Порядок электронного документооборота

при осуществлении информационно-технологического взаимодействия

г. Казань

Редакция № 6 от «16» декабря 2025 года

Акционерное общество «Банк 131» (далее – «Банк»), с одной стороны, и юридическое лицо или индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, 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;
- договора об оказании платежных услуг;
- договора специального банковского счета;
- договора об открытии и порядке ведения корреспондентских счетов;
- договора комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой;
- 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 реализует 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.

2.4. Стороны пришли к соглашению о том, что Заявление может быть подписано Сторонами одним из следующих способов:

2.4.1. на бумажном носителе. При этом Заявление считается полученным с даты его вручения получающей Стороне, согласно данным документа о получении;

2.4.2. в системе дистанционного банковского обслуживания Банка (при наличии заключенного между Сторонами договора о предоставлении соответствующего банковского продукта (услуги) Банка, предусматривающего обмен электронными документами посредством дистанционного банковского

Electronic Document Flow Procedure

in the course of information technology interaction

Kazan

Revision No.6 dated of 16th of December 2025

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 matter

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;
- agreement on payment services;
- agreement on special bank account;
- agreement on opening and maintenance of correspondent accounts;
- comprehensive banking service agreement for legal entities, individual entrepreneurs, and individuals engaged in private practice;
- 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.

2.4 The Parties have agreed that the Statement may be signed by the Parties in one of the following ways:

2.4.1. in hard copy. In this case, the Statement is considered received from the date of its delivery to the receiving Party, according to the receipt document.;

2.4.2. in the Bank's remote banking system (if there is an agreement concluded between the Parties on the provision of the relevant banking product (service) of the Bank, providing for the exchange of electronic documents through remote banking and the Company's connection to the remote banking system (RBS) in accordance with the procedure provided by the Bank). The

обслуживания (ДБО) и присоединения Компании к системе ДБО в предусмотренном Банком порядке). Заявление считается полученным в дату доставки Заявления получающей Стороне согласно отметке в системе ДБО;

2.4.3. путем подписания Заявления усиленной квалифицированной электронной подписью с использованием системы электронного документооборота стороннего оператора (например, «Контур.Диадок», «Такском», «СБИС», иные). При этом Стороны пришли к соглашению о том, что для признания Заявления, переданного через систему ЭДО такого стороннего оператора юридически значимым документом, заключение отдельного соглашения об обмене электронными документами между Банком и Компанией не требуется, необходимым и достаточным является факт подключения каждой Стороной к системе ЭДО такого оператора, заключение соответствующего соглашения с ним, а также фактические действия каждой Стороны по отправке подписанного Заявления другой Стороне в соответствии с правилами оператора системы ЭДО.

2.4.4. путем обмена сканированными копиями подписанного Сторонами Заявления с использованием адресов электронной почты Сторон[1], согласованных в соответствующем договоре, указанном в п.1.1 Соглашения. Сканированная копия Заявления считается полученной на следующий рабочий день с момента ее направления по указанным адресам электронной почты.

2.5. Заявление, подписанное Сторонами способами, указанными в п.п. 2.4.2, 2.4.3 или 2.4.4 Соглашения, является равнозначным по своей юридической силе Заявлению на бумажном носителе, подписанным представителями Сторон собственноручно и заверенным печатью (при наличии).

2.6. При подписании Заявления способом согласно п.2.4.4 Соглашения, Компания обязуется направить Банку подлинник подписанного Заявления на бумажном носителе по почте заказной корреспонденцией или курьером в срок не позднее 10 (Десяти) рабочих дней с даты отправки в Банк сканированной подписанной со стороны Компании копии Заявления. Отсканированная копия Заявления, подписанная уполномоченным лицом Компании и скрепленная печатью (при наличии), обладает юридической силой до момента получения Банком от Компании подлинника Заявления на бумажном носителе. До момента получения от Клиента подлинника Заявления, Банк вправе вводить лимиты на суммы и количество совершаемых Компанией операций. В случае, если Банк не получил от Компании подлинник Заявления в срок, указанный в настоящем пункте, Банк вправе приостановить обмен электронными документами по настоящему Соглашению с уведомлением Компании. При этом Банк не несет ответственности за любые убытки Компании.

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

Statement is considered received on the date of delivery of the Statement to the receiving Party according to the mark in the RBS;

2.4.3. by signing the Statement with the Enhanced certified electronic signature using an electronic document flow (EDF) system of a third-party operator (for example, "Contour.Diadoc", "Taxcom", "SBIS", others). At the same time, the Parties agreed that in order to recognize the Statement transmitted through the EDF system of such a third-party operator as a legally significant document, the conclusion of a separate agreement on the exchange of electronic documents between the Bank and the Company is not required, it is necessary and sufficient that each Party connects to the EDF system of such an operator, the conclusion of a corresponding agreement with operator, and also, the actual actions of each Party to send the signed Statement to the other Party in accordance with the rules of the operator of the EDF system.

2.4.4. by exchanging scanned copies of the Statement signed by the Parties using the e-mail addresses of the Parties[2] agreed in the relevant agreements specified in clause 1.1 of the Agreement. A scanned copy of the Statement is considered received on the next business day from the moment it is sent to the specified email addresses.

2.5 The Statement signed by the Parties using the methods specified in clauses 2.4.2, 2.4.3 or 2.4.4 of the Agreement is equivalent in its legal force to a paper Statement signed by the representatives of the Parties in their own hand and stamped (if any).

2.6 When signing the Statement in accordance with clause 2.4.4 of the Agreement, the Company undertakes to send to the Bank the original of the signed Statement in hard copy by registered mail or courier no later than 10 (Ten) business days from the date of sending to the Bank a scanned signed copy of the Statement by the Company. A scanned copy of the Statement, signed by an authorized person of the Company and sealed (if any), is legally binding until the Bank receives the hard copy of the Statement from the Company. Until the moment the hard copy of the Statement is received from the Company, the Bank has the right to impose limits on the amounts and number of transactions performed by the Company. If the Bank has not received the Statement in hard copy from the Company within the time period specified in this clause, the Bank has the right to suspend the exchange of electronic documents under this Agreement with the notification of the Company. At the same time, the Bank is not responsible for any losses of the Company.

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.

---

[1] ***Для Банка Заявление необходимо направлять на адрес для Общих вопросов: accounting@131.ru***

[2] ***For the Bank, the Statement should be sent to the e-mail for General Questions: accounting@131.ru***

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.

3.5. В случаях, предусмотренных соответствующими договорами, Стороны осуществляют взаимодействие используя адрес электронной почты, указанные в таких договорах.

4. Электронная подпись

4.1. Соглашение предусматривает использование усиленной неквалифицированной электронной подписи в рамках информационно-технологического взаимодействия (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, соответствующий требованиям применимого законодательства.

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, проверку целостности, проверку авторства, 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 с использованием API и/или адресов электронной почты, указанных в соответствующем договоре.

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. Проверка целостности электронного документа осуществляется путем проверки Подписи с использованием средств проверки Подписи: процедура проверки Подписи, использованной при

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 In cases provided for in the relevant agreements, the Parties interact using the e-mail address specified in such agreements.

4 Electronic Signature

4.1. The Agreement provides for the use of an enhanced unqualified electronic signature within the framework of information technology interaction (hereinafter referred to as the "Signature"), which ensures verification of authorship, authenticity, and integrity of the signed electronic documents.

5 Electronic Signature Instruments

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. allow you to establish the fact of modifications in a signed electronic document after its signing;

5.1.2. ensure the practical impossibility of calculating a Signature Key from an electronic signature or from a Signature Verification Key.

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 Electronic Document Flow Procedure

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. Electronic document flow includes the following stages: creation, transmission, authenticity verification, integrity verification, authorship verification, recording, and storage of electronic documents.

6.3. Electronic document creation includes the direct electronic document generation and its signing with a Signature using Signature Key.

6.4. Signed electronic document transmittal is carried out using API and/or e-mail addresses specified in the relevant agreement.

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. Integrity verification of an electronic document is performed by validating the Signature using Signature verification tools: the verification procedure for a Signature applied to an electronic

подписании электронного документа, с нарушенной целостностью даст отрицательный результат (сообщит об ошибке Подписи).

В случае получения отрицательного результата проверки целостности электронного документа такой документ считается недействительным (не имеет юридической силы), некорректным и проверяющая Сторона должна немедленно сообщить об этом другой Стороне.

6.7. Проверка авторства электронного документа представляет собой проверку того, что Подпись считается принадлежащей Стороне – если физическое лицо, действующее от имени указанной Стороны на основании учредительных документов юридического лица или доверенности, является владельцем сертификата ключа проверки Подписи.

Стороны признают, что используемые способы защиты электронных документов, которые обеспечивают формирование и проверку Подписи, достаточны для подтверждения авторства, подлинности и целостности электронных документов.

6.8. 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.

6.9. 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, указанными в п. 1.1 Соглашения договорами (при наличии в них соответствующих условий) 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.

document with compromised integrity will yield a negative result (report a Signature error).

If the integrity verification returns a negative result, such document shall be deemed invalid (legally void), defective, and the verifying Party must immediately notify the other Party.

6.7. Verification of an electronic document's authorship constitutes verification that the Signature is deemed to belong to the Party - provided that the individual acting on behalf of said Party under the entity's constitutive documents or power of attorney is the holder of the Signature verification key certificate.

The Parties acknowledge that the employed electronic document security methods, which enable the generation and verification of the Signature, are sufficient to confirm the authorship, authenticity and integrity of electronic documents.

6.8. Electronic document accounting is performed by maintaining electronic logs of incoming and outgoing electronic documents signed with the Signature. The electronic log maintenance is executed through the Bank's software, hardware, and technical means. The moment of receipt of an electronic document is the moment of its recording in the accounting log.

6.9. Storage of electronic documents received by the Bank or sent from the Bank shall be maintained in the Bank's archive for the retention periods established for the respective document types, but not less than five years from the date of receipt of the electronic document. In case of disputes regarding the content of electronic documents, the electronic documents stored in the Bank's archive shall prevail.

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. 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. 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.

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.

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) 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.

Signature Keys are changed by signing a new Statement by the Parties.

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. 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.

13.2. Новая редакция Соглашения вступает в силу и подлежит 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 Соглашения 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 Соглашения 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.

15. Прочие условия

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:

15.1.1. Приложение № 1 - «Заявление»;

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

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

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

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.

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
Корр. сч. 30101810822029205131 в Операционно-кассовом центре № 6 Волго-Вятского главного управления Центрального банка Российской Федерации
БИК: 049205131

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. Miscellaneous

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. Appendix No. 1 - “Statement”;

15.1.2. Appendix No. 2 – “Instructions for ensuring information security”;

15.1.3. Appendix No. 3 – “Procedure for dealing with conflict situations”.

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. 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. 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 Transaction and Cash Center No. 6 of the Volgo-Vyatsky Main Directorate of the Central Bank of the Russian Federation
BIC (Russian Central Bank Identification Code): 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 условиями 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 Корр. сч. /Correspondent account 30101810822029205131 в Операционно-кассовом центре № 6 Волго-Вятского главного управления Центрального банка Российской Федерации / in the Transaction and Cash Center No. 6 of the Volgo-Vyatsky Main Directorate of the Central Bank of the Russian Federation БИК/BIC (Russian Central Bank Identification Code): 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 12 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, в том числе настроить еженедельное проведение полной антивирусной проверки устройства.
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.), а также обеспечено раздельное хранение переносного компьютера и ключевого носителя.
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: (8 800 100 13 10 с 9 часов 00 минут до 18 часов 00 минут (в рабочие дни), либо направить уведомление с использованием адресов электронной почты, указанных в Заявлении либо договоре, предусмотренном п.1.1 Соглашения, 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);

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

Information Security Policy

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 12 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 software with automatic signature database updates at all workstations, including configuration of weekly full-system antivirus scans

12. If a portable computer (laptop) is used as an API workstation, the following must be enforced: Connection to public networks in open-access areas (co-working spaces, cafes, etc.) must be prohibited. The portable computer and cryptographic key storage device must be stored separately when not in use.

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: 8 800 100 13 10 from 9:00 a.m. to 6:00 p.m. business days), or send a notification using the email addresses specified in the Statement either in the agreements specified in the clause 1.1. of the Agreement or come to the Bank in person to block compromised Signature Keys and then replace them.

15. The following incidents shall be classified as Signature Key Compromise Events:

- Loss or misplacement of the Signature key storage device (including cases where it is later recovered);

- передача ключа Подписи по открытым каналам связи;
- перехват ключа электронной подписи вредоносным программным обеспечением;
- обнаружение ошибок в работе «API», в том числе, возникающих в связи с попытками нарушения информационной безопасности;
- увольнение ответственного сотрудника, имевшего доступ к ключу Подписи;
- случаи, когда невозможно достоверно установить, что произошло с ключевым носителем Подписи, в том числе случаи выхода ключевого носителя Подписи из строя.

16. При обнаружении несанкционированных операций или утрате «API» немедленно уведомить Банк.
17. Блокировать сеанс пользователя во время отсутствия на рабочем месте (путем одновременного нажатия клавиш Windows: Win+L или Ctrl+Alt+Del (Заблокировать), MacOS: Ctrl+Cmd+Q), а также завершать сеансы работы после окончания необходимости их использования.
18. Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы по API, заблокировать 3389 (RDP Remote desktop), не допускать установку на компьютер никаких программ для удаленного управления (Team Viewer, Ассистент, AnyDesk, VNC и т.п.).
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., дистрибутивы которых получены из надежных источников.
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 доступом к «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».

- Unauthorized access or potential compromise of Signature keys and/or their access credentials (e.g., password breaches leading to fraudulent electronic document submissions);
- Transmission of Signature keys over unsecured communication channels;
- Interception of electronic signature keys by malware or malicious software;
- API malfunctions or errors indicating potential security breaches (including failed intrusion attempts);
- Termination of employment of personnel with authorized access to Signature keys;

  Unaccounted key storage incidents, including cases where the Signature key device is damaged or its status cannot be reliably determined.

16. In case of unauthorized operations or loss of the "API", immediately notify the Bank.
17. Lock the user session when away from the workstation (by pressing Windows: Win+L or Ctrl+Alt+Del → Lock, macOS: Ctrl+Cmd+Q). Additionally, ensure all active sessions are terminated after they are no longer needed.
18. Disable remote and terminal connections to API workstations, including blocking port 3389 (RDP/Remote Desktop) and prohibiting installation of any remote control software (TeamViewer, AnyDesk, VNC, remote assistance tools, etc.).

19. Enable security logging in the operating system.
20. Use only licensed software – operating systems, malware protection tools, office suites, etc., obtained from reliable sources.
21. Ensure the possibility of timely updating of system and application software.
22. Dedicate a desktop computer only for “API” work.
23. Access to the premises where a computer with API access is located is provided only to authorized persons of the Company.
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. 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. When servicing a computer, IT employees ensure control over the actions they perform.
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. 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.

Проверка подлинности подписи в оспариваемом электронном документе осуществляется одним из следующих способов:
1. Выполнение в командной строке (терминале) операционной системы, где установлен OpenSSL, команды: $ openssl dgst -sha256 -verify public.pem -signature sha256.sign myfile.txt.

Указанная команда используется для проверки Подписи файла myfile.txt с помощью ключа проверки из файла public.pem и ключа из файла sha256.sign. Если результатом команды является «Verified OK» — это означает успешную проверку подписи.

2. Вызов функции в PHP-скрипте: $isValid = openssl_verify($data, $decodedSignature, $publicKey, OPENSSL_ALGO_SHA256).

Функция проверяет подлинность Подписи для заданных данных $data с использованием ключа проверки $publicKey и алгоритма хеширования SHA-256 (OPENSSL_ALGO_SHA256). Если результатом проверки является 1 – подпись верна, 0 – неверна, -1 – ошибка.

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

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 authenticity verification of a signature in a disputed electronic document is performed using one of the following methods:

1.Executing a command in the operating system's command line (terminal) where OpenSSL is installed. The specified command is used to verify the Signature of the myfile.txt file using the verification key from the public.pem file and the key from the sha256.sign file. If the command result is "Verified OK", this indicates successful signature verification.

2.Calling a function in a PHP script. The function verifies the authenticity of the Signature for the given data using the verification key and SHA-256 hashing algorithm. If the verification result is 1 - the signature is valid, 0 - invalid, -1 - error.

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.

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.	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. 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.