Порядок электронного документооборота

при осуществлении информационно-технологического взаимодействия

г. Казань

Редакция № 4 от «29» ноября 2024 года

Акционерное общество «Банк 131» (далее – «Банк»), с одной стороны, и юридическое лицо или индивидуальный предприниматель, заключившие с Банком договор и(или) договоры, указанные в п. 1.1., (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:

- договора об информационно-технологическом обслуживании при осуществлении переводов денежных средств;
- договора о приеме электронного средства платежа при продаже товаров (работ/услуг) в сети Интернет;
- договора процессинга;
- договора оказания услуг по обмену информацией;
- иных заключенных Сторонами сделок, предусматривающих указание на Порядок электронного документооборота (если иное прямо не указано в таких сделках Сторон).

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.

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-технологического 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, если иные сроки не согласованы Сторонами в договорах, указанных в п. 1.1 настоящего Соглашения.

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.

Electronic Document Flow Procedure

in the course of information technology interaction

Kazan

Revision No. 4 dated of 29th of November 2024

Bank 131 Joint Stock Company (hereinafter referred to as the "Bank"), on the one hand, and a legal entity or individual entrepreneur who has entered into an agreement and/or agreements specified in clause 1.1 with the Bank (hereinafter referred to as the "Company"), on the other hand, collectively referred to as the “Parties”, have entered into this Agreement as follows:

1. Subject of Agreement

1.1 This Agreement establishes the procedure for organizing and conducting electronic document flow between the Parties using electronic signature within the framework of:

- agreement on information and technology service when performing funds transfer;
- online payment service agreement;
- processing agreements;
- contracts for the provision of information exchange services;
- other transactions concluded by the Parties providing for an indication of the Procedure for electronic document management (unless otherwise expressly stated in such transactions of the Parties).

1.2 List and forms of electronic documents that the Parties can sign and transfer to each other under this Agreement are determined by the Bank and posted at https://developer.131.ru.

1.3 The companies exercise their right to exchange electronic documents signed with an electronic signature only through their duly authorized representatives. Such representatives can be both capable individuals who are endowed by the Company’s constituent documents with the right to act individually on behalf of the Company without a power of attorney, and capable individuals acting on behalf of the Company on the basis of a power of attorney.

2 Procedure for concluding Agreement

2.1 This Agreement consists of the Electronic Document Flow Procedure itself and Statement to recognize and verify an electronic signature key (hereinafter referred to as the “Statement”, Appendix No. 1). The current version of the Agreement is available at https://developer.131.ru.

2.2 The agreement is not a public offer. The Bank has the right to refuse to enter into the Agreement with the Company.

2.3 The Agreement is concluded by the Parties accepting the terms of the Electronic Document Flow Procedure and signing the Statements in two copies. The agreement is considered concluded from the date of the Statement signed.

3 Procedure for information technology interaction

3.1 The Parties carry out information technological interaction in accordance with the Information Exchange Protocol (hereinafter referred to as “API”) and Information Security Instructions (Appendix No. 2), which current editions and descriptions are posted at https://developer.131.ru/.

3.2 The Bank has the right to unilaterally make changes to API. If the changes made may affect the fulfillment by the Parties of their obligations under the Agreement, the Bank will send a notice to the Company at least 5 (five) business days before the date such changes enter into force, unless other terms are agreed upon by the Parties in the agreements specified in clause 1.1 of the Agreement.

3.3 The Parties independently and at their own expense maintain their own hardware and technical infrastructure necessary to execute the Agreement, take possible measures to protect information transmitted under the Agreement from unauthorized access, copying and distribution, including those provided for by applicable law.

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.	3.4 The Company agrees that the Bank cannot guarantee the Company the absence of interruptions associated with technical malfunctions, maintenance, as well as the complete and error-free operation of API and communication channels. The Parties undertake to promptly inform each other (by email and/or telephone) about all cases of technical malfunctions or other circumstances that obstruct the proper execution of this Agreement.
3.5. В случаях, предусмотренных соответствующими договорами, Стороны осуществляют взаимодействие используя адрес электронной почты, указанные в таких договорах.	3.5 In cases provided for in the relevant agreements, the Parties interact using the e-mail address specified in such agreements.
4. Электронная подпись	4 Electronic Signature
4.1. Соглашение предусматривает использование усиленной неквалифицированной электронной подписи (далее – «Подпись»), которая позволяет обеспечить подтверждение авторства, подлинности и целостности подписанных электронных документов.	4.1 The Agreement provides for the use of an Enhanced Unqualified Electronic Signature (hereinafter referred to as the “Signature”), which allows to confirm authorship, authenticity and integrity of signed electronic documents.
5. Средства электронной подписи	5 Electronic Signature Instruments
5.1. Для создания и проверки Подписи, создания ключа Подписи и ключа проверки Подписи должны использоваться средства электронной подписи, которые:	5.1 To create and verify a Signature, create a Signature Key and a Signature Verification Key, there should be used Electronic Signature Instruments that:
5.1.1. позволяют установить факт изменения подписанного электронного документа после момента его подписания;	5.1.1 allow you to establish the fact of modifications in a signed electronic document after its signing;
5.1.2. обеспечивают практическую невозможность вычисления ключа Подписи из электронной подписи или из ключа проверки Подписи.	5.1.2 ensure the practical impossibility of calculating a Signature Key from an electronic signature or from a Signature Verification Key.
5.2. Компания обязана самостоятельно и за свой счет выбрать средства электронной подписи и создать ключ Подписи и ключ проверки Подписи, соответствующий требованиям применимого законодательства.	5.2 The Company is obliged to independently and at its own expense select Electronic Signature Instruments and create a Signature Key and a Signature Verification Key that meets the requirements of applicable law.
6. Порядок электронного документооборота	6 Electronic Document Flow Procedure
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.	6.1 Before interaction via Electronic Document Flow, the Bank and the Company exchange Signature Verification Keys. The Bank's Signature Verification Key can be published in the public domain https://developer.131.ru.
6.2. Электронный документооборот включает следующие этапы: создание, передачу, проверку подлинности, учет и хранение электронных документов.	6.2 Electronic Document Flow includes the following stages: creation, transmittal, authentication, management and storage of electronic documents.
6.3. Создание электронного документа включает в себя непосредственное формирование электронного документа и его подписание Подписью с использованием ключа Подписи.	6.3 Electronic document creation includes the direct electronic document generation and its signing with a Signature using Signature Key.
6.4. Передача подписанного электронного документа осуществляется с использованием API и/или адресов электронной почты, указанных в соответствующем договоре.	6.4 Signed electronic document transmittal is carried out using API and/or e-mail addresses specified in the relevant agreement.
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.	6.5 Verifying the authenticity of an electronic document includes checking the compliance of the electronic document with the requirements for its format and filling procedure, as well as verifying the authenticity of the Signature using Signature Verification Key. To verify the Signature, the Parties use Electronic Signature Instrument that: 1. generates a hash from the source electronic document according to the algorithm defined in the Statement; 2. converts the received Signature using Signature Verification Key; 3. compares the value obtained in step 1 with the value obtained in step 2. If the values match, then the authenticity of the Signature is considered confirmed. If they do not match, then it is considered that the authenticity of the Signature has not been confirmed, and the verifying Party should immediately notify the other Party about it.
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.	6.6 Electronic documents are managed by maintaining electronic logs of incoming and outgoing electronic documents signed with a Signature. Electronic log books are maintained using Bank's software, hardware and technical means. The moment when electronic document is received is the moment it is reflected in the log book.

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.

6.7 Electronic documents received by the Bank or generated by the Bank are stored in the Bank's archive for the period established for documents of corresponding type, but not less than five years from the date of electronic document receipt. In case of disputes regarding the content of electronic documents, priority shall be given to electronic documents stored in Bank's archives.

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, указанными в п. 1.1 Соглашения договорами (при наличии в них соответствующих условий) и законодательством Российской Федерации.

7 Recognition of electronic documents

7.1 The Parties acknowledge that electronic documents signed with a Signature are equivalent in legal force to documents on paper, signed with one's own hand and certified by a seal (if any).

7.2 Legal consequences provided for an electronic document occur only if a positive result of verifying the Signature of this electronic document is received, subject to compliance with the requirements for format and procedure for filling out the electronic document established by this Agreement, agreements specified in clause 1.1 of the Agreement (if there are relevant conditions) and the legislation of the Russian Federation.

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.

8 Liability of the Parties

8.1 The Parties assume all risks associated with operability of their equipment and communication channels, safety and confidentiality of Signature Keys.

8.2 In case of failure or improper fulfillment of obligations by one of the Parties, the other Party has the right to demand from such Party the fulfillment of its obligations, as well as compensation for damage caused to it.

8.3 The Company is responsible for Signature Key confidentiality, as well as for employees' actions when using the Signature. The Bank is not responsible for losses incurred by the Company in connection with unauthorized use of the Signature by unauthorized persons.

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 незамедлительно, но не позднее чем в течение 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.

9 Confidentiality

9.1 The Parties undertake to ensure the confidentiality of Signature Keys, in particular, not to allow to use their Signature Keys without the Parties' consent. Do not use Signature Key if there is reason to believe that the confidentiality of this Signature key has been violated.

9.2 The Party that compromised Signature Key is responsible for electronic documents signed using the compromised Signature key. Signature Key of a Party is considered valid until the date the other Party receives a notice of cancellation (revocation) of the corresponding Signature key.

9.3 The Parties undertake to inform immediately, but no later than within one calendar day, each other about all cases of violation of the confidentiality of the Signature keys (including loss, theft, unauthorized access to Signature key). In this case, execution of the Agreement is suspended until Signature Keys are changed. Signature Keys are changed by signing a new Statement by the Parties.

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.

10 Force majeure

10.1 The Parties are released from liability for partial or complete failure to fulfill obligations under the Agreement in case of force majeure circumstances, such as: natural and man-made disasters, military actions, civil disorders, epidemics, pandemics, collapse of the global economic and financial system, adoption of restrictive regulations. Force majeure circumstances also include: fault or failure of software, hardware and equipment, failure or shutdown of communication systems, power supply, intervention of third parties (DDoS attack), etc.

10.2 If force majeure circumstances occur, the Party affected by them should notify the other Party within 3 (three) calendar days. A Party that misses the notification period forfeits the right to refer to these circumstances as a basis for releasing from liability.

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) рабочих дней с момента ее получения.

12. Уведомления

12.1. Если иной порядок не предусмотрен Соглашением и/или договором (договорами), указанными в п. 1.1. Соглашения, 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 договоров, указанных в п. 1.1. Соглашения.

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. Банк вправе в одностороннем, внесудебном порядке отказаться от исполнения Договора и расторгнуть его, уведомив об этом Компанию за 1 (один) рабочий день, в случае выявления в деятельности Компании признаков мошеннической, противоправной или необоснованно небезопасной деятельности, которая может привести к нарушению условий настоящего Договора и(или) законодательства Российской Федерации, а также к имущественным и репутационным убыткам Банка.

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

11 Dispute resolution procedure

11.1 This Agreement is subject to regulation and interpretation in accordance with the laws of the Russian Federation (applicable law).

11.2 In case of disagreements regarding the terms of the Agreement, the Parties shall take all measures to resolve them through negotiations.

11.3 Any disputes between the Parties, which subject is challenging the content of an electronic document, are referred for resolution to a specially created expert commission. Members of the expert commission are formed in equal proportions from representatives of the Parties. The Commission should establish authorship, authenticity and integrity of the Signature of the disputed electronic document. The work results of the expert commission are documented in an act that should be signed by the Parties. From the moment the act is signed, the Parties recognize the indisputability of the information specified in this act. The procedure for dealing with conflict situations is specified in Appendix No. 3.

11.4 If it is impossible to resolve disagreements through negotiations, disputes are resolved in the Arbitration Court of the Republic of Tatarstan using the rules of substantive and procedural law of the Russian Federation.

11.5 A written pre-trial claim procedure for resolving disputes is mandatory. Deadline for responding to a claim is 15 (fifteen) working days from the date of its receipt.

12 Notifications

12.1 Unless a different procedure is provided for in the Agreement and/or agreement(s) specified in clause 1.1. of the Agreement, any letters, notifications and documents transmitted by the Parties to each other under the Agreement by e-mail will be considered duly sent and received if they are sent from/to the e-mail addresses specified by the Parties in the Statement.

12.2 E-mail address of the Parties (clause 12.1) is changed by sending an e-mail from the previously specified e-mail addresses containing a clear indication of the new e-mail address for communication.

13 Change of Agreement

13.1 The Bank has the right to unilaterally, out of court, amend and/or make additions to the Agreement by posting a new revision of the Agreement at https://developer.131.ru.

13.2 The new revision of the Agreement comes into force and is to be applied to the legal relations of the Parties after 10 (ten) calendar days from the date of its posting at https://developer.131.ru.

13.3 The Company is obliged to independently and timely familiarize itself with the new revisions of the Agreement. If the Bank does not receive a written notice from the Company about termination of the Agreement before the new revision of the Agreement comes into force, the new revision of the Agreement is considered unconditionally accepted by the Company, and conclusion of an additional agreement to the Agreement is not required.

14 Validity period and termination procedure

14.1 Validity period of the Agreement is limited to the validity period of the contracts specified in clause 1.1. of the Agreements.

14.2 The Bank has the right to unilaterally refuse to fulfill the Agreement by notifying the Company at least 30 (thirty) calendar days in writing.

14.3 The Bank has the right to unilaterally, out of court, cancel the Agreement and terminate it by notifying the Company 1 (one) business day in advance, if signs of fraudulent, illegal or unreasonably unsafe activity are detected in the Company's activities, which may lead to a violation of the terms of this Agreement and (or) the legislation of the Russian Federation, as well as property and reputational losses of the Bank.

14.4 Obligations of the Parties that arose before termination of the Agreement remain until they are fully fulfilled.

15. Прочие условия	15 Miscellaneous
15.1. Настоящее Соглашение составлено на русском и английском языках. В случае возникновения противоречий приоритетным считается текст на русском языке. Все приложения являются неотъемлемыми частями Соглашения, а именно:	15.1 This Agreement is drawn up in Russian and English. In case of discrepancies, the text in Russian shall take precedence. All Appendices are integral parts of the Agreement. Specifically:
15.1.1. Приложение № 1 - «Заявление»;	15.1.1 Appendix No. 1 - “Statement”;
15.1.2. Приложение № 2 – «Инструкция по обеспечению информационной безопасности»;	15.1.2 Appendix No. 2 – “Instructions for ensuring information security”;
15.1.3. Приложение № 3 – «Порядок разбора конфликтных ситуаций».	15.1.3 Appendix No. 3 – “Procedure for dealing with conflict situations”.
15.2. Стороны не вправе передать свои права и обязанности по Соглашению третьим лицам без предварительного письменного согласия другой Стороны.	15.2 The Parties do not have the right to transfer their rights and obligations under the Agreement to third parties without the prior written consent of the other Party.
15.3. 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.	15.3 If any provision of this Agreement is found to be invalid or unenforceable under applicable law, such provision shall be construed by the Parties in accordance with applicable law, and the validity and enforceability of any other provision of the Agreement will not be affected.
16. Реквизиты Банка Акционерное общество «Банк 131» Лицензия Банка России №3538 от 29.11.2024 ОГРН 1241600056390 ИНН/КПП 1655505780 / 165501001 Адрес: 420012, Российская Федерация, Республика Татарстан, город Казань, улица Некрасова, дом 38 Кор/сч. 30101810822029205131 в Отделении-НБ Республика Татарстан БИК: 049205131	16 Bank details Bank 131 Joint Stock Company License of the Bank of Russia No. 3538 dated 29/11/2024 OGRN (Primary State Registration number) 1241600056390 INN (Taxpayer Identification number)/KPP (Tax Registration Reason Code) 1655505780/ 165501001 Address: 420012, 38 Nekrasova street, Kazan, Republic of Tatarstan, Russian Federation Correspondent account 30101810822029205131 in the Branch of the National Bank of the Republic of Tatarstan RCBIC: 049205131

Appendix No. 1

to the Electronic Document Flow Procedure in the course of information technology interaction

STATEMENT TO RECOGNIZE AND VERIFY AN ELECTRONIC SIGNATURE KEY

Стороны/Parties	**Банк/Bank**	**Компания/Company**
Полное наименование/Full name	Акционерное общество «Банк 131»/ Bank 131 Joint Stock Company	[•]
Полное ФИО и паспортные данные владельца Подписи/Full name and passport details of the owner Signatures	[•]	*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/ Such representatives can be both capable individuals who are endowed by the Company's constituent documents with the right to act individually on behalf of the Company without a power of attorney, and capable individuals acting on behalf of the Company on the basis of a power of attorney* _____/_____
Действующий на основании/Acting on the basis	[•]	*Устав, Доверенность, иной документ в соответствии с действующим законодательством/Charter, Power of Attorney, other document in accordance with current legislation*
Алгоритм Подписи/Signature Algorithm	RSA (2048 bit)	RSA (2048 bit)
Ключ проверки Подписи/Verification Key	Ключ проверки Подписи Банка опубликован в открытом доступе по адресу: https://developer.131.ru/Bank's Signature Verification Key is published in the public domain at https://developer.131.ru	[•]
Адрес электронной почты/E-mail address	[•]	[•]

Подписывая настоящее Заявление, Компания подтверждает, что она ознакомлена и согласна с Порядком электронного документооборота при осуществлении информационно-технологического взаимодействия (https://developer.131.ru) и его условиям без каких-либо правок, оговорок или исключений./By signing this Statement, the Company confirms that it is familiar with and agrees with the Electronic Document Flow Procedure when carrying out information and technological interaction (https://developer.131.ru) and its terms without any amendments, reservations or exceptions.

Банк/Bank	Компания/Company
Акционерное общество «Банк 131»/ Bank 131 Joint Stock Company Лицензия Банка России/License of the Bank of Russia No. 3538 dated 29/11/2024 ОГРН/OGRN (Primary State Registration number) 1241600056390 ИНН/INN (Taxpayer Identification number) 1655505780 КПП/KPP (Tax Registration Reason Code) 165501001 Адрес: 420012, Российская Федерация, Республика Татарстан, город Казань, улица Некрасова, дом 38/Address: 420012, 38 Nekrasova street, Kazan, Republic of Tatarstan, Russian Federation Корсчет/Correspondent account 30101810822029205131 в Отделении-НБ Республика Татарстан/in the Branch of the National Bank of the Republic of Tatarstan БИК/RCBIC: 049205131	[COMPANY NAME] [COMPANY ADDRESS] [REGISTRATION NUMBER] [INN (Taxpayer Identification number)/KPP (Tax Registration Reason Code)] [BANK DETAILS]
[ФИО]/[Full name] [Должность]/[Position] _____/_____ Date: _____	[ФИО]/[Full name] [Должность]/[Position] _____/_____ Date: _____

Приложение № 2
к Порядку электронного документооборота при осуществлении информационно-технологического взаимодействия

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) 598-31-39 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:

Appendix No. 2
to the Electronic Document Flow Procedure in the course of information technology interaction

Information Security Instructions

In order to ensure information security when working with the Information Exchange Protocol (hereinafter referred to as "API"), the Company is vested with the following responsibilities:

1. Keep the Electronic Signature Key (hereinafter referred to as the "Signature Key") only in a place inaccessible to unauthorized persons.
2. It is not allowed to:
   - make unauthorized copies;
   - transfer Signature Key to persons not authorized to see it.
3. Do not use as a password:
   - sequences of characters consisting of only numbers (including dates, telephone numbers, car numbers, etc.);
   - sequences of repeated letters or numbers;
   - consecutive characters in the keyboard layout or alphabet;
   - first and last names;
   - INN (Taxpayer Identification number) or other details of the Company.
4. The password should:
   - be at least 8 characters;
   - contain numbers, lowercase and capital letters;
   - contain at least 1 character that is not a letter or number.
5. The computer should have password protection installed to enter the device's operating system.
6. The user's password in the device's operating system should be changed by the Company at least once a quarter.
7. Store the access password to the Signature Key separately from the Signature Key.
8. It is strictly prohibited to write passwords on paper or in text files at the workplace, leave them in easily accessible places, or transfer them to unauthorized persons.
9. Use Signature key only when signing electronic documents.
10. Use Signature key only for signing electronic documents within the framework of using "API".
11. Use licensed anti-malware protection tools in the workplace with the ability to automatically update malicious code signature databases.
12. If a portable computer (laptop) is used as a computer for API working, its connection to public networks in places with free access to the Internet (office centers, cafes, etc.) should be excluded.
13. Perform constant monitoring of messages sent when API is running.
14. If signs of Signature Key compromise are detected or malicious code is detected in the computer used to operate API, you should immediately notify the Bank by phone: (843) 598-31-39 from 9:00 a.m. to 6:00 p.m. business days), or come to the Bank in person to block compromised Signature Keys and then replace them.
15. Events related to Signature Keys compromise include, but are not limited to:

• утеря (утрата) носителя ключа Подписи, в том числе, с последующим его обнаружением;	• loss (forfeit) of Signature Key carrier, including with its subsequent discovery;
• обнаружение факта или угрозы использования (копирования) ключа Подписи и/или пароля доступа к ключам Подписи неуполномоченными лицами (несанкционированная отправка электронных документов);	• detection of the fact or threat of use (copying) of Signature Key and/or password for access to Signature Keys by unauthorized persons (unauthorized sending of electronic documents);
• обнаружение ошибок в работе «API», в том числе, возникающих в связи с попытками нарушения информационной безопасности;	• detection of errors in API operation, including those arising in connection with attempts to violate information security;
• увольнение ответственного сотрудника, имевшего доступ к ключу Подписи.	• dismissal of the responsible employee who had access to Signature Key.
16. При обнаружении несанкционированных операций или утрате «API» немедленно уведомить Банк.	16. If unauthorized transactions are detected or is lost, immediately notify the Bank.
17. Использовать комбинации клавиш «Ctrl + Alt + Del» для идентификации пользователя в операционной системе.	17. Use the key combination “Ctrl + Alt + Del” to identify the user in the operating system.
18. Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы по API, заблокировать 3389 (RDP Remote desktop).	18. Disable the ability for remote and terminal connections to computers used to work via API, block 3389 (RDP Remote desktop).
19. Включить в операционной системе журнал безопасности.	19. Enable security logging in the operating system.
20. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д.	20. Use only licensed software - operating systems, anti-malware tools, office suites, etc.
21. Обеспечить возможность своевременного обновления системного и прикладного программного обеспечения.	21. Ensure the possibility of timely updating of system and application software.
22. Выделить стационарный компьютер только для работы «API».	22. Dedicate a desktop computer only for “API” work.
23. Доступ в помещение, где размещен компьютер с доступом к «API», предоставлять только уполномоченным лицам Компании.	23. Access to the premises where a computer with API access is located is provided only to authorized persons of the Company.
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.	24. It is recommended that the computer from which electronic documents are prepared and sent to the Bank be separated into a separate network segment with its obligatory exclusion from the Company’s general local network.
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.	25. Prevent access to computers used to work on API by unauthorized persons and organization personnel not authorized to work on API and/or servicing computers.
26. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.	26. When servicing a computer, IT employees ensure control over the actions they perform.
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.	27. The Bank does not send e-mails asking for Signature Keys and/or password used in API and never requests this information from the Company. When contacting persons on behalf of the Bank by telephone, e-mail, or SMS messages with a request to provide confidential information (passwords, code words, etc.), do not provide this information at any time and report this to the Bank.
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».	28. The Company is independently and solely responsible for ensuring confidentiality of passwords, Signature Keys, and other data received from the Bank or generated by the Company independently for the purposes of their use when operating API, as well as for ensuring confidentiality and non-disclosure of data, documents and information received and (or) sent using "API".

Приложение № 3
к Порядку электронного документооборота при осуществлении информационно-технологического взаимодействия

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 установленном законодательством порядке.

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.

Appendix No. 3
to the Electronic Document Flow Procedure in the course of information technology interaction

Procedure for dealing with conflict situations

Any disputes between the Parties, which subject is establishing Signature authenticity in an electronic document, i.e. integrity of the text and authenticity of the sender of an electronic document is submitted for permission to a specially created expert commission.

The expert commission is convened on the basis of a written application (claim) of any of the Parties. In the said application, the Party indicates details of the disputed signed electronic document and the persons authorized to represent interests of this Party as part of the expert commission.

No later than 3 (three) working days from the receipt of the application (claim) by the other Party, the Parties determine the date, place and time of the work start for the Expert Commission, determine which Party provides premises and configure Electronic Signature Instruments.

The powers of the members of the expert commission are confirmed by powers of attorney issued in the manner prescribed by the law.

Members of the expert commission are formed in equal proportions from representatives of the Parties.

The disputed electronic document is examined in the presence of all members of the expert commission.

Examination is performed in four stages:
1. The Parties jointly install, configure and test an electronic signature instrument.
2. The Parties provide their Signature Keys and Signature Verification Keys used to create the Signature of the disputed electronic document.
3. The expert commission compares the provided Signature Verification Keys with the keys specified in the Application. Signature Verification Keys and codes that match are recognized as authentic.
4. If the third stage is successfully completed, the expert commission verifies the authenticity of the Signature in the disputed electronic document.

The results of the examination are formalized in the form of a written conclusion - an act of the expert commission, signed by all members of the expert commission. The report is drawn up immediately after completion of the last examination stage. The act records results of all examination stages, as well as all essential details of the disputed electronic document. The act is drawn up in two copies, one for each of the Parties. The report of the expert commission is final and is not subject to revision.

Confirmation of Signature authenticity in the act will mean that the disputed electronic document has legal force and entails the emergence of corresponding rights and obligations for the Parties.

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.	If there is no agreement on controversial issues and voluntary execution of the decision of the expert commission, all materials on these issues may be submitted to the court for consideration in accordance with the terms of the Agreement.