Эксперт Банк Профессиональный Подход к Финансам

Приложение № 3
к Правилам комплексного банковского обслуживания
Клиентов-юридических лиц, индивидуальных предпринимателей,
а также физических лиц, занимающихся в установленном
законодательством Российской Федерации
порядке частной практикой в АО «Эксперт Банк»

УТВЕРЖДЕНО
Решением Правления «21» мая 2019 г.
Документ вступает в силу с «07» июня 2019 г.

УСЛОВИЯ
предоставления и дистанционного банковского обслуживания
с использованием Системы Faktura.ru

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Авторизация	подтверждение полномочий Клиента на получение информационных услуг, формирование и передачу Распоряжения Банку с использованием Системы Faktura.ru путем ввода Имени пользователя (логина) и Пароля
Аналог собственноручной подписи (АСП)	персональный идентификатор Клиента, являющийся Контрольным параметром правильности заполнения всех обязательных реквизитов электронных документов и неизменности их содержания
Банк	Акционерное общество «Эксперт Банк»
Владелец ключа АСП	физическое лицо, открытый ключ АСП которого зарегистрирован в системе дистанционного банковского обслуживания «Faktura.ru» в соответствии с настоящими Условиями
Договор об использовании системы дистанционного банковского обслуживания «Faktura.ru» (Договор)	Договор, заключенный между Банком и Клиентом в рамках Договор КБО в соответствии с настоящими Условиями
Заявление о присоединении	Заявление, заполняемое Клиентом по форме Банка с целью получения Банковской услуги, предоставляемой Банком в соответствии с Правилами и настоящими Условиями
Ключ	общее название пары взаимосвязанных секретного и открытого ключей АСП
Кодовое слово	информация, указанная Клиентом при открытии счета, и используемая для идентификации Клиента при обращении в Банк по телефону
Логин	условное наименование, число или иная информация, позволяющая идентифицировать Клиента
Одноразовый пароль	уникальная последовательность символов, предоставленная Клиенту Банком посредством SMS – сообщения на указанный Клиентом номер мобильного телефона. Одноразовый пароль предоставляется Банком Клиенту для каждой совершаемой Клиентом операции по перечислению денежных средств со Счета.
Пароль	последовательность символов, которая вводится с использованием виртуальной клавиатуры в Системе.

Открытый ключ АСП	уникальная последовательность символов, соответствующая секретному ключу АСП и предназначенная для подтверждения с использованием СЗИ подлинности АСП в ЭД.
Секретный ключ АСП	уникальная последовательность символов, известная Владельцу ключа АСП и предназначенная для создания в ЭД АСП с использованием СЗИ
Ключевой носитель	информационный носитель, содержащий Ключ либо предназначенный для записи Ключа
Интернет-банк	система дистанционного банковского обслуживания «Faktura.ru» с использованием Смарт-карты либо с использованием одноразовых паролей
Компрометация ключа	- утрата доверия к тому, что используемый секретный ключ недоступен третьим лицам либо утеря ключевой информации вследствие программно-аппаратного сбоя. К событиям, связанным с компрометацией ключа, относятся в том числе: - утрата ключевого носителя; - утрата ключевого носителя с последующим обнаружением; - утрата логина, пароля к входу в Интернет-банк по системе одноразовых паролей; - увольнение сотрудников, имевших доступ к ключевым носителям; - утрата ключей от сейфа в момент нахождения в нем ключевого носителя; - прекращение полномочий владельца ключа АСП по работе с ЭД в СКБ; - временный доступ третьих лиц к ключевому носителю; - иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к ключу третьих лиц
Рабочий ключ	ключ, предназначенный для обеспечения авторства и целостности ЭД, передаваемых в Системе нескомпрометированный и срок действия которого не истек.
Система дистанционного банковского обслуживания «Faktura.ru» (Система)	совокупность программного, информационного и аппаратного обеспечения Банка и Клиента, реализующая электронный документооборот между Банком и Клиентом.
Сертификат ключа	документ на бумажном носителе, заверенный печатью Банка, а также электронный документ, который включает в себя открытый ключ АСП и который используется для подтверждения подлинности АСП и идентификации Владельца ключа АСП
Средства защиты информации (СЗИ)	программные средства, посредством которых осуществляются все операции, связанные с шифрованием ЭД, формированием и проверкой АСП, а также изготовление ключей.
Счет расчетный/банковский	счет в валюте Российской Федерации, иностранной валюте, открываемый юридическим лицам, индивидуальным предпринимателям, а также физическим лицам, занимающимся в установленном действующим законодательством Российской Федерации порядке частной практикой для совершения расчетов, связанных с предпринимательской деятельностью или частной практикой
Тарифы	Тарифы по расчетно-кассовому обслуживанию юридических лиц и индивидуальных предпринимателей, а также физических лиц, занимающихся в установленном действующим законодательством Российской Федерации порядке частной практикой, действующие на дату оплаты услуги.
Уполномоченное лицо	сотрудник Клиента, уполномоченный Клиентом на совершение любых действий, связанных с использованием аналога собственноручной подписи в соответствии с настоящими Условиями
Условия	настоящие Условия предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru
Электронный платежный документ (ЭПД)	платежный документ, в котором информация представлена в электронно-цифровой форме, отправленный с использованием Системы Faktura.ru

Электронный документы (ЭД)	любой не платежный документ, в котором информация представлена в электронно-цифровой форме, отправленный с использованием Системы Faktura.ru.
Электронная подпись (ЭП)	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.
Электронное средство платежа (ЭСП)	средство и (или) способ, позволяющее Клиенту удостоверять (с помощью уникальных цифровых реквизитов – номера и кода) документы в электронной форме в целях осуществления перевода Электронных денежных средств.
SMS-сообщение	короткое сообщение, используемое для передачи информации в сетях сотовой связи с помощью мобильного телефона

Иные термины, используемые в настоящих Условиях, имеют то же значение, что и в Договоре КБО.

2. Формы документов

2.1. Перечень технических средств рабочего места Клиента для работы в системе ДБО «Faktura.ru» - Приложение №1.
2.2. Рекомендации Клиенту по обеспечению безопасности – Приложение №2
2.3. Процедура подтверждения достоверности документа – Приложение №3
2.4. Заявление на выдачу Сертификата ключа проверки электронной подписи – Приложение № 4
2.5. Акт приема-передачи сертификата – Приложение №5
2.6. Уведомление об отмене действия ключей электронной подписи – Приложение №6
2.7. Заявка на подключение Интернет-банка с использованием системы Faktura.ru и получение Смарт-карты – Приложение №7
2.8. Заявка на подключение Интернет-банка с использованием системы Faktura.ru по технологии одноразовых паролей – Приложение №8
2.9. Акт приема-передачи устройства Смарт-карты для входа в Интернет–банк - Приложение №9
2.10. Памятка пользователя Системы дистанционного банковского обслуживания с использованием Системы Faktura.ru в АО ”Эксперт Банк” с использованием технологии одноразовых паролей (Приложение № 10)

3. Общие положения

3.1.Настоящие Условия являются типовыми для всех Клиентов и определяют положения договора присоединения, заключаемого между Банком и Клиентом в соответствии с п.1 ст.428 Гражданского Кодекса Российской Федерации.
3.2.Заключение Договора осуществляется путем присоединения Клиента к настоящим Условиям в рамках договора КБО на основании Заявления о присоединении, надлежащим образом заполненного и подписанного Клиентом, а также соответствующих форм документов, являющихся неотъемлемой частью Договора. Заключение Договора означает принятие Клиентом настоящих Условий и Тарифов полностью, согласие с ними и обязательство их неукоснительно соблюдать. Банк подтверждает Клиенту факт заключения Договора путем выдачи Клиенту второго экземпляра Заявления, с отметкой Банка об акцепте во второй части Заявления.
3.3.Настоящие Условия определяют условия и порядок обмена документами Банка и Клиента, в которых информация представлена в электронной форме и заверена электронной подписью с помощью Системы Дистанционного Банковского Обслуживания «Faktura.ru» (http://www.faktura.ru).
3.4.В электронном документообороте между Банком и Клиентом участвуют: Оператор - ЗАО «Центр Цифровых Сертификатов и/или Удостоверяющий Центр «AUTHORITY», осуществляющий информационное и технологическое обслуживание Банка в Корпоративной Информационной Системе «BeSafe», Банк как Агент удостоверяющего центра Оператора, Клиент.
3.5.Электронный документооборот по обмену электронными документами между Банком и Клиентом осуществляется в порядке и на условиях, определённых Правилами электронного документооборота Корпоративной Информационной Системы «BeSafe» компании «Центр Финансовых Технологий», расположенных на веб-сервере по адресу http://www.besafe.ru.
3.6.Информационный обмен в рамках Системы осуществляется по открытым каналам связи, в том числе с использованием сети Интернет.
3.7.Для обеспечения конфиденциальности ЭД при его передаче по открытым каналам связи, а также для обеспечения авторства и целостности ЭД в Системе используются программные средства защиты информации, реализующие алгоритмы шифрования, формирования и проверки АСП.
3.8.На основании настоящих условий с использованием Системы осуществляется:
- обмен электронными платежными документами с Банком к своим счетам в рублях РФ и иностранной валюте, открытым в Банке на основании соответствующих договоров банковского счета, заключенных между Банком и Клиентом;
- прием/передачу иных ЭД, определенных действующим законодательством РФ и заключенными Сторонами договорами, соглашениями.

3.9.В целях реализации настоящих Условий Система является электронным средством платежа - средством, позволяющим Клиенту Банка составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации.
3.10.Клиентская часть Системы может быть представлена Клиенту в виде доступа к Web-серверу системы «Faktura.ru» посредством сети Интернет.
При подключении и работе в Системе Клиент использует ключевые носители, которые предоставляются Банком на основании Заявления Клиента:
- Устройство хранения секретного ключа Смарт-карты, который предоставляется Банком по заявлению Клиента (Приложение №7).
- Логин для входа в Интернет-банк с использованием системы одноразовых паролей, при предоставлении доступа Клиенту к Системе Банк генерирует Логин Клиента, который указывается в Приложении №8 к настоящим Условиям. Клиент получает SMS-сообщение с паролем доступа к Системе на телефонный номер, указанный в Приложении № 8. Полученный пароль является временным и должен быть изменён клиентом самостоятельно при первом входе в Систему. Вход в Систему возможен только при выполнении условия смены пароля при первом входе. Рекомендации для клиента по составлению пароля содержатся в Памятке пользователя (Приложение № 10). Банк при этом не несет ответственности за доставку SMS-сообщения Клиенту по причине возможных сбоев у мобильных операторов и в самой Системе. В случае неполучения SMS-сообщения с паролем доступа в течение 3 (Трех) рабочих дней с момента заключения Договора, Клиент должен лично обратиться в подразделение Банка, в котором он заключал Договор для устранения возникших проблем с получением доступа к Системе.

3.11.Стороны признают, что получение Банком по Системе ЭД документов, подписанных АСП Клиента, юридически тождественно получению аналогичного документа на бумажном носителе, заверенного подписями уполномоченных лиц и печатью Клиента, оформленного в соответствии с действующим законодательством Российской Федерации и нормативными документами Банка России. В случае подключения Интернет-банка с использованием системы одноразовых паролей, настоящими условиями предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на Счете Клиента, электронными средствами платежа с использованием в них аналога собственноручной подписи в виде Одноразового пароля. Клиент дает право Банку использовать ЭД наравне с заверенными документами на бумажном носителе. В том числе Стороны признают, что переданные по Системе и подписанные АСП:
- выписки о движении денежных средств по Счету Клиента;
- приложения к выпискам по списанным и зачисленным на Счет Клиента суммам
- платежные поручения;
- банковские ордера;
- мемориальные ордера;
- платежные ордера;
- заявление о присоединении, заполняемые Клиентом с целью получения Банковских продуктов;
- анкеты Клиента, представителей Клиента, Бенефициарных владельцев, Выгодоприобретателей;
- документ свободного формата (в том числе вложенный файл в документ свободного формата);
- иные документы
- эквивалентны подобным документам на бумажных носителях и влекут аналогичные им права и обязанности Сторон.

3.12.Клиент признает, что ЭД, направленные Сторонами друг другу по Системе, а также журналы учета ЭД, ведущиеся в Системе, могут быть представлены Банком в качестве доказательств в Арбитражном суде в случае рассмотрения спора, возникшего в результате применения Системы.
3.13.Любые ЭД, передаваемые Клиентом в Системе, должны быть заверены АСП Клиента.
3.14.Замена ключей с соблюдением требований настоящих Условий не влияет на юридическую силу ЭД, если он был подписан рабочим на момент подписания ключом.
3.15.Система считается введенной в эксплуатацию с даты подписания Акта приема-передачи сертификата (Приложение № 5 к настоящим Условиям).
3.16.Клиент признает, что использование Системы влечет дополнительные риски несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами. Меры по снижению указанных рисков приведены в Рекомендациях Клиенту по обеспечению безопасности (Приложение №2 к настоящим Условиям).
3.17.Информирование Клиента о совершенных в Системе операциях производится путем предоставления выписки, а также путем изменения статуса ЭД в Системе.
3.18.Проведение операций по ЭПД и ЭД с использованием Системы осуществляется в соответствии с графиком обслуживания Клиентов, расположенным на стендах Банка и на сайте Банка в сети Интернет по адресу: **http://www.expertbank.com**.

4.ПРАВА И ОБЯЗАННОСТИ БАНКА

4.1. Банк обязуется:
4.1.1. Произвести аккредитацию Клиента в Системе.

4.1.2. Принимать от Клиента по Системе ЭПД и иные ЭД.
4.1.3. Информировать Клиента путем направления ЭД о совершении каждой операции по счету с использованием ЭСП в Системе не позднее дня, следующего за днем совершения операции.
4.1.4. По требованию Клиента предоставлять по Системе в виде ЭД: выписки по его счету, документы и информацию, связанные с использованием ЭСП, сведения о доставке документов и результатах обработки, извещения и письма произвольной формы.
4.1.5. Принимать к исполнению ЭПД, ЭД подлинность которых подтверждена ЭП Клиента.
4.1.6. Подтверждать прием к исполнению ЭПД, ЭД, направленных Клиентом, квитанциями о приеме, которые передаются по Системе.
4.1.7. Фиксировать и хранить информацию о совершенных операциях по счету Клиента не менее трех лет с момента их совершения.
4.1.8. Банк не несет ответственности за задержку в формировании выписки по счету Клиента, если она связана с задержкой получения Банком информации о проведенных операциях по его корреспондентскому счету от Банка России.
4.1.9. Приостанавливать на срок не более 2 (Двух) рабочих дней использование Клиентом Системы в случаях выявления Банком операций по Счету, совершаемых с использованием Системы, соответствующих признакам осуществления перевода денежных средств без согласия Клиента, и исполнения распоряжений Клиента о совершении операции по списанию денежных средств.

Признаки осуществления перевода денежных средств без согласия Клиента устанавливаются Банком России и размещаются на его официальном сайте в информационной телекоммуникационной сети «Интернет».

В рамках настоящего пункта Условий Банк незамедлительно направляет Клиенту запрос на подтверждение исполнения распоряжения. Запрос направляется Банком с использованием Системы, а также путем отправки SMS-сообщений, в случае если Клиентом оформлено заявление на предоставление данной услуги.

При получении от Клиента подтверждения возобновления исполнения распоряжения, Банк незамедлительно возобновляет использование Клиентом Системы и исполняет распоряжение Клиента о совершении операций.

При неполучении от Клиента подтверждения Банк по истечении 2 (Двух) рабочих дней, после дня совершения Банком действий по приостановлению операций по Счету, возобновляет исполнение распоряжения по Счету и возобновляет использование Системы.
4.1.10. Приостанавливать зачисление денежных средств на Счет Клиента сроком до 5 (Пяти) рабочих дней со дня получения от оператора по переводу денежных средств, обслуживающего плательщика, соответствующего уведомления о приостановлении совершения операции в сумме перевода денежных средств и незамедлительно, с использованием Системы, а также путем отправки SMS-сообщений, в случае если Клиентом оформлено заявление на предоставление данной услуги, уведомить Клиента, о необходимости предоставления документов, подтверждающих обоснованность переведенных денежных средств.

В случае непредоставления Клиентом обосновывающих документов Банк в течение 2 (Двух) рабочих дней по истечении указанного пятидневного срока осуществляет возврат денежных средств оператору по переводу денежных средств, обслуживающему плательщика.

В случае предоставления Клиентом в течение 5 (Пяти) рабочих дней подтверждающих документов, Банк осуществляет зачисление денежных средств на Счет Клиента.
4.1.11. Предоставлять Клиенту рекомендации по снижению повторного осуществления перевода денежных средств без согласия Клиента путем направления уведомлений с использованием Системы, а также путем отправки SMS-сообщений, в случае если Клиентом оформлено заявление на предоставление данной услуги

4.2. Банк вправе:
4.2.1. Отказать Клиенту в приеме от него распоряжения на проведение операции по счету на основании ЭПД, в соответствии с Федеральным законом от 07.08.2001г. №115-ФЗ и Правилами внутреннего контроля Банка в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. При этом Банк вправе принять от Клиента надлежащим образом оформленные расчетные документы на бумажном носителе.
4.2.2. Не принимать к исполнению ЭПД, ЭД Клиента в случае их ненадлежащего оформления либо при сомнении в подлинности ЭП. При получении таких ЭПД, ЭД сообщать должностным лицам Клиента об оставлении ЭПД, ЭД без исполнения.
4.2.3. Задержать либо отказать в исполнении ЭПД, ЭД в случае, если для выполнения операции требуется согласно действующему законодательству РФ и договору, соглашению с Клиентом дополнительные документы, передача которых в электронной форме невозможна.
4.2.4. При необходимости требовать от Клиента предоставления надлежащим образом оформленных документов на бумажном носителе, подтверждающих операции, проведенные по счету Клиента на основании ЭПД, ЭД.
4.2.5. Приостановить или прекратить использование Клиентом ЭСП на основании полученного от Клиента уведомления, в том числе, в случае утраты ключей ЭП (их носителей) и (или) об использовании ЭСП без согласия Клиента.
4.2.6. Приостановить расчетное обслуживание Клиента с использованием Системы в следующих случаях:
- возникновение технических неисправностей при работе с Системой - до их устранения;
- возникновение спорной ситуации, связанной с использованием настоящего Договора - до разрешения

спора;
- неисполнение Клиентом требования Банка о предоставлении документов и/или ответа на запрос в срок, указанный в письменном запросе Банка или запросе, направленном по Системе - до исполнения требования Банка;
- при наличии обстоятельств, свидетельствующих о неправомерном использовании Клиентом или третьими лицами ЭСП;
- при нарушении Клиентом использования порядка ЭСП, предусмотренного настоящим договором.

5.ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА.

5.1. Клиент обязуется:
5.1.1. Получить для работы в Системе устройство хранения секретного ключа Смарт-карту (Приложение №9) и (или) Логин для входа в Интернет-банк Системы по технологии одноразовых паролей (Приложение №8) на уполномоченных лиц в течение 30 (Тридцати) календарных дней с момента подписания Заявления на присоединение к настоящим Условиям.
5.1.2. Перед началом работы с Системой в течение 14 рабочих дней с момента получения ключей ЭП направить в Банк тестовый платёжный документ (платёжное поручение) на сумму 1 рубль с указанием в поле «назначение платежа» фразы: «тестовый документ». При использовании уже сформированной ЭП на основании ранее заключенного договора о дистанционном банковском обслуживании направление тестового платежного документа не требуется.
5.1.3. Не производить не согласованных с Банком изменений в программном обеспечении Системы.
5.1.4. Не тиражировать и не передавать третьим лицам предоставляемое Банком программное обеспечение и документацию.
5.1.5. Обеспечить до начала работ с Системой наличие технических и программных средств в соответствии с Приложением № 1 к настоящему Договору.
5.1.6. Выполнять требования к программно-техническим средствам, необходимые для работы Системы.
5.1.7. Соблюдать установленные правила работы в соответствии с документацией по работе с Системой и действующим законодательством РФ.
5.1.8. Производить сверку реквизитов получаемых от Банка ЭД и выписок по счету.
5.1.9. Обеспечить использование ЭП только уполномоченными сотрудниками Клиента, к которым относятся лица, наделенные правом подписи и заявленные в карточке с образцами подписей и оттиска печати. Банк не несет ответственности в случае распоряжения средствами на счете неуполномоченными сотрудниками Клиента с использованием Системы.
5.1.10. Хранить в тайне ключи, логины, имена и пароли, используемые при работе в Системе, а также изменять указанные ключи, имена и пароли по первому требованию Банка.
5.1.11. Клиент обязан незамедлительно, но не позднее дня, следующего за днем получения уведомления от Банка в соответствии с п.4.1.3. настоящих Условий, информировать Банк (Приложение № 6) об использовании ЭСП без согласия Клиента, а также об обстоятельствах, которые делают возможным создание документов и передачу их в электронном виде лицами, не имеющими соответствующих полномочий, в частности, но не ограничиваясь: об утрате, хищении ключей ЭП (их носителей), несанкционированном копировании ключей ЭП, передаче их по линии связи в открытом виде, а также о случаях повреждения носителей, содержащих ключи.
В случае несвоевременного уведомления Банка о случаях, указанных в п. 5.1.11. настоящих Условий, Клиент несет ответственность по операциям, совершенным неуполномоченными лицами с использованием секретного ключа до момента блокировки Банком действия ключа.
5.1.12. Клиент обязуется соблюдать рекомендации Клиенту по обеспечению безопасности, указанные в Приложении № 2 к настоящим Условиям.
5.1.13. В случаях приостановления Банком исполнения распоряжения о совершении операций по Счету, указанных в п.4.1.9, 4.1.10. настоящих Условий, Клиент обязан по запросу Банка незамедлительно предоставить подтверждение возобновления исполнения операций.
При неполучении от Клиента подтверждения возобновления операций по Счету в рамках настоящего пункта Условий, Банк по истечении 2 (Двух) рабочих дней самостоятельно возобновляет исполнение операций по Счету.
5.1.14. В случаях приостановления Банком зачисления денежных средств на Счет Клиента в сумме перевода денежных средств, указанных в п.4.1.10. настоящих Условий, Клиент обязан в течение 5 (Пяти) рабочих дней, со дня направления запроса Банка, предоставить документы, подтверждающие обоснованность получения переведенных денежных средств.

5.2. Клиент вправе:
5.2.1. Приостановить исполнение ЭПД, ЭД, переданных по Системе, либо временно блокировать работу в Системе, позвонив по телефону в Банк и назвав кодовое слово, указанное в Приложении 7 и (или) Приложении 8. При этом возобновление обслуживания Клиента возможно только после получения Банком письменного заявления Клиента о необходимости возобновить обслуживание Клиента с использованием Системы.
5.2.2. Отозвать ЭПД, переданный по Системе, при условии, что ЭПД находится в стадии обработки, не передан в платежную систему Банка России и Банк имеет возможность его отозвать. Отзыв ЭПД осуществляется Банком только при условии приема Банком от Клиента сообщения по Системе с полным указанием реквизитов (№ п/п, дата, сумма) отзываемого ЭПД.
5.2.3. Использование ЭПД, ЭД не изменяет содержания установленных законодательством РФ и договорами

прав и обязанностей Клиента и Банка, содержания платежных и иных документов и правил заполнения их реквизитов.

6. ОТВЕСТВЕННОСТЬ СТОРОН

6.1. Соблюдение положений Условий является обязательным для Банка и Клиента.
6.2. Клиент несет ответственность за достоверность предоставляемых Банку сведений, послуживших основанием для заключения Договора.
6.3. Банк несет ответственность за неразглашение предоставленных Клиентом сведений финансового и персонального характера и за сохранение банковской тайны. Сведения о проводимых операциях могут быть представлены третьим лицам в порядке, установленном действующим законодательством Российской Федерации.
6.4. Банк не несет ответственность за сбой в работе Системе по вине Клиента, в том числе в случаях:
- модификации Системы Клиентом;
- внесения изменений в конфигурацию Системы Клиентом;
- удаления элементов Системы Клиентом;
- повреждения операционной системы Клиента вредоносными программами;
- нестабильной работы операционной системы или аппаратного обеспечения клиентского рабочего места,
- несвоевременной смены ключей Клиентом,
- сбоя на дисковых и/или иных носителях информации.

6.5. Банк не несет ответственность за убытки Клиента, возникшие в результате:
- нарушения или невыполнения Клиентом настоящих Условий;
- в результате умышленной или неосторожной утраты (порчи, передачи, утери, разглашения) Клиентом применяемых в Системы паролей, ключей, конфиденциальной информации и/или программного обеспечения;
- несвоевременного сообщения Клиентом в Банк о компрометации своих ключей;
- несанкционированного доступа третьих лиц к Клиентскому рабочему месту;
- заражения Клиентского рабочего места вредоносными программами.
- за ущерб, возникший вследствие действия непреодолимой силы, влияющей на функционирование Системы, в виде стихийных бедствий, отключения электроэнергии, повреждения линий связи, решений органов власти, общественных явлений.
- за убытки, возникшие вследствие неисполнения Клиентом обязанности, предусмотренной п.5.1.14. настоящих Условий.

6.6. Банк не несет ответственность, если операции по Счету задерживаются в результате ошибок Клиента и/или третьих лиц, допущенных при заполнении реквизитов документов при оформлении Клиентом и/или третьими лицами распоряжения на перечисление денежных средств со Счета и в других случаях, возникших не по вине Банка.
6.7. Банк не несет ответственность за возможные технические помехи в работе линий связи, приводящие к невозможности передачи (приема) Клиентом ЭД в соответствии с настоящими Условиями.
6.8. Стороны обязуются за собственный счет организовать рабочие места для работы в Системы в соответствии с Условиями и поддерживать в рабочем состоянии свои программно-технические средства.
6.9. Стороны обязуются использовать свои программно-технические средства в целях выполнения условий Договора.
6.10. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по Договору, если такое неисполнение произошло в результате:
-изменения действующего законодательства Российской Федерации (принятие решений органами законодательной и/или исполнительной власти о введении каких-либо обременений на доходы либо ограничения в совершении каких-либо действий и т.п.);
-технических неисправностей, возникших по вине третьих лиц (сбои в подаче электроэнергии, отсутствие компьютерно-модемной связи и т.п.). При наступлении таких обстоятельств Сторона, подвергшаяся их воздействию, должна в трехдневный срок известить об их наступлении другую Сторону. Извещение должно содержать данные о характере обстоятельств и, по возможности, оценку их влияния на исполнение Стороной своих обязательств по Договору. При прекращении действия таких обстоятельств Сторона, подвергшаяся их воздействию, обязана в трехдневный срок известить об этом другую Сторону. Извещения со стороны Банка публикуются на Официальном сайте Банка. При этом срок исполнения обязательств отодвигается соразмерно времени, в течение которого действовали такие обстоятельства, если исполнение обязательств остается возможным.

7.СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ ПО ДОГОВОРУ

7.1. Клиент оплачивает комиссионное вознаграждение за услуги, оказываемые Банком по Договору, согласно Тарифам, которые устанавливаются и могут изменяться Банком в одностороннем порядке. При использовании Клиентом уже сформированной ЭП на основании ранее заключенного договора о дистанционном банковском обслуживании, оплата за подключение к системе «Faktura.ru» не производится.
7.2. Клиент предоставляет Банку право списывать с его счета плату за предоставленные услуги по Договору, в соответствии с действующими на момент списания Тарифами.
7.3. Уведомление Клиента об изменении Тарифов производится путём размещения информации на стендах в помещении Банка и/или на сайте Банка в сети Интернет по адресу: http://www.expertbank.com.

8.СРОКИ ДЕЙСТВИЯ ДОГОВОРА

8.1. Договор вступает в силу с даты передачи второго экземпляра Заявления о присоединении и соответствующих Приложений с отметками Банка Клиенту при условии исполнения Клиентом положений п. 5.1.1. настоящих Условий и действует в течение неопределенного срока до полного исполнения Сторонами обязательств. Обслуживание Клиента с использованием Системы начинается со следующего дня после подписания Акта приема-передачи сертификата ЭП (Приложение № 5 настоящих Условий). При использовании уже сформированной ЭП на основании ранее заключенного договора о дистанционном банковском обслуживании обслуживание Клиента с использованием Системы начинается со дня присоединения к настоящим Условиям.
8.2. В случае, если ни одна из Сторон не заявила о расторжении Договора за один месяц до истечения срока действия, Договор считается продленным на следующий год. Такой же порядок пролонгации действует и в дальнейшем. При этом Клиент совершает все необходимые действия по продлению сертификата ЭП согласно документации к Системе.
8.3. Сторона вправе расторгнуть Договор в одностороннем порядке, предупредив в письменном виде о своем намерении другую Сторону за 15 (пятнадцать) календарных дней до предполагаемой даты расторжения.
8.4. Договор расторгается автоматически в случае закрытия всех счетов Клиента в Банке, указанных в Приложениях 7,8.

9.ПРОЧИЕ УСЛОВИЯ

9.1. Все споры и разногласия, возникающие по настоящему соглашению, разрешаются Сторонами путем переговоров.
9.2. При получении Клиентом информации об операции по счету, совершенной с использованием ЭСП в Системе, с которой не согласен, Клиент вправе оспорить такую операцию, предоставив в Банк заявление о несогласии с операцией с использованием Системы.
9.3. Для разрешения спорной ситуации, связанной с отказом Клиента от авторства или содержания ЭПД, ЭД, Стороны обращаются к разработчику Системы. Техническая экспертиза проводится по месту нахождения разработчика Системы.
9.4. Банк рассматривает заявление Клиента, в том числе при возникновении споров, связанных с использованием ЭСП в срок не более 30 (тридцати) дней со дня получения заявления Банком, а в случае трансграничного перевода денежных средств - в срок не более 60 (Шестидесяти) дней со дня получения заявления. В случае если Банку требуется дополнительная информация от Клиента и/или разработчика Системы, Клиент информируется о промежуточном результате рассмотрения заявления с указанием нового срока предоставления решения о результате рассмотрения заявления, при этом новый срок предоставления решения по заявлению рассчитывается от даты предоставления дополнительной информации.
Информация о результатах рассмотрения заявления доводится до сведения Клиента в письменной форме путем направления по Системе, либо по адресу, предоставленному Клиентом в Банк, либо вручена представителю Клиента в Банке под роспись.
9.5. На время разрешения спорной ситуации, связанной с исполнением настоящих Условий, Банк имеет право приостановить действие настоящего Договора в одностороннем порядке. Приостановление действия Договора не прекращает обязательств Клиента и Банка по переводу денежных средств по счету Клиента, возникших до момента приостановления действия Договора.
9.6. Клиент предварительно до заключения Договора уведомлен о порядке использования ЭСП, а также о том, что несоблюдение указанного порядка использования влечет возникновение повышенного риска использования ЭСП и возможность приостановления Банком использования ЭСП.
9.7. Споры, по которым не достигнуто соглашение Сторон, разрешаются в Арбитражном суде по месту нахождения Банка (филиала Банка). К отношениям Сторон по настоящему Договору применяется право Российской Федерации.
9.8. Все приложения, изменения, дополнения и особые условия к настоящим Условиям оформляются в письменной форме, подписываются уполномоченными представителями обеих Сторон и являются неотъемлемой частью Договора.
9.10. Заключение Договора не лишает Клиента права передавать в Банк платежные и иные документы на бумажном носителе.

Приложение № 1
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

Перечень технических средств рабочего места Клиента для работы в системе ДБО «Faktura.ru»

Для функционирования Системы программно-аппаратный комплекс Клиента должен удовлетворять следующим базовым требованиям:

1. Компьютер с операционной системой Microsoft Windows. Актуальный список поддерживаемых версий операционных систем размещен на сайте **www.faktura.ru**;
2. Конфигурация компьютера должна удовлетворять минимальным требованиям, предъявляемым установленной на него Операционной системой;
3. Установлено лицензионное программное обеспечение антивирусной защиты, с актуальным обновлением вирусной базы.
4. Доступ к сети Интернет. Клиент самостоятельно настраивает все аппаратные и программные средства для обеспечения возможности работы с сетью Интернет по протоколам http, https

Контактная информация службы технической поддержки клиентов:

1. телефон круглосуточного информационного-центра: **8-800-200-55-75 (звонок бесплатный);**
2. электронный адрес службы сопровождения: **support@faktura.ru**
3. телефон службы сопровождения сервиса Faktura.ru: **(383) 335-80-88**
4. телефон технических специалистов Банка: **(3812) 21-91-91**

Адреса сети Интернет для доступа к Системе:

1. адрес web-сайта Банка: **http://www.expertbank.com**
2. адрес сервиса Faktura.ru: **https://faktura.ru/b2b/pages**

Приложение №2
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

РЕКОМЕНДАЦИИ Клиенту по обеспечению безопасности

1. При работе с системой ДБО «Faktura.ru» через Интернет

1.1. **Обеспечьте безопасность компьютера, с использованием которого осуществляется работа в Системе:**

1.1.1. Перед входом в Систему необходимо удостовериться в том, что на компьютере, с использованием которого осуществляется работа в Систему, отсутствуют вредоносные программы, на компьютере установлено, активировано и работает современное лицензионное антивирусное программное обеспечение, регулярно обновляются его антивирусные базы. Только регулярные обновление антивирусных баз и проведение антивирусных проверок позволит Вам своевременно обнаружить и предотвратить появление вредоносных программ (особенно важно контролировать обновление, если нет постоянного подключения к Интернету).

1.1.2. На компьютере рекомендуется использовать только лицензионное программное обеспечение, регулярно устанавливать рекомендуемые производителями обновления, как операционной системы, так и прикладного программного обеспечения, в том числе браузера, это позволит устранить выявленные уязвимости.

1.1.3. Рекомендуется использовать на вашем компьютере персональный межсетевой экран для входа в Интернет. Это позволит значительно снизить риск удаленного управления злоумышленниками из Интернет и локальной сети вашим компьютером и кражи вашей конфиденциальной информации.

1.1.4. Рекомендуется осуществлять работу в Системе с использованием отдельной учетной записи в операционной системе компьютера, защищенной сложным паролем, известным только Вам. При возможности рекомендуется осуществлять доступ в Систему с выделенного компьютера, используемого исключительно для работы с Системой. Права пользователя в операционной системе компьютера должны быть минимально необходимыми, должна быть запрещена установка прикладного программного обеспечения за исключением необходимого для работы в Системе.

1.1.5. Рекомендуется избегать работы в Системе с «недоверенных» компьютеров (в Интернет-кафе или другие общедоступные компьютеры, а так же «чужие» компьютеры временно используемые вами и т.п.). Крайне не желательно использование для работы в Системе публичных беспроводных сетей (например, бесплатный Wi-Fi. В выше описанных случаях существенно повышается риск кражи ваших конфиденциальных данных и денежных средств. Если же данные рекомендации Вами не выполнены, то сразу же при первой возможности измените пароль, войдя в Систему с «доверенного» Компьютера.

2. Не оставляйте без присмотра компьютер с активной Системой.

3. По возможности исключите посещение с данного компьютера сайтов сомнительного содержания и любых других потенциально опасных Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов полученных из недостоверных источников.

1.2. Выполняйте правила безопасности при работе в системе ДБО «Faktura.ru»

1.2.1 Перед вводом логина и пароля при входе в Систему убедитесь, что соединение установлено именно со стартовой страницей Системы и в адресной строке web-браузера отображается **http://www.expertbank.com** либо **http://www.faktura.ru**.

При работе с Системой для обеспечения конфиденциальности весь трафик между Банком и вашим компьютером шифруется с помощью защищенного протокола. Перед началом работы в Системе необходимо удостовериться, что соединение установлено в защищенном режиме ИЗ.

1.2.3. После окончания работы в Системе обязательно завершайте сеанс работы.

1.3 Соблюдайте правила безопасности при работе с ключевыми носителями:

1.3.1 Уделите вопросу хранения ключей Системы должное внимание. Помните, что наличие ключа позволяет заверить от Вашего имени документ и передать его на исполнение в Банк. Для большей безопасности храните ключи на съемных защищенных ключевых носителях (eToken).

1.3.2 Подключайте ключевой носитель к компьютеру только на время подписи документов. Не держите ключевые носители постоянно подключенными к компьютеру. Ни в коем случае не храните ключи на жестком диске компьютера.

1.3.3 Постарайтесь внедрить использование для отправки документов двух подписей (2-х ключей). Украсть два ключа сложнее, чем один.

1.3.4 При вводе ключа и пароля особое внимание, обращайте на правильное отображение названия ключа.

1.3.5 При компрометации секретных ключей или компьютера, увольнения ответственного сотрудника или ИТ специалиста Вашей компании, который имел доступ к компьютеру или к секретным ключам незамедлительно сообщите в Банк для блокировки ключей и генерации новых.

1.4 Соблюдайте правила безопасности при использовании паролей

1.4.1 Для работы в Системе необходимо использовать только сложные пароли, удовлетворяющие

следующим требованиям:
- пароль должен иметь длину от 6 до 20 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков !#$%&()*+-./:;<=>?[\;
- пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.);
- пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера вашей банковской карты и т.п.);
- пароль не должен содержать словарных слов (passw0rd, football, shadow, sergey, natalia, русские слова, набранные в английской кодировке, например, Сергей - CHшк|);
- пароль не должен совпадать с предыдущими паролями и не должен совпадать с именем входа;
- пароль не должен быть копией или комбинаций паролей используемых Вами в других системах (операционная система компьютера, электронная почта, развлекательный ресурсы в Интернет и т.п.).

1.4.2 Никогда не сообщайте свой пароль третьим лицам, в том числе коллегам, родственникам и сотрудникам Банка, вводите пароль только при работе в Системе. Сотрудник Банка не имеет права запрашивать у Вас пароль, даже если вы самостоятельно обратились в Банк. Вводите пароль только в Систему, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль.
1.4.3 Не записывайте свой пароль там, где доступ к нему могут получить третьи лица. Запрещается сохранять пароль на компьютере, мобильном устройстве, а так же на иных электронных носителях, доступ к которым могут получить третьи лица.
1.4.4 Рекомендуется осуществлять смену пароля доступа к Системе не реже одного раза в 3 месяца.
1.4.5 При возникновении подозрений, что Ваш пароль стал известен третьим лицам, необходимо незамедлительно сменить пароль или заблокировать доступ в Систему, обратившись в Банк по телефону техподдержки.
В случае утраты, а так же при возникновении любых подозрений, что Ваши логин и пароль стали известны третьим лицам (в том числе представившихся сотрудниками Банка) незамедлительно заблокируйте Вашу учетную запись в Систему. Вы можете сделать это, связавшись с Банком по телефону техподдержки.
1.5 Остерегайтесь мошенничества:
1.5.1 Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по СМС или e-mail с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, кодовое слово, Ф.И.О., паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли и другие конфиденциальные данные). Не отвечайте на такие сообщения.
1.5.2 Банк никогда не связывается с просьбой установить или обновить программное обеспечение, в своих электронных письмах никогда не рассылает программы. Не открывайте подозрительные файлы, присланные вам по электронной почте.
1.5.3 При получении подозрительного сообщения якобы от имени Банка не отвечайте на него, не переходите по ссылкам указанным в подозрительном сообщении (даже если адрес похож на адрес сайта Банка). В сообщениях Банка никогда не будет просьбы зайти в Систему по указанной в сообщении ссылке.
1.5.4 При работе с Системой обратите внимание на страницу входа и интерфейс, если вы заметите любые отличия, не заявленные ранее Банком, или возникнут иные причины для возникновения подозрений в том что сайт поддельный, необходимо незамедлительно прекратить работу и обратиться в Банк по телефону техподдержки (никогда не связывайтесь по телефону указанному на подозрительной странице).
1.5.5 Если вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в Систему.
1.5.6 Банк никогда не направляет сообщений о блокировке/разблокировке Вашей учетной записи в Систему. Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности Системы вследствие проведения каких-либо регламентных работ. Если вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону техподдержки (никогда не связывайтесь с Банком по телефону указанному в подозрительном сообщении).
1.5.7 Обращайте внимание на появление подозрительной активности на Вашем компьютере, например, самопроизвольные движение курсора на экране, набор текста и т.п. Обращайте внимание на невозможность зайти на сайт Системы, при том, что другие Интернет-сайты у Вас загружаются, а так же на невозможность войти в Систему по причине несовпадения логина и пароля, при том, что они корректны. Обращайте внимание на «зависания» Системы, при нормальной работе других Интернет сайтов. Данные факты могут свидетельствовать о заражении Вашего компьютера вредоносными программами. Избегайте работы в Системе с зараженных компьютеров, если на зараженном компьютере уже осуществлялась работа в Системе, то незамедлительно заблокируйте Вашу учетную запись в Системе. Вы можете сделать это, связавшись с Банком по телефону техподдержки.
1.5.8 В случае если, по Вашему мнению, произошло несанкционированное списание денежных средств, необходимо незамедлительно обратиться в Банк с сообщением о несанкционированном списании. В случае если операция не совершалась ни Клиентом, ни его Представителем, а так же имеются иные признаки незаконного завладения денежными средствами (кражи) с использованием Системы, то после обращения в Банк Вам рекомендуется оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава

21 УК РФ). После чего предоставить в Банк копию заявления о возбуждении уголовного дела, либо копию талона-уведомления, подтверждающего непосредственное обращение в правоохранительные органы и содержащего порядковый номер из книги учета сообщений о преступлениях содержащую отметку правоохранительного органа о его приеме.

Помните, что Ваше оперативное обращение в Банк может предотвратить несанкционированное списание, либо приостановить списание денежных средств, снизив Ваши финансовые потери.

2. При эксплуатации средств защиты информации

2.2 Рекомендации по организационному обеспечению безопасности средств защиты информации (далее - СЗИ):

- в организации Клиента выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СЗИ;
- в организации Клиента разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СЗИ;
- к работе с СЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СЗИ.

2.3 Рекомендации по размещению СЗИ и режиму охраны:

- помещения, в которых размещаются технические средства клиентского рабочего места со встроенными СЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ;
- размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;
- размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
- входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;
- окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией;
- размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна;
- в режимные помещения допускаются руководители организации Клиента, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов;
- системные блоки компьютеров с СЗИ оборудуются средствами контроля вскрытия;
- ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СЗИ.

2.4 Рекомендации по обеспечению безопасности ключевой информации:

- необходимо по возможности производить резервное копирование рабочих ключевых носителей с ключами АСП;
- ключевые носители в организации Клиента берутся на поэкземплярный учет в выделенных для этих целей журналах;
- учет и хранение ключей поручается руководством Клиента специально выделенным сотрудникам;
- для хранения ключевых носителей с ключами АСП выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
- хранение ключей допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное применение, не предусмотренное правилами пользования СЗИ;
- ключевые носители с рабочими ключами (копиями рабочих ключей) хранятся раздельно с обеспечением условия невозможности их одновременной компрометации;
- при транспортировке ключевых носителей с секретной ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию**.**

3. При использовании мобильных устройств (телефонов, смартфонов, КПК, планшетов и т.п.) с подключенной услугой «Мобильный банк»

- не оставляйте свое мобильное устройство без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг. Установите на устройстве пароль, данная возможность доступна для любых современных мобильных устройств.
- при потере мобильного устройства подключенной услугой «Мобильный банк» Вам следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Банка для блокировки услуги «Мобильный банк**».**

Помните, что в случае потери или кражи мобильного устройства, «новый» владелец получит возможность присвоить все средства с вашего счета в банке.

- при смене номера телефона, на который подключена услуга «Мобильный банк», Вам необходимо отключить услугу «Мобильный банк» от старого номера телефона и подключить услугу на новый номер, так как операторы сотовой связи могут передать номер телефона другому абоненту, если он будет неактивным длительное время.
- при внезапном прекращении работы SIM-карты необходимо обратиться к оператору сотовой связи за уточнением причин — в отношении Вас возможно проведение мошеннических действий третьими лицами.
- не подключайте к услуге «Мобильный банк» устройства, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников Банка.
- при подозрении, что от Вашего имени осуществляются несанкционированные Вами операции, Банк по своей инициативе может временно заблокировать услуги Мобильный Банк. Для возобновления потребуется связаться с Банком и подтвердить легитимность подключения и сделанных операций.
- не переходите по ссылкам, приходящим из недостоверных источников, в том числе на известные сайты. Также не стоит переходить по ссылкам и устанавливать приложения/обновления безопасности, пришедшие по SMS/электронной почте, в том числе от имени Банка.
- не скачивайте на устройство мобильной связи приложения из непроверенных источников.
- при установке на устройство дополнительных программ обращайте внимание на полномочия, которые необходимы программе. Если программе требуются излишние полномочия это повод проявить настороженность. Обращайте внимание на такие опасные разрешения: доступ и отправка SMS, доступ к Интернет.
- установите на телефон антивирусное ПО и своевременно его обновляйте.
- не взламывайте телефон (например, через Jailbreaking), так как это отключает защитные механизмы, заложенные производителем. В результате ваш телефон становится уязвимым к заражению вирусным ПО.
- отключайте в настройках вашего iPhone возможность использовать голосовое управление Siri на заблокированном экране.

Приложение № 3
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

ПРОЦЕДУРА ПОДТВЕРЖДЕНИЯ ДОСТОВЕРНОСТИ ДОКУМЕНТА

1. При невозможности разрешения спора в отношении авторства и/или подлинности документа, подписанного электронной подписью, путем переговоров, Банк обращается к разработчику Системы, имеющему эталон программного обеспечения Системы (далее - Разработчик), с письменным заявлением о проведении экспертизы для разрешения спора.
Разработчик принимает участие в урегулировании разногласий между Сторонами при условии заблаговременного предоставления Разработчику всех документов, касающихся возникших разногласий, документов, подтверждающих полномочия Сторон, государственную регистрацию Сторон, а также иных документов, дополнительно затребованных Разработчиком.
Заключение об авторстве и/или подлинности электронного документа делается только представителями Разработчика и признается Сторонами Договора достаточным и окончательным для разрешения спора.

2. Документы направляются Разработчику Банком в недельный срок с момента поступления письменного заявления от заинтересованной Стороны.

3. Для разрешения спора о подлинности документа, подписанного секретным ключом, заинтересованная Сторона предоставляет:
1) спорный документ в электронном виде;
2) спорный документ на бумажном носителе;
3) документ о признании электронной подписи (с использованием секретного ключа и сертификата), подписанный Клиентом, с указанием идентификатора сертификата (DN) Клиента.

4. Подтверждением подлинности электронного документа является единовременное наличие следующих условий:
1. подтверждена подлинность секретного ключа, использованного для подписи спорного документа;
2. подтверждена целостность спорного документа;
3. идентификатор сертификата (DN), содержащийся в документе о признании электронной подписи, и идентификатор сертификата (DN), полученный в результате работы Эталонного Модуля Проверки подписи документа, совпадают;
4. получен положительный результат проверки спорного документа на соответствие технологии Системы.
В указанном случае Разработчиком составляется заключение о признании подлинности документа, подписанного секретным ключом.

5. При отсутствии одного или нескольких из вышеперечисленных условий (п.4), Разработчиком составляется заключение о не признании подлинности документа, подписанного секретным ключом. Заключение Разработчика является доказательством при дальнейшем разбирательстве спора.

Приложение № 4
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

АГЕНТУ Удостоверяющего центра «AUTHORITY»
АО "ЭКСПЕРТ БАНК"
/ в Удостоверяющий центр «AUTHORITY»

Заявление на выдачу Сертификата ключа проверки электронной подписи

Прошу Удостоверяющий центр «AUTHORITY» создать и выдать уполномоченному лицу организации ООО "Наименование Организации" (наименование организации), действующ (-ему) (-ей) на основании _____, *Сертификат ключа проверки электронной подписи (Класс 2 Сертификата)* с параметром *Идентификатора владельца сертификата:* CN=Ivanov Ivan Ivanovich, O=OOO Naimenovanie Organizacii', L=Novosibirsk, C=RU Уникальный номер запроса (только для удаленной выдачи): _____.

С Правилами *Электронного документооборота* корпоративной информационной *Системы «BeSafe»* (далее - *«Система «BeSafe»*), которые расположены в сети Интернет по адресу www.besafe.ru, ознакомлены, согласны и обязуемся выполнять.

Признаем, что получение документа, подписанного *Электронной подписью Участника Системы "BeSafe"* (далее - *«Участник»*), юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц *Участника* и оттиском печати *Участника*. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что *Ключ электронной подписи, Электронная подпись* и *Сертификат ключа проверки электронной подписи Участника* созданы в соответствии с Правилами *Системы «BeSafe»*.

Реквизиты *Клиента:*

ФИО уполномоченного лица организации	*Иванов Иван Иванович*
Наименование организации	*ООО " Наименование Организации "*
Контактный телефон	X-XXX-XXX-XX-XX
E-mail	mail@mail.com

Настоящим соглашаюсь с обработкой своих персональных данных ЗАО «Центр Цифровых сертификатов» и признаю, что персональные данные, заносимые в Сертификаты, относятся к общедоступным персональным данным.

_____ (подпись уполномоченного лица организации)
Иванов Иван Иванович (Ф.И.О. уполномоченного лица организации)

М.П. (если применимо)

принято *Агентом Удостоверяющего центра/ Удостоверяющим центром*:
АО "ЭКСПЕРТ БАНК" (полное наименование)
_____ (дата)
_____ (подпись уполномоченного лица)
_____ (ФИО уполномоченного лица)
М.П.__

Приложение №5
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

АКТ ПРИЕМА - ПЕРЕДАЧИ *СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (ПРИМЕР)*

г._____ "__" _____ 20__ г.

Юридическое лицо Общество с ограниченной ответственностью "Примерный", именуемое в дальнейшем Клиент", представленное своим уполномоченным лицом Иванов Иван Иванович с одной стороны, и АО "ЭКСПЕРТ БАНК", именуемое в дальнейшем "Агент", в лице Петров Петр Петрович, действующ(-его)(-ей) на основании _____, с другой стороны, в соответствии с Правилами работы Удостоверяющего Центра «AUTHORITY», составили настоящий Акт приема - передачи о следующем:

1. Агент произвел проверку данных Клиента, Удостоверяющий центр осуществил изготовление Сертификата ключа проверки электронной подписи (далее - «Сертификат») и передал 22.12.2017 Сертификат Клиенту, а Клиент принял оригинал следующего Сертификата на Ключевой носитель:

Идентификатор *Владельца сертификата*	CN=Ivanov Ivan Ivanovich, O=Obshhestvo s ogranichennojj otvetstvennostju 'Primerniy', L=Tjumen, C=RU
Номер *Сертификата*	3c5c013
Алгоритм подписи	SHA1withRSA
Заверен	CN=Class 2 CA, O=Center of Financial Technologies, C=RU
Годен с	22-12-2017
Годен до	22-12-2018
Алгоритм *Ключа проверки электронной подписи*	ГОСТ Р 34.10-20XX
Ключ проверки электронной подписи	03 60 39 f1 52 17 91 ab 1f 21 c7 20 13 41 77 cc 26 63 c4 a3 ec 51 e5 98 ed ca 6e b1 24 c9 20 cb cb f5 1a 19 91 ce ab 64 76 82 01 ac f7 b2 85 83 f8 c4 07 f2 01 24 b8 6d 52 65 7b 2b 9d 91 54 ad 21 c1
Алгоритм отпечатка	SHA-1
Отпечаток	32 9c be c1 02 49 33 02 12 0f 19 2f bb 32 0f ec 15 ea ef 58

2. Обязательства Агента перед Клиентом выполнены в точном соответствии с Правилами работы Удостоверяющего Центра «AUTHORITY», претензий у Клиента не имеется.

От АГЕНТА

_____ (Петров Петр Петрович)
фио

М.П.

От КЛИЕНТА

_____ (Иванов Иван Иванович)
фио

М.П.

Приложение № 6
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

УВЕДОМЛЕНИЕ
об отмене действия ключей электронной подписи

_____
(наименование клиента)

уведомляет АО «Эксперт Банк» о том, что с «_____ » _____ 20___г.

считать недействительными ключи электронной подписи со следующими номерами:

_____
(перечислить номера сертификатов (см. Приложение № 5 к Условиям)

_____/_____/
(должность) *(ФИО)*

М. П.

Отметка Банка:

Ключи выведены из действия
Дата: _____
Время: _____
Подпись: _____/_____/

Банк:

_____/_____/
М.П.

Клиент:

_____/_____/
М.П.

Приложение № 7
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

Заявка на подключение Интернет-банка с использованием системы Faktura.ru и получение Смарт-карты

Реквизиты Клиента

Полное наименование Организации		
ИНН/КПП		
Должность Руководителя		
Ф.И.О.		
Страна, город		
Адрес регистрации /в соответствии с Уставом/		
Адрес местонахождения исполнительного органа		
Телефон /с кодом города/		
Факс /с кодом города/		
E-mail		
IP адрес организации	□ Динамический	□ Статический, укажите IP ___.___.___.___
При наличии статического IPадреса, желаете ли ограничить этим IP адресом вход в ДБО?	□ДА	□НЕТ

1.Просим Вас предоставить устройство хранения секретного ключа Смарт-карту в количестве _____шт. (_____), для использования в электронном документообороте по системе ДБО.

2.Просим зарегистрировать следующих лиц в качестве уполномоченных лиц Клиента для работы в системе Faktura.ru (заполняется на каждое лицо):

2.1. ФИО полностью _____

Должность сотрудника _____

Ответственное лицо, определяющее права доступа сотрудников (Да/Нет) _____

Права по счетам (да\нет)	**Номер счета**		
создавать платежные документы			
подтверждать остатки по счету			
запрашивать выписку			
зачисление средств в заявлении на конверсию валюты			
создавать распоряжения по списанию валютной выручки с транзитного счета			
списание средств в заявлении на конверсию валюты			
подписывать и отправлять документы. приоритет подписи			
Права по документам (да\нет)			
создание документов валютного контроля			
создание документов свободного формата			
создание заявлений на депозит			
создание реестров на перечисление заработной платы			

2.2. ФИО полностью _____

Должность сотрудника _____

Ответственное лицо, определяющее права доступа сотрудников (Да/Нет) _____

Права по счетам (да\нет)	**Номер счета**		
создавать платежные документы			
подтверждать остатки по счету			
запрашивать выписку			

зачисление средств в заявлении на конверсию валюты			
создавать распоряжения по списанию валютной выручки с транзитного счета			
списание средств в заявлении на конверсию валюты			
подписывать и отправлять документы. приоритет подписи			
Права по документам (да\нет)			
создание документов валютного контроля			
создание документов свободного формата			
создание заявлений на депозит			
создание реестров на перечисление заработной платы			

При наличии в организации лиц, обладающих правом подписи, комплект ключей предоставляется по количеству подписей: по одному ключу каждому лицу, которому принадлежит право подписи. ЭПД подписывается подписями, сочетание которых установлено соглашением к договору банковского счета, заключенному между Клиентом и Банком. Право подписи документов предоставляется только лицам, указанным в Карточке с образцами подписей и оттиска печати в соответствии с предоставленными им полномочиями.

3.Просим сохранить (изменить) полномочия в системе Faktura.ru ранее зарегистрированных лиц.

ФИО полностью _____

Должность сотрудника _____

Ответственное лицо, определяющее права доступа сотрудников (Да/Нет) _____

Права по счетам (да\нет)	**Номер счета**		
создавать платежные документы			
подтверждать остатки по счету			
запрашивать выписку			
зачисление средств в заявлении на конверсию валюты			
создавать распоряжения по списанию валютной выручки с транзитного счета			
списание средств в заявлении на конверсию валюты			
подписывать и отправлять документы. приоритет подписи			
Права по документам (да\нет)			
создание документов валютного контроля			
создание документов свободного формата			
создание заявлений на депозит			
создание реестров на перечисление заработной платы			

4.Кодовое слово/фраза:_____(заполняется Клиентом).

Кодовое слово/фраза меняется по мере необходимости по заявлению Клиента.

Должность: _____Ф.И.О.

«___» _____ 20___ г.

Подпись:_____

М.П.

ОТМЕТКИ БАНКА

Реквизиты организации и полномочия лиц с правом подписи, соответствуют Карточке с образцами подписей и оттиска печати Клиента:

_____ _____

(ФИО сотрудника) *(подпись)*

Дата принятия заявления: «____» _____ 20_____г.

Приложение №8
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

Заявка на подключение Интернет-банка банка с использованием системы Faktura.ru по технологии одноразовых паролей

Реквизиты Клиента

Полное наименование Организации:	
ИНН/КПП	
Должность Руководителя	
Ф.И.О.	
Страна, город	
Адрес регистрации /в соответствии с Уставом/	
Адрес местонахождения исполнительного органа	
Телефон /с кодом города/	
Факс /с кодом города/	
E-mail	

1. Просим Вас предоставить логин для входа в Интернет-банк для использования в электронном документообороте по системе ДБО.

2. Просим зарегистрировать следующих лиц в качестве уполномоченных лиц Клиента для работы в системе Faktura.ru (заполняется на каждое лицо):

2.1.ФИО полностью_____

Должность сотрудника_____

Ответственное лицо, определяющее права доступа сотрудников (Да/Нет) _____

Права по счетам (да\нет)	**Номер счета**		
создавать платежные документы			
подтверждать остатки по счету			
запрашивать выписку			
зачисление средств в заявлении на конверсию валюты			
создавать распоряжения по списанию валютной выручки с транзитного счета			
списание средств в заявлении на конверсию валюты			
подписывать и отправлять документы. приоритет подписи			
Права по документам (да\нет)			
создание документов валютного контроля			
создание документов свободного формата			
создание заявлений на депозит			
создание реестров на перечисление заработной платы			

2.2.ФИО полностью _____

Должность сотрудника _____

Ответственное лицо, определяющее права доступа сотрудников (Да/Нет) _____

Права по счетам (да\нет)	**Номер счета**		
создавать платежные документы			

подтверждать остатки по счету			
запрашивать выписку			
зачисление средств в заявлении на конверсию валюты			
создавать распоряжения по списанию валютной выручки с транзитного счета			
списание средств в заявлении на конверсию валюты			
подписывать и отправлять документы. приоритет подписи			
Права по документам (да\нет)			
создание документов валютного контроля			
создание документов свободного формата			
создание заявлений на депозит			
создание реестров на перечисление заработной платы			

При наличии в организации лиц, обладающих правом подписи, комплект ключей предоставляется по количеству подписей: по одному ключу каждому лицу, которому принадлежит право подписи. ЭПД подписывается подписями, сочетание которых установлено соглашением к договору банковского счета, заключенному между Клиентом и Банком. Право подписи документов предоставляется только лицам, указанным в Карточке с образцами подписей и оттиска печати в соответствии с предоставленными им полномочиями.

3.Просим сохранить (изменить) полномочия в системе Faktura.ru ранее зарегистрированных лиц.

ФИО полностью _____

Должность сотрудника _____

Ответственное лицо, определяющее права доступа сотрудников (Да/Нет) _____

Права по счетам (да\нет)	**Номер счета**		
создавать платежные документы			
подтверждать остатки по счету			
запрашивать выписку			
зачисление средств в заявлении на конверсию валюты			
создавать распоряжения по списанию валютной выручки с транзитного счета			
списание средств в заявлении на конверсию валюты			
подписывать и отправлять документы. приоритет подписи			
Права по документам (да\нет)			
создание документов валютного контроля			
создание документов свободного формата			
создание заявлений на депозит			
создание реестров на перечисление заработной платы			

4.Кодовое слово/фраза:_____ **(заполняется Клиентом).**

Кодовое слово/фраза меняется по мере необходимости по заявлению Клиента.

5.Номер мобильного телефона (используется для получения первоначального пароля доступа к Системе и Одноразовых паролей для подтверждения совершения операций)

+7										

6.Адрес электронной почты

Настоящим заявляю о присоединении к настоящим Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru. Все разделы Условий, включая действующие Тарифы разъяснены мне в полном объеме.

Должность: _____Ф.И.О

«___» _____ 20___ г.

Подпись:_____

М.П.

ОТМЕТКИ БАНКА

Реквизиты организации и полномочия лиц с правом подписи, соответствуют Карточке с образцами подписей и оттиска печати Клиента:

_____ _____
(ФИО сотрудника) *(подпись)*

Дата принятия заявления: «____» _____ 20_____г.

Логин (используется для получения доступа к Системе и приостановления обслуживания):

Учетная запись клиента активирована “____” _____ 20__ г.

Номер договора _____

Приложение № 9

к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

Акт приема-передачи Смарт-карты для входа в Интернет-банк

«___» _____ 20___г.

Настоящим Актом подтверждается, что АО «Эксперт Банк», именуемое в дальнейшем Банк, в лице _____, действующего на основании _____передал, а _____, именуемое в дальнейшем Клиент, в лице _____, действующего на основании _____ получил, устройство - Смарт-карту, в количестве _____ штук для использования его в рамках Договора о дистанционном банковском обслуживании с использованием Системы Faktura.ru **№ NUMDOG_DBO1 от DATEDOG_STR_DBO1 г.** в качестве Средства формирования и проверки электронной подписи (далее – «ЭП»).

Номер Смарт-карты: _____.

Первоначальный код доступа к Смарт-карте (PIN):_____.

Код разблокировки доступа к Смарт-карте:_____.

После получения Смарт-карты Клиент обязуется сменить первоначально заданные Банком коды доступа к Смарт-карте и её разблокирования.

Клиент подтверждает, что корпус переданного Устройства не имеет видимых признаков повреждения и взлома.

Клиент обязуется использовать и хранить Смарт-карту в соответствии с установленными **Правилами и требованиями по работе со Смарт-картой (Приложение 1 к настоящему Акту)**.

Клиент проинформирован о сроке действия лицензии шифрования ЭП, встроенной в него, по истечении которой Клиент обязуется произвести замену **Смарт-карты** за свой счет.

Клиент подтверждает, что будет использовать Смарт-карту в соответствии с техническими требованиями договора.

Клиент согласен, что для использования Смарт-карты необходимо установить на своем рабочем месте (местах) программные настройки с сайта: http://www.faktura.ru.

В работе со Смарт-картой Клиент обязуется использовать инструкцию по работе со Смарт-картой, размещенную на сайте http://www.faktura.ru.

Настоящий акт составлен на 1 странице в двух экземплярах, имеющих одинаковую юридическую силу.

От Банка передал:	**От Клиента получил:**
_____ /_____/	_____ / _____ /
« ___» _____ 20__ г.	«___ » _____20__г.
М.П.	М.П.

Приложение 1
к Акту приема-передачи Смарт-карты
от “___” _____ 20___ г.

Правила и требования по работе со Смарт-картой

Общие сведения о Смарт-карте

Смарт-Карта имеет сертификат ФСБ о соответствии требованиям, предъявляемым к СКЗИ по классу КС2 и к средствам ЭП в соответствии с № 63-ФЗ от 06.04.2011 г. «Об электронной подписи», а также сертификат ФСТЭК о соответствии требованиям, предъявляемым по 4-му уровню контроля отсутствия недекларированных возможностей (НДВ4).

Объем доступной перепрограммируемой памяти EEPROM составляет 64 килобайта.

- Поддержка алгоритма ГОСТ Р 34.10-2001: генерация ключевых пар с проверкой качества, импорт ключевых пар, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет.
- Поддержка алгоритма ГОСТ 34.11-94: Вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП.
- Поддержка алгоритма ГОСТ Р 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).
- Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357), расшифрование по схеме EC El-Gamal.
- Поддержка алгоритма RSA: поддержка ключей размером до 2048 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи.
- Генерация последовательности случайных чисел требуемой длины.

Назначение и область применения Смарт-карты

Смарт-карта подключается к компьютеру и не требует для работы дополнительного оборудования.

Использование Смарт-карты делает принципиально невозможным хищение секретных ключей ЭП, используемых при работе в системе «Faktura.ru». В том числе при работе в «недоверенной» программной среде.

Секретный ключ ЭП генерируется внутри Смарт-карты, хранится в защищенной памяти Смарт-карты и никогда, никем и ни при каких условиях не может быть из Смарт-карты скопирован.

Формирование ЭП клиента происходит в соответствии с ГОСТ Р34.10-2001 непосредственно внутри Смарт-карты: на вход – ключ принимает электронный документ, на выходе выдает ЭП под данным документом.

Доступ ко всем криптографическим функциям Смарт-карты предоставляется только после ввода пользователем корректного PIN-кода.

Подготовка Смарт-карты к работе

Перед началом работы со Смарт-картой пользователю необходимо предварительно настроить компьютер со Смарт-картой в системе с сайта: http://www.faktura.ru

Важно!

Не передавайте Смарт-карту третьим лицам! Не сообщайте третьим лицам PIN-код доступа к секретному ключу ЭП! В случае утери (хищения) Смарт-карты немедленно свяжитесь с банком.

Приложение № 10
к Условиям предоставления и дистанционного банковского обслуживания с использованием Системы Faktura.ru

Памятка пользователя Системы дистанционного банковского обслуживания с использованием Системы Faktura.ru в АО ”Эксперт Банк” с использованием технологии одноразовых паролей.

Соблюдайте правила безопасности при работе в Faktura.ru:
УБЕДИТЕСЬ в наличии символа замка в правом нижнем углу веб-страницы или справа/слева от адресной строки. Этот символ указывает на то, что веб-сайт работает в защищенном режиме.
ПРИ СОСТАВЛЕНИИ ПАРОЛЯ Соблюдайте следующие требования:

- Пароль не должен содержать менее 8-ми знаков;
- Пароль должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы (@,#,$,%,^,&,*)

ЗАПОМНИТЕ, что для входа в Интернет-банк вам требуется вводить только ваш ЛОГИН и ПАРОЛЬ. НЕ НУЖНО вводить номер вашего мобильного телефона, номер вашего счета для входа или дополнительной проверки персональной информации в Интернет-банке.
НИКОГДА и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в Интернет-банк или для подтверждения платежей.
ИСПОЛЬЗУЙТЕ виртуальную клавиатуру для ввода пароля.
В СЛУЧАЕ УТЕРИ мобильного телефона, на который приходят SMS-сообщения с разовым паролем, немедленно заблокируйте SIM-карту.
БУДЬТЕ БДИТЕЛЬНЫ:
в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в банк с целью оперативного блокирования доступа.

Устанавливаются следующие требования к оборудованию рабочего места Клиента:

- Установленное лицензионное программное обеспечение антивирусной защиты, с актуальным обновлением вирусной базы.
- Доступ к сети Интернет. Клиент самостоятельно настраивает все аппаратные и программные средства для обеспечения возможности работы с сетью Интернет по протоколам http, https.

СЛУЖБА ПОДДЕРЖКИ Faktura.ru - support@faktura.ru

Телефоны круглосуточной клиентской поддержки Faktura.ru: 8-800-200-92-50

Телефоны круглосуточной клиентской поддержки Банка: 8-800-333-31-31

Адреса сети Интернет для доступа к Системе:

Адрес web-сайта Банка: **http://www.expertbank.com**
Адрес сервиса Faktura.ru: **https://faktura.ru/b2b/pages**