Порядок электронного документооборота
при осуществлении информационно-технологического взаимодействия

г. Казань
Редакция № 1 от 25 июня 2020 года

Общество с ограниченной ответственностью «Банк 131» (далее – «Банк»), с одной стороны, и юридическое лицо, заключившее с Банком договор об информационно-технологическом обслуживании при осуществлении переводов денежных средств и/или договор о приеме электронного средства платежа при продаже товаров (работ/услуг) в сети Интернет (далее – «Компания»), с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1. Предмет Соглашения
   1.1. Настоящее Соглашение устанавливает порядок организации и проведения электронного документооборота с использованием электронной подписи между Сторонами в рамках: i) договора об информационно-технологическом обслуживании при осуществлении переводов денежных средств; ii) договора о приеме электронного средства платежа при продаже товаров (работ/услуг) в сети Интернет.
   1.2. Перечень и формы электронных документов, которые Стороны могут подписывать и передавать друг другу в рамках настоящего Соглашения, определяются Банком и размещены по адресу: https://developer.131.ru.
   1.3. Компания реализуют свое право на обмен электронными документами, подписанными электронной подписью, только через своих надлежаще уполномоченных представителей. Такими представителями могут быть как дееспособные физические лица, наделенные учредительными документами Компании правом единолично действовать от имени Компании без доверенности, так и дееспособные физические лица, действующие от имени Компании на основании доверенности.
2. Порядок заключения Соглашения
   2.1. Настоящее Соглашение состоит из самого Порядка электронного документооборота и Заявления о признании и сверке ключа электронной подписи (далее – «Заявление», приложение № 1). Актуальная редакция Соглашения размещена по адресу: https://developer.131.ru.
   2.2. Соглашение не является публичной офертой. Банк вправе отказаться от заключения Соглашения с Компанией в случае, если Компания не имеет заключенного с Банком договора об информационно-технологическом обслуживании при осуществлении переводов денежных средств и/или договора о приеме электронного средства платежа при продаже товаров (работ/услуг) в сети Интернет.
   2.3. Соглашение заключается путем принятия Сторонами условий Порядка электронного документооборота и подписания Заявления в двух экземплярах. Соглашение считается заключенным с даты подписания Заявления.
3. Порядок информационно-технического взаимодействия
   3.1. Стороны осуществляют информационно-технологическое взаимодействие в соответствии с Протоколом информационного обмена (далее – «API») и Инструкцией по обеспечению информационной безопасности (приложение № 2), актуальные редакции и описания которых размещены по адресу: https://developer.131.ru/.
   3.2. Банк вправе в одностороннем порядке вносить изменения в API. Если вносимые изменения могут повлиять на исполнение Сторонами своих обязательств по Соглашению, то Банк направит Компании уведомление не менее чем за 5 (пять) рабочих дней до даты вступления таких изменений в силу.
   3.3. Стороны самостоятельно и за свой счет поддерживают собственную аппаратно-техническую инфраструктуру, необходимую для исполнения Соглашения, предпринимают возможные меры для защиты передаваемой в рамках Соглашения информации от несанкционированного доступа, копирования и распространения, в том числе, предусмотренные применимым законодательством.
   3.4. Компания соглашается, что Банк не может гарантировать Компании отсутствие перерывов, связанных с техническими неисправностями, проведением профилактических работ, а также полную и безошибочную работоспособность API и каналов связи. Стороны обязуются своевременно информировать (по электронной почте и/или телефону) друг друга обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих надлежащему исполнению настоящего Соглашения.
4. Электронная подпись

4.1. Соглашение предусматривает использование усиленной неквалифицированной электронной подписи (далее – «Подпись»), которая позволяет обеспечить подтверждение авторства, подлинности и целостности подписанных электронных документов.

5. Средства электронной подписи
   5.1. Для создания и проверки Подписи, создания ключа Подписи и ключа проверки Подписи должны использоваться средства электронной подписи, которые:
      5.1.1. позволяют установить факт изменения подписанного электронного документа после момента его подписания;
      5.1.2. обеспечивают практическую невозможность вычисления ключа Подписи из электронной подписи или из ключа проверки Подписи.
   5.2. Компания обязана самостоятельно и за свой счет выбрать средства электронной подписи и создать ключ Подписи и ключ проверки Подписи.
6. Порядок электронного документооборота
   6.1. Перед началом взаимодействия по электронному документообороту Банк и Компания обмениваются ключами проверки Подписи. Ключ проверки Подписи Банка может быть опубликован в открытом доступе по адресу: https://developer.131.ru.
   6.2. Электронный документооборот включает следующие этапы: создание, передачу, проверку подлинности, учет и хранение электронных документов.
   6.3. Создание электронного документа включает в себя непосредственное формирование электронного документа и его подписание Подписью с использованием ключа Подписи.
   6.4. Передача подписанного электронного документа осуществляется исключительно с использованием API.
   6.5. Проверка подлинности электронного документа включает в себя проверку соответствия электронного документа требованиям к его формату и порядку заполнения, а также проверку подлинности Подписи с использованием ключа проверки Подписи.
   Для проверки Подписи Стороны используют средство электронной подписи, которое:
      1. формирует хэш из исходного электронного документа по алгоритму, определенному в Заявлении;
      2. преобразует полученную Подпись с использованием ключа проверки Подписи;
      3. сравнивает значение, полученное на шаге 1 со значением, полученным на шаге 2.

   Если значения совпали, то подлинность Подпись считается подтвержденной. Если не совпали, то считается, что подлинность Подписи не подтверждена, и проверяющая Сторона должна немедленно сообщить об этом другой Стороне.
   6.6. Учет электронных документов осуществляется путем ведения электронных журналов учета поступающих и исходящих электронных документов, подписанных Подписью. Ведение электронных журналов учета осуществляется программно-аппаратными и техническими средствами Банка. Моментом получения электронного документа является момент его отражение в журнале учета.
   6.7. Хранение электронных документов, поступивших в Банк или исходящих от Банка, осуществляется в архиве Банка в течение сроков, установленных для документов соответствующего вида, но не менее пяти лет с момента получения электронного документа. В случае возникновения споров относительно содержания электронных документов приоритет имеют электронные документы, хранящиеся в архиве Банка.
7. Признание электронных документов
   7.1. Стороны признают, что электронные документы, подписанные Подписью, являются равнозначными по своей юридической силе документам на бумажном носителе, подписанным собственноручно и заверенным печатью (при наличии).
   7.2. Предусмотренные для электронного документа правовые последствия наступают только в случае, если получен положительный результат проверки Подписи этого электронного документа, при условии соблюдения требований к формату и порядку заполнения электронного документа, установленных настоящим Соглашением и законодательством Российской Федерации.
8. Ответственность Сторон
   8.1. Стороны принимают на себя все риски, связанные с работоспособностью своего оборудования и каналов связи, сохранностью и конфиденциальностью ключей Подписи.
   8.2. В случае невыполнения или ненадлежащего выполнения своих обязательств одной из Сторон, другая Сторона имеет право потребовать от такой Стороны исполнения принятых на себя обязательств, а также возмещения причиненного ей ущерба.
   8.3. Компания несет ответственность за конфиденциальность ключа Подписи, а также за действия своих работников при использовании Подписи. Банк не несет ответственности за убытки, понесенные Компанией в связи с несанкционированным использованием Подписи неуполномоченными лицами.
9. Конфиденциальность

9.1. Стороны обязуются обеспечивать конфиденциальность ключей Подписи, в частности, не допускать использование принадлежащих им ключей Подписи без согласия Сторон. Не использовать ключ Подписи при наличии оснований полагать, что конфиденциальность данного ключа Подписи нарушена.

9.2. Сторона, допустившая компрометацию ключа Подписи, несет ответственность за электронные документы, подписанные с использованием скомпрометированного ключа Подписи. Ключ Подписи Стороны считается действующим до даты получения другой Стороной уведомления об аннулировании (отзыве) соответствующего ключа Подписи.

9.3. Стороны обязуются в течение не более чем одного календарного дня информировать друг друга обо всех случаях нарушения конфиденциальности ключей Подписи (в т.ч. утраты, хищения, несанкционированного доступа к ключу Подписи). При этом исполнение Соглашения приостанавливается до проведения смены ключей Подписи. Смена ключей Подписи осуществляется посредством подписания Сторонами нового Заявления.

10. Форс-мажор

10.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по Соглашению в случае наступления форс-мажорных обстоятельств, таких как: стихийные и техногенные катастрофы, военные действия, гражданские беспорядки, эпидемии, пандемии, крах мировой экономической и финансовой системы, принятие нормативных актов ограничительного характера. К числу форс-мажорных обстоятельств также относятся: сбой или отказ программно-аппаратных средств и оборудования, отказ или отключение систем связи, электроснабжения, вмешательство третьих лиц (DDoS-атака) и т.п.

10.2. При наступлении форс-мажорных обстоятельств, Сторона, подвергнувшаяся их влиянию, должна в течение 3 (трех) календарных дней уведомить об этом другую Сторону. Сторона, пропустившая срок уведомления, лишается права ссылаться на указанные обстоятельства, как на основание, освобождающее от ответственности.

11. Порядок разрешения споров

11.1. Настоящее Соглашение подлежит регулированию и толкованию в соответствии с законодательством Российской Федерации (применимое законодательство).

11.2. В случае возникновения разногласий по вопросам исполнения условий Соглашения, Стороны принимают все меры по их разрешению путем переговоров.

11.3. Любые споры между Сторонами, предметом которых является оспаривание содержания электронного документа, передаются для разрешения специально создаваемой экспертной комиссии. Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон. Комиссия должна установить авторство, подлинность и целостность Подписи оспариваемого электронного документа. Результаты работы экспертной комиссии оформляются актом, который должен быть подписан Сторонами. С момента подписания акта Стороны признают бесспорность сведений, указанных в данном акте. Порядок разбора конфликтных ситуаций указан в приложении № 3.

11.4. В случае невозможности урегулировать разногласия путём переговоров, споры разрешаются в Арбитражном суде Республики Татарстан с применением норм материального и процессуального права Российской Федерации.

11.5. Письменный досудебный претензионный порядок урегулирования споров является обязательным. Срок ответа на претензию – 15 (пятнадцать) календарных дней с момента ее получения.

12. Уведомления

12.1. Если иной порядок не предусмотрен Соглашением, и договором об информационно-технологическом обслуживании при осуществлении переводов денежных средств и/или договором о приеме электронного средства платежа при продаже товаров (работ/услуг) в сети Интернет при осуществлении переводов денежных средств, то любые письма, уведомления и документы, передаваемые Сторонами друг другу в рамках Соглашения по электронной почте, буду считаться надлежащим образом отправленными и полученными, если они направлены с/на адреса электронной почты, указанные Сторонами в Заявлении.

12.2. Изменение адреса электронной почты Сторон (п. 12.1), осуществляется посредством отправки электронного сообщения с ранее указанных адресов электронной почты, содержащего четкое указание на новый адрес электронной почты для осуществления связи.

13. Изменение Соглашения

13.1. Банк вправе в одностороннем внесудебном порядке вносить в Соглашение любые изменения и/ или дополнения, посредством размещения по адресу https://developer.131.ru новой редакции Соглашения.

13.2. Новой редакции Соглашения вступает в силу и подлежат применению к правоотношениям Сторон по истечении 10 (десяти) календарных дней с момента ее размещения по адресу: https://developer.131.ru.

13.3. Компания обязана самостоятельно и своевременно знакомиться с новой редакций Соглашения. В случае неполучения Банком до вступления в силу новой редакции Соглашения письменного уведомления Компании о расторжении Соглашения, новая редакция Соглашения считается безоговорочно принятой Компанией, при этом заключение дополнительного соглашения к Соглашению не требуется.

14. Срок действия и порядок расторжения

14.1. Срок действия Соглашения ограничен сроком действия заключенного между Сторонами договора об информационно-технологическом обслуживании при осуществлении переводов денежных средств и/или договора о приеме электронного средства платежа при продаже товаров (работ/услуг) в сети Интернет.

14.2. Банк вправе в одностороннем порядке отказаться от исполнения Соглашения, уведомив об этом Компанию не менее чем за 30 (тридцать) календарных дней в письменной форме.

14.3. Обязательства Сторон, возникшие до расторжения Соглашения, сохраняются до их полного исполнения.

15. Прочие условия

15.1. Настоящее Соглашение составлено на русском и английском языках. В случае возникновения противоречий приоритетным считается текст на русском языке.

15.2. Все приложения являются неотъемлемыми частями Соглашения, а именно:

15.2.1. Приложение № 1 - «Заявление»;

15.2.2. Приложение № 2 – «Инструкция по обеспечению информационной безопасности»;

15.2.3. Приложение № 3 – «Порядок разбора конфликтных ситуаций».

15.3. Стороны не вправе передать свои права и обязанности по Соглашению третьим лицам без предварительного письменного согласия другой Стороны.

15.4. Если какое-либо положение настоящего Соглашения будет признано недействительным или не имеющим законной силы в соответствии с применимым законодательством, то такое положение должно быть приведено Сторонами в соответствие с применимым законодательством, при этом действительность и применимость любого другого положения Соглашения не будет затронута.

16. Реквизиты Банка

Общество с ограниченной ответственностью «БАНК 131»
Лицензия Банка России №3538 от 12.04.2019
ОГРН 1191690025746
ИНН/КПП 1655415696 / 165501001
Адрес: 420012, Российская Федерация, Республика Татарстан,
город Казань, улица Некрасова, дом 38
Кор/сч. 30101810822029205131
в Отделение-НБ Республика Татарстан
БИК: 049205131

Приложение № 2
к Порядку электронного документооборота

Инструкция по обеспечению информационной безопасности

В целях обеспечения информационной безопасности при работе с Протоколом информационного обмена (далее – «API») Компания наделяется следующими обязанностями:

1. Ключ электронной подписи (далее по тексту – «ключ Подписи») хранить только в недоступном для посторонних лиц месте.
2. Не допускается:
   - снимать несанкционированные копии;
   - передавать ключ Подписи лицам, к ним не допущенным.
3. Не использовать в качестве пароля:
   - последовательности символов, состоящие из одних цифр (в том числе даты, номера телефонов, номера автомобилей и т.п.);
   - последовательности повторяющихся букв или цифр;
   - идущие подряд в раскладке клавиатуры или в алфавите символы;
   - имена и фамилии;
   - ИНН или другие реквизиты Компании.
4. Пароль должен:
   - быть не менее 8 символов;
   - содержать цифры, строчные и заглавные буквы;
   - содержать хотя бы 1 символ, не являющийся буквой или цифрой.
5. На компьютере должна быть установлена парольная защита на вход в операционную систему устройства.
6. Пароль пользователя в операционной системе устройства должен меняться Компанией не реже одного раза в квартал.
7. Пароль доступа к ключу Подписи хранить отдельно от ключа Подписи.
8. Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам.
9. Использовать ключ Подписи, только в момент подписания электронных документов.
10. Использовать ключ Подписи, только для подписания электронных документов в рамках использования «API».
11. Применять на рабочем месте лицензионные средства защиты от вредоносного кода с возможностью автоматического обновления баз данных сигнатур вредоносного кода.
12. Если в качестве компьютера для работы по «API» используется переносной компьютер (ноутбук), должно быть исключено его подключение к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.)
13. Осуществлять постоянный контроль отправляемых сообщений при работе «API».
14. В случае выявления признаков компрометации ключа Подписи или выявления вредоносного кода в компьютере, используемом для работы «API», необходимо немедленно уведомить Банк по телефонам: (843) 598-31-40, (843) 598-31-39 с 9 часов 00 минут до 18 часов 00 минут (в рабочие дни), либо лично явиться в Банк с целью блокирования скомпрометированных ключей Подписи с последующей их заменой.
15. К событиям, связанным с компрометацией ключей Подписи, в том числе, относятся:
   - утеря (утрата) носителя ключа Подписи, в том числе, с последующим его обнаружением;
   - обнаружение факта или угрозы использования (копирования) ключа Подписи и/или пароля доступа к ключам Подписи неуполномоченными лицами (несанкционированная отправка электронных документов);
   - обнаружение ошибок в работе «API», в том числе, возникающих в связи с попытками нарушения информационной безопасности;
   - увольнение ответственного сотрудника, имевшего доступ к ключу Подписи.
16. При обнаружении несанкционированных операций или утрате «API» немедленно уведомить Банк.
17. Использовать комбинации клавиш «Ctrl + Alt + Del» для идентификации пользователя в операционной системе.
18. Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы по Системе, заблокировать 3389 (RDP Remote desktop).
19. Включить в операционной системе журнал безопасности.
20. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д.

21. Обеспечить возможность своевременного обновления системного и прикладного программного обеспечения.
22. Выделить стационарный компьютер только для работы «API».
23. Доступ в помещение, где размещен компьютер с «API», предоставлять только уполномоченным лицам Компании.
24. Компьютер, с которого осуществляется подготовка и отправка электронных документов в Банк, рекомендуется выделить в отдельный сегмент сети с обязательным исключением его из общей локальной сети Компании.
25. Исключить доступ к компьютерам, используемым для работы по «API», посторонним лицам и персоналу организации, не уполномоченному на работу по «API» и/или обслуживание компьютеров.
26. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.
27. Банк не осуществляет рассылку электронных писем с просьбой прислать ключи Подписи и/ или пароль используемые в «API» и никогда не запрашивает у Компании эту информацию. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбой сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.) ни при каких обстоятельствах не сообщайте данную информацию и сообщите об этом в Банк.
28. Компания самостоятельно и единолично несет ответственность за обеспечение конфиденциальности паролей, ключей Подписи, и иных данных, полученных от Банка или сгенерированных Компанией самостоятельно для целей их использования при работе «API», а также за обеспечение конфиденциальности и неразглашение данных, документов и сведений, полученных и(или) отправленных с использованием «API».

Приложение № 3
к Порядку электронного документооборота

Порядок разбора конфликтных ситуаций

Любые споры между Сторонами, предметом которых является установление подлинности Подписи в электронном документе, т.е. целостности текста и аутентичности отправителя электронного документа, передаются для разрешения специально создаваемой экспертной комиссии.

Экспертная комиссия созывается на основании письменного заявления (претензии) любой из Сторон. В указанном заявлении Сторона указывает реквизиты оспариваемого подписанного электронного документа и лиц, уполномоченных представлять интересы этой Стороны в составе экспертной комиссии.

Не позднее 3 (трех) рабочих дней с момента получения другой Стороной заявления (претензии), Стороны определяют дату, место и время начала работы Экспертной комиссии, определяют, какая Сторона предоставляет помещение и производит конфигурирование средств электронной подписи.

Полномочия членов экспертной комиссии подтверждаются доверенностями, выданными в простой письменной форме.

Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон.

Экспертиза оспариваемого электронного документа осуществляется в присутствии всех членов экспертной комиссии.

Экспертиза осуществляется в четыре этапа:
1. Стороны совместно устанавливают, конфигурируют и тестируют средство электронной подписи.
2. Стороны предоставляют свои ключи Подписи и ключи проверки Подписи, используемые для создания Подписи оспариваемого электронного документа.
3. Экспертная комиссия сравнивает предоставленные ключи проверки Подписи с ключами, указанными в Заявлении. Ключи проверки Подписи и коды, которые совпали, признаются подлинными.
4. Если третий этап успешно пройден, то экспертная комиссия производит проверку подлинности Подписи в оспариваемом электронном документе.

Результаты экспертизы оформляются в виде письменного заключения - акта экспертной комиссии, подписываемого всеми членами экспертной комиссии. Акт составляется немедленно после завершения последнего этапа экспертизы. В акте фиксируются результаты всех этапов проведенной экспертизы, а также все существенные реквизиты оспариваемого электронного документа. Акт составляется в двух экземплярах – по одному для каждой из Сторон. Акт экспертной комиссии является окончательным и пересмотру не подлежит.

Подтверждение подлинности Подписи в акте, будет означать, что оспариваемый электронный документ имеет юридическую силу и влечет возникновение соответствующих прав и обязательств у Сторон.

В случае отсутствия согласия по спорным вопросам и добровольного исполнения решения экспертной комиссии, все материалы по этим вопросам могут быть переданы на рассмотрение в суд в соответствии с условиями Соглашения.