КОММЕРЧЕСКИЙ БАНК
СЛАВЯНСКИЙ КРЕДИТ

Договор
оказания услуг электронного банкинга в системе «iBank 2» в ООО КБ «Славянский кредит»

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Если не указано иное, термины и определения, используемые в Договоре на оказание услуг электронного банкинга в Системе «iBank 2» в ООО КБ «Славянский кредит» (далее - **Договор),** имеют следующие значения:

«Автоматизированная Банковская Система» (АБС) - комплекс программного и технического обеспечения, направленный на автоматизацию процессов взаимодействия Банка и Клиента.

«Активный ключ ЭЦП Клиента» – Открытый ключ ЭЦП Клиента, зарегистрированный Банком в Системе «iBank 2», срок действия которого не истек и который не был явно заблокирован ответственным сотрудником банка.

Банк - ООО КБ «Славянский кредит», включая его обособленные и внутренние структурные подразделения.

«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).

«Группа подписи ключа» – полномочия ключа ЭЦП при подписи Электронного документа. По аналогии с собственноручной подписью, образец которой есть в Банковской карточке с образцами подписей и оттиском печати, 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 Приложении 4 к настоящему Договору (по одной подписи каждой группы).

«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).

Клиент - юридическое лицо (резидент РФ или нерезидент), за исключением кредитной организации, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой.

«Открытый ключ ЭЦП Клиента» – ключ (последовательность байт), зависящий от Секретного ключа ЭЦП Клиента, самостоятельно генерируемый Клиента с использованием средств Системы «iBank 2», и предназначенный для проверки Банком подлинности ЭЦП в Электронном документе, сформированном Клиентом.

«Пара ключей ЭЦП» – Секретный ключ ЭЦП и соответствующий ему Открытый ключ ЭЦП.

Персональный аппаратный криптопровайдер (ПАК) – электронное средство платежа, специализированное аппаратное средство (USB-токен), предназначенное для генерации пары ключей ЭЦП, хранения сгенерированных секретных ключей ЭЦП, формирования ЭЦП под документами с использованием встроенного в устройство **СКЗИ**. Применяется в целях повышения безопасности электронного документооборота между Клиентом и Банком и полного исключения возможности несанкционированного копирования или хищения секретных ключей ЭЦП.

«Подлинная ЭЦП» – Электронная цифровая подпись в Электронном документе, проверка которой с использованием соответствующего Открытого ключа ЭЦП дает положительный результат.

«Секретный ключ ЭЦП Клиента» – ключ (последовательность байт), генерируемый уполномоченным сотрудником Клиента с использованием средств Системы «iBank 2», и предназначенный для формирования Клиентом Электронной цифровой подписи в Электронных документах.

«Сертификат открытого ключа ЭЦП Клиента» – бумажный документ с представленным в шестнадцатеричном виде Открытым ключом ЭЦП Клиента, идентификатором ключа, датой начала и окончания действия Открытого ключа ЭЦП Клиента, фамилией, именем и отчеством владельца ключа ЭЦП, заверенный подписью руководителя и имеющий оттиск печати Клиента.

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.

Средство криптографической защиты информации (СКЗИ) – программный модуль или программно-аппаратное средство, входящее в состав Системы «iBank 2», обеспечивающее защиту информации в соответствии с утвержденными стандартами (ГОСТ 28147-89, ГОСТ Р34.10-2001, ГОСТ Р34.11-94) и сертифицированное в соответствии с действующим законодательством.

Статус расчетного (платежного) документа Клиента в Системе «iBank2» - процесс обработки документов в АБС Банка, поступивших по Системе «iBank 2».

В Системе «iBank 2» предусмотрены следующие статусы документов:

«Новый» — присваивается при создании и сохранении нового документа клиентом, при редактировании и сохранении существующего документа, а также при импорте документа из файла, сформированного в программах 1С-Бухгалтерия, Бизнес-Пак и других бухгалтерских про-граммах. Документ в статусе Новый банк не рассматривает и не обрабатывает;

«Подписан» — присваивается в случае, если документ подписан, но число подписей под доку-ментом меньше необходимого. При внесении изменений в документ в таком статусе и его последующем сохранении статус документа меняется на Новый;

«Доставлен» — присваивается документу, когда число подписей под документом соответствует необходимому для его рассмотрения банком. Статус Доставлен является для банка указанием начать обработку документа (исполнить или отвергнуть);

«На обработке» — присваивается при принятии документа к обработке;

«На исполнении» — присваивается при принятии документа к исполнению. Принятие документа к исполнению означает, что документ оформлен верно, денежных средств достаточно на

счете клиента, нет ограничений на исполнение данного платежа. Документ обработан в АРМ «Операционист. Корпоративные клиенты», денежные средства списаны со счета Клиента и готовы к отправке в Главное Управление Банка России по Центральному Федеральному округу г. Москва;

«Исполнен» — присваивается документу при его исполнении банком и получении подтверждения списания по выписке из Главного Управления Банка России по Центральному Федеральному округу г. Москва;

«Отвергнут» — присваивается документу, не принятому к исполнению. Клиент может или отредактировать и сохранить документ (статус станет Новый), или удалить документ (статус станет Удален);

«Удален» — присваивается документу, удаленному пользователем. Удалению подлежат только документы в статусе Новый, Подписан или Отвергнут.

Сторона - Банк или **Клиент.**

Стороны - Банк и **Клиент.**

Счет - расчетный счет в рублях РФ, текущий валютный счет в иностранной валюте (транзитный валютный счет, открывающийся одновременно с текущим валютным счетом), открытый Клиенту в ООО КБ «Славянский кредит».

Тарифы Банка – тарифы комиссионного вознаграждения по банковским операциям и другим услугам, оказываемым Клиентам ООО КБ «Славянский кредит», утвержденные приказами по Банку.

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

«Электронная цифровая подпись» (ЭЦП) – совокупность байт, однозначно сопоставляемая Электронному документу и используемая подтверждения авторства и целостности Электронного документа.

«IP-фильтрация» - ограничение возможности подключения к Системе «iBank2» через глобальную сеть Интернет. (порядок предоставления данной услуги описан в Приложении №8 к настоящему Договору).

“SMS-Банкинг” – информационно-оповестительный канал, предназначенный для уведомления клиентов о событиях, происходящих в Системе «iBank 2» посредством рассылки SMS-сообщений на сотовые телефоны (порядок предоставления данной услуги описан в Приложении № 8 к настоящему Договору).

2. ПРЕДМЕТ ДОГОВОРА.

2.1. Банк, имеющий Лицензию ФСБ РФ № 15478 Н от 10 октября 2016г. на техническое обслуживание шифровальных (криптографических) средств, на распространение шифровальных (криптографических) средств, на предоставление услуг в области шифрования информации, и Клиент заключили настоящий Договор присоединения Клиента к изложенным в Договоре условиям (акцепта условий) в соответствии со статьей 428 Гражданского кодекса Российской Федерации путем передачи Клиентом (его уполномоченным представителем) в Банк **Заявления на заключение договора на оказание услуг электронного банкинга в системе «iBank 2» в ООО КБ «Славянский кредит»**, оформленного в двух экземплярах по форме Приложения № 1 к настоящему Договору.

2.2. Банк оказывает Клиенту услуги электронного банкинга с использованием Системы «iBank 2», позволяющей обмениваться следующими электронными документами:

- платежное поручение;
- поручение на покупку иностранной валюты;
- поручение на продажу иностранной валюты;
- распоряжение на обязательную продажу иностранной валюты;
- поручение на конвертацию;
- заявление на перевод иностранной валюты;
- выписки по счету;
- справка о валютных операциях;
- справка о подтверждающих документах;
- паспорт сделки по контракту;
- паспорт сделки по кредитному договору;
- подтверждающие документы для осуществления денежных переводов;
- отзыв документа;
- информационное письмо.

Передача иной информации по сети не является основанием для возникновения у Сторон обязательств по договору. Инициатором сеансов связи с Банком, как правило, является Клиент.

2.3. Текст Договора публикуется на сайте Банка в сети Интернет по адресу: http://www.slavcred.ru/, размещается на стендах в операционных залах Банка. По запросу Клиента текст Договора может быть передан Клиенту на бумажном носителе или выслан в электронной форме в формате PDF по адресу электронной почты, указанному в запросе.

3. СОГЛАШЕНИЯ СТОРОН.

3.1. Стороны признают, что применяемая в Системе «iBank 2» криптографическая защита информации, обеспечивающая шифрование, контроль целостности и создание ЭЦП с применением ПАК и СКЗИ достаточна для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства Электронных документов.

3.2. Стороны признают, что применяемая в ПАК технология генерации и хранения Секретного ключа ЭЦП и формирования ЭЦП под документом полностью исключает возможность получения прямого доступа к Секретному ключу ЭЦП с целью его копирования, переноса на внешний носитель или использования для формирования ЭЦП вне ПАК.

3.3. ПАК являются собственностью Банка и предоставляются для использования Клиенту на безвозмездной основе во временное пользование.

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

3.5. Стороны признают, что подделка ЭЦП Клиента, то есть создание Подлинной ЭЦП Электронного документа от имени Клиента, невозможна без использования Секретного ключа ЭЦП Клиента.

3.6. Стороны признают, что Электронные документы, заверенные необходимым количеством ЭЦП, 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 ЭЦП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

3.7. Стороны признают, что Электронные документы с ЭЦП Клиента, полученные Банком по Системе «iBank 2», являются доказательным материалом для решения спорных вопросов в соответствии с Приложением № 3 настоящего Договора («Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций»), в том числе предусмотренных п.п. 4.4.6.-4.4.10. и 4.5.4. настоящего Договора. Электронные документы, не имеющие необходимого количества ЭЦП, при наличии спорных вопросов не являются доказательным материалом.

3.8. Стороны признают, что Открытый ключ ЭЦП Клиента, содержащийся в Сертификате Открытого ключа ЭЦП Клиента, заверенном подписью руководителя и оттиском печати Клиента, принадлежит соответствующему сотруднику Клиента.

3.9. Стороны признают, что срок действия Секретного ключа ЭЦП Клиента устанавливается Банком и не может превышать два года с момента регистрации Открытого ключа ЭЦП Клиента в Системе «iBank 2». Замена Секретного ключа ЭЦП Клиента с истекшим сроком производится без взимания дополнительной платы.

3.10. Стороны признают, что основным способом уведомления (информирования) Клиента о каждой операции, совершенной с использованием ПАК, является отображение статуса расчетного (платежного) документа Клиента в Системе «iBank2».

3.11. Стороны признают, что обязанность Банка по направлению Клиенту уведомлений о совершенных операциях способом, указанным в п. 3.10. настоящего Договора, считается исполненной с момента отображение Банком статуса расчетного (платежного) документа Клиента в Системе «iBank2».

3.12. Стороны признают, что безотзывность перевода денежных средств, осуществленного в рамках Системы «iBank2», наступает с момента списания денежных средств с банковского счета Клиента, что соответствует отображенному в Системе статусу расчетного (платежного) документа - «На исполнении».

3.13. Стороны признают, что в качестве форм уведомления Клиента о совершенных операциях могут быть использованы следующие способы:

получение Клиентом электронной выписки по Системе «iBank2»;

получение Клиентом выписки на бумажном носителе в Центральном и (или) дополнительных офисах Банка;

отправка SMS-сообщения Клиенту в момент совершения операции (далее – SMS-информирование) через *информационно-оповестительный* канал «SMS-Банкинг».

SMS-сообщение содержит идентификатор ключа проверки ЭЦП, Ф.И.О. владельца ЭЦП, а также дополнительную информацию в зависимости от индивидуальной настройки Клиентом параметров SMS-сообщений. При направлении Банком SMS-сообщения Клиенту, SMS-сообщение считается полученным Клиентом в дату отправления SMS-сообщения Банком в соответствии с имеющейся у Банка информацией для связи с Клиентом. Подключение к услуге «SMS-Банкинг» является дополнительным сервисом для Клиентов.

3.14. Стороны признают, что в случае, если, в соответствии с имеющимися в Банке учредительными документами Клиента, срок полномочий сотрудника Клиента истек, Секретный ключ ЭЦП данного сотрудника Клиента блокируется до продления срока полномочий.

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

3.16. Стороны признают, что поступившее в Банк информационное письмо, подписанное ЭЦП, с вложенным файлом в виде отсканированной копии документа, составленного на бумажном

носителе, признаётся Сторонами представлением Клиентом копии указанного документа, заверенного уполномоченными лицами Клиента и его печатью.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН.

4.1. Стороны обязуются при осуществлении электронных платежей руководствоваться правилами и техническими требованиями, установленными законодательством Российской Федерации, а также соответствующими приложениями к настоящему Договору.

4.2. Каждая Сторона имеет право запрашивать, и обязана предоставлять по запросам другой Стороны бумажные копии электронных расчетных документов, оформленные надлежащим образом.

4.3. Каждая Сторона обязана за собственный счет поддерживать в рабочем и исправном состоянии свои программно – технические средства, используемые при проведении электронных платежей по договору.

4.4. Права и обязанности Банка:

4.4.1. Банк обязан принимать к исполнению Электронные документы, полученные по Системе «iBank 2» от Клиента, подписанные необходимым количеством ЭЦП Клиента и соответствующие действующему законодательству РФ.

4.4.2. Банк обязан предоставлять Клиенту необходимые инструкции (рекомендации) для работы с Системой «iBank 2».

4.4.3. Банк обязан передать Клиенту ПАК и Инструкцию по первичной регистрации Клиента до начала работы Клиента в Системе «iBank 2». При этом Банк обязан предать не менее одного ПАК. Факт передачи фиксируется в Акте передачи по форме Приложения № 2 к настоящему Договору.

4.4.4. Банк обязан по письменному требованию Клиента блокировать в Системе «iBank 2» существующие Активные ключи ЭЦП Клиента и регистрировать новые Открытые ключи ЭЦП Клиента.

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

4.4.6. Банк обязан информировать Клиента о совершении каждой операции с использованием ПАК не позднее следующего рабочего дня после даты ее совершения способом, указанным в п. 3.10. настоящего Договора.

4.4.7. Банк обязан предоставлять Клиенту электронные выписки по счету, сформированные с использованием Системы «iBank2», за указанный Клиентом период.

Банк обязуется предоставлять Клиенту по его письменному требованию выписки по счету на бумажном носителе его уполномоченному представителю в Центральном и (или) дополнительных офисах Банка.

Выписка содержит информацию о всех совершенных операциях, а также об остатке средств на счете Клиента.

4.4.8. Банк обязан рассмотреть письменное уведомление Клиента, указанное в п.п. 4.5.4. настоящего Договора, в порядке и в сроки, установленные Приложением № 3 к настоящему Договору («Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций»).

4.4.9. Банк обязан возвратить Клиенту суммы операций, признанных правомерно опротестованными, на его счет не позднее следующего рабочего дня с даты принятия Банком решения о возврате средств Клиенту.

4.4.10. В случае, если Банк не исполняет обязанность, установленную п.п. 4.4.6. настоящего Договора, Банк обязан возместить Клиенту сумму операции, о которой Клиент не был информирован и которая была совершена без согласия Клиента. При этом Клиент обязан представить в Банк соответствующее письменное уведомление. Сроки рассмотрения Банком письменного уведомления Клиента, а также сроки возврата Клиенту сумм совершенных операций, соответствует срокам, установленным п.п. 4.4.8. и 4.4.9. настоящего Договора.

В случае, если Банк исполняет обязанность, предусмотренную п.п. 4.4.6. настоящего Договора, и Клиент не представил Банку через своего уполномоченного представителя уведомление, оформленное в соответствии с требованиями п.п. 4.5.4 настоящего Договора, Банк не обязан возместить Клиенту суммы операций, совершенных без его согласия.

4.4.11. Банк имеет право по своему усмотрению без уведомления Клиента блокировать Активный ключ сотрудника ЭЦП Клиента и потребовать от Клиента смены Пары ключей ЭЦП.

4.4.12. Банк имеет право после предварительного предупреждения отказать Клиенту в приеме от него распоряжений на проведение операций по банковскому счету (вкладу), подписанных ЭЦП Клиента**,** в случае выявления Банком сомнительных операций Клиента**,** а также, если Клиентом не были предоставлены в Банк затребованные у него документы.

4.4.13. При наличии обоснованных подозрений о Компрометации Секретных ключей ЭЦП 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.

4.4.14. В случае начала активного использования Клиентом счета, по которому продолжительное время не проводились операции, включая операции по зачислению денежных средств, либо проводятся в незначительных объемах, подпадающего под негативные признаки, указанные в нормативных актах или в иных документах Банка России, Банк имеет право приостановить предоставление Клиенту услуг электронного банкинга с использованием Системы «iBank 2».

4.4.15. Банк вправе возобновить предоставление Клиенту услуг электронного банкинга с использованием Системы «iBank 2» при условии:

- личного обращения в Банк физического лица, исполняющего функции единоличного исполнительного органа Клиента;

- обновления сведений о Клиенте, представителе Клиента, выгодоприобретателе, бенефициарном владельце, предусмотренных федеральными законами и нормативными актами Банка России, а также рассмотрения вопроса о запросе у Клиента документов с расчетом сумм НДФЛ, исчисленных и удержанных им в качестве налогового агента, как минимум за последний отчетный период, документов (в том числе в виде выписок с банковских счетов, открытых клиенту в других кредитных организациях), подтверждающих исполнение Клиентом своей обязанности по уплате налогов или других обязательных платежей в бюджетную систему Российской Федерации, оплату комму-

нальных услуг, арендных платежей за недвижимое имущество и иных платежей, связанных с деятельностью Клиента, и анализа представленных клиентом документов;

- представления Клиентом объяснений о причинах начала активного использования счета, подтверждаемых соответствующими договорами (контрактами) и (или) иными документами.

4.5. Права и обязанности Клиента**:**

4.5.1. На основании имеющихся у Банка лицензий ФСБ РФ Клиент имеет право осуществлять эксплуатацию предоставленной(го) Банком сертифицированной(го) ФСБ ПАК и СКЗИ в Системе «iBank 2» без получения лицензии ФСБ РФ на использование криптографических средств.

4.5.2. Перед началом эксплуатации Системы «iBank 2» Клиент обязан получить в Банке и самостоятельно установить на своем рабочем месте драйвер ПАК и необходимое программное обеспечение, зарегистрироваться в Системе «iBank 2». Инструкция по установке драйвера ПАК, установке необходимого программного обеспечения и регистрации в системе доступна на официальном сайте Банка https://www.slavcred.ru/.

4.5.3. Клиент обязуется использовать предоставленный ПАК только в Системе «iBank 2» без права его продажи или передачи каким-либо способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны уполномоченных органов за соблюдением требований и условий осуществления лицензионной деятельности.

4.5.4. Клиент обязан обеспечивать сохранность и целостность ПАК. В случае утраты ПАК и/или его использования без согласия Клиента Клиент обязан незамедлительно об этом информировать Банк по одному из телефонов: (495) 775-34-56, 775-34-94, сообщив администратору Системы «iBank 2» Блокировочное слово. По факту поступившего сообщения Банк принимает меры по временному блокированию ПАК. Временное блокирование ПАК не влечет возникновение у Банка обязательства по возмещению Клиенту сумму операции, совершенной без его согласия.

Клиент обязан незамедлительно представить в Банк соответствующее письменное уведомление (Приложение № 6) после обнаружения факта утраты ПАК и/или его использования без согласия Клиента, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции. В письменном уведомлении должна быть указана информация об обстоятельствах утраты ПАК, а также его реквизиты. Письменное уведомление является единственным доказательством утраты Клиентом ПАК, а также основанием для рассмотрения Банком вопроса о возможности возврата Клиенту суммы операций, совершенных без его согласия.

В указанных в настоящем подпункте случаях, а также в случае порчи ПАК, Клиент имеет право на повторное подключение, при предоставлении Банку письменного уведомления, составленного в произвольной форме, в котором будут указаны причины повторного подключения Клиента к Системе «iBank 2», и подписании Акта передачи ПАК (USB-токен) (Приложение № 2). При этом до повторного подключения к Системе «iBank 2», Клиент обязан уплатить Банку комиссионное вознаграждение в размере, установленном Тарифами Банка.

4.5.5. 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. Клиент несет ответственность за присутствие на компьютере, на котором осуществляется эксплуатация Системы «iBank 2», программ (в том числе вирусного характера), которые могут нарушить функционирование банковской части Системы «iBank 2» в размере нанесенного ущерба (стоимости ликвидации последствий данного нарушения).

4.5.6. Клиент обязан ознакомится с описанием механизмов защиты Системы «iBank 2» и Памяткой клиента о возможных угрозах хищения денежных средств с использованием Системы «iBank 2» и способах защиты (Приложение № 10 к настоящему Договору). Описание доступно на сайте по адресу https://www.slavcred.ru/. 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.

4.5.7. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к Системе «iBank 2» незамедлительно после момента обнаружения.

4.5.8. Клиент обязан незамедлительно после момента обнаружения извещать Банк обо всех случаях Компрометации Секретных ключей ЭЦП.

4.5.9. Клиент обязан в случае прекращения использования Системы «iBank 2 вернуть ПАК, предоставленный Банком**.** Факт передачи фиксируется в Акте возврата (Приложение № 9 к настоящему Договору).

4.5.10. Клиент обязан заполнять Электронные документы в Системе «iBank 2» в соответствии с действующим Положением ЦБ РФ «О правилах осуществления перевода денежных средств» от 19 июня 2012 г. № 383-П.

4.5.11. Клиент обязан хранить в секрете пароль к Секретному ключу ЭЦП и не передавать третьим лицам носитель с Секретным ключом ЭЦП, используемым в Системе «iBank 2».

4.5.12. Клиент обязан допускать к эксплуатации Системы «iBank 2» только сотрудников, указанных в Банковской карточке с образцами подписи и оттиском печати. В случае переизбрания (переназначения) сотрудника, обладающего правом подписи финансовых документов ЭЦП, для каждого такого сотрудника Клиент должен сформировать новый Секретный ключ ЭЦП, распечатать и предоставить в Банк соответствующий ему Сертификат открытого ключа ЭЦП Клиента. Секретный ключ ЭЦП, принадлежавший бывшему сотруднику Клиента, аннулируется Банком в одностороннем и бесспорном порядке.

4.5.13. Клиент обязан по требованию Банка прекратить использование указанного Банком Секретного ключа ЭЦП, сгенерировать новую Пару ключей ЭЦП и зарегистрировать новый Открытый ключ ЭЦП в Банке.

4.5.14. Клиент имеет право досрочно прекратить действие своего Активного ключа ЭЦП и потребовать от Банка блокировать этот Активный ключ ЭЦП, оформив уведомление по форме Приложения 5 к настоящему Договору.

4.5.15. Клиент имеет право по своему усмотрению генерировать новые Пары ключей ЭЦП Клиента и регистрировать в Банке новые Открытые ключи ЭЦП Клиента**.**

4.5.16. Клиент имеет право, позвонив в Банк по одному из телефонов: (495) 775-34-56, 775-34-94, сообщить администратору Системы «iBank 2» Блокировочное слово для временного блокирования ЭЦП Клиента, до момента подачи им письменного уведомления об отмене действия Пары ключей ЭЦП Клиента (Приложение № 5) или о возобновлении работы в Системе «iBank 2», составленного в произвольной форме. По факту поступившего сообщения Банк принимает меры по временному блокированию ЭЦП Клиента.

4.5.17. Клиент имеет право получить дополнительный ПАК (USB-токен), в том числе в случаях, указанных в п.п. 4.5.4. настоящего Договора, при предоставлении Банку письменного уведомления, составленного в произвольной форме, в котором будут указаны причины его дополнительного подключения к Системе «iBank 2», и после подписании им Акта передачи ПАК (USB-

токен) (Приложение № 2). При этом до подключения к Системе «iBank 2», Клиент обязан уплатить Банку комиссионное вознаграждение в размере, установленном Тарифами Банка.

4.5.18. Клиент имеет право, заполнив Приложения № 7 и № 7.1 к настоящему Договору, подключить дополнительные сервисы Системы «iBank 2».

4.6. Совместные обязательства и ответственность Сторон:

4.6.1. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами Секретного ключа ЭЦП Клиента**.**

4.6.2. Банк не несет ответственности за убытки, понесенные Клиентом вследствие ошибок, отказов и несвоевременных действий лиц, в пользу которых осуществляется расчетная операция по поручению Клиента.

4.6.3. Банк не несет ответственности за сбои в Системе «iBank 2», если они происходят по вине либо в силу ошибок или неквалифицированной работы с пакетом программ сотрудников Клиента.

4.6.4. 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.

4.6.5. В случае возникновении спорных ситуаций между Банком и Клиентом при использовании Системы «iBank 2», в том числе в случаях, предусмотренных п.п. 4.4.6., 4.4.8. – 4.4.10., 4.5.4. настоящего Договора, Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций» (Приложение № 3 к настоящему Договору), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации.

4.6.6. 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.

4.6.7. 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.

5. ПОРЯДОК ОБСЛУЖИВАНИЯ КЛИЕНТА.

5.1. 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.

5.2. Документы, поступившие в Банк, принимаются к исполнению согласно действующему режиму операционного дня по обслуживанию клиентов ООО КБ «Славянский кредит».

5.3. При получении Электронного документа Банк производит проверку подлинности ЭЦП сотрудников Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчётном счёте Клиента. В случае отбраковки Электронный документ Банком к исполнению не принимается.

6. ПОРЯДОК ОПЛАТЫ.

6.1. За оказываемые Банком услуги по установке Системы «iBank 2» взимается единовременная плата в размере, установленном Тарифами Банка.

6.2. Банк, не позднее следующего дня после даты подключения Клиента к Системе «iBank 2», списывает на условии заранее данного акцепта Клиента абонентскую плату за услуги, предлагаемые Клиенту в текущем месяце.

6.3. Банк ежемесячно, не позднее 1-го рабочего числа текущего месяца, за который производится оплата, списывает на условии заранее данного акцепта Клиента абонентскую плату за услуги Системе «iBank 2».

6.4. Банк ежемесячно, не позднее 1-го рабочего числа текущего месяца, за который производится оплата, списывать на условиях заранее данного акцепта Клиента абонентскую плату за предоставление дополнительных сервисов Системы «iBank 2».

6.5. Банк вправе в одностороннем порядке изменять Тарифы Банка с уведомлением Клиента на сайте Банка в сети Интернет по адресу: http://www.slavcred.ru/, а также на стендах в операционных залах Банка. Изменения вступают в силу через 14 календарных дней с даты их размещения в установленном настоящим пунктом порядке.

6.6. В случае отсутствия на счетах Клиента денежных средств в размере, необходимом для уплаты абонентской платы за услуги Системе «iBank 2», в даты, указанные в п.п. 6.2 , 6.3 и 6.4 настоящего Договора, Банк имеет право на следующий банковский день отключить Клиента от Системы «iBank 2».

6.7. Клиент имеет право возобновить работу по Системе «iBank 2» после поступления на его счет/а денежных средств в размере, необходимом для уплаты абонентской платы за услуги Системы «iBank 2», и подачи письменного заявления в Банк о подключении к указанной Системе.

7. СРОК ДЕЙСТВИЯ ДОГОВОРА.

7.1. Настоящий Договор вступает в силу с момента подписания Заявления на заключение договора на оказание услуг электронного банкинга в системе «iBank 2» в ООО КБ «Славянский кредит» обеими сторонами и заключается на срок – до последнего дня календарного года (до 31 декабря).

При не уведомлении Банком Клиента или Клиентом Банка о прекращении действия настоящего Договора не менее, чем за 30 дней до окончания его действия, настоящий Договор считается пролонгированным на тех же условиях и на следующий календарный год.

7.2. Настоящий Договор подлежит расторжению в случае расторжения Договора на расчетно-кассовое обслуживание.

8. ВНЕСЕНИЕ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ.

8.1. Об изменении условий Договора Клиент информируется Банком путем размещения соответствующей информации на сайте Банка в сети Интернет по адресу: http://www.slavcred.ru/ и в операционных залах Банка**.** Изменения вступают в силу через 7 календарных дней с даты их размещения в установленном данным пунктом порядке, за исключением случая, предусмотренного п**.** 6.5. настоящего Договора.

8.2. Стороны обязуются незамедлительно сообщать друг другу необходимую информацию, сведения об изменении своего правового статуса, места своего нахождения и реквизитов. В противном случае виновная Сторона несет ответственность за все возможные отрицательные последствия.

9. РАЗРЕШЕНИЕ СПОРОВ.

9.1. При возникновении разногласий и споров по настоящему Договору Стороны обязуются разрешать их путем переговоров с учетом взаимных интересов в соответствии с Приложением № 3 к настоящему Договору.

9.2. В случае невозможности достижения взаимной договоренности между Сторонами разногласия и споры подлежат разрешению в Арбитражном суде г. Москвы в соответствии с законодательством Российской Федерации.

10. ПРИЛОЖЕНИЯ.

10.1. Приложения к Договору:

Приложение № 1 «Заявление на заключение договора оказания услуг электронного банкинга в Системе «iBank 2 в ООО КБ «Славянский кредит»;

Приложение № 2 «АКТ № ____ передачи ПАК (USB-токена)»;

Приложение № 3 «ПОЛОЖЕНИЕ о порядке проведения технической экспертизы при возникновении спорных ситуаций»;

Приложение № 4 «ПЕРЕЧЕНЬ Электронных документов передаваемых по Системе «iBank 2» и необходимое количество ЭЦП»;

Приложение № 5 «УВЕДОМЛЕНИЕ об отмене действия Секретного и соответствующего ему Открытого ключей ЭЦП сотрудника Клиента»;

Приложение № 6 «УВЕДОМЛЕНИЕ об отмене действия ПАК»;

Приложение № 7 «Заявление о подключении (отключении) дополнительных сервисов Системы «iBank 2» (SMS-Банкинг);

Приложение № 7.1 «Заявление о подключении (отключении) дополнительных сервисов Системы «iBank 2» (IP-фильтрация);

Приложение № 8 «Порядок предоставления дополнительных сервисов (услуг) по Системе «iBank2» (Порядок предоставления услуги «SMS-Банкинг»);

Приложение № 8.1 «Порядок предоставления дополнительных сервисов (услуг) по Системе «iBank2» (Порядок предоставления услуги «IP-фильтрация»);

Приложение № 9 «АКТ №_____ возврата ПАК (USB-токен)»;

Приложение № 10 «Памятка Клиента о возможных угрозах хищения денежных средств с использованием Системы «iBank 2» и способах защиты;

Приложение № 11 «Сертификат ключа проверки электронной подписи сотрудника Клиента с Системе «iBank 2» создается и предоставляется Клиентом в Банк»;
являются неотъемлемой его частью.

11. РЕКВИЗИТЫ.

Полное наименование: Коммерческий банк «Славянский кредит» (общество с ограниченной ответственностью).
Сокращенное наименование: ООО КБ «Славянский кредит»
Место нахождения: 119415, г. Москва, проспект Вернадского, д. 87, корп. 2.
ОГРН 1027739736254
ИНН 7709024276
КПП 772901001
код ОКПО 29351476
Код ОКВЭД 64.19
БИК 044525805
к/счет 30101810845250000805 в Главном Управлении Банка России по Центральному Федеральному округу г. Москва.

ПРИЛОЖЕНИЕ № 1
к Договору оказания услуг электронного банкинга в Системе «iBank 2»

ЗАЯВЛЕНИЕ
на заключение договора оказания услуг электронного банкинга в системе «iBank 2»
в ООО КБ «Славянский кредит»

Наименование Клиента (далее - Клиент)_____
полное официальное наименование организации. Фамилия, Имя, Отчество индивидуального

_____
предпринимателя или физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой

Местонахождение Клиента: _____
адрес местонахождения организации; адрес места жительства (места пребывания) индивидуального предпринимателя

_____
или физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой

ИНН Клиента: _____ ОГРН/ОГРНИП Клиента: _____
Адрес электронной почты Клиента:_____
Контактный телефон Клиента: _____
Клиент является по законодательству Российской Федерации резидентом нерезидентом

Настоящим в соответствии со статьей 428 Гражданского кодекса Российской Федерации Клиент присоединяется к действующей редакции **Договора оказания услуг электронного банкинга в системе «iBank 2» в ООО КБ «Славянский кредит».**

Настоящим подтверждаем, что ознакомились с **Договором оказания услуг электронного банкинга с Системе «iBank 2» в ООО КБ «Славянский кредит»,** понимаем текст этого Договора, выражаем свое согласие с ним и обязуемся его выполнять.

Просим выдать ПАК (USB-токен) до начала работы в Системе «iBank 2» в количестве___(_____) штук(и).

Представитель Клиента: _____,
должность, Фамилия, Имя, Отчество представителя (указываются полностью)

действующий на основании _____
наименование документа - Устав, Доверенность (указываются номер доверенности и дата ее совершения), иной соответствующий документ

Подпись Клиента (Представителя Клиента):_____ Печать Клиента:

Дата: «____»_____20___ г.

ОТМЕТКИ БАНКА:

Идентификацию Клиента осуществил _____
должность

_____/ _____/
подпись Ф.И.О

Дата: «___» _____20__ г.

Уполномоченный представитель Банка _____
должность уполномоченного представителя Банка

_____/ _____/
подпись Ф.И.О.

Дата: «___» _____20__ г. м.п.

ПРИЛОЖЕНИЕ **№ 2**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

«___»_____20___г.

АКТ № ____
передачи ПАК (USB-токена)

Коммерческий банк «Славянский кредит» (общество с ограниченной ответственностью), именуемый в дальнейшем «Банк», в лице _____, с одной стороны, и _____, в лице _____, действующего на основании _____ именуемый (ая) в дальнейшем «Клиент» с другой стороны, вместе в дальнейшем именуемые «Стороны», принимая во внимание Договор оказания услуг электронного банкинга в системе «iBank 2» в ООО КБ «Славянский кредит», составили настоящий акт о том, что Банком надлежащим образом передано, а Клиентом получен:

- ПАК (USB-токен) № _____;
- ПАК (USB-токен) № _____;
- ПАК (USB-токен) № _____;
- ПАК (USB-токен) № _____;
- Инструкцию по первичной регистрации Клиента в Системе «iBank 2».

С момента подписания Сторонами настоящего акта Банк считается исполнившим свои обязательства по передаче необходимого для работы Клиента в системе «iBank 2» ПАК.

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

БАНК	КЛИЕНТ
_____	_____
(Ф.И.О., подпись)	(Ф.И.О., подпись)
М. П.	М.П.

ПРИЛОЖЕНИЕ **№ 3**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

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 ЭЦП Клиента в Электронных документах.

2. При возникновении спорной ситуации Клиент представляет Банку в письменном виде заявление (уведомление), содержащее существо претензии с указанием на Электронный документ, на основании которого Банк выполнил операции по счёту Клиента. В заявлении также должно быть указано лицо (лица), уполномоченное представлять интересы Клиента в разрешительной комиссии.

3. Банк обязан в течение пяти рабочих дней с момента получения заявления (уведомления) Клиента сформировать разрешительную комиссию для рассмотрения заявления (уведомления). В состав комиссии включаются представители Клиента и представители Банка. По специальному требованию одной из Сторон с состав комиссии могут быть включены независимые эксперты. Независимый эксперт должен иметь высшее профессиональное образование или профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области 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. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых в Системе «iBank 2».

7. 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.

8. В результате рассмотрения спорной ситуации разрешительная комиссия должна определить подлинность ЭЦП Клиента в приложенном Электронном документе и правомерность выполнения Банком операций по счету Клиента.

9. Разрешительная комиссия проводит рассмотрение заявления (уведомления) в срок не более пяти рабочих дней с момента формирования комиссии. Рассмотрение заявления (уведомления) включает следующие этапы:

9.1. Разрешительная комиссия проводит техническую экспертизу ключа (ключей) ЭЦП Клиента.

9.1.1. С использованием штатного программного обеспечения Системы «iBank 2» АРМ «Интернет-банкинг для корпоративных клиентов» (АРМ) выполняется распечатка Сертификата Открытого ключа ЭЦП Клиента, соответствующего Секретному ключу ЭЦП Клиента, которым был подписан спорный Электронный документ. По согласованию Сторон печатная форма Сертификата может быть получена с использованием ПО АРМ «Администратор».

9.1.2. Распечатанный сертификат сверяется с Сертификатом Открытого ключа ЭЦП Клиента, заверенным подписью уполномоченного лица Клиента и являющимся приложением к договору.

Сверяются ID ключа и его шестнадцатеричное представление. При обнаружении расхождений ситуация далее не рассматривается, комиссия составляет акт о выявленном несоответствии.

9.2. Разрешительная комиссия проводит техническую экспертизу подлинности ЭЦП Клиента в Электронном документе.

9.2.1. С использование штатного ПО Системы «iBank 2» АРМ «Операционист» выбирается спорный Электронный документ и выполняется операция «Проверить ЭЦП».

9.2.2. При невозможности получить доступ к документу через АРМ «Операционист», комиссией могут использоваться специализированные утилиты от разработчика Системы «iBank 2» для выгрузки документа из Базы данных Системы «iBank 2» и автономной проверки.

9.3. По взаимному согласию членов комиссии, автономную проверку подлинности ЭЦП может провести независимая организация, в том числе разработчик и/или обладатель исключительных прав на систему «iBank 2». Эксперт, проводящий автономную проверку подлинности ЭЦП, должен иметь высшее профессиональное образование или профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области 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 выгрузки спорного документа из базы данных системы «iBank 2»;

- копии Сертификатов Открытого ключа ЭЦП Клиента, заверенные обеими Сторонами;

- подписанное обеими Сторонами письмо с просьбой о проведении проверки.

По результатам проверки независимая организация формирует заключение о подлинности ЭЦП 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.

9.4. 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 ЭЦП в оспариваемом Электронном документе и его обоснование.

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

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

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

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

10.2. Банк не предъявляет Сертификаты Открытого ключей ЭЦП Клиента, заверенные подписью руководителя и имеющие оттиск печати Клиента, соответствующие Секретным ключам ЭЦП Клиента, которыми был подписан спорный Электронный документ.

10.3. Хотя бы одна ЭЦП Клиента в Электронном документе оказалась не подлинной.

10.4. Клиент предоставляет Уведомление об отмене действия Секретного и соответствующего ему Открытого ключей ЭЦП Клиента, подписанное уполномоченным должностным лицом Банка

и имеющее оттиск печати Банка. При этом указанная в Уведомлении дата окончания действия Пары ключей ЭЦП сотрудника Клиента раньше даты подписи, указанной в рассматриваемом Электронном документе.

11. В случае, когда Банк предъявляет Электронный документ и Сертификаты Открытых ключей ЭЦП Клиента, подлинность ЭЦП Клиента в Электронном документе разрешительная комиссия считает признанной; принадлежность Клиенту Открытых ключей ЭЦП Клиента считается подтвержденной. В этом случае, Банк не несёт ответственности перед Клиентом за операции, выполненные по счёту Клиента.

12. Если Клиент настаивает на том, что данный документ он не создавал или не подписывал одной или несколькими ЭЦП, комиссия может вынести определение о компрометации Секретного ключа (ключей) ЭЦП Клиента, что не снимает с Клиента ответственности за данный документ.

КЛИЕНТ

_____

(Ф.И.О., подпись)

М. П.

ПРИЛОЖЕНИЕ **№ 4**
к Договору оказания услуг электронного банкинга в Системе «iBank 2» в ООО КБ «Славянский кредит»

ПЕРЕЧЕНЬ
Электронных документов передаваемых по Системе «iBank 2» и необходимое количество ЭЦП.

	Наименование Электронного документа	**Количество ЭЦП**
1	Платежное поручение	
2	Поручение на покупку иностранной валюты	
3	Поручение на продажу иностранной валюты	
4	Заявление на безналичную конверсию иностранной валюты в другую иностранную валюту или российские рубли	
5	Распоряжение на обязательную продажу валюту	
6	Заявление на перевод иностранной валюты	
7	Выписки по счету	
9	Справка о валютных операциях	
10	Отзыв документа	
11	Информационное письмо	

КЛИЕНТ

_____
(Ф.И.О., подпись)

М. П.

ПРИЛОЖЕНИЕ **№ 5**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

УВЕДОМЛЕНИЕ
об отмене действия Секретного и соответствующего ему Открытого ключей ЭЦП сотрудника Клиента

_____
(наименование клиента банка, ИНН)

уведомляет Банк о том, что с «____»_____20___г. считать недействительным Открытый ключ ЭЦП Клиента, со следующим идентификатором _____.

Соответствующий ему Секретный ключ ЭЦП Клиента утрачивает силу для дальнейшего применения с вышеуказанной даты.

КЛИЕНТ

_____/_____/
(Ф.И.О., подпись)

М. П.

ПРИЛОЖЕНИЕ **№ 6**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

УВЕДОМЛЕНИЕ
об отмене действия ПАК

_____
(наименование клиента банка, ИНН)

уведомляет Банк о том, что с «____»_____20___г. считать недействительным ПАК Клиента, со следующим идентификатором _____, полученный от Банка на основании Акта № ___ передачи ПАК от «___»_____20___г.

_____
_____
_____
_____.
(обстоятельства утраты Клиентом ПАК)

КЛИЕНТ

_____/_____ _____ /
(Ф.И.О., подпись)

М. П.

ПРИЛОЖЕНИЕ **№ 7**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

ЗАВЛЕНИЕ
о подключении (отключении) дополнительных сервисов Системы «iBank 2» (SMS-Банкинг)

_____ в лице _____, просит Вас подключить (отключит) дополнительный сервис в Системе «iBank 2», позволяющий обеспечить безопасность и минимизировать риски доступа третьих лиц и хищения денежных средств Клиента.

1.1. Каналы получения информации из Системы «iBank 2»:

№ п/п	Название	Подключить	Отключить	Отметки Банка об исполнении
1	SMS – Банкинг	☐	☐	

Номер мобильного телефона, ответственного сотрудника, которому будут приходить уведомления через SMS-Банкинг: +7_____.

«___»_____20___г.

КЛИЕНТ

_____/_____/
(Ф.И.О., подпись)

М. П.

ПРИЛОЖЕНИЕ **№ 7.1**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

ЗАВЛЕНИЕ
о подключении (отключении) дополнительных сервисов Системы «iBank 2» (IP-фильтрация)

_____ в лице _____, просит Вас подключить (отключит) дополнительный сервис в Системе «iBank 2», позволяющий обеспечить безопасность и минимизировать риски доступа третьих лиц и хищения денежных средств Клиента.

1.1. IP-фильтрация:

IP-фильтрация:

☐	доступ через глобальную сеть Интернет:	
	№п/п IP-адрес и/или маска IP-сети	Вкл. Выкл.
	1 _____ . _____ . _____ . _____ / _____	☐ ☐
	2 _____ . _____ . _____ . _____ / _____	☐ ☐
	3 _____ . _____ . _____ . _____ / _____	☐ ☐
	4 _____ . _____ . _____ . _____ / _____	☐ ☐
	5 _____ . _____ . _____ . _____ / _____	☐ ☐
☐	без ограничений IP-адресов (отключить IP-фильтрацию)	

С «Памяткой о возможных угрозах хищения денежных средств с использованием системы «iBank 2» и способах защиты» ознакомлен и предупрежден о возможных рисках в случае моего отказа от использования данных сервисов

_____ _____ _____
Должность **Подпись** **Ф.И.О.**

КЛИЕНТ

_____/_____/
(Ф.И.О., подпись)

М. П.

ПРИЛОЖЕНИЕ **№ 8**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

Порядок предоставления дополнительных сервисов (услуг) по Системе «iBank 2»

Порядок предоставления услуги «SMS-Банкинг»

Банк подключает Клиенту *информационно-оповестительный* канал "SMS-Банкинг" – канал, предназначенный для уведомления клиентов о событиях, происходящих в Системе «iBank 2» посредством рассылки sms-сообщений на сотовые телефоны. Услуга предоставляется только Клиентам подключённым к Системы «iBank 2».

Для подключения/отключения услуги "SMS-Банкинг" Клиент заполняет Заявление (Приложение № 7 к настоящему Договору), в котором выбирает соответствующий пункт и указывает номер мобильного телефона ответственного сотрудника, для получения сообщений через SMS-Информирование.

Банк не несет ответственности за действия sms-центра и операторов сотовой связи, в том числе за сроки доставки Клиенту sms-сообщений.

Клиент самостоятельно осуществляет смену телефонных номеров для sms-информирования с момента подключения *информационно-оповестительного* канала.

Банк не несет ответственности за неблагоприятные последствия для Клиента, связанные с неправильно или некорректно заполненной подпиской на *информационный-оповестительный* канал "SMS-Банкинг".

«___»_____20___г.

КЛИЕНТ

_____/_____/
(Ф.И.О., подпись)

М. П.

ПРИЛОЖЕНИЕ **№ 8.1**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

Порядок предоставления дополнительных сервисов (услуг) по Системе «iBank 2»

Порядок предоставления услуги «IP-фильтрация»

Банк подключает Клиенту дополнительную услугу «IP-фильтрация» - ограничение возможности подключения к системе Клиент-Банк («iBank2») (далее «Система») через глобальную сеть Интернет либо с помощью модема при звонке на сервисный номер Банка.

Для подключения/отключения услуги «IP-фильтрация» Клиент предоставляет в Банк Заявление (Приложение № 7.1. к настоящему Договору). Работа с Системой «iBank 2» Банка от лица сотрудников Клиента, разрешается только с учётом «разрешений», указанных в Заявлении. Иные подключения к Системе от лица сотрудников Клиента запрещены.

При необходимости изменения IP-адресов Клиент обязуется предоставить в Банк новое Заявление с перечнем новых IP-адресов. Банк обязуется изменить настройки Системы в соответствии с указаниями Клиента не позднее дня, следующего за днем приема данного Заявления.

«___»_____20___г.

КЛИЕНТ

_____/_____/
(Ф.И.О., подпись)

М. П.

ПРИЛОЖЕНИЕ **№ 9**
к Договору оказания услуг электронного банкинга в Системе «iBank 2»
в ООО КБ «Славянский кредит»

«___»_____20___г.

Экз. №____

АКТ № ____
возврата ПАК (UBS-токена)

_____, в лице _____, действующего на основании _____, именуемый (ая) в дальнейшем «Клиент» с одной стороны, Коммерческий банк «Славянский кредит» (общество с ограниченной ответственностью), именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с другой стороны, и, вместе в дальнейшем именуемые «Стороны», принимая во внимание Договор оказания услуг электронного банкинга в системе «iBank 2» в ООО КБ «Славянский кредит», составили настоящий акт о том, что Клиентом надлежащим образом передано, а Банком получен:

- ПАК (USB-токен) № _____;
- ПАК (USB-токен) № _____;
- ПАК (USB-токен) № _____;
- ПАК (USB-токен) № _____;

С момента подписания Сторонами настоящего акта Клиент считается исполнившим свои обязательства по передаче Банку ПАК.

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

КЛИЕНТ	БАНК
_____	_____
(Ф.И.О., подпись)	(Ф.И.О., подпись)
М. П.	М.П.

ПРИЛОЖЕНИЕ **№ 10**
к Договору оказания услуг электронного банкинга в Системе «iBank 2» в ООО КБ «Славянский кредит»

ПАМЯТКА КЛИЕНТА

о возможных угрозах хищения денежных средств с использованием Системы «iBank 2»

и способах защиты

Для исключения несанкционированного доступа в систему электронного банкинга ООО КБ «Славянский кредит» проводит комплекс мероприятий для усиления Вашей информационной и финансовой безопасности. Представляем Вам «Памятку о возможных угрозах хищения денежных средств с использованием Системы «iBank 2» и способах защиты», а также предлагаем ряд мер, которые повысят уровень Вашей информационной и финансовой безопасности.

Хищение денежных средств с расчетных счетов возможно при получении злоумышленниками доступа к Секретным ключам ЭЦП и паролям. Для того, чтобы предотвратить хищение и использование Вашего Секретного ключа ЭЦП ООО КБ «Славянский кредит» настоятельно рекомендует придерживаться приведенных ниже правил:

- Для хранения файлов с Секретными ключами ЭЦП Клиента использовать внешние носители ПАК (USB-токены)**.** При этом владелец такого внешнего носителя должен хранить его в условиях, исключающих доступ к нему третьих лиц, например, личный сейф.
- Использовать **IP-фильтрацию -** дополнительный сервис, запрещающий пользование Секретными ключами ЭЦП Клиента на компьютерах вне вашего офиса. IP-фильтрация позволяет быть уверенным в том, что информация, передаваемая в банк, будет обработана только в случае совпадения IP-адреса передающего компьютера с IP-адресом клиента, хранящимся в базе данных банка;
- Использовать **SMS-Банкинг**. Сервис позволяет оперативно получать информацию о входе в систему, о поступлении платежных поручений, о движении средств и т.д. При получении сообщения о несанкционированной операции Вы должны связаться с Банком для её приостановки.
- Не хранить на носителях с Секретными ключами ЭЦП Клиента какую-либо другую информацию;
- Не допускать использования «пустых» или простых паролей, например 123456, qwerty, для всех учётных записей, имеющих право входа в Windows. Осуществлять периодическую смену паролей, рекомендуемая частота смены паролей -1 раз в месяц;
- Не передавать Секретные ключи ЭЦП Клиента ИТ-сотрудникам для проверки работы Системы «iBank 2» и проверки настроек взаимодействия с Банком. При необходимости проведения проверок владелец ключа ЭЦП должен лично подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа «iBank 2», и ввести пароль, исключая умышленное наблюдение посторонними лицами;
- Не передавать Секретные ключи ЭЦП Клиента замещающим сотрудникам (заместителям, временно исполняющим обязанности). Для таких сотрудников необходимо получить персональные ЭЦП и внести их в банковскую карточку;
- При увольнении ответственного или технического сотрудника, имевшего доступ к Секретному ключу ЭЦП Клиента, обязательно заблокировать его ключ ЭЦП;
- При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с Системой «iBank 2», проверить их на отсутствие вредоносных программ;
- В случае если работа в Системе «iBank 2» продолжительна, отключать и извлекать носители с Секретными ключами ЭЦП Клиента, если они не используются для работы. Носители с Сек-

ретными ключами ЭЦП Клиента должны находиться в компьютере только в момент подписания документов, и извлекаться сразу после подписания документов;

- По возможности выделить отдельный компьютер, который будет использоваться только для работы с Системой «iBank 2» и не выполнять на этом компьютере никакие другие задачи;
- Ограничить доступ к компьютерам, используемым для работы с Системой «iBank 2» и исключить к ним доступ персонала, не работающего с Системой «iBank 2»;
- Исключить обслуживание компьютеров, используемых для работы с Системой «iBank 2», нелояльными ИТ-сотрудниками;
- При обслуживании компьютера ИТ-сотрудниками, обеспечивать контроль над выполняемыми ими действиями;
- На компьютерах, используемых для работы с Системой «iBank 2», исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т. п. По возможности, полностью запретить все соединения (входящие и исходящие) с сетью Интернет, разрешив только доступ к необходимым ресурсам;
- Использовать только лицензионное программное обеспечение, обеспечив автоматическое обновление системного и прикладного программного обеспечения;
- Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечив возможность автоматического обновления антивирусных баз, а также еженедельную полную антивирусную проверку;
- Применять на рабочем месте специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение и т.п.;
- Осуществлять антивирусную проверку любых файлов и программ, загружаемых из сети Интернет, полученных по электронной почте или на внешних носителях (дискеты, флеш-накопители, CD/DVD и др.);
- Проводить полную антивирусную проверку после любых действий внештатных ИТ-специалистов или других сотрудников, выполнявших операции на компьютере, используемом для работы с системой. Например, решение технических проблем: подключения к сети Интернет, установки или обновления бухгалтерских и информационно-правовых программ;
- Не допускать работу под учётной записью Windows, имеющей права администратора. Необходимо использовать учётную запись с ограниченными правами в операционной системе Windows, установленной на компьютере;
- Запрещать использование любых средств удалённого (дистанционного) доступа, которые обычно используется ИТ-специалистами для удалённой поддержки. Заблокировать возможность использования таких средств с помощью файрвола (программного и/или аппаратного);
- При возникновении подозрений на копирование/перехват Секретных ключей ЭЦП Клиента или наличие в компьютере вредоносных программ – обязательно заблокировать ключи ЭЦП;
- Если Вы заметили проявление необычного поведения программного обеспечения Системы «iBank 2» или какие-то изменения в интерфейсе программы – позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии программного обеспечения. Если нет – заблокировать ключи ЭЦП.

Хищение денежных средств с расчетных счетов при получении злоумышленниками доступа к Секретным ключам ЭЦП Клиента и паролям с целью направления в Банк платежных поручений, заверенных от Вашего лица похищенным ключом ЭЦП предположительно могут осуществить:

- ответственные сотрудники Вашей организации, ранее имевшие доступ к Секретным ключам ЭЦП Клиента;
- штатные ИТ-сотрудники Вашей организации, имеющие или имевшие технический доступ к носителям (дискеты, флеш-носители, жесткие диски и пр.) с Секретными ключами ЭЦП Клиента, а также доступ к компьютерам организации, с которых осуществлялась работа по Системе «iBank 2»;

- нештатные, приходящие по вызову, ИТ-специалисты, обслуживающие компьютеры Вашей организации, осуществляющие профилактику и подключение к Интернету, установку и обновление бухгалтерских и информационно-правовых программ (другого программного обеспечения) на компьютеры, с которых осуществлялась или осуществляется работа по Системе «iBank 2»;
- другие злоумышленники путем заражения через Интернет Ваших компьютеров вредоносными программами, через уязвимости системного и прикладного программного обеспечения с последующим дистанционным хищением Секретных ключей ЭЦП Клиента и паролей.

Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием действующих Секретных ключей ЭЦП Клиента, имеющие обычные реквизиты получателей и типовые назначения платежа.

ООО КБ «Славянский кредит» напоминает Вам о том, что:

- **сотрудники Банка не имеют доступа к Вашим Секретным ключам ЭЦП Клиента** и не может от Вашего имени сформировать корректную ЭЦП под электронным платежным поручением;
- **Банк не осуществляет рассылку электронных писем с просьбой прислать Ваш Секретный ключ ЭЦП Клиента или пароль**;
- **Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.** В случае если Вы получили подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление Секретных ключей ЭЦП Клиента и паролей, необходимо незамедлительно сообщить об этом в Службу технической поддержки клиентов Банка;
- ответственность за конфиденциальность Ваших Секретных ключей ЭЦП Клиента лежит на Вас, как единственных владельцах Секретных ключей ЭЦП Клиента;
- если Вы сомневаетесь в конфиденциальности своих Секретных ключей ЭЦП Клиента или есть подозрение в их компрометации (копировании), Вы должны незамедлительно заблокировать Ваши ключи ЭЦП;
- изменение пароля доступа к Секретному ключу ЭЦП Клиента не защищает Вас от использования злоумышленниками ранее похищенного ключа;

Для получения дополнительной информации по техническим вопросам Вы можете обратиться:

Служба технической поддержки: (495) 775-34-74, (495) 380-16-01.