|  |  |
| --- | --- |
| **Порядок электронного документооборота** при осуществлении информационно-технологического обслуживания в рамках Условий осуществления расчетов с использованием СБП (Условия СБП)г. Казань Редакция № 1 от «01» марта 2022 года **В рамках настоящего Порядка электронного документооборота (далее – Порядок, ЭДО), применяются термины и определения, указанные в Условиях осуществления расчетов с использованием СБП, если иное не указано в настоящем Порядке.**Общество с ограниченной ответственностью «Банк 131» (далее – «Банк»), с одной стороны, и юридическое лицо или индивидуальный предприниматель, заключившее(-ий) с Банком Соглашение об использовании СБП (в соответствии с Условиями СБП) (далее – «Клиент»), с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение о нижеследующем: 1. Предмет Соглашения
	1. Настоящее Соглашение устанавливает порядок организации и проведения электронного документооборота с использованием Электронной подписи между Сторонами в рамках Соглашения об использовании СБП.
	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/ [.](https://developer.131.ru/)
	3. Клиент 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 Клиента правом единолично действовать от имени последнего без доверенности, так и дееспособные физические лица, действующие от имени Клиента на основании доверенности. Уполномоченные Представители Клиента определяются Клиентом в Заявлении[[1]](#footnote-1).
2. Порядок заключения Соглашения
	1. Настоящее Соглашение состоит из настоящего Порядка и Заявления о признании и сверке ключа электронной подписи (далее – «Заявление», приложение № 1). Актуальная редакция Соглашения размещена по адресу: https://developer.131.ru/.
	2. Соглашение не является публичной офертой. Банк вправе отказаться от заключения Соглашения с Клиентом в случае, если Клиент не имеет заключенного с Банком соглашения об использовании СБП.
	3. Соглашение заключается путем принятия Сторонами условий Порядка и подписания Заявления в двух экземплярах. Соглашение считается заключенным с даты подписания Заявления.
3. Порядок информационно-технического взаимодействия
	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/
	2. Банк вправе в одностороннем порядке вносить изменения в API и ЭДО, в порядке, указанном в Условиях СБП.
	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.
	4. Клиент соглашается, что Банк не может гарантировать Клиенту отсутствие перерывов, связанных с техническими неисправностями, проведением профилактических работ, а также полную и безошибочную работоспособность API и каналов связи. Клиент обязуется своевременно информировать Банк обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих надлежащему исполнению настоящего Соглашения, в соответствии с Условиями СБП.
4. Электронная подпись
	1. Соглашение предусматривает использование усиленной неквалифицированной электронной подписи (далее – «Электронная подпись»), которая позволяет обеспечить подтверждение авторства, подлинности и целостности подписанных Электронных документов.
5. Средства электронной подписи
	1. Для создания и проверки Электронной подписи, создания ключа Электронной подписи и ключа проверки Электронной 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 Электронной подписи из электронной подписи или из ключа проверки Электронной подписи. * 1. Клиент обязан самостоятельно и за свой счет выбрать средства Электронной подписи и создать ключ Электронной подписи и ключ проверки Электронной подписи, в соответствии с Условиями СБП и требованиями законодательства РФ.
1. Порядок электронного документооборота
	1. Перед началом осуществления электронного документооборота Банк и Клиент обмениваются ключами проверки Электронной подписи. Ключ проверки Электронной подписи Банка может быть опубликован в открытом доступе по адресу: https://developer.131.ru/.
	2. Электронный документооборот включает следующие этапы: создание, передачу, проверку подлинности, учет и хранение Электронных документов.
	3. Создание Электронного документа включает в себя непосредственное формирование Электронного документа и его подписание Электронной подписью с использованием ключа Электронной подписи.
	4. Передача подписанного Электронного документа осуществляется исключительно с использованием API.
	5. Проверка подлинности Электронного документа включает в себя проверку соответствия Электронного документа требованиям к его формату и порядку заполнения, а также проверку подлинности Электронной подписи с использованием ключа проверки Электронной подписи.

Для проверки Электронной подписи Стороны используют средство Электронной подписи, которое: * + 1. формирует хэш из исходного Электронного документа по алгоритму, определенному в Заявлении;
		2. преобразует полученную Электронной подпись с использованием ключа проверки Электронной подписи;
		3. сравнивает значение, полученное на шаге 1 со значением, полученным на шаге 2.

Если значения совпали, то подлинность Электронной подпись считается подтвержденной. Если не совпали, то считается, что подлинность Электронной подписи не подтверждена, и проверяющая Сторона должна немедленно сообщить об этом другой Стороне. * 1. Учет Электронных документов осуществляется путем ведения электронных журналов учета поступающих и исходящих Электронных документов, подписанных Электронной подписью. Ведение электронных журналов учета осуществляется программно-аппаратными и техническими средствами Банка. Моментом получения Электронного документа является момент его отражение в журнале учета.
	2. 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.
1. Признание Электронных документов
	1. Стороны признают, что Электронные документы, подписанные Электронной подписью, являются равнозначными по своей юридической силе документам на бумажном носителе, подписанным собственноручно и заверенным печатью (при наличии).
	2. Предусмотренные для Электронного документа правовые последствия наступают только в случае, если получен положительный результат проверки Электронной подписи этого Электронного документа, при условии соблюдения требований к формату и порядку заполнения Электронного документа, установленных настоящим Соглашением, Условиями СБП, Банковскими правилами, Правилами и Стандартами ОПКЦ СБП и законодательством Российской Федерации.
2. Ответственность Сторон
	1. Стороны принимают на себя все риски, связанные с работоспособностью своего оборудования и каналов связи, сохранностью и конфиденциальностью ключей Электронной подписи.
	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.
	3. Клиент несет ответственность за конфиденциальность ключа Электронной подписи, а также за действия своих работников при использовании Электронной подписи. Банк не несет ответственности за убытки, понесенные Клиентом в связи с несанкционированным использованием Электронной подписи неуполномоченными лицами.
3. Конфиденциальность
	1. Стороны обязуются обеспечивать конфиденциальность ключей Электронной подписи, в частности, не допускать использование принадлежащих им ключей Электронной подписи без согласия Сторон. Не использовать ключ Электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа Электронной подписи нарушена.
	2. Сторона, допустившая компрометацию ключа Электронной подписи, несет ответственность за Электронные документы, подписанные с использованием скомпрометированного ключа Электронной подписи. Ключ Электронной подписи Стороны считается действующим до даты получения другой Стороной уведомления об аннулировании (отзыве) соответствующего ключа Электронной подписи.
	3. Стороны обязуются в течение не более чем одного календарного дня информировать друг друга обо всех случаях нарушения конфиденциальности ключей Электронной подписи (в т.ч. утраты, хищения, несанкционированного доступа к ключу Электронной подписи). При этом исполнение Соглашения приостанавливается до проведения смены ключей Электронной подписи. Смена ключей Электронной подписи осуществляется посредством подписания Сторонами нового Заявления.
4. 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. 1. 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 Электронной 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 – 30 (Тридцать) календарных дней с момента ее получения. 1. Уведомления

12.1.Если иной порядок не предусмотрен настоящим Соглашением, и Соглашением об использовании СБП, то любые письма, уведомления и документы, передаваемые Сторонами друг другу в рамках Соглашения по электронной почте, адреса которой указаны в Заявлении буду считаться надлежащим образом отправленными и полученными, если они направлены с/на адреса электронной почты, указанные Сторонами в Заявлении. Указанный порядок не применяется в случаях, предусмотренных Условиями СБП и/или Правилами, а также в установленном законодательством РФ случаях.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. 1. 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/[.](https://developer.131.ru/) 13.3.Клиент обязан самостоятельно и своевременно знакомиться с новой редакций Соглашения. В случае неполучения Банком до вступления в силу новой редакции Соглашения письменного уведомления Клиента о расторжении Соглашения, новая редакция Соглашения считается безоговорочно принятой Клиентом, при этом заключение дополнительного соглашения к Соглашению не требуется. 1. Срок действия и порядок расторжения

14.1.Срок действия Соглашения ограничен сроком действия заключенного между Сторонами Соглашения об использовании СБП. 14.2.Банк вправе в одностороннем порядке отказаться от исполнения Соглашения, уведомив об этом Клиента не менее чем за 30 (тридцать) календарных дней любым доступным Банку способом. 14.3.Обязательства Сторон, возникшие до расторжения Соглашения, сохраняются до их полного исполнения. 1. Прочие условия

15.1.Настоящее Соглашение составлено на русском и английском языках. В случае возникновения противоречий приоритетным считается текст на русском языке. 15.2.Все приложения являются неотъемлемыми частями Соглашения, а именно: 15.2.1.Приложение № 1 - «Заявление»; 15.2.2.Приложение № 2 – «Инструкция по обеспечению информационной безопасности»; 15.2.3.Приложение № 3 – «Порядок разбора конфликтных ситуаций». 15.3.Стороны не вправе передать свои права и обязанности по Соглашению третьим лицам без предварительного письменного согласия другой Стороны. 15.4.Если какое-либо положение настоящего Соглашения будет признано недействительным или не имеющим законной силы в соответствии с применимым законодательством Российской Федерации, то такое положение должно быть приведено Сторонами в соответствие с применимым законодательством, при этом действительность и применимость любого другого положения Соглашения не будет затронута. 1. Реквизиты Банка

Общество с ограниченной ответственностью «БАНК 131» Лицензия Банка России №3538 от 12.04.2019 ОГРН 1191690025746 ИНН/КПП 1655415696 / 165501001 Адрес: 420012, Российская Федерация, Республика Татарстан, город Казань, улица Некрасова, дом 38 Кор/сч. 30101810822029205131 в Отделение-НБ Республика Татарстан БИК: 049205131  | **Procedure of Electronic Document Flow**during information technology serviceswithin the framework of the Terms of Settlements using FPS(SBP Terms)KazanRevision No. 1 dated "01" March 2022**Within the framework of this Procedure of Electronic Document Flow (hereinafter referred to as the Procedure, EDF), the terms and definitions specified in the Terms of Settlements using SBP are applied, unless otherwise specified in this Procedure.**Limited Liability Company "Bank 131" (hereinafter referred to as the "Bank"), on the one hand, and a legal entity or an individual entrepreneur who has entered into an Agreement with the Bank on the use of SBP (in accordance with the Terms of SBP) (hereinafter referred to as the "Customer”), on the other hand, collectively referred to as the “Parties”, have entered into this Agreement as follows:1. Subject of the Agreement
	1. This Agreement establishes the procedure for organizing and conducting electronic document flow using an Electronic Signature between the Parties under the Agreement on the use of SBP.
	2. The list and forms of Electronic Documents that the Parties may sign and transfer to each other under this Agreement are determined by the Bank and posted at: https://developer.131.ru/[.](https://developer.131.ru/)
	3. The Customer exercises his right to exchange Electronic Documents signed with an Electronic Signature only through his duly authorized Representatives. Such Representatives can be both capable individuals, endowed by the constituent documents of the Customer with the right to act solely on behalf of the latter without a power of attorney, and capable individuals acting on behalf of the Customer on the basis of a power of attorney. Authorized Representatives of the Customer are determined by the Customer in the Application[[2]](#footnote-2).
2. Procedure for Concluding the Agreement
	1. This Agreement consists of this Procedure and the Application for recognition and verification of an electronic signature key (hereinafter referred to as the "Application", Appendix No. 1). The current version of the Agreement is available at: https://developer.131.ru/.
	2. The agreement is not a public offer. The Bank has the right to refuse to conclude the Agreement with the Customer if the Customer does not have an agreement concluded with the Bank on the use of SBP.
	3. The Agreement is concluded by the Parties accepting the terms of the Procedure and signing the Application in two copies. The Agreement is considered concluded from the date of signing the Application.
3. The Order of Information and Technical Interaction
	1. The Parties carry out information technology interaction in accordance with the Data Communications Protocol (hereinafter referred to as "API") and Instructions for Ensuring Information Security (Appendix No. 2), the current versions and descriptions of which are available at: https://developer.131.ru/
	2. The Bank has the right to unilaterally make changes to API and EDF, in the manner specified in the Terms of SBP.
	3. The Parties independently and at their own expense maintain their own hardware and technical infrastructure necessary for the execution of the Agreement, take all possible measures to protect the information transmitted under the Agreement from unauthorized access, copying and distribution, including those provided for by applicable law.
	4. The Customer agrees that the Bank cannot guarantee the Customer the absence of interruptions due to technical malfunctions, preventive maintenance, as well as the full and error-free operation of the API and communication channels. The Customer undertakes to promptly inform the Bank of all cases of technical malfunctions or other circumstances that prevent the proper execution of this Agreement, in accordance with the Terms of SBP.
4. Electronic Signature
	1. The Agreement provides for the use of an enhanced encrypted non-certified digital signature (hereinafter referred to as the "Electronic Signature"), which allows you to confirm the authorship, authenticity and integrity of the signed Electronic Documents.
5. Means of Electronic Signature
	1. To create and verify an Electronic Signature, create an Electronic Signature key and an Electronic Signature verification key, electronic signature tools must be used that:

5.1.1. allow to establish the fact of a change in the signed Electronic Document after the moment of its signing;5.1.2. ensure the practical impossibility of calculating the Electronic Signature key from the electronic signature or from the Electronic Signature verification key.* 1. The Customer is obliged to independently and at his own expense select the means of the Electronic Signature and create an Electronic Signature key and an Electronic Signature verification key, in accordance with the SBP Terms and the requirements of the legislation of the Russian Federation.
1. The Procedure for Electronic Document Flow
	1. Prior to the commencement of electronic document flow, the Bank and the Customer shall exchange keys for verifying the Electronic Signature. The Bank's Electronic Signature Verification Key may be made publicly available at: https://developer.131.ru/.
	2. Electronic Document Flow includes the following stages: creation, transfer, authentication, accounting and storage of Electronic Documents.
	3. Creation of an Electronic Document includes the direct generation of an Electronic Document and its signing with an Electronic Signature using the Electronic Signature key.
	4. Handing over of Electronic Document is carried out exclusively using API.
	5. Examination of authenticity of the Electronic Document includes verification of the compliance of the Electronic Document with the requirements for its format and filling procedure, as well as verification of the Electronic Signature using the Electronic Signature verification key.

To verify the Electronic Signature, the Parties use the Electronic Signature tool, which:* + 1. generates a hash from the original Electronic Document according to the algorithm specified in the Application;
		2. converts the received Electronic Signature using the Electronic 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 Electronic Signature is considered confirmed. If they do not match, then it is considered that the authenticity of the Electronic Signature has not been confirmed, and the verifying Party must immediately inform the other Party about this.* 1. Accounting of Electronic Documents is carried out by maintaining electronic registers of incoming and outgoing Electronic Documents signed with an Electronic Signature. Maintenance of electronic log books is carried out by software, hardware and technical means of the Bank. The moment of receipt of the Electronic Document is the moment of its reflection in the register.
	2. Storage of Electronic documents received by the Bank or outgoing from the Bank are kept in the Bank's archive within the time limits established for documents of the corresponding type, but not less than five years from the date of receipt of the Electronic Document. In the event of disputes regarding the content of the Electronic Documents, the Electronic Documents stored in the Bank's archive shall have priority.
1. Recognition of Electronic Documents
	1. The Parties acknowledge that Electronic Documents signed with an Electronic Signature are equivalent in their legal force to paper documents signed by hand and stamped (if any).
	2. The legal consequences provided for the Electronic Document occur only if a positive result of verification of the Electronic Signature of this Electronic Document is obtained, subject to compliance with the requirements for the format and procedure for filling out the Electronic Document established by this Agreement, the SBP Terms, the Banking Rules, the Rules and Standards of the Operational and Payment Clearing Center (OPCC) of SBP and the legislation of the Russian Federation.
2. Responsibility of the Parties
	1. The Parties assume all risks associated with the performance of their equipment and communication channels, the safety and confidentiality of the Electronic Signature keys.
	2. In case of non-fulfillment or improper fulfillment of its obligations by one of the Parties, the other Party has the right to demand from such Party the fulfillment of the obligations assumed, as well as compensation for the damage caused to it.
	3. The Customer is responsible for the confidentiality of the Electronic Signature key, as well as for the actions of its employees when using the Electronic Signature. The Bank shall not be liable for losses incurred by the Customer in connection with the unauthorized use of the Electronic Signature by unauthorized persons.
3. Confidentiality
	1. The Parties undertake to ensure the confidentiality of the Electronic Signature keys, in particular, not to allow the use of their Electronic Signature keys without the consent of the Parties. Do not use the Electronic Signature key if there is reason to believe that the confidentiality of this Electronic Signature key has been violated.
	2. The Party that compromised the Electronic Signature key is responsible for the Electronic Documents signed using the compromised Electronic Signature key. The Electronic Signature Key of the Party shall be considered valid until the date of receipt by the other Party of the notice of cancellation (revocation) of the corresponding Electronic Signature key.
	3. The Parties undertake, within no more than one calendar day, to inform each other about all cases of violation of the confidentiality of the Electronic Signature keys (including loss, theft, unauthorized access to the Electronic Signature key). At the same time, the execution of the Agreement is suspended until the change of the keys of the Electronic Signature is carried out. Changing the keys of the Electronic Signature is carried out by signing a new Application by the Parties.
4. Force Majeure

10.1. The parties are released from liability for partial or complete failure to fulfill obligations under the Agreement in the event of force majeure, such as: natural and man-made disasters, military operations, civil unrest, epidemics, pandemics, the collapse of the global economic and financial system, the adoption of regulations restrictive nature. Force majeure circumstances also include: failure or failure of software and hardware and equipment, failure or shutdown of communication systems, power supply, interference by third parties (DDoS attack), etc.10.2. In the event of force majeure circumstances, the Party affected by them must notify the other Party within 3 (three) calendar days. A party that has missed the notification period is deprived of the right to refer to these circumstances as a basis for exemption from liability.1. Settlement of Disputes

11.1. This Agreement shall be governed by and interpreted in accordance with the laws of the Russian Federation (applicable law).11.2. In the event of disagreements regarding the implementation of the terms of the Agreement, the Parties shall take all measures to resolve them through negotiations. 11.3. Any disputes between the Parties, the subject of which is the contestation of the content of the Electronic Document, are submitted for resolution by a specially created expert commission. The composition of the expert commission is formed in equal proportions from representatives of the Parties. The Commission shall establish the authorship, authenticity and integrity of the Electronic Signature of the disputed Electronic Document. The results of the work of the expert commission are documented in an act to be signed by the Parties. From the moment of signing the act, the Parties recognize the indisputability of the information specified in this act. The procedure for analyzing conflict situations is indicated 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 substantive and procedural law of the Russian Federation.11.5. A written pre-trial claim procedure for settling disputes is mandatory. The term for responding to a claim is 30 (thirty) calendar days from the date of its receipt.1. Notifications

12.1. Unless otherwise provided by this Agreement and the Agreement on the use of SBP, then any letters, notifications and documents transmitted by the Parties to each other under the Agreement by e-mail, the addresses of which are indicated in the Application, will be considered properly sent and received if they sent from/to the email addresses specified by the Parties in the Application. The specified procedure does not apply in cases provided for by SBP Terms and/or Rules, as well as in cases established by the legislation of the Russian Federation.12.2. Changing the email address of the Parties (clause 12.1) is carried out by sending an electronic message from the previously indicated email addresses containing a clear indication of the new email address for communication.1. Modification of the Agreement

13.1. The Bank has the right to unilaterally and extrajudicially introduce any amendments and/or additions to the Agreement by posting a new revision of the Agreement at: https://developer.131.ru/.13.2. The new version of the Agreement shall enter into force and 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/[.](https://developer.131.ru/) 13.3. The Customer is obliged to familiarize itself with new revisions of the Agreement independently and in a timely manner. If the Bank does not receive a written notice from the Customer about the termination of the Agreement before the entry into force of the new revision of the Agreement, the new revision of the Agreement is considered unconditionally accepted by the Customer, and the conclusion of an additional agreement to the Agreement is not required.1. Validity and Termination Procedure

14.1. The term of the Agreement is limited by the term of the Agreement concluded between the Parties on the use of SBP.14.2. The Bank has the right to unilaterally refuse to execute the Agreement by notifying the Customer at least 30 (thirty) calendar days in advance by any means available to the Bank.14.3. Obligations of the Parties that arose prior to the termination of the Agreement shall remain until their full execution.1. Other Conditions

15.1. This Agreement is made in Russian and English. In case of contradictions, the text in Russian shall prevail.15.2. All Appendices are integral parts of the Agreement, namely:15.2.1. Appendix No. 1 - "Application";15.2.2. Appendix No. 2 - "Instruction for Ensuring Information Security";15.2.3. Appendix No. 3 - "Procedure for the Analysis of Conflict Situations".15.3. The Parties are not entitled to transfer their rights and obligations under the Agreement to third parties without the prior written consent of the other Party.15.4. If any provision of this Agreement is recognized as invalid or unenforceable in accordance with the applicable legislation of the Russian Federation, then such provision must be brought into compliance by the Parties with the applicable law, while the validity and applicability of any other provision of the Agreement will not be affected.1. Bank Details

Limited Liability Company "BANK 131"License of the Bank of Russia No. 3538 dated April 12, 2019OGRN 1191690025746TIN/KPP 1655415696 / 165501001Address: 420012, Russian Federation, Republic of Tatarstan,Kazan, Nekrasova Street, 38Corr/acc. 30101810822029205131 in Branch-NB Republic of TatarstanBIK: 049205131 |

**ЗАЯВЛЕНИЕ О ПРИЗНАНИИ И СВЕРКЕ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ**

**APPLICATION FOR RECOGNITION AND VERIFICATION OF ELECTRONIC SIGNATURE KEY**

|  |  |  |
| --- | --- | --- |
| **Стороны** | **Банк** | **Компания** |
| Полное наименование | Общество с ограниченной ответственностью «Банк 131» | [•] |
| Полное имя владельца ПодписиFull name of the owner of the Signature | [•]  | *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 natural persons, endowed by the constituent documents of the Customer with the right to act solely on behalf of the Customer without a power of attorney, and capable natural persons acting on behalf of name of the Customer on the basis of a power of attorney* |
| Действующий на основанииacting on the basis of | [•] | *Устав, Доверенность, иной документ в соответствии с действующим законодательством* *Charter, power of Attorney, or other document in accordance with the current legislation of the Russian Federation* |
| Алгоритм ПодписиSignature algorithm | RSA (2048 bit) | RSA (2048 bit) |
| Ключ проверки ПодписиPublic Key | Ключ проверки Подписи Банка опубликован в открытом доступе по адресу: <https://developer.131.ru> | **[•]** |
| Адрес электронной почтыEmail | [•] | [•] |

Подписывая настоящее Заявление, Клиент подтверждает, что он ознакомлена и согласна с Порядком электронного документооборота при осуществлении информационно-технологического обслуживания в рамках Условий осуществления расчетов с использованием СБП ( https://developer.131.ru/) и его условиям без каких-либо правок, оговорок или исключений.

By signing this Application, the Customer confirms that it is familiar with and agrees with the Procedure for Electronic Document Flow during information technology services within the framework of the Terms of settlements using SBP (https://developer.131.ru/ ) and its terms and conditions without any modifications, stipulations or exceptions.

|  |  |
| --- | --- |
| Банк | Компания |
| ОБЩЕСТВО С ОГРАНИЧЕННОЙОТВЕТСТВЕННОСТЬЮ «БАНК 131»Лицензия Банка России №3538 от 12.04.2019ОГРН: 1191690025746ИНН/КПП: 1655415696 / 165501001Адрес: 420012, Российская Федерация, Республика Татарстан, город Казань, улица Некрасова, дом 38Корсчет 30101810822029205131 в Отделение-НБ Республика Татарстан БИК: 049205131 | [НАЗВАНИЕ КОМПАНИИ][АДРЕС КОМПАНИИ][РЕГИСТРАЦИОННЫЙ НОМЕР][ИНН/КПП][БАНКОВСКИЕ РЕКВИЗИТЫ] |
| [ФИО/ Full Name][Должность / Position]\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [ФИО/ Full Name][Должность / Position]\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |
| --- | --- |
| Приложение № 2 к Порядку электронного документооборота**Инструкция по обеспечению информационной безопасности**В целях обеспечения информационной безопасности при работе с Протоколом информационного обмена (далее – «API») в рамках Условий СБП, Клиент наделяется следующими обязанностями: 1. Ключ Электронной подписи (далее по тексту – «ключ Электронной подписи») хранить только в недоступном для посторонних лиц месте и доступен исключительно уполномоченным Представителям Климента.
2. Не допускается:
	* снимать несанкционированные копии;
	* передавать ключ Электронной 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 Клиента.
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 Клиентом не реже одного раза в квартал.
7. Пароль доступа к ключу Электронной подписи хранить отдельно от ключа Электронной 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 Электронной подписи, только в момент подписания Электронных документов.
10. Использовать ключ Электронной подписи, только для подписания Электронных документов в рамках использования «API» согласно Условиям СБП.
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 Электронной подписи или выявления вредоносного кода в компьютере, используемом для работы «API», необходимо немедленно уведомить Банк по телефонам: (843) 598-31-40, (843) 598-31-39 с 9 часов 00 минут до 18 часов 00 минут (в рабочие дни), либо лично явиться в Банк с целью блокирования скомпрометированных ключей Электронной подписи с последующей их заменой.
15. К событиям, связанным с компрометацией ключей Электронной подписи, в том числе, относятся:
	* утеря (утрата) носителя ключа Электронной подписи, в том числе, с последующим его обнаружением;
	* обнаружение факта или угрозы использования (копирования) ключа Электронной подписи и/или пароля доступа к ключам Электронной подписи неуполномоченными лицами (несанкционированная отправка Электронных документов);
	* обнаружение ошибок в работе «API», в том числе, возникающих в связи с попытками нарушения информационной безопасности;
	* увольнение ответственного сотрудника Клиента, имевшего доступ к ключу Электронной подписи.
16. При обнаружении несанкционированных операций или утрате «API» немедленно уведомить Банк.
17. Использовать комбинации клавиш «Ctrl + Alt + Del» для идентификации пользователя в операционной системе.
18. Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы c API, заблокировать 3389 (RDP Remote desktop).
19. Включить в операционной системе журнал безопасности.
20. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д.
21. Обеспечить возможность своевременного обновления системного и прикладного программного обеспечения.
22. Выделить стационарный компьютер только для работы «API».
23. Доступ в помещение, где размещен компьютер с «API», предоставлять только уполномоченным лицам Клиента.
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 Клиента.
25. Исключить доступ к компьютерам, используемым для работы по «API», посторонним лицам и персоналу Клиента, 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 Электронной подписи и/ или пароль используемые в «API» и никогда не запрашивает у Клиента 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.

Клиент самостоятельно и единолично несет ответственность за обеспечение конфиденциальности паролей, ключей Электронной подписи, и иных данных, полученных от Банка или сгенерированных Клиентом 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». | Annex No. 2 to the Procedure of Electronic Document Flow**Instructions for Ensuring Information Security**In order to ensure information security when working with the Data Communications Protocol (hereinafter referred to as “API”) under the SBP Terms, the Customer is vested with the following obligations:1. The Key of the Electronic Signature (hereinafter referred to as the “Key of the Electronic Signature”) is kept only in a place inaccessible to unauthorized persons and is available exclusively to authorized Representatives of Customer.
2. It is not allowed to:
	* make unauthorized copies;
	* hand over the Key of the Electronic Signature to persons not admitted to it.
3. The following must not be used as a password:
	* a sequence of characters consisting of only digits (including dates, phone numbers, car numbers, etc.);
	* a sequence of repeated letters or numbers;
	* consecutive characters on the keyboard layout or in the alphabet;
	* names and surnames;
	* TIN or other details of the Customer.

 1. Password must:
	* be at least 8 characters;
	* contain numbers, lowercase and uppercase letters;
	* contain at least 1 character that is not a letter or number.
2. Password protection must be installed on the computer to enter the operating system of the device.
3. The user password in the operating system of the device must be changed by the Customer at least once a quarter.
4. Store the password for access to the Key of the Electronic Signature separately from the Key of the Electronic Signature.
5. It is strictly forbidden to write down passwords on paper or in text files at the workplace, leave them in easily accessible places, or transfer them to unauthorized persons.
6. Use the Key of the Electronic Signature only at the time of signing the Electronic Documents.
7. Use the Key of the Electronic Signature only for signing Electronic Documents within the framework of using "API" in accordance with the SBP Terms.
8. Apply licensed anti-malware tools at the workplace with the ability to automatically update malware signature databases.
9. If a portable computer (laptop) is used as a computer for working with "API", its connection to public networks in places of free access to the Internet (office centers, cafes, etc.) shall be impossible.
10. Constant monitoring of sent messages during the operation with "API" shall be carried out.
11. If signs of compromise of the Key of the Electronic Signature or malicious code are detected in the computer used for the operation with "API", it is necessary to immediately notify the Bank by phone: (843) 598-31-40, (843) 598-31-39from 9:00 to 18:00 (working days), or personally appear in the Bank in order to block compromised Keys of the Electronic Signature with their subsequent replacement.
12. The events associated with the compromise of the Keys of the Electronic Signature include, among other things:
	* loss of the Key of Electronic Signature carrier, including its subsequent discovery;
	* detection of the fact or threat of use (copying) of the Key of Electronic Signature and/or the password for access to the Keys of Electronic Signature by unauthorized persons (unauthorized sending of Electronic Documents);
	* detection of errors in the operation of "API", including those arising in connection with attempts to violate information security;
	* dismissal of a responsible employee of the Customer who had access to the Key of the Electronic Signature.
13. If unauthorized transactions are detected or API is lost, notify the Bank immediately.
14. Use key combinations "Ctrl + Alt + Del" to identify the user in the operating system.
15. Disable the possibility of remote and terminal connections to computers used to work with API, block 3389 (RDP Remote desktop).
16. Enable the security log in the operating system.
17. Use only licensed software - operating systems, anti-malware tools, MS Office packages, etc.

 1. Ensure the possibility of timely updating of system and application software.
2. Allocate a desktop computer only for "API" work.
3. Access to the premises where the computer with "API" is located should be provided only to authorized persons of the Customer.
4. The computer from which the preparation and sending of Electronic Documents to the Bank is carried out is recommended to be allocated to a separate network segment with its obligatory exclusion from the general local network of the Customer.
5. Exclude access to computers used to work with "API" by unauthorized persons and personnel of the Customer who are not authorized to work with "API" and/or maintain computers.
6. When servicing a computer, control over the actions IT staff performs shall be provided.
7. The Bank does not send e-mails with a request to send the Electronic Signature Keys and/or the password used in "API" and never asks the Customer for this information. When being addressed on behalf of the Bank by phone, e-mail, via SMS messages of persons with a request to provide confidential information (passwords, code words, etc.), under no circumstances provide this information and inform the Bank about it.

The Customer is independently and solely responsible for ensuring the confidentiality of passwords, Electronic Signature Keys, and other data received from the Bank or independently generated by the Customer for the purpose of their use in the work of "API", as well as for ensuring the confidentiality and non-disclosure of data, documents and information received and (or) sent using "API". |

|  |  |
| --- | --- |
| Приложение № 3 к Порядку электронного документооборота**Порядок разбора конфликтных ситуаций**Любые споры между Сторонами, предметом которых является установление подлинности Электронной 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 Российской Федерации 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 Электронной подписи и ключи проверки Электронной подписи, используемые для создания Электронной подписи оспариваемого Электронного документа.
3. Экспертная комиссия сравнивает предоставленные ключи проверки Электронной подписи с ключами, указанными в Заявлении. Ключи проверки Электронной подписи и коды, которые совпали, признаются подлинными.
4. Если третий этап успешно пройден, то экспертная комиссия производит проверку подлинности Электронной 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 Электронной 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 Арбитражный суд Республики Татарстан, в порядке и на условиях, указанных в Соглашении об использовании СБП.  | Appendix No. 3 to the Procedure of Electronic Document Flow**The Procedure for Analysis of Conflict Situations**Any disputes between the Parties, the subject of which is an establishment of the authenticity of the Electronic Signature in an Electronic Document, i.e. the integrity of the text and the authenticity of the sender of the Electronic Document are transferred for settlement 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 shall indicate the details of the disputed signed Electronic Document and the persons authorized to represent the interests of this Party as part of the expert commission.Not later than 3 (three) working days from the moment the other Party receives the application (claim), the Parties shall determine the date, place and time of the start of the work of the expert commission, determine which Party provides the premises and configures the tools of the Electronic Signature. The powers of the members of the expert commission are confirmed by powers of attorney issued in accordance with the procedure established by the legislation of the Russian Federation. The composition of the expert commission is formed in equal proportions from representatives of the Parties. Examination of the disputed Electronic Document is carried out in the presence of all members of the expert commission. The review is carried out in four stages: 1. The Parties jointly install, configure and test the Electronic Signature tool.
2. The Parties provide their Electronic Signature keys and Electronic Signature verification keys used to create the Electronic Signature of the disputed Electronic Document.
3. The Expert Commission compares the provided keys for verifying the Electronic Signature with the keys specified in the Application. Keys for verifying the Electronic Signature and codes that match are recognized as authentic.
4. If the third stage is successfully passed, then the expert commission checks the authenticity of the Electronic Signature in the disputed Electronic Document.

The results of the examination are drawn up in the form of a written opinion – a report of the expert commission, signed by all members of the expert commission. The report is drawn up immediately after the completion of the last stage of the examination. The report records the results of all stages of the examination, as well as all the essential details of the disputed electronic document. The report is drawn up in two copies - one for each of the Parties. The report of the expert commission is final and not subject to revision.Confirmation of the authenticity of the Electronic Signature in the report shall mean that the disputed Electronic Document has legal force and entails the emergence of appropriate rights and obligations for the Parties.In the absence of agreement on controversial issues and voluntary execution of the decision of the expert commission, all materials on these issues may be submitted for consideration to the Arbitration Court of the Republic of Tatarstan, in the manner and on the terms specified in the Agreement on the use of SBP.  |

1. Заявление об использовании СБП/Заявление на изменение пользователей СБП. [↑](#footnote-ref-1)
2. Application for the use of SBP/Application for the change of users of SBP. [↑](#footnote-ref-2)