

ДОГОВОР
обмена электронными документами
с использованием системы электронного банкинга "iBank2" (для юридических лиц и индивидуальных предпринимателей)

Общество с ограниченной ответственностью Коммерческий Банк «Столичный Кредит», именуемый в дальнейшем «**Банк**», действуя в соответствии с действующим законодательством Российской Федерации, предлагает юридическим лицам и индивидуальным предпринимателям, именуемым в дальнейшем «**Клиент**», услуги обмена электронными документами с использованием системы электронного банкинга "iBank2" в порядке и на условиях изложенным в настоящем Договоре. Для целей настоящего Договора, Банк и Клиент совместно именуются «**Стороны**».

Настоящий Договор является официальным публичным предложением (публичной офертой) юридическим лицам и индивидуальным предпринимателям заключить договор обмена электронными документами с использованием системы электронного банкинга "iBank2" на изложенных условиях.

Договор обмена электронными документами с использованием системы электронного банкинга "iBank2" является договором присоединения. Заключение Договора обмена электронными документами с использованием системы электронного банкинга "iBank2" между Банком и Клиентом осуществляется путем присоединения Клиента к Договору и изложенным в нем условиям в целом в соответствии со статьей 428 Гражданского кодекса Российской Федерации и производится путем передачи Клиентом (его уполномоченным представителем) в Банк надлежащим образом оформленного на бумажном носителе Заявления на подключение к системе "iBank2" (Приложение № 1) и акцептом (принятием) Банком этого Заявления. Заявление составляется и передается в 2 (двух) экземплярах. Один экземпляр остается у Банка, другой возвращается Клиенту (его уполномоченному представителю).

Текст Договора публикуется на официальном сайте Банка - www.capitalkredit.ru.

1. Термины, применяемые в Договоре

Термины, применяемые в тексте настоящего Договора, используются в следующем значении:

1.1. Система «iBank 2» – совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, с целью предоставления Клиенту услуг по настоящему Договору.

1.2. «Электронный документ» (ЭД) – совокупность байт, содержащая финансовый документ или информационное сообщение в Системе «iBank 2».

1.3. «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.

1.4. «Ключ электронной подписи» (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания ЭП.

1.5. «Ключ проверки электронной подписи» (Ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП.

1.6. «Пара ключей электронной подписи» (Пара ключей ЭП) – Ключ ЭП и соответствующий ему Ключ проверки ЭП.

1.7. «Подлинная электронная подпись» – электронная подпись в ЭД, проверка которой с использованием соответствующего ключа проверки ЭП дает положительный результат.

1.8. «Активная пара ключей ЭП» – пара ключей ЭП, зарегистрированных Банком в системе «iBank 2», и используемых Клиентом для работы в системе «iBank 2».

1.9. «Сертификат ключа проверки электронной подписи» (сертификат ключа проверки ЭП) – электронный документ выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

1.10. «Удостоверяющий центр» – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

1.11. «Группа подписи ключа» – полномочия ключа электронной подписи при подписи Электронного документа. По аналогии с собственноручной подписью, образец которой есть в банковской карточке, обычно различают первую и вторую подпись (группу подписи). Электронный документ может исполняться Банком только после того, как под ним собрано столько подписей, сколько указано в Заявлении на подключение к системе "iBank2" (Приложение № 1) (по одной подписи каждой группы).

1.12. «Аппаратное средство усиленной ЭП» – специализированное аппаратное средство, предназначенное для генерации пары ключей ЭП, хранения сгенерированных ключей ЭП, формирования ЭП под документами в соответствии с утвержденными стандартами (ГОСТ Р34.10-2012, ГОСТ Р34.11-2012) с использованием встроенного в устройство сертифицированного СКЗИ (USB-токен, смарт-карта).

1.13. «Программное средство усиленной ЭП» – программный модуль, входящий в состав Системы «iBank 2», предназначенный для генерации пары ключей ЭП, формирования ЭП под документами, обеспечивающий защиту

информации в соответствии с утвержденными стандартами (ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2018) и сертифицированный в соответствии с действующим законодательством.

1.14. «Блокировочное слово» – уникальное слово, определяемое Клиентом при регистрации в Системе «iBank 2». Блокировочное слово может быть использовано Клиентом для блокирования своей работы в «iBank 2» по телефонному звонку в Банк (например, в случае компрометации ключа).

1.15. «Компрометация ключа» – утрата, хищение, несанкционированное копирование, передача закрытого ключа в линию связи в открытом виде, любые другие виды разглашения содержания ключа, а также случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника).

1.16. «Средство подтверждения» - электронное или иное средство, используемое для подтверждения электронных документов. Средство подтверждения считается действительным на определенный момент времени, если одновременно выполнены следующие условия: на этот момент времени средство подтверждения указано Клиентом в Заявлении на подключение к системе "iBank2" (Приложение № 1) либо в письменном заявлении Клиента, оформленном в соответствии с Приложением № 6 к настоящему Договору, срок действия средства подтверждения не истек, средство подтверждения не было отменено Клиентом или Банком, а также Банком получено согласие о предоставлении ООО КБ «Столичный Кредит» права на получение и обработку персональных данных по форме Приложения № 10 к Договору.

1.17. «Одноразовый пароль» — динамическая аутентификационная информация, генерируемая для единичного использования.

1.18. «Оператор связи» - телекоммуникационная компания, осуществляющая услуги связи, в том числе услуги по доставке sms - сообщений на мобильные телефоны (устройства), в том числе Клиента.

1.19. «Облачная электронная подпись» (электронная подпись в облаке, ОЭП) - аналог обычной электронной подписи. По технологии облачной ЭП создание, хранение ключей ЭП и формирование ЭП осуществляется не на аппаратном средстве ЭП (USB-токен, смарт-карта), а на защищенных ресурсах (сервер) Банка («облако»).

1.20. Отдельные значения терминов и определений не раскрытые в настоящем Договоре, приведены в Правилах электронного документооборота в системе электронного банкинга «iBank2» ООО КБ «Столичный кредит», опубликованных на сайте Банка в сети Интернет (<https://capitalkredit.ru>).

2. Предмет Договора

2.1. Банк оказывает Клиенту услуги электронного банкинга с использованием Системы «iBank 2», позволяющей передавать Электронные документы и принимать выписки и информационные сообщения.

2.2. Настоящий Договор имеет свою юридическую силу при наличии действующего Договора банковского счёта, заключённого между Сторонами.

3. Соглашения Сторон

3.1. Стороны признают, что применяемая в Системе «iBank 2» криптографическая защита информации, обеспечивающая шифрование, контроль целостности и создание ЭП с применением Программных, Аппаратных средств усиленной ЭП, а также ОЭП достаточна для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства Электронного документа.

3.2. Стороны признают, что применяемая в «iBank 2» технология генерации и хранения Ключа электронной подписи, формирования ЭП под документом с использованием Аппаратного средства усиленной ЭП, либо с использованием ОЭП (облачное хранилище) полностью исключает возможность получения прямого доступа к Ключу электронной подписи с целью его копирования, переноса на внешний носитель или использования для формирования ЭП вне устройства, или вне облачного хранилища.

3.3. Аппаратные средства ЭП являются собственностью Банка и предоставляются для использования, за плату, в соответствии с Тарифам Банка.

3.4. Стороны признают, что при произвольном изменении Электронного документа, заверенного Электронной подписью, ЭП становится не подлинной, то есть проверка подлинности ЭП дает отрицательный результат.

3.5. Стороны признают, что подделка ЭП Клиента, то есть создание Подлинной ЭП в Электронном документе от имени Клиента, практически невозможно без использования ключа электронной подписи Клиента.

3.6. Стороны признают, что Электронные документы с ЭП сотрудников Клиента, полученные Банком по Системе «iBank 2», являются доказательным материалом для решения спорных вопросов в соответствии с Приложением № 2 настоящего Договора («Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций»). Электронные документы, не имеющие необходимого количества ЭП, при наличии спорных вопросов не являются доказательным материалом.

Правила настоящего договора относительно сотрудников Клиента равнозначно применяются и непосредственно к Клиенту, являющимся Индивидуальным предпринимателем.

3.7. Стороны признают, что ключ проверки электронной подписи сотрудника Клиента, содержащийся в Сертификате ключа проверки электронной подписи (в электронной форме, выданном аккредитованным удостоверяющим центром), принадлежит соответствующему сотруднику Клиента.

3.8. Стороны признают в качестве единой шкалы времени при работе с Системой «iBank 2» Московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

3.9. Стороны признают, что применяемые в Системе «iBank 2» механизмы дополнительного подтверждения документов с помощью одноразового пароля, являются надежными. Документы, требующие подтверждения одноразовым паролем, принимаются Банком к исполнению только в случае надлежащего подтверждения одноразовым паролем, полученным со Средства подтверждения Клиента или с зарегистрированного при написании Заявления на подключение к системе "iBank2" (Приложение № 1) или по форме Приложения № 6 мобильного телефона сотрудника Клиента.

3.10. Стороны признают, что подделка одноразового пароля, то есть подтверждение Электронного документа от имени Клиента, практически невозможна без владения Средством подтверждения или зарегистрированным в системе мобильным телефоном.

3.11. Стороны признают, что Электронные документы, заверенные необходимым количеством ЭП, юридически эквивалентны соответствующим документам на бумажном носителе, оформленным в установленном порядке (имеющим необходимые подписи и оттиск печати), обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы без необходимого количества ЭП сотрудников Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

3.12. Стороны признают, что для уведомления Клиента о произведенных транзакциях в Системе «iBank 2» в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ от «О национальной платежной системе» и Положением Банка России от 29 июня 2021 года №762-П «О правилах осуществления перевода денежных средств», Банку необходимо и достаточно отправить sms-сообщение на номер мобильного телефона, зарегистрированного в Системе в соответствии с Заявлением Клиента на подключение к системе "iBank2" (Приложение № 1) и/или по Заявлению Клиента по форме Приложения № 6 к Договору. В случае получения Банком подтверждения от Оператора связи об успешной отправке СМС-сообщения, Клиент считается уведомленным о произведенной Клиентом транзакции в системе «iBank2».

3.13. Стороны принимают и обязуются руководствоваться Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций, изложенным в Приложении 2 к настоящему Договору.

3.14. Клиент подтверждает, что ознакомлен с информацией, указанной в Приложении 7 к настоящему Договору и Правилами электронного документооборота в системе электронного банкинга «iBank2» ООО КБ «Столичный кредит», опубликованными на сайте Банка в сети Интернет (<https://capitalkredit.ru>).

3.15. Стороны признают, что отмена действий пары ключей ЭП сотрудника Клиента и средства подтверждения осуществляются только после письменного уведомления Банка Клиентом в установленной Банком форме (Приложение 3 и 5 соответственно к настоящему Договору).

3.16. Стороны признают, что в случае передачи необходимых для работы Клиента аппаратных средств факт передачи фиксируется подписями Сторон в Акте передачи по форме Приложения 4 к настоящему Договору в момент передачи носителя соответствующего программного (аппаратного) средства.

3.17. Стороны признают, что первоначальная регистрация номера(ов) мобильного(ых) телефона(ов) в качестве средства получения одноразовых паролей осуществляется на основании данных заявления на подключение к системе «iBank2» в момент присоединения Клиента к настоящему Договору. Внесение дальнейших изменений в виде регистрации или прекращения регистрации номера(ов) мобильного(ых) телефона(ов) в качестве средства получения одноразовых паролей осуществляется по письменному заявлению Клиента, оформленному в соответствии с Приложением 6 к настоящему Договору.

3.18. Стороны признают, что отказом от получения одноразовых паролей на вход в систему «iBank2», а также отказом на получение одноразовых паролей на подтверждение платежа в виде sms-сообщений Клиент увеличивает риск несанкционированного доступа в систему третьих лиц, вредоносного обеспечения и прочих фактов, приводящих к явному и/или неявному несанкционированному доступу в систему «iBank2». Отказ от получения одноразовых паролей на вход в систему «iBank2», а также отказ от получения одноразовых паролей на подтверждение платежа в виде sms-сообщений оформляется путем подачи заявления, установленной банком формы (Приложение 8 к настоящему Договору).

3.19. Стороны признают, что в случае проведения операций над группой документов (групповая подпись документов) Клиент увеличивает риск несанкционированного доступа в систему третьих лиц, вредоносного обеспечения и прочих фактов, приводящих к явному и/или неявному несанкционированному доступу в систему «iBank2». Согласие на проведение операций над группой документов (отказ от подписи единичного документа) оформляется путем подачи заявления, установленной банком формы (Приложение 9 к настоящему Договору).

3.20. Приложения 3,5,6 и 8 подписываются в соответствии с условиями, установленными пунктами 3.13 - 3.18 настоящего Договора.

4. Права и обязанности Банка

4.1. Банк обязан принимать к исполнению Электронные документы, полученные по Системе «iBank 2» от Клиента, подписанные необходимым количеством ЭП лиц, уполномоченных работать в системе «iBank2» и соответствующие действующему законодательству РФ.

4.2. Банк обязан по запросу Клиента предоставлять Клиенту необходимую документацию в соответствии с Приложением № 7 (рекомендации для работы с Системой «iBank 2», инструкции по генерации ключа облачной подписи).

4.3. Банк в случае решения клиента использовать носитель аппаратного средства усиленной ЭП (USB-токен, смарт-карта), обязан передать Клиенту аппаратные средства усиленной ЭП до начала работы Клиента в Системе «iBank 2», после оплаты Клиентом права использования носителя аппаратного средства ЭП, в соответствии тарифами Банка. Факт передачи указанных средств фиксируется в Актах передачи по форме Приложения 4. Клиент может генерировать ключи облачной подписи (ОЭП) самостоятельно или воспользоваться услугой, оказываемой специалистом Банка по генерации ОЭП, согласно тарифам Банка.

4.4. Банк в случае решения Клиента использовать носитель аппаратного средства усиленной ЭП (USB-токен, смарт-карта), обязан предоставить Клиенту не менее одного Аппаратного средства усиленной ЭП, необходимые рекомендации и системное ПО для использования устройства.

4.5. Банк обязан по письменному требованию Клиента заблокировать в Системе «iBank 2» существующую Пару ключей ЭП сотрудника Клиента и регистрировать новые Ключи проверки ЭП сотрудников Клиента.

4.6. Банк обязан по телефонному звонку Клиента временно заблокировать работу Клиента в Системе «iBank 2», если Клиент подтверждает свои полномочия Блокировочным словом.

4.7. Банк имеет право по своему усмотрению без уведомления Клиента заблокировать Активную пару ключей ЭП Клиента и потребовать от Клиента смены Пары ключей ЭП.

4.8. При наличии обоснованных подозрений о Компрометации Ключа электронной подписи сотрудников Клиента, Банк имеет право не производить исполнение полученных от Клиента Электронных документов и требовать от Клиента предоставления оформленных в установленном порядке платежных документов на бумажном носителе. Банк обязан незамедлительно, но не позднее 24 (двадцати четырех) часов, сообщить Клиенту о возникновении подобных подозрений и необходимости предоставить платежные документы на бумажном носителе.

4.9. Банк уведомляет Клиента о проведенных транзакциях в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ от «О национальной платежной системе» и Положением Банка России от 29 июня 2021 года №762-П «О правилах осуществления перевода денежных средств».

4.9.1. В случае наличия у Банка оснований полагать, что операция совершается без добровольного согласия Клиента, либо выявления Банком операции соответствующей признакам осуществления перевода денежных средств без добровольного согласия клиента Банк вне зависимости от установления клиентом ограничений по счету/вкладу осуществляет мероприятия в соответствии с требованиями Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе» (далее: Федеральный Закон N 161-ФЗ):

- приостанавливает прием к исполнению распоряжения Клиента на два дня.
- после приостановления исполнения распоряжения о совершении операции Банк **незамедлительно** одним из способов (или несколькими способами) предусмотренным п.4.9.7 настоящего Договора, предоставляет Клиенту информацию:

- а) о приостановлении приема к исполнению распоряжения Клиента на два дня;

- б) о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия клиента;

- в) о возможности Клиента подтвердить распоряжение **не позднее одного дня**, следующего за днем приостановления Банком приема к исполнению указанного распоряжения, способами, указанными в п.4.9.7.1 настоящего Договора.

4.9.2. Банк при предоставлении Клиенту информации в соответствии с п. 4.9.1 настоящего Договора вправе в дополнение к подтверждению в соответствии с подпунктом в) п.4.9.1 настоящего Договора запросить у Клиента информацию, что перевод денежных средств не является переводом денежных средств без добровольного согласия клиента.

4.9.3. При получении от Клиента подтверждения распоряжения, Банк незамедлительно принимает к исполнению подтвержденное распоряжение, за исключением случая, предусмотренного пунктом 4.9.5 настоящего Договора и при отсутствии иных установленных законодательством Российской Федерации оснований не принимать распоряжение клиента к исполнению.

4.9.4. При неполучении от Клиента подтверждения распоряжения, в соответствии с подпунктом в) пункта 4.9.1 настоящего Договора и (или) информации, запрошенной в соответствии с пунктом 4.9.2 настоящего Договора, указанное распоряжение **не принимается Банком к исполнению**.

4.9.5. В случае, если, несмотря на направление Клиентом **подтверждения распоряжения**, Банк получил от Банка России информацию, содержащуюся в Базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, Банк приостанавливает прием к исполнению **подтвержденного распоряжения Клиента на два дня** со дня направления Клиентом подтверждения распоряжения. Банк в порядке, предусмотренном пунктом 4.9.7 настоящего Договора, незамедлительно уведомляет Клиента о приостановлении приема к исполнению **подтвержденного распоряжения клиента с указанием причины такого приостановления и срока такого приостановления**.

4.9.6. В случае приостановления приема к исполнению подтвержденного распоряжения Клиента в соответствии с пунктом 4.9.5 настоящего Договора, по истечении **двух дней** со дня направления Клиентом подтверждения распоряжения в соответствии с подпунктом в) пункта 4.9.1 настоящего Договора Банк **незамедлительно принимает к исполнению** подтвержденное распоряжение Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не принимать подтвержденное распоряжение Клиента к исполнению.

4.9.7. Банк уведомляет Клиента о приостановлении использования ЭСП, о приостановлении приема к исполнению распоряжения Клиента, о праве Клиента подать в **порядке**, установленном Банком России, заявление в Банк России, в том числе через Банк, **об исключении сведений**, относящихся к Клиенту и (или) его ЭСП из Базы данных любым доступным способом (одним или несколькими):

- в личном кабинете ДБО «iBank2»;
- посредством СМС-сообщения;
- посредством письменного почтового уведомления;
- с использованием электронной почты (E-mail) или посредством телефонных соединений;
- иные способы, которые регламентированы законодательством и настоящими договором и позволяют установить факт уведомления клиента.

Обязанность Банка по направлению Клиенту уведомлений считается исполненной при направлении уведомления

4.9.7.1. Клиент подтверждает распоряжение, предоставляет Банку уведомления, информацию, предусмотренную п. 4.9.2 настоящего Договора (одним или несколькими способами):

- в личном кабинете ДБО «iBank2»;
- посредством письменного почтового уведомления;
- с использованием электронной почты (E-mail).

4.9.8. Банк при получении от Банка России информации, содержащейся в **Базе данных**¹, которая содержит сведения, относящиеся к **Клиенту и (или) его электронному средству платежа**, и если отсутствуют сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемые в соответствии с частью 8 статьи 27 Федерального закона N 161-ФЗ Банк, **вправе приостановить использование** Клиентом ЭСП на период нахождения сведений, относящихся к Клиенту и (или) его ЭСП, в Базе данных.

4.9.9. Банк **приостанавливает** использование Клиентом ЭСП, если от Банка России получена информация, содержащаяся в Базе данных, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа, **при наличии сведений** федерального органа исполнительной власти в сфере внутренних дел **о совершенных противоправных действиях**, получаемых в соответствии с частью 8 статьи 27 Федерального закона N 161-ФЗ, **на период нахождения указанных сведений в Базе данных**.

4.9.10. После приостановления использования Клиентом ЭСП в случаях, указанных в пунктах 4.9.8 и 4.9.9 настоящего Договора, Банк незамедлительно уведомляет Клиента, способом предусмотренным п. 4.9.7 настоящего Договора, о приостановлении использования ЭСП, а также о праве Клиента подать в **порядке**, установленном Банком России, заявление в Банк России, в том числе через Банк, **об исключении сведений**, относящихся к Клиенту и (или) его электронному средству платежа, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из Базы данных.

4.9.11. При приостановлении или прекращении использования Клиентом ЭСП в случаях, указанных в пунктах 4.5-, 4.8 настоящего Договора, Банк в день такого приостановления или прекращения, предоставляет Клиенту информацию, способом, предусмотренным п. 4.8.7 настоящего Договора, о приостановлении или прекращении использования ЭСП, с указанием причины такого приостановления или прекращения.

4.10. Банк оставляет за собой право на одностороннее расторжение договора в случае наличия у Клиента задолженности по абонентской плате за использование данной системы за период равный 1 (одному) календарному месяцу. Последующее возобновление договора производится на общих основаниях.

4.11. Банк оставляет за собой право на приостановление действия настоящего Договора в случае, если решением/постановлением Налогового органа, Суда, или Судебного пристава-исполнителя на денежные средства Клиента, находящиеся на расчетном счете, наложен арест. В случае наложения ареста на денежные средства Клиента, находящиеся на расчетном счете, абонентская плата по Договору не взимается. По факту отмены решения о приостановлении операций по расчетному счету Клиента, действие договора возобновляется.

4.12. Банк оставляет за собой право отказать Клиенту в приеме от него распоряжений на проведение операций по банковскому счету, подписанных аналогом собственноручной подписи, в случае:

- выявления сомнительных операций (после предварительного уведомления Клиента), установленных действующим законодательством РФ, нормативными актами о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения и перейти на прием от Клиента расчетных документов только на бумажном носителе.

4.13. Банк имеет право в одностороннем порядке вносить изменения в настоящий Договор, Приложения, Тарифы с предварительным уведомлением Клиента в срок за 5 (Пять) календарных дней до даты их вступления в силу путем размещения информации на информационных стендах Банка в местах обслуживания клиентов и/или на сайте Банка по адресу: www.capitalkredit.ru.

5. Права и обязанности Клиента

5.1. На основании имеющихся у Банка лицензий ФСБ Клиент имеет право осуществлять эксплуатацию предоставленных Банком сертифицированных ФСБ Программных и Аппаратных средств усиленной ЭП в Системе «iBank 2».

5.2. Перед началом эксплуатации Системы «iBank 2» Клиент обязан получить в Банке и самостоятельно установить на своем рабочем месте программные модули системы «iBank 2», Программные и Аппаратные средства усиленной ЭП (при решении Клиента использовать аппаратное средство).

5.3. Клиент обязуется использовать предоставленные средства усиленной ЭП только в Системе «iBank 2» без права их продажи или передачи каким-либо способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны уполномоченных органов за соблюдением требований и условий осуществления деятельности, связанной с использованием криптографических средств.

5.4. Клиент обязан обеспечивать сохранность и целостность программного комплекса Системы «iBank 2», включая предоставленные средства усиленной ЭП.

¹ Базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, а именно без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием, формирование и ведение которой осуществляются Банком России на основании части 5 статьи 27 Федерального закона от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе»;

5.5. Клиент обязан обеспечивать информационную безопасность рабочих мест ответственных сотрудников, уполномоченных использовать Систему «iBank 2» для взаимодействия с Банком. Клиент обязан исключить или максимально ограничить доступ к этим рабочим местам лиц, чья деятельность не связана с осуществлением электронного документооборота с банком.

5.6. Клиент обязан ознакомиться с описанием механизмов защиты системы «iBank 2» и памяткой клиенту об обеспечении информационной безопасности своего компьютера. Описание доступно на сайте банка по адресу https://ibank.capitalkredit.ru/faq.html#security_arrangements_IB. В случае если знаний Клиента недостаточно для адекватной оценки механизмов защиты системы и (или) обеспечения информационной безопасности своего компьютера, Клиент вправе обратиться к услугам сторонних специалистов. При этом оплата услуг специалистов производится Клиентом самостоятельно.

5.7. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к Системе «iBank 2» незамедлительно после момента обнаружения, любым доступным Клиенту способом, в том числе по средствам телефонной связи, электронной почты, с обязательным указанием кодового слова.

5.8. Клиент обязан незамедлительно после момента обнаружения извещать Банк обо всех случаях Компрометации ключей электронной подписи, любым доступным Клиенту способом, в том числе по средствам телефонной связи, электронной почты, с обязательным указанием кодового слова.

5.9. Клиент обязан в случае прекращения использования Системы «iBank 2» уничтожить полученные в Банке Программные средства усиленной ЭП и вернуть Аппаратные средства усиленной ЭП, предоставленные Банком.

5.10. Клиент обязан заполнять Электронные документы в Системе «iBank 2» в соответствии с действующим законодательством, в частности Положением Банка России «О правилах осуществления перевода денежных средств» от 29 июня 2021 г. № 762-П.

5.11. Клиент обязан хранить в секрете пароль к ключу электронной подписи и не передавать третьим лицам носитель с ключом электронной подписи, используемым в Системе «iBank 2».

5.12. Клиент обязан обеспечивать использование ключей электронной подписи только их владельцами (ответственными сотрудниками) в соответствии с установленными правами подписи.

5.13. Клиент обязан по требованию Банка прекратить использование указанного Банком ключа электронной подписи, сгенерировать новую Пару ключей ЭП и зарегистрировать новый Ключ проверки электронной подписи в Банке.

5.14. Клиент имеет право досрочно прекратить действие своей Активной пары ключей ЭП и потребовать от Банка заблокировать эту Пару ключей ЭП, оформив уведомление по форме Приложения 3.

5.15. Клиент имеет право по своему усмотрению генерировать новые Пары ключей ЭП и регистрировать в Банке новые Ключи проверки электронной подписи.

5.16. Клиент имеет право, позвонив по контактному телефону Банка и сообщив ответственному сотруднику Банка Блокировочное слово, временно заблокировать свою работу в Системе «iBank 2» до момента письменного уведомления об отмене действия Пары ключей ЭП или о возобновлении работы.

5.17. Клиент имеет право отказаться от получения одноразовых паролей на вход в систему «iBank 2», а также отказаться от получения одноразовых паролей на подтверждение платежа в виде sms-сообщений, принимая во внимание увеличение операционных рисков и возлагая на себя ответственность за причиненный в связи с этим ущерб.

5.18. Клиент имеет право на групповую подпись документов принимая во внимание увеличение операционных рисков и возлагая на себя ответственность за причиненный в связи с этим ущерб.

6. Совместные обязательства и ответственность Сторон

6.1. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами Ключа электронной подписи Клиента.

6.2. При расторжении настоящего Договора Стороны несут ответственность по всем Электронным документам, сформированным в Системе «iBank 2», в соответствии с настоящим Договором и действующим законодательством РФ.

6.3. В случае возникновения конфликтных ситуаций между Клиентом и Банком при использовании Системы «iBank 2», Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций» (Приложение 2), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. Действия Сторон согласно вышеуказанному Положению являются обязательной составляющей процедуры досудебного урегулирования споров.

6.4. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Системы «iBank 2», предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной стороны, участвующей в настоящем Договоре.

6.5. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств по настоящему Договору в случае возникновения обстоятельств непреодолимой силы. Обстоятельства непреодолимой силы понимаются в соответствии с п. 3 ст. 401 ГК РФ. Сторона, ссылающаяся на обстоятельства непреодолимой силы, обязана незамедлительно, но не позднее 48 (сорока восьми) часов, информировать в письменной форме другую Сторону о наступлении и прекращении подобных обстоятельств и об их влиянии на возможность исполнить обязательство. Отсутствие уведомления возлагает на нарушившую Сторону обязанность возместить другой Стороне ущерб, который в случае своевременного уведомления мог быть предотвращен.

7. Порядок обслуживания Клиента

7.1. Банк осуществляет прием Электронных документов, передаваемых по Системе «iBank 2», круглосуточно. При невозможности передачи документов в Банк с использованием Системы «iBank 2» документы могут поступить от Клиента на бумажном носителе.

7.2. Банк не несет ответственности за задержку в формировании выписок по счетам Клиента, если она связана с неполучением Банком информации о проведенных операциях по его корреспондентским счетам от банков-корреспондентов при Банке России.

7.3. При получении Электронного документа Банк производит в автоматизированном режиме проверку подлинности ЭП сотрудников Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчетном счете Клиента. В случае отбраковки Электронный документ Банком к исполнению не принимается.

7.4. В случае отмены платежа, изменения реквизитов, назначения платежа, суммы платежа Клиент обязуется известить об этом Банк, направив электронное письмо используя систему «iBank 2», а также подтвердить вышеуказанные изменения телефонным звонком, используя кодовое слово не позднее 20 (двадцати) минут с момента выставления платежа.

7.5. Банк не несет ответственности за работу непосредственно им не контролируемых каналов и оборудования связи, при помощи которых предоставляется доступ Клиента к СЭД.

7.6. Обслуживание Клиента по Системе «iBank 2» Банк осуществляет в соответствии с тарифами, установленными Банком и акцептованными Клиентом. Банк оставляет за собой право одностороннего изменения тарифов с обязательным уведомлением об этом Клиента не менее чем за 5 (пять) календарных дней до вступления в действие новых тарифов. Если Клиент не согласен обслуживаться в соответствии с новыми тарифами, он обязан расторгнуть данный договор в соответствии с п. 8.2. до наступления даты ввода в действие новых тарифов.

8. Срок действия Договора

8.1. Настоящий Договор вступает в силу с момента его заключения Сторонами и считается заключенным на неопределенный срок, но не более срока действия Договора(ов) банковского счета, заключенного(ых) между Сторонами. Прекращение Договора(ов) банковского счета, заключенного(ых) между Сторонами, влечет прекращение настоящего Договора.

8.2. Любая из Сторон вправе расторгнуть Договор в одностороннем порядке не ранее, чем через месяц после письменного уведомления об этом противоположной Стороны.

9. Заключительные положения

9.1. Споры по настоящему Договору решаются путем переговоров с учетом взаимных интересов в соответствии с Приложением 2. Все неурегулированные споры, возникающие между сторонами, рассматриваются в соответствии с действующим законодательством РФ в Арбитражном суде г. Москвы.

9.2. Изменение и дополнение условий настоящего Договора и Приложений к настоящему Договору производится Банком в одностороннем порядке, при этом соответствующее изменение/дополнение оформляется в виде новой редакции настоящего Договора, которая размещается на Официальном сайте Банка по адресу: www.capitalkredit.ru. Новая редакция настоящего Договора вступает в силу через 5 (Пять) рабочих дней с даты уведомления Клиента путем размещения новой редакции Договора на Официальном сайте Банка - www.capitalkredit.ru и/или на информационных стендах Банка в местах обслуживания клиентов.

9.3. Заключив настоящий Договор, Клиент выражает свое согласие на передачу и прием электронных документов в рамках электронного банкинга с использованием системы «iBank 2» на условиях, предложенных Банком.

9.4. Во всем, что не предусмотрено настоящим Договором, Стороны руководствуются положениями действующего законодательства.

10. Реквизиты Банка

БАНК:

Наименование:	Общество с ограниченной ответственностью Коммерческий банк «Столичный Кредит»
Юридический адрес:	105005, г.Москва, ул. Бауманская, д. 54, стр. 1
Почтовый адрес:	105005, г.Москва, ул. Бауманская, д. 54, стр. 1
Банковские реквизиты:	к/с 30101810000000000683 в ОКЦ №1 ГУ Банка России по ЦФО, БИК
ИНН:	044525683
КПП:	7718103767
ОГРН:	770101001
тел.:	1027739199927
факс:	(495) 229 -00-50
телекс:	(495) 795-07-61
e-mail :	485439 INT RU info@capitalkredit.ru



ЗАЯВЛЕНИЕ

на подключение к системе «iBank2»

1. Настоящим клиент _____ (далее - Клиент)
полное официальное наименование организации с организационно-правовой формой/Ф.И.О. Индивидуального предпринимателя
в соответствии со статьей 428 Гражданского кодекса Российской Федерации присоединяется к действующей редакции **Договора обмена электронными документами с использованием системы электронного банкинга "iBank2" (для юридических лиц и индивидуальных предпринимателей)** (далее – Договор), размещенного на сайте ООО КБ «Столичный Кредит» (далее – Банк) www.capitalkredit.ru, и просит подключить его к системе электронного банкинга "iBank2"

2. ИНН(К/ИО) Клиента _____ КПП Клиента _____ ОГРН/ОГРНИП Клиента _____
Местонахождение Клиента _____

3. Счета Клиента в ООО КБ «Столичный Кредит», по которым необходимо оказание услуг с использованием системы «iBank2»:

№ п/п	Счет в банке (20 знаков)	Наименование счета
1		
2		
3		
4		
5		

4. Лица, уполномоченные работать в системе «iBank2» (в соответствии с карточкой с образцами подписи и оттиска печати Клиента)²:

ФИО пользователя	
Занимаемая должность	
Документ (вид, номер, кем и когда выдан)	
Номер мобильного телефона для использования в целях, оговоренных в Договоре, а также в качестве средства подтверждения, в том числе для получения одноразовых паролей	
Валюта счета	Номер счета
1.	
2.	
3.	
4.	
5.	

в случае отсутствия второго лица в графе «ФИО пользователя» прописывается: «не предусмотрено»

ФИО пользователя	
Занимаемая должность	
Документ (вид, серия, номер, кем и когда выдан)	
Номер мобильного телефона для использования в целях, оговоренных в Договоре, а также в качестве средства подтверждения, в том числе для получения одноразовых паролей	

² Лица, уполномоченные работать в системе «iBank2» (в том числе без права подписи) допускаются к работе в системе только при условии получения Банком согласия о предоставлении ООО КБ «Столичный Кредит» права на получение и обработку персональных данных по форме Приложения № 10 к Договору.

Валюта счета	Номер счета
1.	
2.	
3.	
4.	
5.	

просмотр информации без права подписи (в случае отсутствия такого лица в графе «ФИО пользователя» прописывается: «не предусмотрено»)

ФИО пользователя	
Занимаемая должность	
Документ (вид, серия, номер, кем и когда выдан)	

5. Перечень электронных документов, передаваемых по Системе «iBank 2» и необходимое количество ЭП:

	Наименование Электронного документа	Количество ЭП (нужное подчеркнуть)
1	Платежное поручение	1 или 2
2	Платежное требование	1 или 2
3	Инкассовое поручение	1 или 2
4	Заявление об отказе от акцепта	1 или 2
5	Аккредитив	1 или 2
6	Заявление на перевод иностранной валюты	1 или 2
7	Поручения на обязательную продажу	1 или 2
9	Поручения на продажу иностранной валюты	1 или 2
10	Поручения на покупку иностранной валюты	1 или 2
11	Поручения на конвертацию иностранной валюты	1 или 2
12	Поручения на обратную продажу иностранной валюты	1 или 2
13	Отзыв	1 или 2
14	Письмо	1 или 2

6. Прошу подключить к тарифам по операциям, связанным с организацией и осуществлением электронного документооборота. С действующими тарифами на обслуживание клиента по системе "iBank2" и порядком их взимания ознакомлен.

_____/_____
подпись ФИО (полностью)

7. В целях использования системы электронного банкинга "iBank2" (отметить один из вариантов А или В):

Вариант А: предоставить аппаратные средства усиленной ЭП ^[1]	да ☐ нет ☐
Вариант В: использовать облачную электронную подпись (ОЭП)	да ☐ нет ☐

8. Блокировочное слово – уникальное слово, определяемое Клиентом при регистрации в Системе «iBank 2». Блокировочное слово может быть использовано Клиентом для блокирования своей работы в «iBank 2» по телефонному звонку в Банк (например, в случае компрометации ключа)

^[1]. Передача указанных средств и их носителей оформляется подписанием акта приема-передачи по форме Приложения № 4 к Договору.

9. Клиент подтверждает, что до заключения Договора проинформирован Банком об условиях работы в системе «iBank2», условиях использования ЭП, иных условиях Договора, а также ознакомлен с памяткой об обеспечении информационной безопасности. Клиент проинформирован об ограничениях способов и мест использования, мерах безопасного использования ЭП, случаях повышенного риска использования ЭП, способах и сроках уведомления о совершении каждой операции с использованием ЭП

подпись	ФИО (полностью)

Клиент:

Руководитель/Индивидуальный предприниматель _____ / _____ /
подпись ФИО

М.П. _____

« _____ » _____ 20 ____ г. _____
(контактный телефон)

Отметка о приеме:

Работник банка _____
(должность) (подпись) (расшифровка)

Дата/время приема « ____ » _____ 20__ г. ____:____



Приложение №2 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2"(для юридических лиц и
индивидуальных предпринимателей)»

ПОЛОЖЕНИЕ

о порядке проведения технической экспертизы при возникновении спорных ситуаций

1. В настоящем Положении под спорной ситуацией понимается существование претензий у Клиента к Банку (вместе в дальнейшем именуются Сторонами), справедливость которых может быть однозначно установлена в результате проверки Электронных подписей сотрудников Клиента в Электронных документах.
2. При возникновении спорной ситуации Клиент представляет Банку в письменном виде заявление, содержащее существо претензии с указанием на оспариваемую операцию по счёту Клиента. В заявлении также должно быть указано лицо (лица), уполномоченное представлять интересы Клиента в разрешительной комиссии.
3. Банк обязан в течение 5 (Пяти) рабочих дней с момента получения заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента и представители Банка. По согласованию Сторон в состав комиссии могут быть включены независимые эксперты. Независимый эксперт должен иметь высшее профессиональное образование в области информационной безопасности или в области информационных технологий, а также стаж работы в области информационной безопасности не менее 5 лет.
4. Банк обязан письменно, не позднее, чем за три рабочих дня до начала работы разрешительной комиссии, уведомить Клиента о назначенной дате, времени и месте начала работы комиссии.
5. Стороны обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов.
6. В случае если Клиент не направит своих представителей для участия в работе разрешительной комиссии, рассмотрение спорной ситуации осуществляется без представителей Клиента. В этом случае в Акте делается запись об отсутствии представителя Клиента.
7. В результате рассмотрения спорной ситуации разрешительная комиссия должна определить подлинность ЭП сотрудника Клиента в приложенном Электронном документе и обоснованность выполнения Банком операций по счёту Клиента.
8. Разрешительная комиссия проводит рассмотрение заявления в срок не более пяти рабочих дней с момента формирования комиссии. Рассмотрение заявления включает следующие этапы:
 - 8.1. Разрешительная комиссия проводит техническую экспертизу ключа (ключей) электронной подписи сотрудника(ов) Клиента.
 - 8.1.1. С использованием штатного программного обеспечения Системы «iBank 2» АРМ «Интернет-банкинг для корпоративных клиентов» выполняется распечатка заявления на выпуск сертификата ключа проверки ЭП сотрудника Клиента, соответствующего Ключу электронной подписи сотрудника клиента, которым был подписан спорный Электронный документ. По согласованию Сторон печатная форма Сертификата может быть получена с использованием штатного программного обеспечения Системы «iBank 2» АРМ «Администратор».
 - 8.1.2. Распечатанный сертификат сверяется с Сертификатом ключа проверки ЭП сотрудника Клиента, заверенным подписью уполномоченного лица Клиента и являющимся приложением к договору - сверяются шестнадцатеричные представления Ключей проверки ЭП. При обнаружении расхождений ситуация далее не рассматривается, комиссия составляет акт о выявленном несоответствии.
 - 8.2. Разрешительная комиссия проводит техническую экспертизу подлинности ЭП Клиента в Электронном документе.
 - 8.2.1. С использованием штатного ПО Системы «iBank 2» АРМ «Операционист» выбирается спорный Электронный документ и выполняется операция «Проверить ЭП».
 - 8.2.2. При невозможности получить доступ к документу через АРМ «Операционист», комиссией могут использоваться специализированные утилиты от разработчика Системы «iBank 2» для загрузки документа из Базы данных Системы «iBank 2» и автономной проверки.
 - 8.3. По взаимному согласию членов комиссии, автономную проверку подлинности ЭП может провести независимая организация, в том числе разработчик системы «iBank 2» - ОАО «БИФИТ». Эксперт, проводящий автономную проверку подлинности ЭП, должен иметь высшее профессиональное образование в области информационной безопасности или в области информационных технологий, а также стаж работы в области информационной безопасности не менее 5 лет.

В этом случае Банком не позднее пяти рабочих дней с момента принятия согласованного решения о проведении независимой экспертизы в независимую организацию направляются материалы для проведения проверки:

 - файлы, полученные в результате загрузки спорного документа из базы данных системы «iBank 2»;
 - копии заявлений на выпуск сертификатов ключа проверки ЭП сотрудников Клиента, заверенные обеими Сторонами;
 - подписанное обеими Сторонами письмо с просьбой о проведении проверки.

По результатам проверки независимая организация формирует заключение о подлинности ЭП в предоставленном документе и высылает его в адрес Банка.

Срок проведения независимой экспертизы не должен превышать одного календарного месяца с момента принятия согласованного решения о проведении независимой экспертизы.

В случае проведения независимой экспертизы подлинности ЭП в спорном электронном документе на возмездной основе, расходы по проведению экспертизы подлинности ЭП оплачивает Банк.

Если в результате проведения независимой экспертизы на возмездной основе будет подтверждена подлинность ЭП в спорном электронном документе, Клиент обязан возместить Банку стоимость проведения экспертизы подлинности ЭП на основании письменного требования Банка и выставленного счета.

8.4. На основании данных технической экспертизы разрешительная комиссия составляет акт, содержащий

- фактические обстоятельства, послужившие основанием возникновения разногласий;
- все реквизиты оспариваемого документа;
- порядок работы членов комиссии;
- вывод о подлинности ЭП в оспариваемом Электронном документе и его обоснование.

В случае если проводилась независимая проверка подлинности ЭП, к Акту прилагается подготовленное независимой организацией заключение о подлинности ЭП

Акт составляется непосредственно после завершения оценки всех обстоятельств, подлежащих установлению разрешительной комиссией, в двух экземплярах по экземпляру для каждой Стороны и подписывается всеми членами комиссии.

9. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

9.1. Банк не предъявляет Электронный документ, подписанный Клиентом, на основании которого Банк выполнил операции по счёту Клиента.

9.2. Банк не предъявляет заявление на выпуск сертификатов ключа проверки ЭП сотрудников Клиента, заверенные подписью руководителя и имеющие оттиск печати Клиента, соответствующие Ключам электронной подписи сотрудников Клиента, которыми был подписан спорный Электронный документ.

9.3. Хотя бы одна ЭП Клиента в Электронном документе оказалась не подлинной.

9.4. Клиент предоставляет Уведомление об отмене действия Пары ключей ЭП сотрудника Клиента, подписанное уполномоченным должностным лицом Банка и имеющее оттиск печати Банка. При этом указанная в Уведомлении дата окончания действия Пары ключей ЭП сотрудника Клиента раньше даты подписи, указанной в рассматриваемом Электронном документе.

10. В случае, когда Банк предъявляет Электронный документ и заявление на выпуск сертификатов ключей проверки ЭП сотрудника Клиента, подлинность ЭП Клиента в Электронном документе признана разрешительной комиссией, принадлежность Клиенту Сертификатов ключей проверки ЭП сотрудников Клиента подтверждена, Банк не несёт ответственности перед Клиентом по выполненным операциям по счёту Клиента.

11. Если Клиент настаивает на том, что данный документ он не создавал или не подписывал одной или несколькими ЭП, комиссия может вынести определение о Компрометации Ключа (ключей) электронной подписи Клиента, что не снимает с Клиента ответственности за данный документ.



Приложение № 3 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2" (для юридических
лиц и индивидуальных предпринимателей)

УВЕДОМЛЕНИЕ
об отмене действия Пары ключей ЭП сотрудника Клиента

(наименование клиента банка)

уведомляет Банк о том, что с «___» _____ 20__ г. считать недействительным Ключ проверки электронной подписи со следующим идентификатором _____.

Соответствующий ему Ключ электронной подписи утрачивает силу для дальнейшего применения с вышеуказанной даты.

Руководитель _____
(наименование клиента банка)

(ФИО руководителя)

(подпись)

М.П.



Приложение № 4 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2" (для юридических
лиц и индивидуальных предпринимателей)

АКТ № _____
передачи аппаратных средств усиленной ЭП

Общество с ограниченной ответственностью Коммерческий банк «Столичный Кредит», именуемое в дальнейшем «Банк», в лице _____ с одной стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего(ей) на основании _____, с другой стороны, вместе в дальнейшем именуемые «Стороны», принимая во внимание Договор оказания услуг электронного банкинга в системе «iBank 2», составили настоящий акт о том, что Банком надлежаще передан, а Клиентом получен носитель Рег. № _____ со следующими программными средствами:

Банком надлежаще переданы, а Клиентом получены со следующие аппаратные средства усиленной ЭП:

USB-токен «Рутокен ЭЦП 2.0»

С момента подписания Сторонами настоящего акта Банк считается исполнившим свои обязательства по передаче необходимых для работы Клиента средств в полном объеме.

Настоящий акт составлен в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

БАНК

(Ф.И.О., подпись)

М. П.

КЛИЕНТ

(Ф.И.О., подпись)

М. П.



Приложение № 5 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2" (для юридических
лиц и индивидуальных предпринимателей)

УВЕДОМЛЕНИЕ
об отмене действия Средства подтверждения

(наименование клиента банка)
уведомляет Банк о том, что с «___» _____ 20__ г. считать недействительным Средство подтверждения
_____ Клиента, со следующим идентификатором _____,
полученное от Банка на основании Акта № ___ приема-передачи от __.__._____.

Руководитель _____ (наименование клиента банка) _____ (ФИО руководителя) _____ (подпись)

М.П.



Приложение № 6 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2" (для юридических
лиц и индивидуальных предпринимателей)

ЗАЯВЛЕНИЕ

о регистрации (прекращении регистрации) мобильного телефона в качестве средства получения одноразовых паролей *

(наименование клиента банка)
просит Банк, с «___» _____ 20__ г. зарегистрировать (прекратить регистрацию) в системе «iBank 2» номер(а)
мобильного телефона _____ в качестве средства получения одноразовых паролей.

Ранее заявленные номера мобильных телефонов для подключения одноразовых паролей (указать):

Настоящим сотрудник _____
(наименование клиента банка)

(ФИО сотрудника Клиента)

подтверждает принадлежность ему указанного номера (ов) мобильного телефона и согласие на получение в любое время
суток одноразовых паролей на мобильный телефон с вышеуказанным номером.

*В случае оформления Клиентом Заявления на новый номер мобильного телефона для получения одноразовых паролей,
указываются все ранее заявленные номера мобильных телефонов сотрудника Клиента, указанного в Заявлении. Не
указанные в Заявлении ранее заявленные номера мобильных телефонов сотрудника Клиента, указанного в заявлении, для
получения одноразовых паролей отключаются Банком от получения таких паролей.

Руководитель _____
(наименование клиента банка)

(ФИО руководителя)

(подпись)

М.П.



Приложение № 7 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2"(для юридических
лиц и индивидуальных предпринимателей)

Рекомендации для работы с Системой «iBank 2».

Вопросы безопасности

Механизмы защиты информации в системе «iBank 2».

«iBank 2» относится к классу систем защищенного электронного документооборота.

Для обеспечения аутентичности (доказательства авторства) и целостности документа используется механизм ЭП под электронными документами.

Для обеспечения конфиденциальности используется механизм шифрования данных. При взаимодействии через Интернет осуществляется шифрование и контроль целостности передаваемой информации, проводится криптографическая аутентификация сторон.

В системе реализованы российские криптографические алгоритмы в соответствии с ГОСТ Р 34.12-2018 (шифрование, имитовставка), ГОСТ Р 34.11-2012 (хеш-функция) и ГОСТ Р 34.10-2012 (Электронная подпись).

Для использования функций криптографической защиты в системе «iBank 2» встроена поддержка многоплатформенных криптобиблиотек, сертифицированных ФСБ.

Дополнительные механизмы безопасности корпоративных клиентов.

- SMS-информирование клиентов о входе в систему, о поступлении в банк платежных документов, о движении средств по счетам клиентов.
- Расширенная многофакторная аутентификация при входе в систему с использованием одноразовых паролей.
- Механизм дополнительного подтверждения платежных поручений одноразовыми паролями (дополнительно к ЭП).

В качестве источников одноразовых паролей в системе «iBank 2» используются SMS-сообщения

Какие меры безопасности необходимо соблюдать при работе в Internet-Банкинге?

Меры безопасности при работе с ЭП:

- Для защиты ключей ЭП от хищения вредоносными программами рекомендуется использовать USB-токен или смарт-карту «Рутокен ЭЦП 2.0»;
- Пароль на доступ к ключу ЭП должен быть известен только Вам как владельцу;
- Не допускайте постоянного и бесконтрольного подключения к компьютеру USB-токена и смарт-карты «Рутокен ЭЦП 2.0»;
- Не передавайте «Рутокен с ключами ЭП никому;
- Не пользуйтесь Internet-Банкингом в Интернет-кафе, а также там, где Вы не уверены в безопасности компьютеров;
- При увольнении ответственного сотрудника, имевшего доступ к ключу ЭП, обязательно сообщите в Банк и заблокируйте ключ;
- При возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно сообщить в Банк и заблокировать ключи ЭП.

Меры по защите компьютера, с которого осуществляется работа в Internet-Банкинге:

- Соблюдайте регламент ограниченного физического доступа к данному компьютеру. Должен быть утвержден список сотрудников организации, включая ответственных сотрудников и технический персонал, которым разрешен доступ к компьютерам, с которых осуществляется работа в Internet-Банкинге.
- Рекомендуется использовать отдельный компьютер исключительно для работы в Internet-Банкинге. Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.
- Используйте в работе только лицензионное ПО. Не загружайте и не устанавливайте ПО полученное из непроверенных источников.
- Старайтесь использовать современные операционные системы (ОС). Данные системы являются более защищенными, в отличие от предыдущих, зачастую устаревших версий. Своевременно устанавливайте исправления и обновления для ОС. Включите автоматическое обновление ОС, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости ОС.
- Используйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений.

- Используйте и оперативно обновляйте специализированное ПО для защиты информации — антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.
- Не подключайте к компьютеру непроверенные на наличие вирусов отчуждаемые носители.
- Регулярно проверяйте Ваш компьютер на вирусы, как минимум раз в неделю.

Правила безопасной работы в Интернете:

- Не нажимайте на всплывающие окна, которые содержат рекламу. Желательно настроить Ваш браузер на автоматическую блокировку таких окон.
- Не посещайте непроверенные и небезопасные сайты. Вы можете непреднамеренно загрузить на свой компьютер вирусы и шпионские программы.
- Не читайте подозрительных электронных писем от незнакомых людей, они могут содержать вирусы. Читайте темы сообщений внимательно, если не уверены, что письмо пришло из надежного источника, не открывайте его. Не доверяйте дружественному тону сообщений или срочности содержащейся в них просьбы. В подозрительных письмах не нажимайте на содержащиеся в письме ссылки, а также не открывайте вложенные файлы, особенно если в письме указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл, который имеет файловое расширение ".exe".
- Максимально ограничьте использование Интернет-пейджеров. Будьте внимательнее к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений просканируйте свой компьютер на наличие вирусов или шпионского ПО.

Меры по безопасному использованию облачной ЭП

- При использовании web-браузера в качестве интерфейса для осуществления доступа к сервису облачной ЭП отключите функции автоматического сохранения пароля и логина. *(По умолчанию эта опция может быть включена во многих популярных браузерах, служит она для повышения удобства, однако в ущерб безопасности)*
- Используйте и оперативно обновляйте специализированное ПО для защиты информации — антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр./ *(По мимо стандартного функционала защиты компьютера от вирусов, во многие современные антивирусные продукты встроены дополнительные фишки безопасности, как то модули анти-фишинга, контроля целостности настроек браузера, проверка защищенных соединений, возможности вводить пароль используя виртуальную клавиатуру, которая появляется на странице авторизации к облачному сервису. Это обеспечивает защиту от кейлоггеров и троянов – программ, записывающих и отправляющих злоумышленнику данные введенные пользователями с клавиатуры).*
- Убедитесь в том, что на страничке авторизации к облачному сервису используется защищенный протокол HTTPS, обеспечивающий шифрованную передачу данных от пользователя к серверу. Так же обращайте внимание на сертификат сайта, подтверждающий его легитимность. *(как правило это выглядит в виде небольшой иконки с изображением зеленого замочка рядом с URL-адресом открытой страницы, щелкнув по которому можно получить дополнительную информацию).*
- При использовании смартфонов как средства доступа будьте уверены в том, что вы не используете «рутованную» версию прошивки Android или установленный Jailbreak для гаджетов от Apple. Модифицированные и не поддерживаемые официальным производителем прошивки для смартфонов могут содержать в себе закладки или недокументированные возможности, которые злоумышленник при определенных условиях с успехом сможет использовать. Не устанавливайте приложения из посторонних источников, а по возможности вообще минимизируйте список софта, который у вас будет установлен на телефоне.
- Не при каких обстоятельствах никогда не сообщайте посторонним лицам, в том числе работникам банка или службе поддержке, никаких кодов, смс-сообщений, парольных и контрольных фраз. Все действия, предусмотренные услугой (сервисом), которые вы можете делать должны выполнять только лично вами без каких-либо посредников. Исключение составляет только первичная идентификация вас как клиента, к примеру, по паспортным данным и ключевой фразе.

Руководства пользователя по использованию ПО и ДБО, а также инструкции по выпуску сертификата ЭП можно получить в службе поддержки Банка, в электронном виде в системе ДБО и на официальном сайте Банка www.capitalkredit.ru.



Приложение № 8 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2" (для юридических
лиц и индивидуальных предпринимателей)

Заявление

(наименование клиента Банка),
в лице _____
(Должность, Ф.И.О.)
отказывается от получения одноразовых паролей на вход в систему «iBank 2», одноразовых паролей на подтверждение
платежа в виде SMS-сообщений, и в этой связи

(наименование клиента Банка)
соглашается с увеличением степени риска несанкционированного доступа в систему третьих лиц, а также внедрения
вредоносного программного обеспечения и прочих фактов, приводящих к явному и/или неявному несанкционированному
доступу к системе управления счетами «iBank2».

В связи с этим _____
(наименование клиента Банка)
принимает ответственность за причиненный ущерб на себя.

Руководитель _____
(наименование клиента банка) (ФИО руководителя) (подпись)

М.П.



Приложение № 9 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2" (для
юридических лиц и индивидуальных предпринимателей)

Заявление

От _____,
(наименование клиента Банка)

в лице _____
(должность, Ф.И.О.)

прошу предоставить возможность одновременного подписания нескольких документов (одно уведомление на подпись одного пакета документов) в системе «iBank2», и в этой связи

(наименование клиента Банка)

соглашаюсь с увеличением риска несанкционированного доступа в систему третьих лиц, вредоносного программного обеспечения и прочих фактов, приводящих к явному и/или не явному несанкционированному доступу в системе «iBank2».

В случае несоблюдения _____
(наименование клиента Банка)

требований по обеспечению безопасности ключевой информации указанных в п. 6.1 Договора СЭД, Банк не несет ответственности за ущерб, причиненный _____,
(наименование клиента Банка)

а также за возникновение чрезвычайных ситуаций и несанкционированного доступа третьих лиц к системе управления счетами _____ в системе «iBank2».
(наименование клиента Банка)

Руководитель _____
(наименование клиента банка)

(ФИО руководителя)

(подпись)

МП



Приложение № 10 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2" (для юридических
лиц и индивидуальных предпринимателей)

Согласие

о предоставлении ООО КБ «Столичный Кредит» права на получение и обработку персональных данных

Я, _____
(должность, наименование юридического лица, ФИО)

выражаю свое согласие предоставить оператору ООО КБ «Столичный Кредит» (ИНН 7718103767, адрес: 105005 г. Москва, ул. Бауманская, д.54, стр.1) право на получение и обработку, в том числе автоматизированную, распространение своих персональных данных согласно Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных» (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, телефон, электронная почта, занимаемая должность, иная информация (ИНН, СНИЛС и т.д.)), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение в целях заключения и исполнения договорных обязательств, а также в целях получения мной информации (в т.ч. формирования для меня предложений) о новых продуктах и услугах Банка.

Обработка Оператором моих персональных данных, указанных в настоящем Согласии (далее – Согласие) и в иных предоставленных мною документах, а также моих биометрических персональных данных (при наличии), означает совершение любых действий с использованием средств автоматизации и/или без средств автоматизации, в том числе сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Персональные данные, указанные в настоящем Согласии, включая, фамилия, имя, отчество; данные документа, удостоверяющего личность; адрес; иные данные указанные в настоящем Согласии; а также гражданство; год, месяц, число и место рождения; контактные телефоны, почтовые адреса, адреса электронной почты и другие сведения, предоставленные мною и полученные Оператором (в том числе в электронном виде) при приеме на обслуживание и в процессе оказания мне услуг, заключения и/или исполнения договоров с Оператором, содержащиеся в заявлениях, письмах, соглашениях и иных документах, а также любую иную информацию, доступную либо полученную Оператором от государственных и иных органов и организаций, предоставляются в целях приема на обслуживание и в процессе оказания мне услуг, принятия решения о предоставлении Заемщику кредита, принятия решения о предоставлении мне кредита(-ов), заключения и/или исполнения договоров с Оператором. В указанных целях Оператор может осуществлять передачу моих персональных данных в объеме, необходимом для указанных целей, третьим лицам, которым Оператор поручает обработку персональных данных на основании заключаемых с этими лицами договорами и при условии, что они обязуются обеспечить безопасность персональных данных при их обработке и предотвращение их разглашения. Указанные лица вправе осуществлять действия с моими персональными данными аналогичные действиям, которые вправе осуществлять Оператор.

Согласие предоставляется на срок 10 (десять) лет и может быть отозвано путем предоставления в Банк заявления об отзыве в письменной форме.

« ____ » _____ 20__ г.

_____ / _____ /



Приложение №11 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2"(для юридических лиц и
индивидуальных предпринимателей)»

Заявление на выпуск СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ "iBank"

1. Наименование организации _____

2. Место нахождения юр. Лица _____

3. ОГРН* _____ дата внесения в ЕГРЮЛ (ЕГРИП)* «__» _____

4. ИНН (КИО) _____ 5. КПП* _____

6. Тел. _____ 7. Факс* _____ 8. E-mail* _____

9. Сведения о владельце ключа
Фамилия, имя, отчество _____
Должность _____
Документ, удостоверяющий личность _____

серия _____ номер _____ дата выдачи «__» _____
кем выдан _____
код подразделения _____

10. Примечания* _____

* обязательно для заполнения

Настоящим подтверждаю согласие на обработку банком моих персональных данных _____

подпись

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа проверки ЭП _____ Идентификатор устройства _____

Наименование криптосредств _____

«_____»

Алгоритм _____ ID набора параметров алгоритма _____

Представление ключа проверки ЭП в шестнадцатеричном виде

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Личная подпись владельца ключа проверки ЭП



Срок действия (заполняется банком):

с «__» _____ 20__ г.

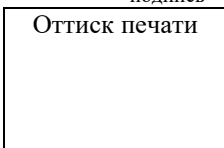
по «__» _____ 20__ г.

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках договора на обслуживание в системе "iBank" N _____ от "___" _____ 20__ г.

Достоверность приведенных данных подтверждаю

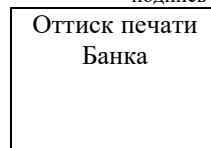
Руководитель организации

_____/_____
подпись / Ф.И.О.



Уполномоченный представитель банка

_____/_____
подпись / Ф.И.О.

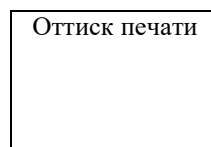


Дата приема сертификата
ключа проверки ЭП

«__» _____ 20__ г.

Администратор безопасности системы

_____/_____
подпись / Ф.И.О.



Дата регистрации сертификата
ключа проверки ЭП

«__» _____ 20__ г.



Приложение №12 к
Договору обмена электронными документами
с использованием системы электронного банкинга "iBank2"(для юридических лиц и
индивидуальных предпринимателей)»

Заявление на выпуск СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ "iBank"

1. Наименование организации _____

2. Место нахождения юр. Лица _____

3. ОГРН* _____ дата внесения в ЕГРЮЛ (ЕГРИП)* «__» _____

4. ИНН (КИО) _____ 5. КПП* _____

6. Тел. _____ 7. Факс* _____ 8. E-mail* _____

9. Сведения о владельце ключа
Фамилия, имя, отчество _____
Должность _____
Документ, удостоверяющий личность _____

серия _____ номер _____ дата выдачи «__» _____
кем выдан _____
код подразделения _____

10. Примечания* _____

* обязательно для заполнения

Настоящим подтверждаю согласие на обработку банком моих персональных данных _____

подпись

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа проверки ЭП _____ Идентификатор устройства _____
Наименование криптосредств « _____
Алгоритм _____ ID набора параметров алгоритма _____

Представление ключа проверки ЭП в шестнадцатеричном виде

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Личная подпись владельца ключа проверки ЭП

Срок действия (заполняется банком):

с «__» _____ 20__ г.

по «__» _____ 20__ г.

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках договора на обслуживание в системе "iBank" N _____
от "___" _____ 20__ г.

Достоверность приведенных данных подтверждаю

Руководитель организации

_____/_____/_____

подпись

Ф.И.О.

Оттиск печати

Уполномоченный представитель банка

_____/_____/_____

подпись

Ф.И.О.

Оттиск печати
Банка

Дата приема сертификата
ключа проверки ЭП

«__» _____ 20__ г.

Администратор безопасности системы

_____/_____/_____

подпись

Ф.И.О.

Оттиск печати

Дата регистрации сертификата
ключа проверки ЭП

«__» _____ 20__ г.

Доверенность

Банку _____
от клиента _____

Настоящим доверяем ООО КБ "Столичный Кредит" хранить ключ ЭП в защищенном хранилище и использовать его для формирования ЭП под документами системы "iBank".

1. Сведения о ключе проверки ЭП		
1.1	Идентификатор	
1.2	Хранилище	
1.3	Наименование криптосредств	
3.4	Алгоритм	
3.5	ID набора параметров алгоритма	
3.6	Представление ключа проверки ЭП	00 00

Руководитель организации

_____/_____
подпись Ф.И.О.

Оттиск печати