УТВЕРЖДЕНО
Правлением ООО «Крона-Банк»
Протокол № 21 от «20» мая 2020 г.

УСЛОВИЯ
дистанционного банковского обслуживания в ООО «Крона-Банк» с использованием электронной системы «Интернет-Банк»

(вводятся в действие с 11 июня 2020 года)

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификация – удостоверение правомочности обращения Клиента в Банк для совершения банковских операций и/или получения информации по Счетам дистанционно и совершения иных действий в порядке, предусмотренном настоящими Условиями.

Аутентификация входа – процедура проверки соответствия предъявленных Базовых аутентификационных данных и Одноразового ключа (при наличии), либо Цифрового кода/Touch ID, выполняемая перед установлением Сеанса связи. Без успешной Аутентификации входа Сеанс связи не устанавливается.

Аутентификация операции – процедура проверки принадлежности Клиенту полученного Банком посредством Системы электронного документа (ЭД), выполняемая во время сеанса связи с использованием ЭП.

Банк – Общество с ограниченной ответственностью «Крона-Банк» (ООО «Крона-Банк»).

Договор банковского счета – договор банковского счета, в соответствии с которым открыт Счет, заключенный в соответствии со ст. 428 Гражданского кодекса Российской Федерации, представляющий собой совокупность документов: Условия открытия и обслуживания банковских счетов юридических лиц, индивидуальных предпринимателей и лиц, занимающихся частной практикой, в ООО «Крона-Банк», и Заявления о присоединении к указанным Условиям.

Договор о ДБО – договор о дистанционном банковском обслуживании с использованием электронной системы «Интернет-Банк», заключенный между Банком и Клиентом, состоящий из настоящих условий с соответствующими приложениями и Заявления о присоединении к настоящим Условиям.

E-mail-сообщение – сообщение, сформированное в рамках стандарта RFC 2822, используемое для передачи информации в сетях, работающих по протоколу TCP/IP.

Клиент – юридическое лицо/индивидуальный предприниматель/физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой (адвокат, учредивший адвокатский кабинет, арбитражный управляющий, нотариус), заключивший с Банком Договор о ДБО.

Ключ проверки ЭП - уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП (далее – проверка ЭП).

Ключ ЭП – уникальная последовательность символов, предназначенная для создания ЭП.

Компрометация ключа – утрата доверия к тому, что используемые ключи ЭП недоступны посторонним лицам. К событиям, связанным с компрометацией ключей относятся следующие:

- утрата носителей ключевой информации;
- увольнение работников, имевших доступ к ключевой информации;
- временный доступ посторонних лиц к ключевой информации;
- иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к ключу ЭП неуполномоченных лиц.

Контролирующая организация - Клиент Банка – субъект хозяйственной деятельности (хозяйственное общество/индивидуальный предприниматель), являющийся основным по отношению

к иному субъекту хозяйственной деятельности (Контролируемая организация) в силу требований законодательства и/или заключенного между такими субъектами договора и/или в связи с иными особенностями ведения предпринимательской деятельности.

Контролируемая организация - Клиент Банка – субъект хозяйственной деятельности (хозяйственное общество, индивидуальный предприниматель, обособленное/структурное подразделение Контролирующей организации), являющийся контролируемым со стороны Контролирующей организации в силу требований законодательства и/или заключенного между такими субъектами договора и/или в связи с иными особенностями ведения предпринимательской деятельности, и предоставивший в Банк в предусмотренном настоящими Условиями порядке согласие на осуществление Контролирующей организацией в отношении его платежей по счетам Функции контроля за платежами.

Корпоративная информационная система «BeSafe» (КИС «BeSafe», Система) - система организованная Закрытым акционерным обществом «Центр Цифровых Сертификатов» (ИНН 5407187087) для обеспечения договорных и технологических условий формирования и развития финансового и информационного электронного обслуживания и представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот в соответствии с Правилами электронного документооборота корпоративной информационной системы «BeSafe» (далее – Правила). Актуальная версия Правил размещена в сети Интернет по адресу www.besafe.ru.

Логин – состоящий из латинских букв и/или цифр (также при наличии технической возможности – прочих символов), позволяющий Банку однозначно идентифицировать Клиента. В числе идентификаторов может выступать номер мобильного телефона Клиента. Допускается наличие у Клиента более одного Логина. Действие, совершенное Клиентом под любым из своих логинов, считается совершенным Клиентом лично.

Получение нового Логина Клиентом допускается как с сохранением действующего Логина Клиента, так и с его блокировкой. Получение Клиентом нового Логина в обязательном порядке сопровождается установкой Клиентом пароля к новому Логину.

Мобильное приложение – приложение для мобильных устройств Клиентов, являющееся одним из каналов ДБО системы «Интернет-Банк», позволяющая Клиентам управлять своими счетами, получать выписки, совершать операции по переводам денежных средств и платежи, получать информацию по оформленным кредитам и депозитам, заказывать банковские услуги. Полный перечень услуг доступен в системе «Интернет-Банк».

Мобильное устройство – мобильное устройство (телефон, смартфон, планшет и т.п.) на базе операционных систем iOS и Android, на которое устанавливается Мобильное приложение.

Одноразовый код – уникальная последовательность символов, предназначенная для подтверждения операций в Мобильном приложение, направленная Банком Клиенту в виде SMS-сообщения на номер мобильного телефона, зарегистрированный в Банке для целей получения Клиентом Одноразового кода.

Клиент обязан не допускать ситуации переполнения памяти Мобильного устройства, что может стать препятствием для приема SMS-сообщений с Одноразовым кодом.

Пароль – секретная последовательность символов, которая известна только Клиенту. Пароль позволяет убедиться в том, что обратившееся лицо действительно является владельцем представленного Логина. Пароль является электронной подписью Клиента в отношениях Клиента и Банка в рамках сервиса и подтверждает от имени Клиента правильность, неизменность и целостность электронного документа.

Разрешается изменение Пароля Клиентом с использованием средств Системы.

Подтверждение подлинности электронной подписи в электронном документе - положительный результат проверки соответствующим средством электронной подписи с использованием сертификата ключа проверки ЭП принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки ЭП и отсутствия искажений в подписанном данной электронной подписью электронном документе.

PIN-код – код, используемый для входа в Мобильное приложение и подтверждения операций в Мобильном приложении.

PUSH-сообщение – сообщение, используемое для передачи информации с использованием сети Интернет на мобильное устройство под управлением операционных систем iOS, Android OS

(по технологиям Apple Push Notification Service и Google Cloud Messaging). Для приема PUSH-сообщения необходимо иметь на мобильном устройстве установленное программное обеспечение «Мобильное приложение».

Сервис Faktura.ru (система «Интернет-Банк»)/Система – информационно-технологический сервис, позволяющий Сторонам организовать обмен электронными документами, сведениями и прочей информацией, имеющей значение для Сторон.

Сервис «Обмен электронными документами» сети ЦФТ – процессинг» - сервис КИС «BeSafe», предоставляемый оператором сервиса ЗАО «Биллинговый центр» (ИНН 5401152049). Сервис предоставляется в соответствии с Правилами работы сервиса «обмен электронными документами сети «ЦФТ – процессинг» и правилами работы сети «ЦФТ-процессинг».

Сертификат ключа проверки ЭП - электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром либо Уполномоченным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

СКЗИ - сертифицированные средства криптографической защиты информации (сертифицированные криптографические средства), используемые в системе «Интернет-Банк» и программных средствах.

Смарт-ключ «Рутокен» – средство криптографической защиты информации, выполненное в форм-факторе USB-устройства, предназначенное для криптографической защиты информации.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание Ключа ЭП и Ключа проверки ЭП.

Стороны - Банк и Клиент.

Счет - банковский счет в валюте Российской Федерации или в иностранной валюте, открываемый Банком Клиенту на основании заключенного между Банком и Клиентом Договора банковского счета, по которому Банк осуществляет расчетно-кассовое обслуживание Клиента в соответствии с действующим законодательством Российской Федерации и Договором банковского счета.

Тарифы Банка – Тарифы на услуги для юридических лиц и индивидуальных предпринимателей ООО «Крона-Банк».

Удостоверяющий центр (УЦ) – удостоверяющий центр (удостоверяющий центр «Authority»), созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов», который осуществляет изготовление цифровых сертификатов для юридических и физических лиц для возможности осуществления электронного документооборота в рамках КИС «BeSafe». Удостоверяющий центр осуществляет изготовление цифровых сертификатов в соответствии с «Правилами работы Удостоверяющего центра (AUTHORITY)». Актуальная версия указанных Правил размещена в сети Интернет по адресу www.authority.ru.

Уполномоченное лицо Удостоверяющего центра – ООО «Крона-Банк» /Банк.

Уполномоченное лицо Клиента – индивидуальный предприниматель/физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой (адвокат, учредивший адвокатский кабинет, арбитражный управляющий, нотариус), руководитель, главный бухгалтер или физическое лицо, уполномоченное распоряжаться счетом Клиента на основании доверенности или распорядительного акта Клиента и включенное в Карточку с образцами подписей и оттиска печати, и одновременно уполномоченные на использование аналога собственноручной подписи (в соответствии с требованиями нормативных актов Банка России).

Условия – настоящие Условия дистанционного банковского обслуживания с использованием электронной системы «Интернет-Банк».

Электронный документ (ЭД) - документ, в котором информация представлена в электронно-цифровой форме в формате, определенном Банком.

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. Под ЭП понимается неквалифицированная усиленная ЭП в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Условия дистанционного банковского обслуживания с использованием электронной системы «Интернет-Банк» являются договором присоединения в соответствии со ст. 428 Гражданского кодекса Российской Федерации. Клиент присоединяется к Условиям путем подписания Заявления о присоединении к Условиям без каких-либо изъятий и оговорок.

2.2. Настоящие Условия регулируют обмен ЭД, подписанными ЭП, между Банком и Клиентом при: осуществлении расчётов через Банк; получении сведений о движении средств по счетам Клиента, открытым в Банке; осуществлении информационной поддержки Клиента; обмен иной информацией между Клиентом и Банком; а также устанавливают обязательства Сторон по обеспечению информационной безопасности при обмене ЭД.

Технология защиты информации базируется на использовании СКЗИ и гарантирует достоверность и защиту передаваемой информации.

Использование согласованного Сторонами метода криптографической защиты, должно обеспечивать, что никакие помехи в каналах связи и прочие физические воздействия не приведут к каким-либо изменениям в исходных платёжных документах, либо повреждённые документы не будут приняты банковской системой к обработке.

2.3. Банк и Клиент признают систему защиты информации, используемую в Системе, достаточной для защиты от несанкционированного доступа, а также для подтверждения авторства и подлинности ЭД.

2.4. Банк и Клиент имеют право в электронной форме передавать или получать от другой Стороны по системе ДБО любой из электронных документов, перечисленных в Приложении 1 к настоящим Условиям (Виды электронных документов и требования по их оформлению).

ЭД передаются с использованием Системы, при этом обмен документами на бумажных носителях Сторонами не производится, кроме случаев, предусмотренных настоящими Условиями, в частности при возникновении обстоятельств непреодолимой силы или возможных нарушениях работы Системы, а также в иных случаях, предусмотренных соглашениями между Банком и Клиентом.

Стороны признают, что полученные с помощью Системы ЭД юридически эквивалентны документам, составленным на бумажном носителе и заверенным подписями лиц, уполномоченных распоряжаться банковским счетом в соответствии с карточкой образцов подписей и оттиска печати Клиента, и являются основанием для проведения операций по счетам Клиента.

2.5. ЭД порождает обязательства Сторон по нему, если он надлежащим образом оформлен передающей Стороной, заверен ЭП и передан по системе «Интернет-Банк», а принимающей Стороной получен, проверен и расшифрован.

2.6. Стороны обязуются обеспечить допуск к работе в Системе только уполномоченным лицам Клиента в соответствии с Заявлением о присоединении к Условиям и запросами на выдачу сертификатов ключей проверки ЭП.

2.7. Клиент на момент заключения Договора о ДБО, признает факт ознакомления с условиями использования Системы, в том числе с ограничениями способов и мест использования, случаями повышенного риска использования ДБО.

3. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СИСТЕМЕ

3.1. Подключение к Системе производится при наличии у Клиента доступа в Интернет, подключение к которому обеспечивается Клиентом.

3.2. Подключение Клиента к Системе производится на основании предоставленного Клиентом Заявления о присоединении к Условиям дистанционного банковского обслуживания в ООО «Крона-Банк» с использованием электронной системы «Интернет-Банк» (далее – Заявление).

3.3. Создание ключей ЭП, PIN-кодов и секретных паролей осуществляется в соответствии с требованиями Системы.

3.4. Подключение и допуск Клиента к Системе осуществляется в соответствии с Правилами работы сервиса «Обмен электронными документами сети «ЦФТ – процессинг» и Правилами работы сети «ЦФТ-процессинг» на основании заявки Клиента. Сертификат ключа проверки ЭП изготавливается в соответствии с Правилами работы удостоверяющего центра «Authority». Факт выдачи Клиенту Сертификата оформляется Актом приема-передачи (Приложение № 2). Клиент вправе

осуществлять операции и использованием Системы согласно Правилам с момента регистрации Банком Сертификата в Системе.

3.5. Передаваемый Банком Клиенту Сертификат формируется в соответствии с требованиями Системы с учетом требований, установленных действующим законодательством РФ.

3.6. Срок действия Сертификата составляет один календарный год с даты начала действия Сертификата. Сертификат действует в пределах срока должностных полномочий Владельца Сертификата ключа подписи, а в случае их прекращения (без предоставления документов о продлении) автоматически отключается. Продление срока действия Сертификата на новый срок оформляется выдачей нового Сертификата.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Банк обязуется:

4.1.1. Зарегистрировать Клиента в Системе, выдать Уполномоченным лицам Клиента Сертификаты ключей ЭП;

4.1.2. Осуществлять консультативное сопровождение Системы в установленном объёме;

4.1.3. Обеспечивать полную защиту банковской части Системы от несанкционированного доступа третьих лиц и обеспечивать конфиденциальность информации по счетам Клиента;

4.1.4. Принимать к исполнению полученные по Системе ЭД Клиента, оформленные и подписанные (заверенные) Клиентом надлежащим образом, а также осуществлять обработку и исполнение ЭД Клиента в строгом соответствии с установленными нормами, техническими требованиями, стандартами, нормативными актами Банка России и нормативными документами Банка.

4.1.5. Сообщать Клиенту любым доступным Банку способом, в том числе с использованием телефонной связи/электронной почты по соответствующим номерам телефонов/адресам электронной почты, указанным в Заявлении о присоединении к Условиям, а также представленным Клиентом при заключении и исполнении Договора банковского счета, об обнаружении попытки несанкционированного доступа (в том числе и результативной) к Системе ДБО, затрагивающей операции Клиента, не позднее следующего рабочего дня с момента обнаружения попытки.

4.1.6. В случае приостановления операции по переводу денежных средств для проведения контроля в целях предотвращения осуществления перевода денежных средств без согласия Клиента незамедлительно любым доступным Банку способом, в том числе с использованием телефонной связи/электронной почты по соответствующим номерам телефонов/адресам электронной почты, указанным в Заявлении о присоединении к Условиям, а также представленным Клиентом при заключении и исполнении Договора банковского счета:

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

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

4.1.7. Уведомлять Клиента о внесении изменений в настоящие Условия, включая Приложения к ним, – не менее чем за 7 (Семь) календарных дней до введения в действие изменений путем передачи указанной информации с использованием Системы и/или размещения на web-сайте Банка: www.krona-bank.ru.

4.1.8. Уведомлять Клиента о результате проверки ЭП, регистрации (отказе в регистрации), приеме к исполнению, исполнении, отзыве, возврате (аннулировании) ЭД посредством присвоения ЭД соответствующего статуса; дата и время присвоения статуса фиксируется в Системе. В случае отказа в регистрации или исполнении ЭД, к статусу добавляется причина отказа.

Присвоение Банком электронному документу (ЭД) соответствующего статуса в Системе является надлежащим Уведомлением Клиента о совершении операции, в том числе о результатах приема к исполнению, отзыва, возврата (аннулирования) ЭД в соответствии с требованиями законодательства Российской Федерации и не требует дополнительного направления Банком Клиенту какого-либо дополнительного информационного сообщения.

4.1.9. Фиксировать и хранить не менее 3 (Трех) лет направленные Клиенту Уведомления о совершении операции и полученные от Клиента уведомления об утрате/ компрометации/ подозрении на компрометацию ключа ЭП или о совершенной операции с использованием Системы без согласия Клиента.

4.1.10. Обеспечивать возможность направления ему Клиентом уведомления об утрате, о получении доступа к Системе (оборудованию, средствам ДБО, к сертификатам ЭП) лиц, не являющихся уполномоченными лицами Клиента, совершении операций такими лицами, совершении операций с использованием Системы без согласия Клиента.

4.1.11. В порядке, предусмотренном настоящими Условиями, предоставлять Клиенту документы и информацию, которые связаны с использованием Клиентом Системы.

4.2. Банк вправе:

4.2.1. В одностороннем порядке изменять Тарифы за услуги Системы, о чем Банк уведомляет Клиента путем размещения информации на информационных стендах Банка и/или на web-сайте Банка;

4.2.2. Отказать Клиенту в приеме и/или исполнении распоряжения на проведение операции по Счёту, подписанного ЭП, в случаях, предусмотренных действующим законодательством РФ, в том числе, в случае выявления Банком сомнительных операций Клиента (в соответствии с нормативными документами Банка России).

Не принимать к исполнению электронные документы Клиента, оформленные с нарушением Условий и приложений к ним, с уведомлением Клиента не позднее следующего рабочего дня с момента получения такого документа.

В вышеуказанных случаях Клиенту направляется уведомление одним из следующих способов:

- передача представителю Клиента под расписку с одновременным представлением Банку документа, подтверждающего полномочия представителя Клиента;
- заказной почтой с уведомлением о вручении;
- по Системе.

4.2.3. В случае необходимости требовать от Клиента оформления расчетного документа на бумажном носителе, оформленного в соответствии с требованиями Центрального банка Российской Федерации, и не производить платеж до представления указанного документа, о чем Банк обязан сообщить Клиенту любым доступным Банку способом не позднее следующего рабочего дня с момента получения документа в электронной форме;

4.2.4. Приостанавливать прием и отправку ЭД Клиента по Системе в случае смены Уполномоченных лиц Клиента до момента регистрации новых владельцев сертификата ключа проверки электронной подписи;

4.2.5. В одностороннем порядке расторгнуть Договор о ДБО, в любое время, в том числе, но не исключительно, в случаях, если:

– в течение 2-х месяцев подряд Клиентом не уплачивалось комиссионное вознаграждение, либо в течение 2-х месяцев подряд на Счете Клиента отсутствовал необходимый остаток денежных средств для списания Банком в одностороннем порядке сумм комиссионного вознаграждения в соответствии с Тарифами Банка;

– Клиентом не передана в Банк заявка на выдачу сертификата ключа проверки ЭП в течение 30 календарных дней с момента подачи Заявления о присоединении к Условиям, либо если в течение 30 календарных дней с момента истечения срока действия предыдущего сертификата ключа проверки ЭП Клиентом не представлена заявка на изготовление нового сертификата ключа проверки ЭП;

– невыполнения Клиентом иных обязательств, установленных настоящими Условиями.

Расторжение Договора о ДБО означает прекращение права Клиента использовать переданное ему программное обеспечение и СКЗИ (документально двусторонним актом не оформляется).

4.3. Клиент обязуется:

4.3.1. Выполнять требования Условий, действующих на дату осуществления операций;

4.3.2. Обеспечивать защиту клиентского модуля системы «Интернет-Банк» от несанкционированного доступа, а также заражения вредоносным кодом (вирусами). В случае обнаружения неработоспособности системы «Интернет-Банк», признаков несанкционированного доступа к системе «Интернет-Банк», а также признаков заражения клиентского модуля системы «Интернет-Банк» вредоносным кодом (вирусами), не позднее следующего рабочего дня с момента обнаружения сообщить об этом Банку любым доступным способом.

4.3.3. Обеспечивать конфиденциальность ключей ЭП и паролей, используемых Клиентом в Системе.

В случае потери либо полного или частичного повреждения Смарт-ключа «Рутокен» производится перегенерация ЭП с предоставлением нового электронного идентификатора за плату, установленную в соответствии с действующими Тарифами Банка;

4.3.4. Незамедлительно обращаться в Банк любым доступным способом в случае возникновения неполадок в Системе;

4.3.5. Обеспечить сохранность Мобильных устройств с установленным Мобильным приложением, а также Мобильных устройств, номера которых зарегистрированы в Банке для целей получения Клиентом Одноразового кода. В случае утери Мобильного устройства с установленным Мобильным приложением, равно как и Мобильного устройства, номер которого зарегистрирован в Банке для целей получения Клиентом Одноразового кода, незамедлительно отключить SMS-сообщения в Системе или проинформировать об этом Банк.

4.3.6. Незамедлительно сообщить Банку о невозможности получить доступ к мобильному устройству, посредством которого осуществляется использование Мобильного приложения системы «Интернет-Банк» в случае кражи, утери. В случае несвоевременного уведомления Банка о таких обстоятельствах, Банк не несет ответственности перед Клиентом за прямой или косвенный ущерб, причиненный Клиенту противоправными/мошенническими действиями третьих лиц.

4.3.7. Незамедлительно сообщить Банку о смене SIM-карты, в том числе, при сохранении номера Мобильного телефона.

4.3.8. Не предоставлять третьим лицам возможность распоряжения посредством Мобильного приложения денежными средствами, находящимися на Счете, не предоставлять им право использования Кодового слова, SMS-пароля, Логина. Риски, возникающие в связи с получением доступа третьих лиц к указанным в настоящем пункте устройствам и данным, несет Клиент.

4.3.9. Незамедлительно, в день утраты пароля для входа в Мобильное приложение, получения доступа третьих лиц к паролю, утраты Мобильного устройства, утраты или несанкционированного перевыпуска SIM-карты с зарегистрированным номером телефона Клиента, сведения о котором содержатся в Мобильном приложении, на который поступают SMS-пароли, утраты Мобильного устройства с активированным Мобильным приложением, наступления иных случаев компрометации средств авторизации и подтверждения, сообщить об этом Банку любым доступным способом. Риски, возникающие в связи с ненадлежащим исполнением обязанности, указанной в настоящем пункте, несет Клиент.

4.3.10. Незамедлительно информировать Банк обо всех случаях, отрицательного результата, нештатной работы Мобильного приложения, неполучении информационных сообщений.

4.3.11. Оказывать содействие Банку в установлении фактов несанкционированного доступа к Мобильному приложению и компрометации средств авторизации и подтверждения.

4.3.12. Использовать на Мобильных устройствах, применяемых для подключения к Мобильному приложению, только лицензионное программное обеспечение.

4.3.13. Контролировать соответствие суммы платежа и остатка на своих счетах в Банке и осуществлять платежи только в пределах этого остатка. Настоящий пункт не применяется при наличии соглашения о кредитовании банковского счета путем предоставления кредита в форме овердрафт;

4.3.14. Оплачивать услуги Банка в размере и сроки, установленные Тарифами Банка;

4.3.15. В установленные сроки осуществлять необходимые мероприятия по плановой смене действующих ключевых пар и сертификатов ключей ЭП;

4.3.16. В случаях компрометации ключей незамедлительно обращаться в Банк в соответствии с настоящими Условиями;

4.3.17. Ежедневно осуществлять прием от Банка надлежащим образом оформленных ЭД и информационных сообщений.

Кроме того, проверять в Системе уведомления Банка о статусе, присвоенном распоряжениям Клиента по мере направления Клиентом распоряжений в Банк, и изменения Банком статусов, присвоенных распоряжениям в Системе согласно п. 4.1.8. настоящих Условий, а также проверять выписки, направленные Банком в соответствии с п. 8.6. настоящих Условий;

4.3.18. При смене Уполномоченных лиц инициировать формирование новых Ключей ЭП и Сертификатов ключей проверки ЭП;

4.3.19. По первому требованию Банка, но не позднее 2 (Двух) рабочих дней с даты получения такого требования, предоставить копии отправленных или полученных электронных документов

на бумажном носителе, заверенные собственноручной подписью уполномоченного лица и печатью Клиента;

4.3.20. Предоставлять по запросу Банка документы и сведения, необходимые в соответствии с требованиями нормативных документов в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4.3.21. Не позднее следующего рабочего дня после совершения операций по счету с использованием Системы без согласия Клиента, а также в случаях утраты/компрометации/подозрении на компрометацию ключей ЭП, незамедлительно уведомить Банк о случившемся путем подачи заявления на бумажном носителе, подписанного уполномоченным лицом Клиента.

4.4. Клиент вправе:

4.4.1. Получать от Банка консультации по вопросам использования Системы;

4.4.2. Направлять в Банк ЭД по Системе в соответствии с перечнем электронных документов, указанным в Приложении 1 к настоящим Условиям;

4.4.3. Получать от Банка в ЭД по Системе документы в соответствии с перечнем электронных документов, указанным в Приложении 1 к настоящим Условиям;

4.4.4. Обращаться в Банк с заявлением о согласии на предоставление доступа к Системе Контролирующей организации с целью просмотра платежных документов;

4.4.5. Обращаться в Банк с заявлением об установлении/отключении функции просмотра за платежами Контролируемой организации в Системе;

4.4.6. В случае несогласия с изменениями условий настоящего Договора и/или Тарифов Банка, а также в любых иных случаях Клиент имеет право расторгнуть Договор о ДБО в одностороннем порядке, путем направления письменного уведомления в соответствии с п. 10.4. настоящих Условий.

4.5. Стороны обязуются самостоятельно контролировать сроки действия ключей ЭП и производить их смену в порядке, установленном настоящими Условиями.

4.6. Стороны обязуются формировать и в течение не менее 5 (Пяти) лет (а в случае возникновения споров – до их разрешения) поддерживать архивы:

- всех ключей ЭП;
- всех входящих ЭД в принятом виде с ЭП;
- всех исходящих - в исходном виде с ЭП;
- извещений (в электронном виде с ЭП) о приеме электронных документов;
- сообщений свободного формата, подписанных ЭП;
- электронных протоколов сеансов обмена информацией

и несут ответственность за их целостность и достоверность. Порядок формирования и поддержания архивов определяется Банком. Необходимость формирования и поддержания Клиентом архивов иных документов определяется им самостоятельно.

Сроки хранения электронных расчетных документов должны соответствовать срокам хранения, установленным для хранения документов на бумажных носителях. Иные архивы поддерживаются Банком в течение не менее трех лет (а в случае возникновения споров – до их разрешения).

4.7. Стороны признают, что единой шкалой времени при работе в Системе является поясное время по показаниям системных часов автоматизированного рабочего места Банка. Временем поступления ЭД Клиента в Банк считается время записи документа в базу данных Системы на автоматизированном рабочем месте Банка.

5. ПОРЯДОК ПОДКЛЮЧЕНИЯ К МОБИЛЬНОМУ ПРИЛОЖЕНИЮ

5.1. Для получения доступа к мобильной версии, Клиент заполняет заявление на получение логина и пароля в web-версии Интернет-банка Faktura.ru для корпоративных клиентов в разделе «Мобильная версия».

5.2. Клиент самостоятельно устанавливает Мобильное приложение для своей версии операционной системы (iOS или Android), перейдя по соответствующей ссылке на странице входа Интернет-банка Faktura.ru или с авторизированного магазина приложений AppStore или Google Play.

5.3. При первом входе в мобильное приложение Клиенту необходимо ввести временный пароль, выданный Банком, сменить его на постоянный, а также задать 4-значный цифровой код доступа.

5.4. Срок действия сертификата для Мобильного приложения Системы составляет один календарный год с момента активации приложения. Плановая смена сертификата Мобильного приложения Системы осуществляется в соответствии с п. 3.4. настоящих Условий и проводится Клиентом самостоятельно.

5.5. В Мобильном приложении Системы могут быть выполнены следующие операции:

- подтверждение платёжных операций с помощью разовых паролей из SMS-сообщений;
- подтверждение платёжных документов, созданных в Системе;
- совершение переводов между счетами одной организации, физическим и юридическим лицам, оплата в бюджет;
- редактирование, копирование и удаление платёжных документов;
- просмотр баланса, поступлений и списаний по всем Счетам Клиента;
- отслеживание состояний платежей и переводов;
- просмотр выписок и реквизитов;
- доступ к контактной информации Банка.

5.6. В Мобильном приложении установлены следующие лимиты на совершение операций:

- сумма одной операции не может превышать 300 000 (Триста тысяч) рублей 00 копеек;
- в день может быть совершено операций на сумму, не превышающую 1 000 000 (Один миллион) рублей 00 копеек.

5.7. Банк имеет право определять необходимость использования Одноразовых ключей в зависимости от критериев, установленных Банком в настоящих Условиях.

5.8. Перед подключением Мобильного приложения Клиент должен обеспечить работу Мобильного устройства в следующем режиме:

- на Мобильном устройстве должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение;
- для работы Мобильного приложения необходимо иметь мобильное устройство со стабильным Интернет-соединением. Поддерживаемые версии операционных систем указаны в Руководстве пользователя «Мобильное приложение для корпоративных клиентов», размещенных на сайте Faktura.ru в разделе «Ответы на вопросы».
- Клиент должен использовать процедуру аутентификации доступа к Мобильному устройству, посредством ввода логина пароля или кода доступа, или входу по отпечатку пальца.

5.9. Порядок подписания электронных документов с помощью Мобильного приложения:

5.9.1. После формирования ЭД в Мобильном приложении Клиент делает запрос на подписание ЭД с помощью кода подтверждения Мобильного приложения.

5.9.2. После прохождения аутентификации при входе в Мобильном приложении в соответствии с установленным в п. 5.3. настоящих Условий способом, Клиенту предоставляется возможность подписать ЭД, информация о котором отражается в Мобильном приложении, или отклонить подписание.

5.9.3. ЭД должен быть подписан Клиентом в течение 300 секунд (параметр может быть изменен Банком), в противном случае он будет отклонен. В этом случае для подписания ЭД Клиентом должна быть заново инициирована процедура подписания.

5.9.4. В случае если Клиент не подтвердит или отклонит ЭД 3 (Три) раза подряд (параметр может быть изменен Банком), то возможность направления кода подтверждения будет отключена. Для возобновления использования Услуги Клиент должен осуществить повторную активацию Мобильного приложения в соответствии с п. 5.1. настоящих Условий.

5.10. В случаях, когда использование Мобильного приложения предполагает передачу Клиенту либо хранение Банком конфиденциальной информации, Банк и Клиент обязуются принять все необходимые меры организационного и технического характера для предотвращения доступа третьих лиц к такой информации до передачи ее Клиенту, а также во время ее хранения Банком/Клиентом.

5.11. Стороны договорились, что с использованием Мобильного приложения Клиент может осуществлять переводы денежных средств только в валюте Российской Федерации.

5.12. К событиям, приводящим к компрометации ключей Мобильного приложения, относятся следующие события:

- компрометация Смарт-ключа «Рутокен» для входа в web-версию Интернет-банка Faktura.ru для корпоративных клиентов;
- потеря Мобильного устройства с активированным Мобильным приложением;
- увольнение сотрудников, имевших доступ к Мобильному устройству с активированным Мобильным приложением;
- нарушение правил хранения Мобильного устройства Клиента, предусмотренных настоящими Условиями;
- возникновение у Банка или у Клиента подозрений о получении третьими лицами доступа к Мобильному устройству, Мобильному приложению и Ключам;
- Мобильное устройство вышло из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника.

6. ПОРЯДОК ОПЛАТЫ

6.1. За обслуживание Клиента с использованием Системы Клиент уплачивает Банку комиссионное вознаграждение в соответствии с Тарифами Банка.

6.2. Взимание комиссионного вознаграждения осуществляется Банком путём списания суммы тарифа с расчётных счетов Клиента, открытых в Банке, на что Клиент дает Банку свое согласие (заранее данный акцепт).

Клиент вправе оплатить причитающееся Банку вознаграждение путем безналичного перечисления денежных средств со своих счетов, открытых в других кредитных организациях.

6.3. Банк имеет право приостановить прием и отправку ЭД по Системе в случае задержки оплаты комиссионного вознаграждения на срок свыше 5 (Пяти) календарных дней при отсутствии денежных средств на счетах Клиента для их списания, о чем Банк направляет Клиенту соответствующее уведомление по Системе. На время приостановления обслуживания Клиента с использованием Системы комиссионное вознаграждение Банком не взимается.

6.4. Возобновление обслуживания производится не позднее рабочего дня, следующего за днём полного погашения Клиентом задолженности перед Банком.

6.5. При неоплате комиссионного вознаграждения в течение 2-х месяцев подряд, либо в течение 2-х месяцев подряд на счетах Клиента отсутствовал необходимый остаток денежных средств для списания Банком в одностороннем порядке сумм комиссионного вознаграждения в соответствии с Тарифами Банка, Банк имеет право в одностороннем порядке расторгнуть Договор о ДБО в порядке, предусмотренном п. 10.4. настоящих Условий.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Стороны несут ответственность за достоверность информации, представляемой друг другу.

7.2. Стороны не несут ответственности за какие-либо задержки, невозможность оказания услуг электронного документооборота, недостатки в процессе выполнения работ и исполнения обязательств по Договору о ДБО, причинами которых прямо или косвенно являются обстоятельства, выходящие за сферу их реального контроля, включая стихийные бедствия, забастовки, отказ оборудования систем связи, военные действия, правительственные ограничения, запрещения и др.

7.3. За неисполнение или ненадлежащее исполнение обязательств по Договору о ДБО Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

7.4. Банк не несет ответственности за неисполнение или ненадлежащее исполнение поручений Клиента, произошедшее из-за нарушения Клиентом настоящих Условий. Риск неправомерного подписания ЭД ЭП несет Клиент, на уполномоченное лицо которого зарегистрирован Сертификат соответствующего ключа подписи.

7.5. Банк не несет ответственности за сбои в работе Системы по причине изменений, вносимых Клиентом в клиентский модуль Системы без согласования с Банком или в результате ненадлежащего исполнения Клиентом настоящих Условий, изменения конфигурации рабочего места, занесения вирусов.

7.6. Банк не несет ответственности за неисполнение или ненадлежащее исполнение обязательств по Договору о ДБО, произошедшее из-за нарушения Клиентом порядка оплаты услуг Банка.

7.7. Банк не несет ответственность за несвоевременное ознакомление Клиента с уведомлением Банка о совершенных операциях в соответствии с п. 4.1.8. настоящих Условий и несвоевременное уведомление Клиентом Банка о совершении операции с использованием Системы без согласия Клиента в соответствии с п. 4.3.21. настоящих Условий.

8. ОСОБЫЕ УСЛОВИЯ

8.1. Инициатором сеансов связи с Банком всегда является Клиент. Любая просрочка в выполнении Банком своих обязательств, которая произошла из-за отсутствия инициативы Клиента в установлении сеанса связи с Банком, не влечет за собой ответственности Банка (в том числе по уведомлению Клиента о совершенных операциях по счету).

8.2. Каждая из Сторон при подписании ЭД ЭП применяет свои ключи ЭП, а при проверке подписи – ключи проверки ЭП другой Стороны, действующие на момент подписания документа.

Ключи Банка считаются действующими с даты и времени начала действия связанных с этими ключами сертификатов ключей проверки ЭП, выданных Удостоверяющим центром (определяются по атрибуту сертификата ключа проверки ЭП «Действителен с»), и до момента наступления одного из следующих событий: компрометации ключа, плановой или внеплановой смены ключа Банка.

Ключи Клиента считаются действующими с даты и времени начала действия связанных с этими ключами сертификатов ключей проверки ЭП, выданных Удостоверяющим центром (определяются по атрибуту сертификата ключа поверки ЭП «Действителен с») уполномоченному лицу Клиента, и до момента наступления одного из следующих событий:

- аннулирования сертификата ключа проверки ЭП;
- плановой или внеплановой смены ключа Клиента;
- прекращения действия Договора о ДБО.

Плановая смена ключей проводится не реже одного раза в год, внеплановая – в случаях компрометации действующих ключей, непреднамеренного уничтожения ключей и выхода из строя Смарт-ключа «Рутокен». Кроме того, Клиент обязан произвести смену принадлежащих ему ключей по требованию Банка.

8.3. Все процедуры создания, регистрации, хранения, плановой и внеплановой смены криптографических ключей и сертификатов ключей проверки ЭП осуществляются в соответствии с порядком, установленным Правилами и настоящими Условиями.

8.4. Стороны признают и руководствуются всеми терминами, определениями и сокращениями, используемыми в настоящих Условиях и Приложениях к ним.

8.5. Заявление о присоединении к Условиям является дополнением к договору(ам) банковского счета(ов) Клиента, указанного(ым) в Заявлении о присоединении к Условиям, а также иных договоров, предусматривающих электронный документооборот.

8.6. С момента заключения Договора о ДБО изменяется порядок формирования и получения Клиентом выписок по банковскому счету/счетам, указанным в Заявлении Клиента о присоединении к Условиям и/или в Заявлении об обслуживании дополнительных счетов с использованием Системы. Банк формирует выписку по банковскому счету(ам) в электронном виде, которую Клиент обязуется самостоятельно получать ежедневно (по мере совершения операций по счету(ам)) по Системе. В течение действия Договора о ДБО Банк не формирует и не передает Клиенту выписки по банковским счету/счетам, указанным в Заявлении Клиента о присоединении к Условиям и/или в Заявлении об обслуживании дополнительных счетов с использованием Системы на бумажном носителе, за исключением дополнительных запросов Клиента.

8.7. Все операции по счету, совершаемые с использованием Системы с соблюдением требований настоящих Условий и приложений к ним, осуществляются Банком в общем порядке до момента поступления от Клиента уведомления об утрате/компрометации/подозрении на компрометацию ключа ЭП или о том, что операция совершена без согласия Клиента.

9. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

9.1. Все разногласия, споры и конфликтные ситуации (далее – Споры), возникающие между Сторонами вследствие выполнения Договора о ДБО, разрешаются с учетом взаимных интересов путем переговоров в порядке, установленном настоящими Условиями и Приложениями к ним, в том числе Приложением № 3 к настоящим Условиям.

9.2. Сторона, признанная виновной, возмещает убытки другой Стороне.

9.3. Уклонение какой-либо Стороны Договора о ДБО от участия в создании или работе технической комиссии может привести к невозможности ее создания и работы, но не может привести к невозможности урегулирования спора в судебном порядке.

В случае невозможности создания технической комиссии, не достижения соглашения Сторон, отсутствия согласия по спорам или отказа от добровольного исполнения решения комиссии споры по Договору о ДБО передаются на рассмотрение Арбитражного суда по месту заключения Договора о ДБО.

10. СРОК ДЕЙСТВИЯ ДОГОВОРА О ДБО И ПОРЯДОК ЕГО РАСТОРЖЕНИЯ

10.1. Договор о ДБО вступает в силу с момента подписания Банком подписанного Клиентом Заявления о присоединении к Условиям и действует в течение срока действия Договоров банковского счета по всем счетам Клиента, указанным в названном Заявлении о присоединении к Условиям, или иного договора, в рамках исполнения которого была установлена Система ДБО, либо до расторжения Договора о ДБО.

10.2. Возможность обмена ЭД, в соответствии с перечнем видов ЭД по Приложению № 1 к настоящим Условиям возникает с момента выпуска рабочих сертификатов ключей проверки ЭП соответствующие минимальному комплекту ключей подписи, опубликования их в реестре выданных сертификатов Удостоверяющего центра и получения Клиентом посредством Системы ДБО указанных сертификатов ключей проверки ЭП в соответствии с запросом Клиента.

10.3. Все Приложения к настоящим Условиям являются неотъемлемой частью Договора о ДБО и действуют с момента вступления в силу Договора о ДБО, за исключением тех Приложений, в отношении которых прямо предусмотрена необходимость их дополнительного подписания.

10.4. Стороны вправе расторгнуть Договор о ДБО в одностороннем порядке. При этом Сторона, желающая прекратить в одностороннем порядке договорные отношения, обязана письменно уведомить об этом другую Сторону не менее чем за 7 календарных дней до предполагаемого расторжения Договора о ДБО с исполнением всех обязательств, предусмотренных настоящими Условиями. Кроме того, Договор о ДБО расторгается в случаях, предусмотренных действующим законодательством Российской Федерации и/или при расторжении всех договоров по счетам Клиента, открытых в Банке.

10.5. При расторжении Договора о ДБО Клиент обязуется уничтожить все принадлежащие ему ключи ЭП, относящиеся к Договору о ДБО, и не передавать их третьим лицам, за исключением случаев, предусмотренных п. 2.6. настоящих Условий.

10.6. Стороны не несут ответственности за ущерб, возникший вследствие действия обстоятельств непреодолимой силы (стихийные бедствия, технические сбои, а также иные обстоятельства), происшедших по независящим от Сторон причинам, существенно влияющих на функционирование Сторон и препятствующих исполнению Сторонами обязательств по Договору о ДБО.