Клиента)

Дата: _____
(формат ДД.ММ.ГГГГ)

Письмо о смене Логина и Пароля

Просим прислать на электронную почту ***@*.*** новые учетные данные уполномоченному лицу Клиента _____ (Ф.И.О.) для входа в Систему «Интернет-Банк» в связи с _____ (указывается причина смены Логина и/или Пароля).

- Логин
- Пароль

Должность руководителя

_____ / _____ /
подпись *Ф.И.О.*

М.П.

ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРОВ

1.1. Все споры и разногласия, возникающие при исполнении Условий ДБО, Стороны будут стремиться разрешать путем переговоров. На время разрешения спорной ситуации Стороны имеют право приостановить доступ в Систему, уведомив об этом другую Сторону в день приостановки доступа в Систему посредством отправки соответствующего ЭД с использованием Системы с обязательным его дублированием на бумажном носителе в срок не позднее следующего рабочего дня со дня отправки такого ЭД. Соответствующее уведомление на бумажном носителе должно быть подписано уполномоченным лицом и заверено оттиском печати (при наличии) соответствующей Стороны.

При возникновении спора между Клиентом и Банком о факте получения одной Стороной ЭД, направленного другой Стороной, доказательством получения ЭД является изменение в Системе Статуса документа такого ЭД.

1.2. Разбор конфликтных ситуаций о подлинности ЭП под ЭД заключается в доказательстве принадлежности ЭП конкретного ЭД, соответствующему уполномоченному лицу Клиента или Банка. Разбор основывается на математических свойствах алгоритмов, гарантирующих невозможность подделки значения ЭП любым лицом, не обладающим Ключом ЭП или Ключом eToken PASS.

1.3. При не урегулировании между Сторонами возникшего спора, до обращения одной из Сторон в суд, Сторона – инициатор спора в течение 3 (трех) рабочих дней с момента направления спорного ЭД осуществляет подготовку и направляет другой Стороне заявление с использованием Системы с подробным изложением обстоятельств происшедшего и предложением создать комиссию. В случае приостановления доступа к Системе такое заявление направляется на бумажном носителе, подписывается уполномоченным лицом и заверяется оттиском печати (при наличии) соответствующей Стороны. Создание Сторонами указанной комиссии является досудебным претензионным порядком урегулирования спора.

1.4. В предложении о создании комиссии указывается предлагаемое место сбора комиссии, дата и время. Окончательное место, дата и время сбора комиссии определяется по согласованию Сторон не позднее 7 (семи) календарных дней с момента получения предложения о создании комиссии Стороной, в адрес которой такое предложение было направлено.

1.5. В случае если другая Сторона не согласна с существом претензий и не намерена участвовать в работе комиссии, то эта Сторона должна ответить в письменной форме Стороне – инициатору спора не позднее 3 (трех) рабочих дней с момента получения предложения о создании комиссии об отказе в ее участии.

1.6. В состав комиссии должно входить равное количество представителей от каждой Стороны (не менее 2 (двух) представителей от каждой Стороны). В случае рассмотрения спора в отношении ЭД, подписанного Ключом ЭП, при необходимости, с письменного согласия обеих Сторон, в состав комиссии могут быть дополнительно включены специалисты организации-разработчика программного обеспечения Message Pro (разработчик ЗАО «Сигнал-КОМ»). В случае привлечения независимых специалистов их услуги оплачивает Сторона, признанная виновной.

1.7. Стороны предоставляют комиссии следующие документы и материалы:

1.7.1. затребованные Сертификаты на магнитном и бумажном носителях;

1.7.2. подписанный ЭП ЭД, по которому предъявляются претензии.

1.8. Комиссия в двухнедельный срок проводит разбор конфликтной ситуации и по итогам работы составляет акт в двух экземплярах для каждой Стороны (в случае рассмотрения комиссией спора в отношении ЭД, подписанного Ключом ЭП и привлечения в состав комиссии специалистов организации-разработчика программного обеспечения Message Pro (разработчик ЗАО «Сигнал-КОМ») составляется третий экземпляр акта) с указанием существа конфликта, виновной Стороны и сроков устранения конфликтной ситуации.

Для разрешения спора в отношении ЭД, подписанного Ключом ЭП, с целью подтверждения подлинности ЭП в ЭД, используется программное обеспечение Arbiter-PKI (разработчик ЗАО «Сигнал-КОМ»), соответствующее требованиям Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи». Процедура проверки ЭП в ЭД производится в соответствии с документацией на указанное программное обеспечение.

Для разрешения спора в отношении ЭД, подписанного с использованием Ключа eToken PASS, с целью подтверждения подлинности ЭП в ЭД, используются внутренние средства Системы.

1.9. Порядок разрешения конфликта, если одна Сторона отрицает, что передавала второй Стороне спорный ЭД:

1.9.1. если вторая Сторона не может предъявить копию спорного ЭД - конфликт решается в пользу первой Стороны;

1.9.2. если вторая Сторона предъявляет копию спорного ЭД, подписанного первой Стороной:

1.9.2.1. подпись первой Стороны подтверждается в соответствии с п.1.8 настоящего Приложения – конфликт решается в пользу второй Стороны;

1.9.2.2. подпись первой Стороны не подтверждается в соответствии с п.1.8. настоящего Приложения – конфликт решается в пользу первой Стороны.

1.10. Порядок разрешения конфликта, если одна Сторона утверждает, что исполненный второй Стороной спорный ЭД не соответствует переданному ЭД:

1.10.1.если вторая Сторона не может предъявить копию спорного ЭД – конфликт решается в пользу первой Стороны;

1.10.2.если вторая Сторона предъявляет копию спорного ЭД, спорный ЭД проверяется в соответствии с п.1.8. настоящего Приложения:

1.10.2.1.подпись первой Стороны подтверждается – конфликт решается в пользу второй Стороны;

1.10.2.2.подпись первой Стороны не подтверждается – конфликт решается в пользу первой Стороны.

Если все предпринятые меры по добровольному урегулированию спора не принесут удовлетворяющего обе Стороны результата, либо одна из Сторон откажется от участия в комиссии, либо Стороны не смогут в течение 7 (семи) рабочих дней с даты получения одной из Сторон предложения о создании комиссии другой Стороне определить дату сбора комиссии, либо в даты сбора комиссии комиссия не будет собрана, либо лица, прибывшие для участия в ней, не будут наделены полномочиями от Стороны, их направившей на участие, в работе комиссии, принятие решений, подписание актов, указанных в п.1.8 настоящего Приложения, то обязательный досудебный претензионный порядок считается соблюденным Сторонами и спор подлежит разрешению в Арбитражном суде г. Москвы (Российская Федерация) в порядке, предусмотренном Арбитражно-процессуальным кодексом Российской Федерации.