Приложение № А к Условиям дистанционного банковского обслуживания юридических лиц в системе «Интернет-Клиент» в ООО «Банк 131»
Редакция № 1 от «16» декабря 2020г.

Annex No. A to the Rules of Remote Banking Service in the 'Banking App' system for Bank 131 LLC Corporate Clients

Version 1 dated December 16, 2020.

РЕГЛАМЕНТ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ЮРИДИЧЕСКИХ ЛИЦ В ООО «БАНК 131» С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДБО

REGULATIONS ON REMOTE BANKING SERVICE IN THE BANKING APP SYSTEM FOR BANK 131 LLC CORPORATE CLIENTS

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Регламенте дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО (далее - Регламент) используются термины и определения, указанные в

1. TERMS AND DEFINITIONS

Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC Corporate Clients (hereinafter referred to as Rules) conform the terms

Правилах комплексного банковского обслуживания юридических лиц в ООО «Банк 131» (и приложениях к ним), далее – Правила, если иное не указано в настоящем Регламенте.	and definitions specified in the Rules on Integrated Banking Service for Bank 131 LLC Corporate Cleints (and their annexes), hereinafter referred to as the Rules, unless otherwise stated in these Rules.
Временный пароль – пароль, который присваивается Банком Уполномоченному Представителю Клиента при его регистрации в Системе ДБО, действующий до момента установки Статического пароля при первом входе в Систему ДБО.	**Temporary password** is a password which is assigned by the Bank to the Client's Authorized Person when the Client registers in the RBS System and which is valid until the Static Password is set at the first log in to the RBS System.
Заявление – заявление о присоединении к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО.	**Application** denotes application on joining the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC Corporate Clients.
Компрометация Электронной подписи – наличие оснований полагать, что доверие к тому, что используемые ключи/средства Электронной подписи, Аутентификационные данные, Абонентский номер и/или сами Электронные подписи или их носители утрачены/доступны неуполномоченным лицам/могут быть использованы без согласия уполномоченных лиц. К событиям, связанным с Компрометацией Электронной подписи относятся, включая, но не ограничиваясь, следующие: - утрата функциональных ключевых носителей, с последующим обнаружением или без такового; - нарушение правил хранения, использования и уничтожения (в том числе после окончания срока действия) ключа Электронной подписи (усиленной неквалифицированной); - утеря, передача и/или предоставлением доступа неуполномоченным третьим лицам к аппаратным средствам (в том числе мобильным телефонам или иным) и/или SIM-карте с Абонентским номером, в том числе который используется для направления Временного и/или Одноразового пароля; - наличие подозрений, что Средства подтверждения Электронного документа стали известны неуполномоченным третьим лицам; - возникновение подозрений на утечку информации или ее искажение; - несанкционированное копирование или подозрение на копирование Временного, Статического и/или Одноразового пароля, функционального ключевого носителя, аппаратного средства и/или SIM-карты с Абонентским номером; - прекращение полномочий или увольнение Уполномоченных лиц, имеющих доступ к Средству подтверждения; - случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате	**Compromising of the Electronic Signature there** is reason to believe that the keys/tools of the Electronic Signature, Authentication Data, Subscriber Number and/or the Electronic Signatures themselves or their carriers have been lost/accessible to unauthorised persons/can be used without the consent of authorised persons. Events related to the Electronic Signature Compromise include, but are not limited to, the following: - loss of functional key media, with or without subsequent detection; - violation of the rules for storage, use and destruction (including after the expiry date) of the Electronic Signature key (enhanced non-certified); - loss, transfer and/or granting access to hardware (including mobile phones or other) and/or a SIM card with a Subscriber number to unauthorised third parties, including that used to send the Temporary and/or One-time password; - suspicions of the E-Document Validation Tools have become known to unauthorised third parties; - suspicion of information leakage or misrepresentation; - unauthorised copying or suspicion of copying a Temporary, Static and/or One-time password, functional key media, hardware and/or SIM card with a Subscriber number; - termination of powers or dismissal of the Authorised Persons who have access to the Confirmation Tool; - cases where it is impossible to establish reliably what happened to the media containing key information (including cases where the media failed and the possibility that this fact occurred as a result of unauthorised actions of third parties and other types of disclosure of key information was not proved).

несанкционированных действий третьих лиц, другие виды разглашения ключевой информации).

Ключ Электронной подписи - уникальная последовательность символов, предназначенная для создания усиленной неквалифицированной Электронной подписи.

Ключ проверки Электронной подписи - уникальная последовательность символов, однозначно связанная с Ключом Электронной подписи и предназначенная для проверки подлинности усиленной неквалифицированной Электронной подписи.

Логин – уникальная последовательность символов, состоящая из латинских букв и цифр, которая позволяет Банку однозначно идентифицировать (установить) уполномоченного Представителя Клиента при доступе и работе в Системе ДБО (применяется при использовании простой Электронной подписи).

Одноразовый пароль – уникальная последовательность числовых символов, предоставляемая Банком по запросу уполномоченного Представителя Клиента посредством SMS-уведомления на Абонентский номер Клиента (Уполномоченного Представителя Клиента), введение которого требуется для дополнительной аутентификации при доступе в Систему ДБО по Логину и Статическому паролю, и/или дополнительного подтверждения Электронных документов при использовании усиленной неквалифицированной Электронной подписи, и/или для подтверждения Электронных документов простой Электронной подписью.

Оператор Удостоверяющего центра – работник Банка, уполномоченный на выдачу и отзыв сертификатов ключей Электронной подписи (усиленной неквалифицированной).

Оператор Центра регистрации – работник Банка, уполномоченный на регистрацию Клиента/уполномоченного Представителя Клиента в Системе ДБО.

Ответственный работник – работник Банка, уполномоченный на проведение идентификации Клиента и его уполномоченного Представителя, а также на прием от Клиента документов, в том числе Заявлений от Уполномоченных Представителей Клиента, в целях регистрации, предоставления доступа и использования Системы ДБО Клиентом и его уполномоченными Представителями.

Статический пароль – секретная последовательность символов, которая известна только Уполномоченному Представителю Клиента. Статический Пароль используется для входа в Систему ДБО и позволяет убедиться в том, что обратившееся лицо является владельцем представленного Логина – Уполномоченным Представителем Клиента. При регистрации

The Electronic Signature key is a unique sequence of symbols designed to create an enhanced non-certified Electronic Signature.

The Electronic Signature Verification Key is a unique sequence of characters clearly associated with the Electronic Signature Key and intended to verify the authenticity of an enhanced non-certified Electronic Signature.

Login is a unique sequence of symbols consisting of Latin letters and numbers, which enables the Bank to unambiguously identify the Client's Authorized Person when accessing and working in the RBS System (applied when using a simple Electronic Signature).

One-time password is a unique sequence of numerical symbols provided by the Bank at the request of the Client's Authorized Representative by means of SMS-notification to the Client's Subscriber number (Client's Authorized Representative), the introduction of which is required for additional authentication when accessing the RBS System using the Login and Static Password, and/or for additional confirmation of Electronic Documents when using an enhanced non-certified Electronic Signature, and/or for confirmation of Electronic Documents using a simple electronic signature.

Certification Centre Operator is an employee of the Bank authorized to issue and recall Electronic Signature (Enhanced Non-Certified) Key Certificates.

Registration Centre Operator is an employee of the Bank authorized to register the Client/Authorized Person of the Client in the RBS System.

Responsible employee is an employee of the Bank authorized to perform identification of the Client and its authorized representative, as well as to receive documents from the Client, including Applications from the Client's Authorized Persons, for the purpose of registration, access and use of the RBS System by the Client and its Authorized Persons.

Static password is a secret sequence of symbols, which is known only to the Client's Authorized Person. Static Password is used to login to the RBS System to ensure that the applicant is the owner of the submitted Login, a Client Authorized Person. Upon registration of the Client's Authorized Person in the RBS System, a Temporary Password shall be sent to the Subscriber number of such person in the form of an SMS message

уполномоченного Представителя Клиента в Системе ДБО на Абонентский номер такого лица высылается Временный пароль в виде SMS-сообщения, который должен быть изменен при первом входе в Систему ДБО. Статический пароль применяется при использовании Простой Электронной подписи.

Простая электронная подпись (Простая ЭП, ПЭП) - аналог собственноручной подписи Клиента, представленный в виде Одноразового пароля (определенной последовательности символов, известных только уполномоченному Представителю Клиента, позволяющей Банку однозначно идентифицировать (установить) уполномоченного Представителя Клиента при подписании им Электронных документов с использованием Системы ДБО). Одноразовый пароль направляется Банком в виде SMS-сообщения на Абонентский номер уполномоченного Представителя Клиента, указанный в базе данных Банка, в соответствии с представленными Клиентом Заявлением на приобретение/изменение БП и Заявлением / Заявлением на изменение абонентского номера мобильной связи.

Удостоверяющий центр - организационная структура Банка, предназначенная для управления единой инфраструктурой Ключей проверки Электронной подписи с целью обеспечения юридической значимости Электронных документов и контроля целостности информации, защищенной усиленной неквалифицированной Электронной подписью.

Сертификат ключа проверки электронной подписи – документ на бумажном носителе и/или в электронном виде, с указанным в шестнадцатеричном виде Ключом проверки Электронной подписи Клиента, подтверждающий принадлежность Ключа проверки усиленной неквалифицированной Электронной подписи владельцу Сертификата ключа проверки электронной подписи. Сертификат ключа проверки электронной подписи должен быть подписан его владельцам (уполномоченным Представителем Клиента).

Средство подтверждения – уникальная последовательность символов, позволяющая создавать Электронную подпись для подтверждения Электронного документа. В качестве Средства подтверждения в Системе ДБО используются: для создания простой Электронной подписи – Логин, Статический пароль, Одноразовый пароль; для создания усиленной неквалифицированной Электронной подписи — Ключ усиленной неквалифицированной Электронной подписи.

Уполномоченный Представитель Клиента/Уполномоченное лицо – Представитель Клиента, являющийся физическим лицом, указанный в Заявлении на приобретение/изменение БП, Заявлении, а также в Сертификате ключа проверки электронной подписи (при использовании усиленной неквалифицированной Электронной подписи), в том числе имеющий право распоряжаться денежными средствами Клиента на Счете(-ах).

to be changed upon the first login to the RBS System. Static password shall be applied when using Simple Electronic Signature.

Simple electronic signature (Simple ES, SES) is an analogue of the Client's handwritten signature presented in the form of a One-time password (a certain sequence of symbols known only to the Client's Authorized Person, enabling the Bank to unambiguously identify the Client's Authorized Person when signing Electronic Documents using the RBS System). The One-time password shall be sent by the Bank in the form of an SMS message to the Subscriber number of the Client's Authorized Person indicated in the Bank's database in accordance with the Application for purchase/modification of the BP and Application / Application for change of the mobile number submitted by the Client.

Certification Centre is the Bank's organisational structure designed to manage the unified infrastructure of the Electronic Signature Verification Keys in order to ensure the legal significance of the Electronic Documents and control the integrity of information protected by the enhanced non-certified Electronic Signature.

Electronic Signature Verification Key Certificate is a document in paper and/or electronic form with the Client's Electronic Signature Verification Key specified in hexadecimal form, confirming that the Enhanced Non-Certified Electronic Signature Verification Key belongs to the owner of the Electronic Signature Verification Key Certificate. The Electronic Signature Verification Key Certificate shall be signed by the Client's owners (Authorized Person of the Client).

Confirmation Tool is a unique sequence of symbols that enables to create an Electronic Signature to confirm the Electronic Document. The following are used as Confirmation Tool in the RBS System: Login, Static Password, One-time Password are needed for creating a simple Electronic Signature; Enhanced Non-Certified Electronic Signature Key is needed for creating an enhanced non-certified Electronic Signature.

Client Authorized Person/Authorised person is the Client's representative who is a natural person specified in the Application for purchase/modification of BP, Application, as well as in the electronic signature verification key certificate (when using an enhanced non-certified electronic signature), including the right to dispose of the Client's funds in the Account(s).

ENCES (Enhanced Non-Certified Electronic

УНЭП (Усиленная неквалифицированная Электронная подпись) - Электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее Электронный документ;
- позволяет обнаружить факт внесения изменений в Электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

ФКН (Функциональный ключевой носитель) - персональное средство строгой аутентификации и хранения данных, аппаратно поддерживающее работу с Ключом Электронной подписи, позволяющее осуществлять механизм электронной подписи так, что Ключ Электронной подписи не покидает пределы носителя.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Настоящий Регламент регулирует отношения возникшие в процессе оказания Банком услуг по Договору «Интернет-Клиент», при подключении и использовании Клиентом и Уполномоченными Представителями Клиента Системы ДБО и является соглашением между Банком и Клиентом, определяющим порядок и условия взаимодействия при выпуске и использовании Электронной подписи.

2.2 Настоящий Регламент является неотъемлемой и составной частью Условий Банковского продукта «Дистанционное банковское обслуживание с использованием Системы ДБО».

2.3 Для подключения Клиента и Уполномоченного Представителя Клиента к Системе ДБО и ее использования Уполномоченный Представитель Клиента должен присоединиться к Правилам и Условиям Банковского продукта «Дистанционное банковское обслуживание с использованием Системы ДБО», а также к настоящему Регламенту путем подписания Заявления, форма которого определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка.

2.4 При регистрации Уполномоченного Представителя Клиента в реестрах Системы ДБО Уполномоченному Представителю Клиента присваивается регистрационный номер, который указывается в Заявлении такого лица, полученном Банком.

2.5 Обмен Электронными документами между Банком и Клиентом с использованием Системы ДБО осуществляется в рамках Правил (включая приложения к ним), а также приобретенных Клиентом Банковских продуктов и их условий, обслуживание которых может быть осуществлено с использованием Системы ДБО.

Signature) is an electronic signature that:
-was obtained as a result of cryptographic transformation of information using the electronic signature key;
-enables the person who has signed the Electronic Document to be identified;
-enables to detect changes have been made to the Electronic Document after it has been signed;
-is created using electronic signature tools.

FKM (Functional Keystock Medium) is a personal means of strict authentication and data storage, hardware-supported work with the Electronic Signature Key, allowing the electronic signature mechanism to be performed so that the Electronic Signature Key is not out of the medium.

2. GENERAL PROVISIONS

2.1. This Regulation controls relations arising in the process of providing services by the Bank under the Banking App Agreement, at connection and use by the Client and Authorized Persons of the Client of RBS System and is an agreement between the Bank and the Client, defining the order and conditions of interaction at issue and use of Electronic Signature.

2.2. This Regulation is an integral part of the Terms and Conditions of the Remote Banking Services with RBS System Banking Product.

2.3. In order to connect the Client and the Client's Authorized Representative to the RBS System, the Client's Authorized Representative must accede to the Terms and Conditions of the Remote Banking Services with RBS System Banking Product and to the Regulation by signing an Application which form is determined by the Bank and can be found at https://131.ru/contracts and in the Bank's office.

2.4. A registration number is assigned to the Client's Authorized Person, which is indicated in the Application of such person received by the Bank when the Client's Authorized Person is registered in the registers of the RBS System.

2.5. The exchange of Electronic Documents between the Bank and the Client using the RBS system is carried out within the framework of the Rules (including their annexes), as well as the Bank's products purchased by the Client and their terms and conditions, which can be serviced using the RBS system.

2.6. The Client agrees that the Electronic Documents of the Parties within the framework of the

2.6 Клиент соглашается с тем, что Электронные документы Сторон в рамках Системы ДБО признаются Электронными документами, подписанными Электронной подписью (простой или усиленной неквалифицированной (в зависимости от выбранного Стороной способа подписания документа и функциональных возможностей Системы ДБО)), и являются равнозначными документам на бумажных носителях, подписанными собственноручной подписью уполномоченного лица Стороны и скрепленными печатью такой Стороны (при наличии).

2.7 Одной электронной подписью могут быть подписаны несколько связанных между собой Электронных документов (пакет Электронных документов). При подписании Электронной подписью пакета электронных документов каждый из Электронных документов, входящих в этот пакет, считается подписанным Электронной подписью того вида, которой подписан пакет Электронных документов.

2.8 Стороны признают в качестве единой шкалы времени при работе в Системе ДБО местное время по месту расположения подразделения Банка, обслуживающего Клиента. Контрольным является время системных часов аппаратных средств Банка.

2.9 Клиент обязуется обеспечить допуск к работе и работу в Системе ДБО только Уполномоченных Представителей Клиента.

2.10 Используя Систему ДБО Клиент приобретает возможность:

- Формировать, подписывать Электронной подписью и направлять в Банк платежные (расчетные) документы, в соответствии с законодательством Российской Федерации, в том числе платежные поручения, в целях совершения операций по открытым в Банке Счетам Клиента;
- Формировать, подписывать Электронной подписью и направлять в Банк запросы на отзыв платежных (расчетных) документов, в том числе платежных поручений, ранее переданных в Банк;
- Получать от Банка выписки по Счету(-ам) в виде Электронных документов, содержащие информацию об операциях, совершенных по открытому(-ым) в Банке Счету(-ам) Клиента;
- Формировать, направлять и получать в/от Банка информацию свободного формата в виде Электронных документов (в том числе служебно-информационных сообщений), согласно функционально-техническим возможностям Системы ДБО;
- Формировать, подписывать Электронной подписью, направлять и получать в/от Банка Электронные документы, в соответствии с условиями отдельных заключенных Сторонами Договоров о предоставлении банковского продукта, согласно Правилам.

2.11 При получении Электронного документа Банк производит проверку:

1. удостоверение права распоряжения денежными

RBS System shall be deemed to be the Electronic Documents signed by the Electronic Signature (simple or enhanced non-certified (depending on the method of signing the document chosen by the Party and the functionality of the RBS System)) and shall be equivalent to the paper documents signed by the handwritten signature of the authorized person of the Party and sealed of such Party (if any).

2.7. A single electronic signature can be used to sign several linked electronic documents (eDocs package). Each of the Electronic Documents in that Package is considered to be the Electronic Signature of the type to which the Electronic Document Package is signed when the Electronic Signature of an Electronic Document Package is signed.

2.8. The Parties shall recognise the local time at the location of the Bank's customer service unit as a uniform time scale when operating the RBS System. The reference time is the system clock of the Bank's hardware.

2.9. The Client shall ensure that only the Authorized Persons of the Client are allowed to work in the RBS System.

2.10. By using the RBS System, the Client gains an opportunity:

- To form, sign and send to the Bank payment (settlement) documents in accordance with the legislation of the Russian Federation, including payment orders, for the purpose of performing transactions in the Client's Accounts opened with the Bank;
- To form, sign and send to the Bank requests for withdrawal of payment (settlement) documents, including payment orders previously submitted to the Bank;
- To receive from the Bank statements of the Client's account(s) in the form of electronic documents containing information on transactions carried out on the Client's account(s) opened with the Bank;
- To form, send and receive free format information from/to the Bank in the form of electronic documents (including service and information messages) in accordance with the functional and technical capabilities of the RBS System;
- To form, sign with Electronic Signature, send and receive electronic documents to/from the Bank in accordance with the terms and conditions of individual Agreements concluded by the Parties on provision of a banking product in accordance with the Rules.

2.11. Upon receipt of an Electronic Document, the Bank performs an inspection:

1. certification of the right to cash dispose (ES verification, request for individual client's payments of

средствами (проверка ЭП, запрос по отдельным платежам клиента дополнительного подтверждения); 2. контроль целостности (неизменности) реквизитов платежного поручения; 3. структурный контроль (проверка установленных реквизитов и максимального количества символов в реквизитах ПП); 4. контроль значений реквизитов; 5. Контроль достаточности денежных средств. При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный ЭД серверной частью Системы ДБО не принимается и данный результат (электронная квитанция) автоматически направляется Клиенту, а поручение, содержащееся в нем, Банком не исполняется.	additional confirmation); 2. integrity control (invariability) of payment order details; 3. structural control (checking the established details and the maximum number of symbols in the BGC); 4. control of references details; 5. control of cash adequacy. Upon detection of an adverse effect of any of the above circumstances, the received data by the server part of the RBS System shall not be accepted and this result (electronic receipt) shall be automatically sent to the Client, while the Bank shall not execute the order contained therein.
2.12 Формат Электронных документов определяется функционально-техническими возможностями Системы ДБО, экранной формы клиентской части Системы ДБО. Каждый Электронный документ, направляемый Клиентом в Банк с использованием Системы ДБО, должен содержать Электронную подпись Уполномоченного Представителя Клиента. Электронная подпись Клиента, содержащаяся в Электронном документе Клиента, подтверждает авторство Уполномоченного Представителя Клиента и является средством проверки неизменности содержания Электронного документа, так как любое изменение Электронного документа, после его подписания Электронной подписью, нарушает целостность Электронной подписи.	2.12. The format of Electronic Documents is determined by the functional and technical capabilities of the RBS System, the screen form of the RBS Client Part. Each Electronic Document sent by the Client to the Bank using RBS System must contain the Electronic Signature of the Client's Authorized Person. The Client's Electronic Signature contained in the Electronic Document of the Client confirms the authorship of the Client's Authorized Person and is a means of verifying the immutability of the Electronic Document content, as any modification of the Electronic Document after its signature with the Electronic Signature violates the integrity of the Electronic Signature.
2.13 Электронный документ должен быть заверен Электронной подписью только Уполномоченных Представителей Клиента, имеющих право распоряжения денежными средствами на Счете (для платежных (расчетных) Электронных документов), данные о которых указаны в Заявлении на приобретение/изменение БП и Заявлении. Если Электронный документ, должен быть подписан несколькими подписями Уполномоченных Представителей Клиента, в соответствии с Заявлением на приобретение/изменение БП/Карточкой с образцами подписей и оттиском печати и Соглашением о сочетании подписей к КОП, Электронный документ заверяется каждым из Уполномоченных Представителей Клиента - по одной Электронной подписи из первой и второй группы подписей.	2.13. The Electronic document must be certified by the Electronic Signature only of the Client's Authorized Persons who have the right to dispose of funds in the Account (for payment (settlement) Electronic Documents), the details of which are specified in the Application for purchase/modification of BGC and the Application. If the Electronic Document must be signed by several signatures of the Client's Authorized Persons, in accordance with the Application for purchase/modification of the BGC/Banking Sample Signatures and seal card and the Agreement on combination of signatures to the BSS, the Electronic Document shall be certified by each of the Client's Authorized Persons, one of the Electronic Signatures from the first and second groups of signatures.
2.14 Система ДБО автоматически отображает сведения о текущем этапе обработки Клиентом и/или Банком Электронного документа, посредством присвоения Электронному документу определенного статуса и его изменении.	2.14. The RBS system automatically displays information about the current stage of processing the Electronic Document by the Client and/or the Bank by assigning a certain status to the Electronic Document and changing it.
2.15 Система присваивает Электронным документам следующие статусы: • **«Создан»** - присваивается при создании и	2.15. The system assigns the following statuses to Electronic Documents: • **Created** is assigned when a new document is created and saved by the Client. • **Waiting for signature** is assigned to the

сохранении нового документа Клиентом.

- **«Ожидает подписи»** - присваивается документу после его создания и сохранения, до подписания Уполномоченным Представителем Клиента.
- **«Подписан»** - присваивается документу после проставления необходимого числа Электронных подписей Уполномоченным(-и) Представителем(-ями) Клиента.
- **«Отправлен в банк»** - присваивается документу при прохождении контроля соответствия количества подписей заявленного в банке..
- **«Принят»** - присваивается документу после его принятия Банком к исполнению.
- **«Оплачен»** - присваивается документу после его исполнения Банком (в том числе после списания денежных средств со Счета Клиента на основании данного документа).
- **«Отказан»** - присваивается документу если платеж был отклонен Банком либо при попытке создать платеж произошла ошибка.
- **«Аннулирован»** - присваивается документу, не прошедшему проверку по причине его несоответствия требованиям, установленным действующим законодательством Российской Федерации, Правилам, условиям заключенных сделок о приобретении Банковского продукта, Регламента или иных случаях (например, при недостаточном остатке средств на счете для осуществления платежа и др.).
- **«Запрошен отзыв»** - присваивается Электронному документу, по которому Клиент создал запрос на отзыв платежа.
- **«Отозван»** - присваивается документу после исполнения запроса на отзыв документа.

2.16 Созданный и подписанный Электронной подписью Электронный документ Клиент отправляет в Банк с использованием Системы ДБО.

2.17 Банк осуществляет проверку полученного от Клиента Электронного документа и принимает его к исполнению при условии положительного результата проверки.

2.18 Результат проверки Электронного документа считается положительным, если он:

- Оформлен в соответствии с действующим законодательством Российской Федерации;
- Оформлен в соответствии с нормативными документами Банка России и требованиями Банка;
- Оформлен в соответствии с требованиями, установленными заключенными Сторонами сделками, в соответствии с Правилами, и настоящим Регламентом;
- Заверен надлежащей (надлежащими) Электронной(-ыми) подписью(-ями) Уполномоченного(-ых) Представителя(-ей) Клиента, имеющего(-их) право на распоряжение денежными средствами на Счете (для платежных (расчетных) Электронных документов), Электронные подписи прошли проверку в Банке на

document after its creation and preservation, until it is signed by the Client's Authorized Person.

- **Signed** is the status assigned to a document after the Client's Authorized Person(s) has submitted the required number of Electronic Signatures.
- **Sent to the bank** is assigned to a document when passing the control of compliance of the number of signatures declared in the bank.
- **Accepted** is assigned to a document after it has been accepted by the Bank for execution.
- **Paid** is assigned to a document after its execution by the Bank (including after debiting the Client's Account based on this document).
- **Refused** is assigned to a document if a payment has been rejected by the Bank or an error has occurred when attempting to create a payment.
- **Cancelled** is assigned to a document that has not been audited because it does not meet the requirements established by the current legislation of the Russian Federation, the Rules, the terms and conditions of transactions for the purchase of the Bank's Product, Rules or other cases (e.g., if the account balance is insufficient to make a payment, etc.).
- **Requested withdrawal** is assigned to the Electronic document on which the Client has created a withdrawal request for payment.
- **Withdrawn** is assigned to a document after a request to withdraw a document has been made.

2.16. The Client shall send the Electronic Document created and signed by the Electronic Signature to the Bank using the RBS System.

2.17. The Bank shall verify the Electronic Document received from the Client and accept it for execution provided that the verification result is positive.

2.18. The result of an inspection of an Electronic Document is considered positive if it is:

- Registered in accordance with the current legislation of the Russian Federation;
- It was executed in accordance with the regulatory documents of the Bank of Russia and the Bank's requirements;
- Registered in accordance with the requirements established by the transactions concluded by the Parties in accordance with the Rules and these Rules;
- Certified by the appropriate Electronic Signature(s) of the Authorized Person(s) of the Client who has the right to dispose of funds in the Account (for payment (settlement) Electronic Documents), the Electronic Signatures have been verified by the Bank

корректность.	for correctness.
2.19 Электронные документы, оформленные с нарушением требований, приему не подлежат, таким Электронным документам присваивается статус в Системе ДБО «Аннулирован».	2.19. Electronic documents executed in violation of requirements shall not be accepted, such Electronic documents shall be assigned a Cancelled status in the RBS System.
2.20 Клиент может отозвать переданный в Банк Электронный документ, в соответствии с требованиями законодательства Российской Федерации, заключенных Сторонами сделок, правилами совершения операций, с использованием Системы ДБО. Отозваны могут быть только неисполненные Электронные документы, которые не дошли до статуса «Оплачен». Если запрос на отзыв исполнен, Электронному документу присваивается статус "Отозван." В случае невозможности исполнения запроса на отзыв, Электронному документу вернется статус, в котором Электронный документ находился до обработки Банком запроса на отзыв.	2.20. The Client may revoke the Electronic Document submitted to the Bank in accordance with the requirements of the legislation of the Russian Federation, the transactions concluded by the Parties, the rules of transactions using the RBS System. Only non-executed Electronic Documents that have not reached the Paid status may be withdrawn. The Electronic Document is assigned the Withdrawn status if the request for withdrawal is executed. If a revocation request cannot be executed, the Electronic Document is returned to the previous status of the Electronic Document when the Bank processed the revocation request.
2.21 Клиент самостоятельно контролирует (отслеживает) этапы и результаты обработки отправленных в Банк Электронных документов в соответствующих разделах Системы ДБО.	2.21. The Client shall independently control (monitor) the stages and results of processing the Electronic Documents sent to the Bank in the relevant sections of the RBS System.
2.22 Банк и Клиент обмениваются по Системе ДБО следующими Электронными документами: - платежные поручения; - запросы на отзыв документа; - произвольные документы (иные документы или письма, составленные в произвольной форме); - выписки, содержащие информацию о движении средств по счетам.	2.22. The Bank and the Client shall exchange the following Electronic Documents on the RBS System: - payment orders; - requests for withdrawal of the document; - arbitrary documents (other documents or letters drawn up in any form); - statements containing information about the movement of funds in the accounts.
3 ПОРЯДОК ПОДКЛЮЧЕНИЯ КЛИЕНТА К СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ	**3. PROCEDURE FOR CONNECTING THE CLIENT TO THE REMOTE BANKING SERVICE SYSTEM**
3.1 Порядок регистрации Уполномоченного Представителя Клиента в Системе ДБО:	3.1. Registration procedure Authorized Person of the Client in the RBS System:
3.1.1 Под регистрацией Уполномоченного(-ых) Представителя(-ей) Клиента понимается внесение в реестры Системы ДБО регистрационной информации о таком лице(-ах), на основании Заявления о приобретении/изменении БП, Заявления.	3.1.1. Registration of the Client's Authorized Person(s) means entry of registration information about such person(s) into the registers of the RBS System on the basis of the Application for purchase/modification of the BP, Application.
3.1.2 Подача Уполномоченным Представителем Клиента Заявления осуществляется каждым таким лицом лично, путем обращения к Ответственному работнику по юридическому адресу Банка в течение Операционного времени Банка.	3.1.2. Application submitted by the Authorized Person of the Client is made by each such person individually by applying to the responsible employee at the legal address of the Bank within the Bank's Operational Time.
3.1.3 При приеме Заявления Ответственный работник идентифицирует Уполномоченного Представителя Клиента, с использованием документа, удостоверяющего	3.1.3. The responsible employee identifies the Client's Authorized Person using the Client's identity document1 when accepting an Application. The responsible employee has the right to request and the Client's Authorized Person has the right to submit other

личность последнего[1]. Ответственный работник вправе запросить, а Уполномоченный Представитель Клиента должен представить иные документы, необходимые для его Идентификации, в том числе документы, подтверждающие представленные в Банк сведения.

3.1.4 Заявление Уполномоченного Представителя Клиента принимается Ответственным работником после проведения Идентификации такого Представителя Клиента, о чем проставляется соответствующая отметка на Заявлении. Банк вправе отказать в приеме Заявления без объяснения причин такого отказа. Отказ в приеме Заявления влечет отказ в регистрации Уполномоченного Представителя Клиента в Системе ДБО.

3.1.5 В процессе обработки Заявления, после его принятия Банком, Оператор Центра регистрации:

- выполняет регистрационные действия по внесению регистрационной информации в реестры Системы ДБО;
- формулирует и заносит в реестры Системы ДБО специальную парольную фразу (вопрос/ответ), используемую для дополнительной идентификации (аутентификации) Уполномоченного Представителя Клиента;
- при выборе Клиентом метода работы в Системе ДБО с использованием простой Электронной подписи направляет на указанный в Заявлении на приобретение/изменение БП и Заявлении Абонентский номер Уполномоченного Представителя Клиента данные для первого входа в Систему ДБО – Логин и Временный пароль.

При выборе Клиентом метода работы в Системе ДБО с использованием усиленной неквалифицированной Электронной подписи:

Оператор Удостоверяющего центра:

- после выполнения указанных в разделе 4 Регламента действий, подготавливает Функциональный ключевой носитель и помещает его в упаковку установленного Банком образца, оклеивает специальной наклейкой для обеспечения возможности контроля целостности упаковки;
- передает должным образом упакованный Функциональный ключевой носитель Ответственному работнику для передачи уполномоченному Представителю Клиента.

3.2 Факт передачи Функционального ключевого носителя, а также целостность упаковки подтверждается собственноручной подписью Уполномоченного Представителя Клиента в акте о его получении. Форма Акта определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка. В случае нарушения целостности упаковки Функционального ключевого носителя Уполномоченный Представитель Клиента должен

documents required for the Client's Identification, including documents that confirm the information submitted to the Bank.

3.1.4. The application of the Client's Authorized Person shall be accepted by the responsible officer after the Identification of such Client's Representative has been carried out and a corresponding mark shall be made on the Application. The Bank may refuse to accept an Application without explaining the reasons for such refusal. The refusal to accept an Application results in the refusal to register the Client's Authorized Representative in the RBS System.

3.1.5. During the Application processing, after its acceptance by the Bank, the Registration Centre Operator:

- performs registration actions to enter registration information into the RBS system registers;
- formulates and enters into the registers of the RBS System a special password phrase (question/answer) used for additional identification (authentication) of the Client's Authorized Person;
- sends Login and Temporary Password for the first log in to the RBS System to the Client's Subscriber number of the Client's Authorized Representative Subscriber specified in the Application for Purchase/Change of BP and Application when the Client chooses a method of working in the RBS System using a simple Electronic Signature.

When the Client chooses a method of work in the RBS System using an enhanced non-certified Electronic Signature:

Operator of the Certification Centre:

- prepares the Functional Key Carrier and places it in the packaging of the sample set by the Bank, sticks a special sticker to ensure that the integrity of the packaging can be monitored after performing the actions specified in section 4 of the Rules;
- hands over a properly packaged Functional Key Carrier to the Responsible Officer for handing it over to the Client's Authorized Person.

3.2. The fact of transfer of the Functional Key Carrier as well as the integrity of the packaging is confirmed by the handwritten signature of the Client's Authorized Person in the act of receipt. The form of the Act is determined by the Bank and is available at https://131.ru/contracts and in the Bank's office. The Client's Authorized Person must indicate this in the Act if the integrity of the Functional Key Carrier packaging has been compromised. The Parties have determined that the integrity of the Functional Key Carrier

[1] Passport or other identification document in accordance with the laws of the Russian Federation. / Паспорт или иной документ, удостоверяющий личность в соответствии с законодательством Российской Федерации.

указать об этом в Акте. При отсутствии соответствующей отметки в Акте, Стороны определили считать целостность упаковки Функционального ключевого носителя не нарушенной, а сам ФКН надлежащим образом полученным Уполномоченным Представителем Клиента.	packaging has not been breached and that the Functional Key Carrier packaging has been duly received by the Client's Authorized Person if there is no corresponding mark in the Act.
3.3 Уполномоченный Представитель Клиента при использовании Системы ДБО и обмене Электронными документами через нее вправе использовать указанный в Заявлении на приобретение/изменение БП и Заявлении метод работы (способ подписания Электронных документов, с учетом функциональных возможностей Системы ДБО): с использованием простой Электронной подписи либо усиленной неквалифицированной Электронной подписи, с учетом установленных в Системе ДБО ограничений для отдельных категорий Электронных документов.	3.3. The Client's Authorized Representative when using the RBS System and exchanging Electronic Documents through it may use the method of work specified in the Application for Purchase/Change in BP and the Application (method of signing Electronic Documents, taking into account the functionality of the RBS System): with the use of a simple Electronic Signature or an enhanced non-certified Electronic Signature, taking into account the limitations set in the RBS System for certain categories of Electronic Documents.
3.4 Клиент считается подключенным к Системе ДБО, а Уполномоченный Представитель Клиента имеет возможность пользоваться Системой ДБО при наступлении следующих событий: - при использовании простой электронной подписи с момента регистрации Уполномоченного Представителя Клиента в Системе ДБО, и направлении на Абонентский номер такого Уполномоченного Представителя Клиента SMS-сообщения с данными для первоначального входа в Систему ДБО (логин и временный пароль); - при использовании усиленной неквалифицированной Электронной подписи после получения уведомления о выпуске Сертификата ключа проверки Электронной подписи и завершения процедуры формирования Электронной подписи средствами Системы ДБО Уполномоченным Представителем Клиента.	3.4. The Client shall be deemed to be connected to the RBS System and the Client's Authorized Person shall be able to use the RBS System upon the occurrence of the following events: - when using a simple electronic signature from the moment of registration of the Client's Authorized Representative in the RBS System and sending an SMS message with data for initial login to the Client's Subscriber number of such Authorized Representative (login and temporary password); - when using an enhanced non-certified Electronic Signature after receiving notification of the issue of the Electronic Signature Verification Key Certificate and when the Client's Authorized Person has completed the procedure for generation of the Electronic Signature by means of the RBS System.
4 ПОРЯДОК ВЫПУСКА СЕРТИФИКАТОВ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ	**4. PROCEDURE FOR ISSUING ELECTRONIC SIGNATURE KEY CERTIFICATES**
4.1 Для получения Сертификата ключа проверки электронной подписи для работы в Системе ДБО и осуществления обмена Электронными документами, подтвержденной усиленной неквалифицированной Электронной подписью, каждый Уполномоченный Представитель Клиента, данные о котором указаны в Заявлении на приобретение/изменение БП и Заявлении[2], должен лично: - создать с помощью средств Системы ДБО запрос на выпуск Сертификата ключа проверки электронной подписи, в электронном виде и на бумажном носителе;	4.1. In order to obtain the Key Certificate of Electronic Signature Verification for operation in the RBS System and to perform exchange of Electronic Documents confirmed by an enhanced non-certified Electronic Signature, each Authorized Person of the Client whose details are specified in the Application for Purchase/Change of BP and Application2 shall personally: - create a request to issue an electronic signature verification key certificate, electronically and on paper using the RBS System tools; - send this request to the Bank electronically using RBS funds;

[2] The Client's Authorized Persons entitled to dispose of the funds must also be indicated in such Card accepted by the Bank when executing the Card with specimen signatures according to the Rules. / При оформлении Карточки с образцами подписей в соответствии с Правилами, Уполномоченные Представители Клиента, имеющие право распоряжаться денежными средствами, должны быть также указаны в такой карточке, принятой Банком.

- направить в Банк данный запрос в электронном виде с использованием средств Системы ДБО; - предоставить в Банк данный запрос на бумажном носителе, заверенный собственноручной подписью такого Уполномоченного Представителя Клиента; - подписать сертификат ключа проверки Электронной подписи. Инструкция по подключению к системе ДБО и генерации ключей усиленной неквалифицированной Электронной подписи размещена на ресурсе https://131.ru/contracts и в офисе Банка. Запрос на выпуск Сертификата ключа проверки электронной подписи в обязательном порядке должен содержать: полные ФИО Уполномоченного Представителя Клиента (владельца Сертификата ключа проверки электронной подписи), номер Заявления (присваивается Банком), наименование Клиента, адрес местонахождения. Не допускается внесение каких-либо изменений в запрос на выпуск Сертификата ключа проверки электронной подписи, сформированный с использованием средств Системы ДБО. 4.2 При поступлении в Банк запроса на выпуск Сертификата ключа проверки электронной подписи в электронном виде, Оператор Центра регистрации сверяет данные, содержащиеся в указанном запросе в электронном виде с данными, указанными в запросе, представленном Клиентом на бумажном носителе. 4.3 При положительном результате проверки Оператор Центра регистрации обрабатывает поступивший запрос, а Оператор Удостоверяющего центра осуществляет выпуск Сертификата ключа проверки электронной подписи. При отрицательном результате проведенной проверки выпуск Сертификата ключа проверки электронной подписи не осуществляется. Банк вправе не сообщать Клиенту/его Уполномоченному Представителю о причинах отказа в выпуске Сертификата ключа проверки электронной подписи. 4.4 Для получения Уполномоченным Представителем Клиента сгенерированного Сертификата ключа проверки электронной подписи, последний должен явиться в Банк и представить документы, удостоверяющие личность.[3] Выдача сгенерированного Сертификата проверки электронной подписи осуществляется только на основании предоставленного запроса на выдачу сертификата ключа проверки Электронной подписи и при положительном результате проверки представленных документов и сведений в них содержащихся. Уполномоченный Представитель Клиента должен подписать выпущенный сертификат в момент его получения. 4.5 Выпущенный Сертификат ключа проверки электронной подписи подписывается Уполномоченным	- submit this request to the Bank in hard copy, certified by the handwritten signature of such Authorized Person of the Client; - sign the electronic signature verification key certificate. Instructions on connecting to the RBS system and generating the keys of an enhanced non-certified electronic signature are available at https://131.ru/contracts and in the Bank's office. A request to issue an Electronic Signature Verification Key Certificate must necessarily contain the full names of the Client's Authorized Person (owner of the Electronic Signature Verification Key Certificate), the Application number (assigned by the Bank), the Client's name and location address. It is not permitted to make any changes to the request for a Key Certificate of Electronic Signature Verification formed using the RBS system facilities. 4.2. The Operator of the Registration Centre shall verify the data contained in the said request electronically with the data specified in the request submitted by the Client in hard copy when the Bank receives a request to issue an Electronic Signature Verification Key Certificate. 4.3. The Registration Centre Operator processes the incoming request and the Certification Centre Operator issues the Key Certificate of the electronic signature verification if the result of the inspection is positive. The Key Certificate of Electronic Signature Verification shall not be issued if the result of the inspection is negative. The Bank may not to inform the Client/ its Authorized Person of the reasons for refusal to issue an electronic signature verification key certificate. 4.4. In order to receive a generated electronic signature verification key certificate for the Authorized Person of the Client, the latter must come to the Bank and present identity documents3. Signed verification certificates shall only be issued on the basis of a request for a Key Certificate of Electronic Signature Verification and if the result of the submitted documents and information contained therein is positive. The Client's Authorized Person must sign the issued certificate at the time of its receipt. 4.5. The issued Electronic Signature Verification Key Certificate shall be signed by the Client's Authorized Person and then placed on the RBS System.

[3] Passport or other identification document in accordance with the laws of the Russian Federation. / Паспорт или иной документ, удостоверяющий личность в соответствии с законодательством Российской Федерации.

Представителем Клиента и после этого размещается в Системе ДБО.

4.6 Изготовление Сертификатов ключей проверки электронной подписи осуществляется исключительно на основании полученного Банком запроса Уполномоченного Представителя Клиента, который содержит сведения, необходимые для идентификации владельца Сертификата ключа проверки электронной подписи, при условии выполнения положений 4.1. – 4.3. Регламента.

4.7 По окончании процедуры выпуска Сертификата ключа проверки электронной подписи, Уполномоченный Представитель Клиента получает возможность, используя программные средства Системы ДБО, завершить процедуру формирования усиленной неквалифицированной электронной подписи и приступить к ее эксплуатации.

4.8 Банк формирует Сертификат ключа проверки электронной подписи в отношении каждого Уполномоченного Представителя Клиента путём заверения электронной подписью собственного Удостоверяющего центра набора данных, включающих следующую информацию:

- серийный номер Сертификата ключа проверки электронной подписи;
- номер Заявления;
- идентификатор алгоритма, используемого для подписи Электронных документов;
- параметры сертификата издателя;
- период действия Сертификата ключа проверки электронной подписи, состоящий из двух дат: начала и конца периода (включительно);
- полное ФИО владельца Сертификата ключа проверки электронной подписи (Уполномоченного Представителя Клиента);
- информацию о ключе проверки электронной подписи: идентификатор алгоритма и собственно Ключ проверки Электронной подписи.

При формировании Сертификатов ключей проверки электронной подписи применяется криптографический алгоритм ГОСТ Р 34.10-2012. Сертификат ключа проверки Электронной подписи имеет ограниченный срок действия (1 год) с момента его выпуска.

4.8.1 Выпущенный Сертификат ключа проверки электронной подписи подлежит отзыву Банком в случае:

– компрометации Электронной подписи владельца Сертификата ключа проверки электронной подписи соответствующего данному сертификату; получения владельцем Сертификата ключа проверки электронной подписи нового сертификата;

– компрометации Электронной подписи Удостоверяющего центра Банка использованного при формировании Сертификата ключа проверки электронной подписи.

4.6. Key Certificates of electronic signature verification shall be produced only on the basis of a request of the Client's Authorized Person received by the Bank, which contains the information required to identify the owner of the Key Certificate of electronic signature verification, subject to compliance with provisions 4.1. - 4.3 of the Regulation.

4.7. The Client's Authorized Person shall be able to use the software tools of the RBS System to complete the procedure for generation of an enhanced non-certified electronic signature and start its operation upon completion of the procedure for issuing the Electronic Signature Verification Key Certificate.

4.8. The Bank forms an electronic signature verification key certificate in respect of each Authorized Person of the Client by certifying with an electronic signature its own Data Collection Certification Centre, which includes the following information:

- serial number of the electronic signature verification key certificate;
- Application number;
- the identifier of the algorithm used to sign Electronic Documents;
- parameters of the publisher's certificate;
- period of validity of the electronic signature verification key certificate, consisting of two dates: beginning and end of the period (inclusive);
- full name of the owner of the Electronic Signature Verification Key Certificate (Client's Authorized Person);
- information about the electronic signature verification key: the algorithm identifier and the electronic signature verification key itself.

The cryptographic algorithm of GOST R 34.10-2012 is used for the formation of electronic signature verification key certificates. The Key Certificate of Electronic Signature Verification has a limited validity period (1 year) from the date of its issue.

4.8.1. The Electronic Signature Verification Key Certificate issued by the Bank shall be subject to revocation by the Bank in the event of:

- compromise of the Electronic Signature of the owner of the Key Verification Certificate of the electronic signature corresponding to this certificate; receipt by the owner of the Key Verification Certificate of the electronic signature of the new certificate;
- compromise of the Electronic Signature of the Bank's Certification Centre used in the formation of the Electronic Signature Verification Key Certificate.

5 ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

5.1 В качестве средства подтверждения Электронного документа простой Электронной подписью используется Логин, Статический пароль, а также Одноразовый пароль.

5.2 В целях направления Уполномоченным Представителем Клиента Банку Электронного документа, Уполномоченный Представитель Клиента следуя инструкциям в экранных формах веб-интерфейса системы ДБО, используя функциональные кнопки, инициирует подписание соответствующего Электронного документа:

a) Уполномоченный Представитель Клиента вводит необходимые данные, которые запрашивает веб-интерфейс системы ДБО, используя функциональные кнопки и поля для ввода информации.

b) Перед подписанием Электронного документа Уполномоченный Представитель Клиента обязан ознакомиться с ним и быть согласным с его содержанием в полном объеме.

c) Для подписания сформированного Электронного документа посредством веб-интерфейса системы ДБО, Уполномоченный Представитель Клиента инициирует процесс подписания Электронного документа после проверки его содержания, и направляет Банку посредством веб-интерфейса системы ДБО запрос Одноразового пароля.

d) Полученный Банком запрос из веб-интерфейса системы ДБО расценивается как запрос Одноразового пароля для создания простой Электронной подписи. После этого Одноразовый пароль генерируется и направляется Банком на Абонентский номер Уполномоченного Представителя Клиента в SMS-сообщении с информацией об Электронном документе. Направленный Одноразовый пароль имеет ограниченное время действия.

e) Уполномоченный Представитель Клиента обязан обеспечить отсутствие доступа третьих лиц к Абонентскому номеру и устройству, на который Банком направляется одноразовый пароль посредством SMS-сообщения.

f) Перед подписанием Электронного документа Уполномоченный Представитель Клиента обязан ознакомиться с информацией, поступившей в SMS-сообщении, и в случае согласия с описанием подписать простой Электронной подписью Электронный документ. В случае несогласия с описанием Уполномоченный Представитель Клиента не должен подписывать сформированные Электронные документы.

g) Для подписания сформированного Электронного документа посредством простой Электронной подписи, Уполномоченный Представитель Клиента вводит полученный в SMS-сообщении Одноразовый пароль в функциональное поле в веб-интерфейсе системы ДБО, предназначенное для подписания, и нажимает соответствующую электронную кнопку, необходимую для подписания.

h) С момента нажатия Уполномоченным

5. THE PROCEDURE FOR USING A SIMPLE ELECTRONIC SIGNATURE

5.1. The Login, Static Password and One-time Password are used as a means of confirming the Electronic Document with a simple Electronic signature.

5.2. The Client's Authorized Person shall follow the instructions in the screen forms of the web-interface RBS system using functional buttons and initiate signing of the respective Electronic Document in order to send an Electronic Document to the Bank by the Client's Authorized Person:

a) The Client's Authorized Person enters the necessary data that is requested by the web interface of the RBS system with the use of function keys and fields for entering information.

b) The Client's Authorized Person must read it and agree with its content in full before signing the Electronic Document.

c) The Client's Authorized Person initiates the process of signing the Electronic Document after verification of its contents and sends the Bank a request for the One-time password via the web interface of the RBS system in order to sign the generated Electronic Document via the web interface of the RBS system.

d) A request received by the Bank from the web interface of the RBS system is regarded as a one-time password request to create a simple electronic signature. After that the One-time password is generated and sent by the Bank to the Client's Authorized Person Subscriber Number in an SMS message with information about the Electronic Document. The sent one-time password has a limited validity period.

e) The Client's Authorized Person ensures third parties do not have access to the Subscriber Number and device to which the Bank sends a one-time password via SMS.

f) The Client's Authorized Person must read the information received in the SMS message and, in case of agreement with the description, sign the Electronic Document with a simple Electronic signature before signing the Electronic Document. The Client's Authorized Person shall not sign the generated Electronic Documents in case of disagreement with the description.

g) The Client's Authorized Person enters the one-time password received in the SMS message into the functional field in the web interface of the RBS system intended for signing and press the relevant electronic button required for signing to sign the generated

Представителем Клиента специальной функциональной кнопки в веб-интерфейсе системы ДБО Электронный документ считается направленным Банку. i) Получив Электронный документ, Банк осуществляет проверку простой Электронной подписи. Для этого простая Электронная подпись, которая содержится в Электронном документе, сверяется с Одноразовым паролем, направленным в SMS-сообщении. В случае, если они не совпадают, документ не принимается Банком и остается в статусе «Создан» . Указанный документ считается не подписанным и не имеет юридической силы. j) Электронный документ считается подписанным простой Электронной подписью и подлинным (исходящим от Уполномоченного Представителя Клиента) при одновременном соблюдении следующих условий: (1) Электронный документ получен Банком, (2) Электронный документ содержит простую Электронную подпись Клиента, результат проверки которой совпадает с Одноразовым паролем.	Electronic Document by means of a simple Electronic Signature. h) The Electronic Document shall be deemed sent to the Bank as soon as the Client's Authorized Person presses a special functional button in the web interface of the RBS system. i) The Bank checks a simple Electronic Signature upon receipt of an Electronic Document. For this purpose, the simple Electronic Signature, which is contained in the Electronic Document, is checked against the one-time password sent in an SMS message. If they do not match, the document is not accepted by the Bank and remains in the Created status. This document is considered not to be signed and has no legal force. j) An electronic document shall be deemed to be signed by a simple electronic signature and authentic (emanating from the Client's Authorized Person), provided that the following conditions are met: (1) The Electronic document has been received by the Bank, (2) The Electronic document contains the Client's simple Electronic signature, the verification result of which coincides with the One-time password.
5.3 В Электронных документах, подписанных простой Электронной подписью, содержится информация, указывающая на Уполномоченного Представителя Клиента (ФИО, номер заявления, присвоенный при регистрации такого лица в системе ДБО), от имени которого был создан и отправлен Электронный документ. 5.4 Для получения Средств подтверждения Электронного документа для создания простой Электронной подписи Уполномоченный Представитель Клиента должен пройти процедуру регистрации в соответствии с разделом 3 настоящего Регламента и провести смену первоначальных Аутентификационных данных в Системе ДБО (Временного пароля). После входа в Систему ДБО для ее использования и осуществления обмена Электронными документами, Уполномоченный Представитель Клиента должен изменить Временный пароль на Статический пароль, после чего может приступить к обмену Электронными документами с использованием Системы ДБО. В случае невыполнения указанного условия доступ и использованием Системы ДБО не допускается. 5.5 Рекомендуется осуществлять смену Статического пароля для доступа к Системе ДБО не реже одного раза в 3 (Три) месяца. Банк не несет ответственности в случае не выполнения Уполномоченным Представителем Клиента указанной рекомендации, в том числе при наступлении негативных событий. 5.6 Уполномоченный Представитель Клиента может самостоятельно изменить Логин и Статический пароль в Системе ДБО, за исключением случая утраты Статического	5.3. Electronic Documents signed with a simple Electronic Signature contain information indicating the Client's Authorized Person (name, application number assigned when registering such person in the RBS system), on whose behalf the Electronic Document was created and sent. 5.4. The Client's Authorized Person shall go through the registration procedure in accordance with Section 3 of these Rules and change the initial Authentication Data in the RBS System (Temporary password) in order to obtain the Means of Confirmation of the Electronic Document to create a simple Electronic Signature. After logging in to the RBS System for its use and performing exchange of Electronic Documents, the Client's Authorized Representative shall change the Temporary password to a static password, after which it may start exchange of Electronic Documents using the RBS System. Access and use of the RBS System is not allowed in case of failure to comply with this condition. 5.5. It is recommended to change the Static Password to access the RBS System at least once every 3 (three) months. The Bank shall not be liable if the Client's Authorized Person fails to comply with this recommendation, including in case of negative events. 5.6. The Client's Authorized Person may independently change the Login and Static Password in the RBS System, except in case of loss of the Static Password. In case of loss of Static Password and/or Login, the Client's Authorized Person shall

пароля. В случае утраты Статического пароля или/и Логина Уполномоченное лицо Клиента обязан незамедлительно обратиться в Банк для блокирования доступа, в соответствии с разделом 7 настоящего Регламента. Для восстановления доступа в Систему ДБО Уполномоченное лицо Клиента должно лично обратиться в Банк с Заявлением о смене логина и/или пароля /разблокировку доступа в Системе ДБО, форма которого определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка, и документом, удостоверяющим его личность.

5.7 Одноразовый пароль автоматически генерируется Системой ДБО, в том числе в целях дополнительной аутентификации Уполномоченного Представителя Клиента при предоставлении ему доступа в Систему ДБО и/или подтверждения Электронного документа. Уполномоченный Представитель Клиента должен ввести полученный Одноразовый пароль для прохождения процедуры аутентификации и/или подтверждения Электронного документа.

5.8 Одноразовый пароль направляется Банком на Абонентский номер Уполномоченного Представителя Клиента, указанный в программно-аппаратном комплексе Банка на основании сведений, содержащихся в Заявлении на приобретение/изменение БП, Заявлении и/или Заявление о смене абонентского номера мобильной связи.

5.9 Для изменения Абонентского номера Уполномоченного Представителя Клиента, используемого для получения Одноразового пароля такой Уполномоченный Представитель Клиента должен обратиться в Банк и предоставить Заявление на изменение банковского продукта «Дистанционное банковское обслуживание с использованием Системы ДБО», и Заявление на изменение абонентского номера мобильной связи, с предоставлением удостоверяющих личность документов. Смена Абонентского номера Уполномоченного Представителя Клиента осуществляется только после положительного завершения проверки представленных сведений и документов. Банк вправе отказать Клиенту в смене Абонентского номера Уполномоченного Представителя Клиента без объяснения причин такого отказа.

6 ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

6.1 При каждом входе в Систему ДБО за 30 дней до окончания срока действия Сертификата ключа проверки Электронной подписи Система ДБО сообщает о скором его окончании.

6.2 До истечения срока действия Сертификатов ключей проверки Электронной подписи Уполномоченный Представитель Клиента имеет возможность провести

immediately contact the Bank to block access in accordance with Section 7 of these Rules. In order to restore access to the RBS System, the Client's Authorized Person shall personally apply to the Bank with an Application for Change of Login and/or Password / Unlock of Access to the RBS System, the form of which is determined by the Bank and is available at https://131.ru/contracts and in the Bank's office, and with an identity document.

5.7. The one-time password is automatically generated by the RBS System, including for the purpose of additional authentication of the Client's Authorized Representative when granting access to the RBS System and/or confirmation of the Electronic Document. The Client's Authorized Representative shall enter the received One-Time Password in order to pass the procedure of authentication and/or confirmation of the Electronic Document.

5.8. The one-time password is sent by the Bank to the Subscriber number of the Client's Authorized Representative specified in the Bank's software and hardware complex on the basis of information contained in the Application for Purchase/Modification of BP, Application and/or Application for Change of the Mobile Subscriber Number.

5.9. The change of the Subscriber number of the Client's Authorized Representative used for obtaining the One-time password requires applying and submitting an Application for Change of the Mobile Subscriber Number and Application for Change of the Remote Banking Service with the use of RBS System to the Bank by such Authorized Person of the Client with submission of identity documents. The Subscriber number of the Client's Authorized Person shall be changed only after positive completion of verification of submitted information and documents. The Bank shall have the right to refuse the Client to change the Client's Authorized Person Subscriber Number without explaining the reasons for such refusal.

6 THE PROCEDURE FOR THE SCHEDULED CHANGE OF THE ELECTRONIC SIGNATURE VERIFICATION KEY CERTIFICATE

6.1. The RBS System notifies of its imminent expiry upon each login to the RBS System, 30 days prior to the expiry date of the Electronic Signature Verification Key Certificate.

6.2. The Client's Authorized Person shall be able to carry out a scheduled procedure for changing the Electronic Signature Keys using the RBS System and its facilities prior to the expiry of the Electronic

плановую процедуру смены Ключей Электронной подписи с использованием Системы ДБО и ее средств.

6.3 Уполномоченный Представитель Клиента формирует новый Ключ Электронной подписи и запрос на изготовление нового Сертификата ключа проверки электронной подписи. Запрос подписывается действующим ключом Электронной подписи и направляется в Банк с использованием средств Системы ДБО.

6.4 При поступлении в Банк запроса на выпуск Сертификата ключа проверки электронной подписи в электронном виде Оператор Центра регистрации обрабатывает запрос и направляет его Оператору Удостоверяющего центра.

6.5 Оператор Удостоверяющего центра осуществляет выпуск Сертификата ключа проверки электронной подписи. Банк вправе отказать в выпуске Сертификата ключа проверки электронной подписи, запрос на который получен с использованием Системы ДБО, без объяснения причины. В случае отказа Банка в выпуске Сертификата ключа проверки электронной подписи, Уполномоченный Представитель Клиента вправе лично обратиться в Банк для выпуска такого сертификата, в порядке, указанном в разделе 4 настоящего Регламента. Сертификат направляется по Системе ДБО Уполномоченному Представителю Клиента, от которого поступил запрос для его подписания. Уполномоченный Представитель Клиента после подписания Электронной подписью нового Сертификата ключа проверки Электронной подписи направляет его в Банк в форме сообщения свободного формата. После получения Банком подписанного Сертификата ключа проверки электронной подписи, такой сертификат размещается в Системе ДБО.

6.6 Уполномоченный Представитель Клиента завершает процедуру смены Ключа Электронной подписи, используя средства Системы ДБО.

6.7 После завершения процедуры смены Ключа Электронной подписи Уполномоченный Представитель Клиента может использовать исключительно новый Ключ Электронной подписи.

7 ПОРЯДОК БЛОКИРОВКИ И ВОССТАНОВЛЕНИЯ ДОСТУПА К СИСТЕМЕ ДБО

7.1 Основанием для блокировки доступа Клиента и/или его Уполномоченного Представителя к Системе ДБО являются:

7.1.1 получение Банком от Уполномоченного Представителя Клиента Заявления на приобретение/изменение БП (содержащего сведения о смене Уполномоченного Представителя Клиента/изменении его данных/прекращении полномочий или иные сведения, порождающие сомнения Банка в возможности осуществления доступа и/или пользования Системой ДБО Уполномоченным Представителем

Signature Key Certificates.

6.3. The Client's Authorized Person shall form a new Electronic Signature Key and request for a new Electronic Signature Verification Key Certificate. The request shall be signed with a valid Electronic Signature Key and sent to the Bank using RBS System facilities.

6.4. The Registration Centre Operator will process the request and send it to the Certification Centre Operator when the Bank receives a request to issue an electronic signature verification key certificate.

6.5. The Certification Centre operator issues the Key Certificate of Electronic Signature Verification. The Bank may refuse to issue an electronic signature verification key certificate, the request for which has been received using the RBS System, without giving a reason. The Client's Authorized Person may personally apply to the Bank to issue such Certificate according to the procedure set out in Section 4 of these Rules in the event that the Bank refuses to issue an Electronic Signature Verification Key Certificate. The Certificate shall be sent via the RBS System to the Client's Authorized Person from whom a request for signing has been received. After the Client's Authorized Person has signed a new Electronic Signature Verification Key Certificate, the Client's Authorized Person sends it to the Bank in the form of a free format message. The Bank publishes such certificate in the RBS System upon receipt of the signed Electronic Signature Verification Key Certificate.

6.6. The Client's Authorized Person completes the procedure of changing the Electronic Signature Key using the means of the RBS System.

6.7. The Client's Authorized Person may only use the new Electronic Signature Key after the completion of the Electronic Signature Key change procedure.

7 PROCEDURE FOR BLOCKING AND RESTORING ACCESS TO THE RBS SYSTEM

7.1. The ground for blocking the access of the Client and/or his Authorized Person to the RBS System are:

7.1.1. Application to purchase/modify the BP (containing information on the change of the Client's Authorized Person / change of his/her data / termination of powers or other information that causes the Bank's doubts about the possibility of the Authorized Person of the Client to access and/or use the VBS System) receipt by the Bank from the Client's Authorized Person, and RBS System suspend access request, indicating the reasons for such suspension;

Клиента), запроса о приостановлении доступа к Системе ДБО, с указанием причин такого приостановления; 7.1.2 Компрометация Электронной подписи и/или использование Электронной подписи без согласия Уполномоченного Представителя Клиента; 7.1.3 смена Абонентского номера Уполномоченного Представителя Клиента; 7.1.4 замена Карточки с образцами подписей и оттиска печати и/или Соглашения о сочетании электронных подписей, при их оформлении в соответствии с Правилами; 7.1.5 прекращение или изменение полномочий или данных Уполномоченного Представителя Клиента; 7.1.6 утраты Аутентификационных данных, Временного, Одноразового, Статического паролей; 7.1.7 непредставление или представление недостоверных сведений и документов, запрашиваемых Банком, в том числе в целях выполнения требований законодательства Российской Федерации и нормативных актов Банка России; 7.1.8 выявление Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, установленным Банком России или подозрений на их совершение; 7.2 При наступлении событий указанных в пп. 7.1.4, 7.1.7, 7.1.8 доступ в Систему ДБО блокируется всем Уполномоченным Представителям Клиента. 7.3 Порядок блокировки доступа к Системе ДБО дистанционным способом: 7.3.1 Для дистанционной блокировки доступа к Системе ДБО Уполномоченному Представителю Клиента необходимо обратиться в Банк с соответствующим запросом по следующим контактным данным: dbo@131.ru. При этом, Уполномоченный Представитель Клиента должен сообщить уполномоченному работнику Банка следующую информацию: ● свои идентификационные данные; ● специальную парольную фразу. 7.3.2 Аутентификация заявителя при подаче запроса на блокировку доступа к Системе ДБО - Уполномоченного Представителя Клиента осуществляется по специальной парольной фразе, содержащейся в реестрах Системы ДБО. 7.3.3 Подача запроса на блокировку доступа к Системе ДБО Уполномоченного Представителя Клиента возможна только в течение Операционного времени Банка. 7.3.4 Уполномоченный Представитель Клиента может направить заявление на блокировку доступа в Систему ДБО, с использованием сообщений свободного формата Системы ДБО. 7.4 Порядок блокировки доступа к Системе ДБО при личном обращении Уполномоченного Представителя Клиента в Банк: 7.4.1 Уполномоченному Представителю Клиента необходимо обратиться непосредственно в офис Банка, по	7.1.2. Compromising the Electronic Signature and/or using the Electronic Signature without the consent of the Client's Authorized Person; 7.1.3. change of the Subscriber number of the Client's Authorized Person; 7.1.4. replacement of the Card of specimen signatures and seal impression and/or the Agreement on the Combination of Electronic Signatures, when executed in accordance with the Rules; 7.1.5. termination or change of powers or data of the Client's Authorized Person; 7.1.6. loss of Authentication Data, Temporary, One-time and Static passwords; 7.1.7. Failure to submit or submission of unreliable information and documents requested by the Bank, including for the purpose of complying with the requirements of the legislation of the Russian Federation and regulatory acts of the Bank of Russia; 7.1.8. identification by the Bank of a transaction corresponding to the signs of money transfer without the Client's consent or suspicion of such transaction by the Bank of Russia; 7.2. Access to the RBS System is blocked to all Authorized Persons of the Client upon occurrence of the events specified in subclauses 7.1.4, 7.1.7, 7.1.8. 7.3. Procedure for blocking access to the RBS System by remote means: 7.3.1. The Client's Authorized Person must contact the Bank with a request to remotely block access to the RBS System, using the following contact details: dbo@131.ru. Herewith, the Client's Authorized Person notifies the following to the Bank's Authorised employee information: ● their identification data; ● a special passphrase. 7.3.2. Authentication of the Applicant is carried out using a special password phrase contained in the registers of the RBS System, when submitting a request to block access to the RBS System, the Client's Authorized Person. 7.3.3. Submission of a request to block access to the RBS System of the Client's Authorized Person is possible only during the Bank's Operating Time. 7.3.4. The Client's Authorized Person may send an application to block access to the RBS System using free format RBS messages. 7.4. Procedure for blocking access to the RBS System when the Client's Authorized Person addresses the Bank in person: 7.4.1. The Client's Authorized Person applies directly to the Bank's office, at the Client's legal address with a corresponding written application for blocking access to the RBS System signed by this person.

его юридическому адресу, с соответствующим письменным заявлением о блокировании доступа к Системе ДБО, подписанным таким лицом. Одновременно с запросом Уполномоченный Представитель Клиента должен предоставить документы, удостоверяющие его личность и подтверждающие его полномочия. 7.4.2 Подача запроса на блокировку доступа к Системе ДБО Уполномоченного Представителя Клиента возможна только в течение Операционного времени Банка. 7.5 Блокировка доступа осуществляется незамедлительно после получения соответствующего запроса Банком, при условии его получения Банком в Операционное время. В случае, если запрос был получен Банком за пределами Операционного времени, такой запрос будет обработан, а доступ к Системе ДБО заблокирован, в Операционное время ближайшего за датой получения такого запроса Банком Рабочего дня. 7.6 Порядок восстановления доступа к Системе ДБО: 7.7 В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п.7.1.2-7.1.6 разблокировка возможна после: a) получения Банком письменного обращения (Заявления о смене логина и/или статического пароля/разблокировку доступа в системе ДБО) Уполномоченного Представителя Клиента при личном посещении офиса Банка. Форма такого заявления определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка. Одновременно с обращением Уполномоченный Представитель Клиента должен предоставить документы, удостоверяющие его личность и подтверждающие его полномочия. b) При использовании УНЭП проведенной процедуры внеплановой смены сертификата ключа проверки Электронной подписи в соответствии с разделом 9 настоящего Регламента; c) При использовании простой Электронной подписи: смены Статического пароля Уполномоченного Представителя Клиента в соответствии с п.5.6. Регламента; смены Абонентского номера Уполномоченного Представителя Клиента в случае утери и/или прекращения доступа к нему. 7.8 В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п.7.1.8 разблокировка возможна после получения Банком от Клиента подтверждения возобновления совершения операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, установленным Банком России, либо по истечении двух рабочих дней после дня приостановления при неполучении такого подтверждения. 7.9 В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в	Simultaneously with the request, the Client's Authorized Person provides documents proving his/her identity and authority. 7.4.2. Submission of a request to block access to the RBS System of the Client's Authorized Person is possible only during the Bank's Operating Time. 7.5. Access blocking is carried out immediately after receipt of the relevant request by the Bank, provided that the request is received by the Bank during the Operating Time. If a request has been received by the Bank outside of the Operating Time, such request shall be processed and access to the RBS System blocked during the Operating Time of the Business Day closest to the date of receipt of such request by the Bank. 7.6. Procedure for restoring access to the RBS System: 7.7. If the reason for blocking access to the RBS System is due to the circumstances specified in clauses 7.1.2-7.1.6, unlocking is possible after: a) The receipt of a written application (Application for Change of Login and/or Static Password/Unlocking Access in the RBS System) from the Authorized Person of the Client by the Bank when the Authorized Person of the Client personally visits the Bank's office. The form of such application is determined by the Bank and is available at https://131.ru/contracts and in the Bank's office. The Client's Authorized Person submits the documents proving his/her identity and confirming his/her authority simultaneously with the application. b) In the case of an unscheduled change of the electronic signature verification key certificate in accordance with Section 9 of these Rules; c) When using a simple Electronic Signature: change of the static password of the Client's Authorized Person in accordance with Clause 5.6 of the Rules; change of the Client's Authorized Person Subscriber Number in case of loss and/or termination of access to the Client. 7.8. If the reason for blocking access to the RBS System is due to circumstances specified in clause 7.1.8, unblocking may be possible after the Bank has received confirmation from the Client that a transaction has been resumed that corresponds to the signs of money transfer without the Client's consent, as established by the Bank of Russia, or two business days after the day of suspension when such confirmation is not received. 7.9. In the event that the reason for blocking access to the RBS System is due to the circumstances specified in 7.1.7 after the circumstances preceding

п.7.1.7 после устранения обстоятельств, предшествующих такой блокировке.

8 ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ КОМПРОМЕТАЦИИ ИЛИ ПОДОЗРЕНИИ НА КОМПРОМЕТАЦИЮ ЭЛЕКТРОННОЙ ПОДПИСИ

8.1 При выявлении одной из Сторон Компрометации Электронной подписи или ее признаков (подозрений), выявившая Сторона уведомляет об этом другую Сторону.
8.2 Банк уведомляет Клиента о наступлении указанных в п. 8.1 Регламента обстоятельствах любым доступным банку способом, используя имеющиеся в распоряжении Банка контактные данные Клиента, ранее предоставленные Клиентом.

8.3 Клиент уведомляет Банк о наступлении указанных в п. 8.1 Регламента обстоятельствах любым из нижеперечисленных способов:
- Письменное Уведомление о компрометации на бумажном носителе (передается в офисе Банка);
- Сканированная копия письменного Уведомления о компрометации, переданное на электронный адрес Банка: dbo@131.ru. Клиент обязан представить в Банк оригинал такого Уведомления о компрометации на бумажном носителе в течение 2 (Двух) Рабочих дней.

Форма Уведомления о компрометации определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка.
8.4 С момента получения Банком уведомления Клиента или выявления Банком обстоятельств, указанных в п. 8.1 Регламента, доступ Клиента (его Уполномоченных Представителей) к Системе ДБО блокируется до момента разблокировки такого доступа. Клиент уведомлен и согласен, что Банк не несет ответственности, включая финансовую, за любой факт блокировки доступа Клиента и/или его Уполномоченных Представителей к Системе ДБО, в связи с тем, что действия Банка по блокировки доступа к Системе ДБО направлены на обеспечение сохранности средств на Счете, защиту интересов Клиента и недопущению мошеннических операций и практик.

8.5 С момента направления Клиентом Банку или получения Клиентом от Банка уведомления о наступлении указанных в п. 8.1 Регламента обстоятельствах, Клиент не вправе использовать скомпрометированную Электронную подпись (ее ключ и/или средства)/Аутентификационные данные/Абонентский номер. В случае любого использования Клиентом такой Электронной подписи/Аутентификационных данных/Абонентского номера после наступления указанных в настоящем пункте событий клиент самостоятельно несет риск наступления

such blocking have been eliminated.

8 THE PROCEDURE IN THE EVENT OF COMPROMISE OR SUSPICION OF COMPROMISE OF AN ELECTRONIC SIGNATURE

8.1. The identified Party notifies the other Party if one of the Parties identifies the Electronic Signature Compromise, or its signs (suspicions).
8.2. The Bank notifies the Client of the occurrence of the circumstances specified in clause 8.1 of these Rules by any means available to the Bank, using the contact details of the Client previously provided by the Client.
8.3. The Client notifies the Bank of the occurrence of the circumstances specified in clause 8.1 of the Rules by any of the following means:
- Written Notice of Disclosure in hard copy (to be sent to the Bank's office);
- A scanned copy of the written Disclosure Notice sent to the Bank's e-mail address: dbo@131.ru. The Client submits the original of such Paper Disclosure Notice to the Bank within 2 (two) Business Days.

The form of the Disclosure Notice is determined by the Bank and is available at https://131.ru/contracts and in the Bank's office.
8.4. The Client's (their Authorized Persons') access to the RBS System is blocked until such access is unblocked from the moment the Bank receives the Client's notification or the Bank finds out the circumstances specified in clause 8.1 of these Rules. The Client shall be notified and agree that the Bank shall not be responsible, including financially, for any fact of blocking the Client and/or its Authorized Persons' access to the RBS System due to the fact that the Bank's actions aimed at blocking the access to the RBS System are aimed at ensuring safety of funds in the Account, protection of the Client's interests and prevention of fraudulent transactions and practices.

8.5. The Client may not use the compromised Electronic Signature (its key and/or means)/Authentication Data/Subscriber Number as soon as the Client has sent or received a notice from the Bank of the occurrence of the circumstances specified in clause 8.1 of the Rules. In the event that the Client uses such Electronic Signature/Authentication Data/Subscriber Number after the events specified in this clause, the Client shall bear the risk of adverse consequences, including legal and financial ones, for the Client.
8.6. RBS System access unblocking is performed

неблагоприятных последствий для него, в том числе правовых и финансовых.
8.6 Разблокировка доступа к Системе ДБО осуществляется в соответствии с п. 7.7 настоящего Регламента при получении Банком Уведомления о компрометации на бумажном носителе.

9 ПОРЯДОК ПРОВЕДЕНИЯ ВНЕПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

9.1 Указанный раздел применяется в случае использования Клиентом (его Уполномоченными Представителями) усиленных неквалифицированных Электронных подписей. Внеплановая смена Ключей Электронной подписи Уполномоченного Представителя Клиента и соответствующих им Сертификатов ключа проверки Электронной подписи выполняется в случае установленного факта Компрометации Электронной подписи или подозрений на это, в случае изменения регистрационных данных Уполномоченного Представителя Клиента, а также в случае выхода из строя ФКН.

9.2 После получения Банком Уведомления о компрометации Банк отзывает Сертификат скомпрометированного ключа проверки электронной подписи, путем помещения его в список отозванных сертификатов Системы ДБО.
9.3 Для выпуска нового ключа Электронной подписи и соответствующего ему Сертификата ключа проверки Электронной подписи Уполномоченный Представитель Клиента лично обращается в офис Банка с заявлением на выпуск Сертификата ключа проверки Электронной подписи в свободной форме и в указанном в разделе 4 настоящего Регламента порядке с предоставлением документов, удостоверяющих его личность и подтверждающие его полномочия.

10 ПОРЯДОК РАССМОТРЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

10.1 Процедура проверки подлинности Электронной подписи выполняется по инициативе Банка или Клиента. Под процедурой проверки подлинности Электронной подписи, при обмене между Банком и Клиентом Электронными документами с использованием Системы ДБО, подписанными Электронной подписью понимается возникновение у Банка или Клиента сомнений, связанных с непризнанием авторства и (или) целостности Электронного документа, подписанного Электронной подписью Уполномоченного Представителя Клиента.
10.2 Стороны признают информацию, содержащуюся в программно-аппаратных средствах и системных журналах Банка, достаточной для проверки подлинности простой Электронной подписи в Электронном документе. Подтверждение подлинности простой Электронной подписи в Электронном документе осуществляется путем

in accordance with cl. 7.7 of these Rules upon receipt by the Bank of a Notice of Compromising on Paper.

9 PROCEDURE FOR UNPLANNED CHANGE OF THE ELECTRONIC SIGNATURE VERIFICATION KEY CERTIFICATE

9.1. This section applies when the Client (its Authorized Persons) uses enhanced non-certified Electronic Signatures. Unscheduled change of the Electronic Signature Keys of the Client's Authorized Person and the corresponding Electronic Signature Verification Key Certificates is performed in case of the established fact of Compromising the Electronic Signature or suspicion thereof, in case of change of the registration data of the Client's Authorized Person and in case of failure of the FKM.

9.2. The Bank revokes the Certificate of the compromised electronic signature verification key by publishing it on the list of revoked RBS certificates upon receipt by the Bank of a Disclosure Notice.

9.3. The Client's Authorized Person personally applies to the Bank's office for the issue of a free form Electronic Signature Verification Key Certificate according to the procedure specified in Section 4 of these Rules, with the provision of documents proving his/her identity and confirming his/her authority in order to issue a new Electronic Signature Key and a corresponding Electronic Signature Verification Key Certificate.

10 THE PROCEDURE FOR DEALING WITH CONFLICT SITUATIONS

10.1. The procedure for authenticating the Electronic Signature is performed on the initiative of the Bank or the Client. The Electronic Signature Authentication Procedure means the occurrence of doubts by the Bank or the Client related to non-recognition of authorship and/or integrity of the Electronic Document signed with the Electronic Signature of the Authorized Person of the Client, when electronic documents signed with the Electronic Signature are exchanged between the Bank and the Client using the RBS System.
10.2. The Parties acknowledge the information contained in the Bank's hardware and software tools and system logs sufficient to verify the authenticity of a simple Electronic Signature in an Electronic Document. The simple Electronic Signature in the Electronic Document is authenticated by comparing the data specified by the Client's Authorized Person in the settings for the use of the simple Electronic Signature in the RBS System with the data assigned to

сопоставления данных, указанных Уполномоченным Представителем Клиента в настройках использования простой Электронной подписи в Системе ДБО, и данных, присвоенных оспариваемому Электронному документу в Системе ДБО, полученному Банком, а также информации в системных журналах Банка, в соответствии с процедурой, приведенной в п.10.11 настоящего Регламента.

10.3 Подтверждение подлинности усиленной неквалифицированной Электронной подписи в Электронных документах — осуществляется путем проверки соответствующим средством электронной подписи с использованием Сертификата ключа проверки электронной подписи принадлежности такой Электронной подписи в Электронном документе Уполномоченному Представителю Клиента (владельцу сертификата) и отсутствия искажений в подписанном данной Электронной подписью Электронном документе, в соответствии с процедурой, приведенной в п.10.10 настоящего Регламента.

10.4 Процедура проверки подлинности Электронной подписи, при обмене Электронным документами Клиентом и Банком с использованием Системы ДБО, в случае применения Клиентом усиленной неквалифицированной Электронной подписи основывается на математических свойствах алгоритма электронной подписи, реализованного в соответствии с актуальным стандартом Российской Федерации ГОСТ Р 34.10-2012, гарантирующими невозможность подделки значения усиленной неквалифицированной Электронной подписи любым лицом, не обладающим ключом такой Электронной подписи. Итогом разрешения конфликтной ситуации является либо доказательство подлинности, целостности и авторства оспариваемого Электронного документа Клиенту (его Уполномоченному Представителю), либо установление факта приема Банком искаженного Электронного документа.

10.5 На случай возникновения споров Банк обеспечивает хранение в течение установленных законодательством Российской Федерации сроков в специальной базе данных Электронных документов в виде единиц хранения, каждая из которых включает данные Электронного документа, строки Электронной подписи с параметрами усиленной неквалифицированной Электронной подписи, Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента, использованный при создании усиленной неквалифицированной Электронной подписи, историю настроек Системы ДБО для использования простой Электронной подписи в системных журналах Банка, а так же данные Средств подтверждения Электронных документов, использованные при создании простой Электронной подписи в оспариваемом Электронном документе. Банк обеспечивает защиту данных от возможных искажений в процессе хранения. Банк обеспечивает хранение полученного Банком запроса

the contested Electronic Signature in the RBS System received by the Bank and the information in the Bank's system logs in accordance with the procedure set out in clause 10.11 of these Rules.

10.3. Authentication of the enhanced non-certified Electronic Signature in Electronic Documents is performed by means of verification by the appropriate electronic signature means using the Key Certificate of verification of the electronic signature belonging to such Electronic Signature in the Electronic Document to the Client's Authorized Person (certificate holder) and no distortion in the Electronic Document signed by such Electronic Signature in accordance with the procedure set out in clause 10.10 hereof.

10.4. The procedure for verification of the Electronic Signature authenticity is based on the mathematical properties of the electronic signature algorithm implemented in accordance with the current standard of the Russian Federation GOST R 34.10-2012, which guarantees the impossibility of forging the value of the enhanced non-certified Electronic Signature by any person who does not possess the key of such electronic signature, when the Client and the Bank exchange Electronic Documents using the RBS System, in case the Client applies the enhanced non-certified Electronic Signature. The result of the conflict resolution is either proof of authenticity, integrity and authorship of the disputed Electronic Document to the Client (its Authorized Person) or establishment of the fact of acceptance of the distorted Electronic Document by the Bank.

10.5. In the event of a dispute, the Bank ensures the Electronic Documents are stored in a special database in the form of storage units, each of which includes data from the Electronic Document, lines of the Electronic Signature with the parameters of the enhanced non-certified Electronic Signature, within the time limits established by Russian legislation, Certificate of the electronic signature verification key of the Client's Authorized Person used in creating the enhanced non-certified Electronic Signature, history of settings of the RBS System for using the simple Electronic Signature in the Bank's system logs, as well as data of the Electronic Document Validation Tools used in creating the simple Electronic Signature in the disputed Electronic Document. The Bank ensures the protection of data against possible distortions in the storage process. The Bank ensures that the Client's request received by the Bank to produce the first Electronic Signature Verification Key Certificate is stored in paper form.

10.6. The Bank ensures the request for the electronic

Клиента на изготовление первого Сертификата ключа проверки электронной подписи в бумажной форме.

10.6 В случае дистанционного обращения Уполномоченного Представителя Клиента для перевыпуска Сертификата ключа проверки электронной подписи Банк обеспечивает хранение полученного Банком подписанного Уполномоченным Представителя Клиента запроса на изготовление Сертификата ключа проверки электронной подписи в электронной форме.

10.7 Процедура проверки подлинности Электронной подписи, при обмене Электронными документами с использованием Системы ДБО выполняется Согласительной комиссией, в состав которой входят надлежащим образом уполномоченные представители обеих сторон (не менее двух человек от каждой стороны). По соглашению сторон в состав комиссии может быть введен независимый эксперт.

10.8 В случае, если оспариваемый Электронный документ является частью пакета Электронных документов, то процедура проверки подписи осуществляется под пакетом Электронных документов, в состав, которого входит оспариваемый Электронный документ.

10.9 Порядок разрешения конфликтной ситуации.

10.9.1 В случае возникновения необходимости в проведении процедуры проверки подлинности Электронной подписи, при обмене Электронными документами с использованием Системы ДБО, Уполномоченный Представитель Клиента представляет Банку письменное заявление, содержащее существо претензии с указанием на Электронный документ, который он оспаривает.

10.9.2 Банк и Клиент должны в течение не более пяти рабочих дней от даты приема Банком заявления Клиента сформировать Согласительную комиссию для его рассмотрения.

10.9.3 Согласительная комиссия должна закончить свою работу в течение 14 рабочих дней с момента ее создания.

10.9.4 Решение Согласительной комиссии принимается большинством голосов ее участников, оформляется актом и подписывается всеми членами комиссии.

10.9.5 В случае, если стороны не пришли к взаимному соглашению или в случае отказа от добровольного исполнения решения Согласительной комиссии, стороны решают конфликтную ситуацию в судебном порядке.

10.10 Процедура проверки усиленной неквалифицированной Электронной подписи .

10.10.1 Для проверки принадлежности усиленной неквалифицированной Электронной подписи Уполномоченному Представителю Клиента и отсутствия искажений в Электронном документе из базы данных Банка уполномоченным работником Банка извлекается файл Сертификата ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца

signature verification key certificate received by the Bank and signed by the Client's Authorized Person is stored in electronic form in the event of remote access of the Client's Authorized Person for the reissue of the electronic signature verification key certificate.

10.7. The procedure of verification of the authenticity of the Electronic Signature is performed by the Conciliation Commission consisting of duly Authorized Persons of both parties (at least two persons from each party), when exchanging the Electronic Documents using the RBS System. An independent expert may be introduced to the Commission upon agreement of the Parties.

10.8. In the event that the disputed Electronic Document is part of the Electronic Document Package, the signature verification procedure is performed under the Electronic Document Package, which is part of the disputed Electronic Document.

10.9. Procedure for resolving a conflict situation.

10.9.1. The Client's Authorized Person submits a written application containing the substance of the claim to the Bank, indicating the Electronic Document that the Client is contesting, in the event that it is necessary to carry out the procedure of authenticity verification of the Electronic Signature, when exchanging the Electronic Documents using the RBS System.

10.9.2. The Bank and the Client shall form a Conciliation Commission for its consideration, within no more than five working days from the date of receipt of the Client's application by the Bank.

10.9.3. The Conciliation Commission must complete its work within 14 working days of its establishment.

10.9.4. The decision of the Conciliation Commission is taken by a majority vote of its members, is drawn up in an act and signed by all members of the Commission.

10.9.5. The parties resolve the situation in court if they fail to reach a mutual agreement or if they refuse to comply with the Conciliation Commission's decision voluntarily.

10.10. Enhanced Non-Certified Electronic Signature verification procedure.

10.10.1.The Bank's authorised employee retrieves from the Bank's database the file of the Key Signature Validation Key Certificate of the Authorized Person of the Client, the holder of the Key Signature Validation Key Certificate, used in creating the enhanced non-certified Electronic Signature under the contested Electronic Document in order to verify that the enhanced non-certified Electronic Signature belongs to the Authorized Person of the Client and that the

Сертификата ключа проверки электронной подписи, использованный при создании усиленной неквалифицированной Электронной подписи под оспариваемым Электронным документом.	Electronic Signature Validation Key Certificate file of the Authorized Person of the Client is not distorted in the Electronic Document.
10.10.2 Устанавливается принадлежность ключа проверки Электронной подписи, содержащегося в извлеченном файле, владельцу Сертификата ключа проверки электронной подписи по следующей процедуре: ● из базы данных Удостоверяющего центра извлекается первичный Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи. Устанавливается принадлежность ключа проверки Электронной подписи владельцу Сертификата ключа проверки электронной подписи, путем сравнения с ключом проверки Электронной подписи, указанному в запросе на изготовление Сертификата проверки ключа электронной подписи в бумажном виде, имеющимся в распоряжении Банка. Если соответствие не установлено, то принадлежность ключа Электронной подписи данному владельцу Сертификата ключа проверки электронной подписи – Клиенту/Уполномоченному Представителю Клиента не подтверждается; ● из базы данных Удостоверяющего центра извлекается последующий запрос (при наличии такового) на Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи и устанавливается факт его подписания первичным ключом Электронной подписи по содержанию Сертификата ключа проверки электронной подписи. В противном случае - принадлежность ключа данному уполномоченному представителю Клиента не подтверждается; ● вышеуказанные действия последовательно повторяются вплоть до проверки запроса на изготовление Сертификата ключа проверки электронной подписи владельца Сертификата ключа проверки электронной подписи, использованного для создания Электронной подписи под оспариваемым Электронным документом. Если из содержания запроса на изготовление Сертификата ключа проверки электронной подписи в базе данных Удостоверяющего центра не следует, что запрос проверен предыдущим Сертификатом ключа проверки электронной подписи соответствующего Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи, принадлежность ключа Электронной подписи такому Уполномоченному Представителю Клиента не подтверждается. В противном случае - Ключ Электронной подписи признается принадлежащим указанному в его Сертификате ключа проверки электронной подписи Уполномоченному Представителю Клиента.	10.10.2.The electronic signature verification key contained in the extracted file shall belong to the owner of the Electronic Signature Verification Key Certificate according to the following procedure: ● the primary Key Certificate of Electronic Signature Verification of the Authorized Person of the Client, the owner of the Key Certificate of Electronic Signature Verification, is extracted from the Certification Centre database. The ownership of the electronic signature verification key to the owner of the electronic signature verification key certificate is established by comparing it with the electronic signature verification key specified in the request for the production of the electronic signature key verification certificate in paper form available to the Bank. The ownership of the Electronic Signature Key by this owner of the Electronic Signature Verification Key Certificate, the Client/Accredited Representative of the Client, shall not be confirmed if no match has been established; ● a subsequent request (if any) for the Key Certificate of Electronic Signature Verification of the Authorized Person of the Client, the owner of the Key Certificate of Electronic Signature Verification, is extracted from the Certification Authority database and the fact of its signing by the primary key of the Electronic Signature according to the content of the Key Certificate of Electronic Signature Verification is established. Otherwise, the ownership of the key by this Authorized Person of the Client shall not be confirmed; ● The above actions are repeated sequentially until the request for the production of the Key Certificate of Electronic Signature Verification of the owner of the Key Certificate of Electronic Signature Verification used for the production of the Electronic Signature under the contested Electronic Document is verified. If the contents of the request for the production of the electronic signature verification key certificate in the Certification Centre's database do not indicate that the request has been verified by the previous electronic signature verification key certificate of the respective Authorized Person of the Client, the owner of the electronic signature verification key certificate, the ownership of the electronic signature key by such Authorized Person of the Client shall not be confirmed. Otherwise, the Electronic Signature Key shall be deemed to belong to the Client's Authorized Person indicated in his Electronic Signature Verification Key Certificate.
10.10.3 Устанавливается действительность Сертификата ключа проверки электронной подписи Уполномоченного	

Представителя Клиента - владельца Сертификата ключа проверки электронной подписи, на момент получения Банком оспариваемого Электронного документа. Сертификат ключа проверки электронной подписи является недействительным на момент получения Банком оспариваемого Электронного документа, если: ● срок действия Сертификата ключа проверки электронного документа истек; ● данный Сертификат ключа проверки электронной подписи был помещен в список отозванных сертификатов. В противном случае, Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи признается действительным.	10.10.3.The validity of the Key Certificate of Electronic Signature Verification of the Authorized Person of the Client, the holder of the Key Certificate of Electronic Signature Verification, is established as of the date of receipt of the contested Electronic Document by the Bank. The Electronic Signature Verification Key Certificate shall be invalid as at the time of receipt of the contested Electronic Document by the Bank, if: ● the electronic document verification key certificate has expired; ● this Electronic Signature Verification Key Certificate has been published on the list of revoked certificates. Otherwise, the Key Certificate of Electronic Signature Verification of the Authorized Person of the Client, the owner of the Key Certificate of Electronic Signature Verification, shall be deemed valid.
10.10.4 Устанавливается факт блокирования доступа владельцу Сертификата ключа проверки электронной подписи к Системе ДБО на момент получения Банком оспариваемого Электронного документа. В случае, если дата получения Банком Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование доступа в Систему ДБО Уполномоченному Представителю Клиента – владельцу Сертификата ключа проверки электронной подписи раньше даты получения Банком оспариваемого Электронного документа — такой Электронный документ признается недействительным. В противном случае либо при установлении отсутствия факта получения Банком соответствующего Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование доступа в Систему ДБО Уполномоченному Представителю клиента – владельцу Сертификата ключа проверки электронной подписи – оспариваемый Электронный документ признается действительным и корректным.	10.10.4.The fact of blocking the access of the owner of the Key Certificate of verification of the electronic signature to the RBS System at the time of receipt of the contested Electronic Document by the Bank shall be established. Such Electronic Document shall be deemed invalid, if the date of receipt by the Bank of a Notice of Electronic Signature Key Imprinting and/or application for blocking access to the RBS System by the Client's Authorized Person, the holder of the Electronic Signature Verification Key Certificate, is earlier than the date of receipt of the contested Electronic Document by the Bank. Otherwise, or if it is established that the Bank has not received the relevant Electronic Signature Key Disclosure Notice and/or application to block access to the VSS System by the Client's Authorized Person, the holder of the Electronic Signature Verification Key Certificate, the contested Electronic Document shall be deemed valid and correct.
10.10.5 Для разбора конфликтной ситуации используются эталонные программно-аппаратные средства Банка. Используется специальное сертифицированное программное обеспечение, предназначенное для проверки усиленной неквалифицированной Электронной подписи под Электронным документом. 10.10.6 Проверка Электронной подписи оспариваемого Электронного документа производится программой ARBITER-PKI (разработчик ЗАО «Сигнал-КОМ»). По результатам проверки Электронная подпись под оспариваемым Электронным документом признается принадлежащей Уполномоченному Представителю Клиента - владельцу Сертификата ключа проверки	10.10.5.The Bank's reference hardware and software tools are used to analyse conflict situations. Special certified software is used to verify an enhanced non-certified Electronic Signature under an Electronic Document. 10.10.6.The Electronic Signature of the contested Electronic Document is verified by the ARBITER-PKI program (implemented by ZAO Signal-COM). Based on the results of the verification, the Electronic Signature under the contested Electronic Document shall be deemed to belong to the Client's Authorized Person, the owner of the Electronic Signature Verification Key Certificate, if the issued by the mentioned program inspection report has been generated Document's signature status: Valid or Signature confirmed (signature is correct), and

электронной подписи, если в протоколе проверки, выдаваемом указанной в настоящем пункте программой, сформирована запись о том, что **«Статус подписи документа: Действительна»** или **«Подпись подтверждена»** (signature correct), и не принадлежащей Уполномоченному Представителю Клиента - владельцу Сертификата ключа проверки электронной подписи, в противном случае. Протокол проверки усиленной неквалифицированной Электронной подписи распечатывается и подписывается всеми членами Согласительной комиссии.

10.11 Процедура проверки простой Электронной подписи.

Этап 1.

Для проверки принадлежности простой Электронной подписи Уполномоченному Представителю Клиента и проверки правомерности исполнения Банком Электронного документа, из системного журнала Банка извлекается информация об оспариваемом Электронном документе, которая содержит:

- содержимое оспариваемого Электронного документа, полученного Банком;
- информация о лице, подписавшем оспариваемый Электронный документ (полное ФИО, уникальный номер заявления на регистрацию Уполномоченного лица);
- дата и время сеанса;
- дата и время подписания оспариваемого Электронного документа;
- Абонентский номер, на который был отправлен Одноразовый пароль для подтверждения оспариваемого Электронного документа;
- Одноразовый пароль, введенный для подтверждения оспариваемого Электронного документа и операции, дата и время формирования сообщения.

Этап 2.

Устанавливается соответствие Абонентского номера, указанного Клиентом (его Уполномоченным лицом) в полученных Банком документах, Абонентскому номеру хранящемуся в электронных журналах Системы ДБО, на который был направлен Одноразовый пароль на момент подписания оспариваемого Электронного документа. При совпадении информации Согласительная комиссия переходит к этапу 3. При несовпадении информации оспариваемый документ признается некорректным.

Этап 3.

Устанавливается соответствие Одноразового пароля, направленного на Абонентский номер Уполномоченного Представителя Клиента, Одноразовому паролю хранящемуся в электронных журналах Системы ДБО вместе с оспариваемым Электронным документом и введенным Уполномоченным Представителем Клиента при подписании Электронного документа. При совпадении информации Согласительная комиссия переходит к этапу 4. При несовпадении информации оспариваемый документ признается некорректным.

Этап 4.

otherwise, shall not be deemed to belong to the Client's Authorized Person, the owner of the Electronic Signature Verification Key Certificate. The Enhanced Non-Certified Electronic Signature Verification Protocol is printed out and signed by all members of the Conciliation Commission.

10.11. Procedure for checking a simple Electronic Signature.

Stage 1.

In order to verify a simple Electronic Signature belongs to the Authorized Person of the Client and to verify the legality of the Bank's execution of the Electronic Document, information on the contested Electronic Document is extracted from the Bank's system log and contained therein:

- the contents of the contested Electronic Document received by the Bank;
- information on the person who signed the contested Electronic Document (full name, unique application number for registration of the Authorised person);
- date and time of the session;
- date and time of signing of the contested Electronic Document;
- The subscriber number to which the one-time password was sent to confirm the disputed Electronic Document;
- One-time password entered to confirm the disputed Electronic Document and transaction, date and time of message generation.

Stage 2.

The Subscriber Number specified by the Client (his Authorised person) in the documents received by the Bank is established to be in compliance with the Subscriber Number stored in the electronic logs of the RBS System, to which the One-time password was sent at the time of signing the contested Electronic Document. The Conciliation Commission shall proceed to stage 3 if the information matches. The contested document shall be deemed incorrect in the event of a discrepancy of information.

Stage 3.

Compliance of the One-time password sent to the Subscriber number of the Client's Authorized Representative with the One-time password stored in the electronic logs of the RBS System together with the contested Electronic Document and entered by the Client's Authorized Representative upon signing the Electronic Document shall be established. The Conciliation Commission shall proceed to stage 4 if the information coincides. The contested document shall be deemed incorrect in the event of a discrepancy of

Устанавливается факт блокирования доступа Уполномоченного Представителя Клиента, подписавшего оспариваемый Электронный документ, к Системе ДБО на момент получения Банком оспариваемого Электронного документа. Если дата получения Банком Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование доступа в Систему ДБО Уполномоченному Представителю Клиента, подписавшему оспариваемый Электронный документ, раньше даты получения Банком оспариваемого Электронного документа — такой Электронный документ признается некорректным. В противном случае либо при установлении отсутствия факта получения Банком соответствующего Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование доступа в Систему ДБО Уполномоченному Представителю Клиента, подписавшему оспариваемый Электронный документ, - оспариваемый Электронный документ признается действительным и корректным.	information. **Stage 4.** The fact of blocking the access of the Authorized Person of the Client who has signed the contested Electronic Document to the RBS System at the moment when the Bank receives the contested Electronic Document shall be established. If the receipt date by the Bank of a Notice of Electronic Signature Key Imprinting and/or application for blocking access to the RBS System by the Client's Authorized Person who signed the contested Electronic Document is earlier than the date of receipt of the contested Electronic Document by the Bank, such Electronic Document shall be deemed to be incorrect. Otherwise, the contested Electronic Document shall be deemed valid and correct, if it is established that the Bank has not received the relevant Notice on compromising the Electronic Signature key and/or application for blocking the access to the RBS system to the Client's Authorized Person who signed the contested Electronic Document, the contested Electronic Document.
10.12 Ответственность сторон при оспаривании Электронных документов, обмен которыми осуществляется с использованием Системы ДБО, подписанных усиленной неквалифицированной Электронной подписью. 10.12.1 Банк <u>не несет</u> ответственности перед Клиентом в случаях, указанных в Правилах (включая приложения к ним), а также при установлении Согласительной комиссией совокупности следующих фактов при проверке усиленной неквалифицированной Электронной подписи под оспариваемым Электронным документом: ● ключ проверки Электронной подписи в оспариваемом Электронном документе принадлежит Уполномоченному Представителю Клиента - владельцу Сертификата ключа проверки электронной подписи; ● Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента — владельца Сертификата ключа проверки электронной подписи был действителен на момент получения Банком оспариваемого Электронного документа; ● не установлен факт получения Банком от Клиента Уведомления о компрометации ключа Электронной подписи и/или заявления о блокировании доступа в Систему ДБО Уполномоченного Представителя Клиента, с использованием Средства подтверждения Электронного документа, которым был подписан оспариваемый Электронный документ, либо момент получения Банком Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование позже момента	**10.12. Responsibility of the parties in contesting Electronic Documents exchanged with the use of the RBS System and signed by an enhanced non-certified Electronic Signature.** 10.12.1.The Bank shall not be liable to the Client in the cases specified in the Rules (including their annexes), as well as when the Conciliation Commission establishes the following facts when verifying an enhanced non-certified Electronic Signature under the contested Electronic Document: ● the key to the Electronic Signature verification in the disputed Electronic Document belongs to the Client's Authorized Person, who is the holder of the Electronic Signature verification key certificate; ● the electronic signature verification key certificate of the Authorized Person of the Client, the holder of the Electronic Signature Verification Key Certificate, was valid as of the date of receipt by the Bank of the contested Electronic Document; ● it has not been established that the Bank has received a Notice of Electronic Signature Key Compromised and/or Application for Blocking of the Client's Authorized Person's access to the RBS System from the Client using the Electronic Document Validation Tool by which the contested Electronic Document was signed, or the time when the Bank received a Notice of Electronic Signature Key Compromised and/or Application for Blocking after the time when the Bank received the contested Electronic Document. 10.12.2.The Bank shall not be liable to the Client and

получения Банком оспариваемого Электронного документа. 10.12.2 Банк не несет ответственности перед Клиентом и не возмещает Клиенту упущенную выгоду последнего. Ответственность Банка наступает исключительно при наличии доказанной вины последнего и наличием прямой причинно-следственной связи между наступившими событиями, доказанной виной Банка и негативными для Клиента последствиями. 10.12.3 Клиент/Уполномоченный Представитель Клиента несут ответственность перед Банком во всех и любых случаях невыполнения и/или ненадлежащего выполнения Правил (включая приложения к ним), настоящего Регламента, положений законодательства Российской Федерации и требований Банка, а также несут риск наступления любых правовых и/или финансовых последствий, в том числе неблагоприятных для Клиента, Банка, иных лиц, связанные с таким нарушением/ненадлежащим исполнением. **10.13 Ответственность сторон при оспаривании Электронных документов, обмен которыми осуществляется с использованием Системы ДБО, подписанных простой Электронной подписью.** 10.13.1 Банк не несет ответственности перед Клиентом в случаях, указанных в Правилах (включая приложения к ним), а также при установлении Согласительной комиссией совокупности следующих фактов при проверке простой Электронной подписи под оспариваемым Электронным документом: ● не установлен факт получения Банком от Клиента Уведомления о компрометации ключа Электронной подписи и/или заявления о блокировании доступа в Систему ДБО Уполномоченного Представителя Клиента, с использованием Средства подтверждения Электронного документа, которым был подписан оспариваемый Электронный документ, либо момент получения Банком Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование доступа в Систему ДБО позже или равна моменту получения Банком оспариваемого Электронного документа. ● Одноразовый пароль для подписания оспариваемого Электронного документа простой Электронной подписью был отправлен на Абонентский номер, предоставленный Банку Уполномоченным Представителем Клиента, на момент подписания оспариваемого Электронного документа. 10.13.2 Банк не несет ответственности перед Клиентом и не возмещает Клиенту упущенную выгоду последнего. Ответственность Банка наступает исключительно при наличии доказанной вины последнего и наличием прямой причинно-следственной связи между наступившими событиями, доказанной виной Банка и негативными для Клиента последствиями. 10.13.3 Клиент/Уполномоченный Представитель Клиента	shall not compensate the Client for the lost profits of the latter. The Bank's liability shall arise only if there is a proven guilt of the latter and there is a direct causal link between the events that have occurred, the Bank's guilt proven and the consequences for the Client that are negative. 10.12.3.The Client/Accredited Representative of the Client shall be responsible to the Bank in all and any cases of non-fulfillment and/or improper fulfillment of the Rules (including their annexes), these Rules, provisions of the legislation of the Russian Federation and the Bank's requirements, as well as bear the risk of occurrence of any legal and/or financial consequences, including those unfavourable for the Client, the Bank and other persons, related to such violation/ improper fulfillment. 10.13. Responsibility of the parties in contesting Electronic Documents exchanged using the RBS System and signed with a simple electronic signature. 10.13.1.The Bank shall not be liable to the Client in the cases specified in the Rules (including their annexes), as well as when the Conciliation Commission establishes the following facts when checking a simple Electronic Signature under the contested Electronic Document: ● it has not been established that the Bank has received a Notice of Electronic Signature Key Imprinting and/or Application for blocking access to the RBS System from the Client using the Electronic Document Validation Tool by which the disputed Electronic Document was signed, or the time of receipt by the Bank of a Notice of Electronic Signature Key Imprinting and/or Application for blocking access to the RBS System later or equal to the time of receipt by the Bank of the disputed Electronic Document. ● The one-time password for signing the contested Electronic Document by a simple electronic signature has been sent to the Subscriber number provided to the Bank by the Client's Authorized Person at the time of signing the contested Electronic Document. 10.13.2.The Bank shall not be liable to the Client and shall not compensate the Client for the lost profits of the latter. The Bank's liability shall arise only if there is a proven guilt of the latter and there is a direct causal link between the events that have occurred, the Bank's guilt proven and the consequences for the Client that are negative. 10.13.3.The Client/Accredited Representative of the Client shall be responsible to the Bank in all and any cases of non-fulfillment and/or improper fulfillment of the Rules (including their annexes), these Rules, provisions of the legislation of the Russian Federation

несут ответственность перед Банком во всех и любых случаях невыполнения и/или ненадлежащего выполнения Правил (включая приложения к ним), настоящего Регламента, положений законодательства Российской Федерации и требований Банка, а также несут риск наступления любых правовых и/или финансовых последствий, в том числе неблагоприятных для Клиента, Банка, иных лиц, связанные с таким нарушением/ненадлежащим исполнением.

11 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1 Настоящий Регламент составлен на русском и английском языках. В случае возникновения противоречий приоритетным считается текст настоящего Регламента на русском языке.

11.2 Правоотношения Сторон, урегулированные настоящим Регламентом, а также любые иные правоотношения Сторон, связанные с выполнением настоящего Регламента, подлежат регулированию и толкованию в соответствии с законодательством Российской Федерации. В случае если любая из сторон откажется от исполнения решения Согласительной комиссии все споры и разногласия подлежат разрешению в соответствии с настоящим пунктом. Все споры, возникающие между Клиентом и Банком в рамках выполнения настоящего Регламента или в связи с ним, подлежат решению в соответствии с законодательством Российской Федерации, путем переговоров, а в случае невозможности такого решения в Арбитражном суде Республики Татарстан. Клиент вправе обратиться в Банк с письменной претензией, подписанной Уполномоченным Представителем Клиента и скрепленной печатью последнего (при наличии) путем обращения в офис Банка, по его юридическому адресу. Письменный досудебный порядок урегулирования споров с Банком, в рамках настоящего Регламента, является обязательным. Срок ответа на досудебную претензию – 30 (Тридцать) дней с даты ее получения Банком.

11.3 В случае изменения положений законодательства Российской Федерации, при которых положения настоящего Регламента противоречат положениям законодательства, к таким правоотношениям Сторон подлежат применению положения законодательства Российской Федерации. В случае признания какого-либо условия настоящего Регламента недействительным, это не влечет недействительности Регламента в целом и/или любых иных положений настоящего Регламента. Взамен недействительного положения к правоотношениям Сторон подлежат применению нормы законодательства Российской Федерации.

11.4 Банк вправе в одностороннем, внесудебном порядке вносить изменения в настоящий Регламент и/или приложения к нему. Изменения в Регламент вступают в силу и подлежат применению к правоотношениям Сторон

and the Bank's requirements, as well as bear the risk of occurrence of any legal and/or financial consequences, including those unfavourable for the Client, the Bank and other persons, related to such violation/ improper fulfillment.

11 FINAL PROVISIONS

11.1. The Rules have been prepared in Russian and English. In the event of any discrepancies, the Russian language version of these Rules shall take precedence.

11.2. Legal relations of the Parties settled by these Rules, as well as any other legal relations of the Parties related to the implementation of these Rules, shall be settled and interpreted in accordance with the legislation of the Russian Federation. In case any of the Parties refuses to execute the decision of the Conciliation Commission, all disputes and disagreements shall be settled in accordance with this paragraph. All disputes arising between the Client and the Bank within the framework of execution of these Rules or in connection therewith are settled in accordance with the legislation of the Russian Federation, by negotiations, and in case of impossibility of such decision in the Arbitration Court of the Republic of Tatarstan. The Client may apply to the Bank with a written claim signed by the Client's Authorized Person and sealed by the latter (if any) by applying to the Bank's office at its legal address. Written pre-trial settlement procedure of disputes with the Bank under these Rules is mandatory. The deadline for replying to a pre-trial claim is 30 (thirty) days from the date of its receipt by the Bank.

11.3. In the event of changes in the provisions of the legislation of the Russian Federation in which the provisions of these Rules contradict the provisions of the legislation, the provisions of the legislation of the Russian Federation shall apply to such legal relations of the Parties. This shall not entail the invalidity of the Rules as a whole and/or any other provisions of the Rules in the event of invalidity of any provision of these Rules. The provisions of the Russian Federation legislation shall be applied to the legal relations of the Parties in lieu of the invalid provision.

11.4. The Bank may unilaterally and extrajudicially amend these Rules and/or their annexes. Amendments to these Rules goes into effect and are applicable to the legal relations of the Parties after 10 (ten) calendar days from the date of publishing such amendments or a new version of these Rules on the website: https://131.ru/contracts or informing the Client of such amendments in any other way available to the Bank. Prior to each interaction with the Bank, using the RBS System, including sending any Electronic Document to

по истечении 10 (Десяти) календарных дней с момента размещения таких изменений или новой редакции Регламента на ресурсе: https://131.ru/contracts или доведения до сведения Клиента таких изменений любым иным доступным Банку способом. До начала каждого взаимодействия с Банкам, с использованием Системы ДБО, в том числе направления в адрес Банка любого Электронного документа, а также не реже одного раза в 10 (Десять) календарных дней, Клиент и его Уполномоченные Представители обязаны знакомиться с настоящими Регламентом, а также изменениями в нем. Не ознакомление или несвоевременное ознакомление Клиента и/или его Уполномоченных Представителей с изменениями, внесенными в настоящий Регламент, не является основанием для их неприменения к правоотношениям Сторон. В случае несогласия Клиента с изменениями в Регламент, последний вправе расторгнуть Договор «Интернет-Клиент», в порядке и на условиях, указанных в Правилах, если иное не указано в отдельном соглашении Сторон, письменно уведомив об этом Банк не позднее даты вступления таких изменений в силу, согласно настоящему Регламенту. В случае неполучения Банком, до вступления в силу изменений в Регламент письменного уведомления Клиента о расторжении Договора «Интернет-Клиент», изменения считаются безоговорочно принятыми Клиентом, заключение дополнительных соглашений Сторонами не требуется.	the Bank, and at least once every 10 (ten) calendar days, the Client and its Authorized Persons are obliged to familiarize themselves with these Rules, as well as with any amendments thereto. Failure to familiarize or untimely familiarization of the Client and/or his Authorized Persons with the amendments made to these Rules shall not be the basis for their non-application to the legal relations of the Parties. In case the Client does not agree with the amendments to these Rules, the latter has the right to terminate the Internet-Client Agreement in the manner and on the terms specified in the Rules, unless otherwise specified in a separate agreement of the Parties, by notifying the Bank in writing not later than the effective date of such amendments according to these Rules. If the Bank does not receive a written notice from the Client on termination of the Internet-Client Agreement prior to entry into force of amendments to these Rules, the amendments shall be deemed to have been unequivocally accepted by the Client and no additional agreements shall be entered into by the Parties.

Приложение №1 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

ООО «Банк 131»
420012, РФ, Республика Татарстан,
г. Казань, ул. Некрасова, д. 38
ИНН/ОГРН 1655415696/1191690025746

Заявление[4] №_____

о присоединении к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

«____»_____20__г.

Я, _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта)
_____
(кем и когда выдан)

Действующий на основании _____

От имени Клиента _____, регистрационный №/ОГРН _____

настоящим сообщаю ООО «Банк 131» что полностью и безусловно соглашаюсь с Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО (далее – Регламент), ознакомлен и согласен с Регламентом, включая его приложения, и обязуюсь соблюдать все положения Регламента при использовании Системы ДБО.

Прошу зарегистрировать меня в Системе ДБО ООО «Банк 131» и:

□ выдать ФКН Рутокен и *выпустить Сертификат ключа проверки электронной подписи согласно разделу 4 Регламента;*

□ *выдать простую Электронную подпись* и установить Абонентский номер, на который необходимо направлять Логин и Временный Пароль для доступа в Систему ДБО, а также Средства подтверждения - + 7 (____)_____.

Прошу установить следующую кодовую информацию:
вопрос:_____ ответ: _____

Уведомления о совершенных операциях прошу направлять:

☐ по адресу электронной почты:_____

☐ на Абонентский номер: + 7 (____)_____

Настоящим подтверждаю, что указанные в настоящем заявлении Абонентский номер и адрес электронной почты принадлежат исключительно и только мне, иные лица не имеют доступа к ним.

С Приложениями №6,7 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО ознакомлен и согласен, обязуюсь выполнять требования, указанные в них.

Уполномоченное лицо Клиента: _____ _____ *« ____» _____ 20 ___ г.*
(подпись) (расшифровка подписи)

МП

Заполняется Банком

Идентификация Уполномоченного лица Клиента проведена, полномочия и документы проверены, Заявление принято:
_____ _____ _____ « ___» ___ 20 __ г.
(должность) (подпись) (расшифровка подписи.)
Отметка об исполнении:
Заявление выполнено, присвоен № _____ **:**
_____ _____ _____ « ___» ___ 20 __ г.
(должность) **МП.** (подпись) (расшифровка подписи.)

Annex 1 to the Rules of Remote Banking Service in

[4] Номер Заявления присваивается после регистрации Уполномоченного Представителя Клиента в реестрах Системы ДБО.

the ‘Banking App’ system for Bank 131 LLC Corporate Clients / Приложение №1 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

Bank 131 LLC (Bank)
Nekrasova 38, Kazan, Republic of Tatarstan, 420012
INN/OGRN 1655415696/1191690025746

Application[4] No.
on joining the Rules on Remote Banking service in the ‘Banking App’ system for Bank 131 LLC corporate clients /
Заявление №_____
о присоединении к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

_____ _____20__.

I / Я, _____
(full name)
_____
(passport series and number)
_____
(authority issued the passport and date of the issue)

Acting on the basis of / Действующий на основании _____
On behalf of the Client / От имени Клиента_____,
registration No. / регистрационный № _____

I hereby inform Bank 131 LLC that I fully and unconditionally agree with the Rules on Remote Banking Service in the ‘Banking App’ system for Bank 131 LLC corporate clients (hereinafter referred to as the Rules), have read and agree with the Rules, including their annexes, and will comply with all the provisions of the Rules when using the RBS system.

I hereby request to register me in the RBS System of Bank 131 LLC and:

/настоящим сообщаю ООО «Банк 131» что полностью и безусловно соглашаюсь с Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО (далее – Регламент), ознакомлен и согласен с Регламентом, включая его приложения, и обязуюсь соблюдать все положения Регламента при использовании Системы ДБО.

Прошу зарегистрировать меня в Системе ДБО ООО «Банк 131» и:

☐ issue Rutoken FKM and issue an electronic signature verification key certificate in accordance with Section 4 of the Rules; / выдать ФКН Рутокен и выпустить Сертификат ключа проверки электронной подписи согласно разделу 4 Регламента;

☐ issue a simple Electronic Signature and set a Subscriber Number to which the Login and Temporary Password to access the RBS System as well as Confirmation Means - + 7 (____)_____./ выдать простую Электронную подпись и установить Абонентский номер, на который необходимо направлять Логин и Временный Пароль для доступа в Систему ДБО, а также Средства подтверждения - + 7 (____)_____.

I hereby request to set the following code information / Прошу установить следующую кодовую информацию:

Question / вопрос: _____ answer / ответ: _____

I hereby request to send notifications of transactions / Уведомления о совершенных операциях прошу направлять:

☐ at e-mail address: / по адресу электронной почты: _____.

☐ to the Subscriber number: / на Абонентский номер: + 7 (____)_____.

I hereby confirm that the Subscriber number and e-mail address specified in this application belong exclusively and only to me, other persons have no access to them.

I will comply with the requirements specified in Appendices No. 6, 7 to the Rules on Remote Banking Service in the ‘Banking App’ system for Bank 131 LLC corporate clients have been read and agreed. / Настоящим подтверждаю, что указанные в настоящем заявлении Абонентский номер и адрес электронной почты принадлежат исключительно и только мне, иные лица не имеют доступа к ним.

С Приложениями №6,7 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО ознакомлен и согласен, обязуюсь выполнять требования, указанные в них.

Authorised Represenr of the Client:
/ Уполномоченное лицо Клиента: _____ _____ ____ _____ *20* ___ .
(signature) (printed)

Seal (if any)

To be filled in by the Bank / Заполняется Банком

Идентификация Уполномоченного лица Клиента проведена, полномочия и документы проверены, Заявление принято:
_____ _____ _____ « ___» ___ 20 __ г.
(должность) (подпись) (расшифровка подписи.)
Отметка об исполнении:
Заявление выполнено, присвоен № _____ **:**
_____ _____ _____ « ___» ___ 20 __ г.
(должность) **МП.** (подпись) (расшифровка подписи.)

[4] The Application number is assigned after the Client's Authorized Person has been registered in the registers of the RBS System. / Номер Заявления присваивается после регистрации Уполномоченного Представителя Клиента в реестрах Системы ДБО.

Приложение №2 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

АКТ № ___
приема-передачи ФКН Системы ДБО

г. Казань «___» 20__ г.

ООО «Банк 131», именуемое в дальнейшем Банк в лице _____, действующего на основании _____ с одной стороны, и _____ , именуемое в дальнейшем «Клиент», в лице_____, действующего на основании _____, с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», в рамках «Регламента дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО» (заявление о присоединении №_____ от ___ _____ 20__ г.), составили настоящий Акт о нижеследующем:

Банком передан, а Клиентом принят Конверт с персональным (-и) отчуждаемым (-и) носителем (-ми), предназначенным (-ми) для хранения и использования усиленной неквалифицированной Электронной подписи (далее- ФКН), целостность которого не нарушена, с целью использования Системы ДБО в соответствии с Правилами комплексного банковского обслуживания юридических лиц в ООО «Банк 131» и Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО:

п/п	ФИО (Уполномоченного лица клиента)	ФКН
1.		электронный ключ Рутокен «Рутокен ЭЦП 2.0» №_____
2.		электронный ключ Рутокен «Рутокен ЭЦП 2.0» №_____
…		

Передал
ООО «Банк 131»
420012, Республика Татарстан,
г. Казань, ул. Некрасова, д. 38
ИНН/ОГРН 1655415696/1191690025746

от Банка:

_____
(должность)

_____ _____
(подпись) (расшифровка подписи)

Принял
Наименование
Адрес
ИНН/ОГРН(рег. №)

от Клиента:

_____
_
(должность) М.П.

_____ _____
(подпись) (расшифровка подписи)

Annex 2 to the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients / Приложение №2 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

Acceptance and Delivery Certificate No.
of FKM of the RBS Systems /
АКТ № ___
приема-передачи ФКН Системы ДБО

Kazan _____20 _

Bank 131 LLC, hereinafter referred to as the Bank represented by / ООО «Банк 131», именуемое в дальнейшем Банк в лице _____ _____acting under / действующего на основании _____on the one part, / с одной стороны, и _____ _____hereinafter referred to as the Client represented by / именуемое в дальнейшем «Клиент», в лице _____, acting under / действующего на основании _____ on the other part, referred together herein as Parties and individually as a Party, within the scope of the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients (Application on joining No. _____ dated _____ _____20____), have drawn up this Act as follows: / с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», в рамках «Регламента дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО» (заявление о присоединении №_____ от ___ _____ 20__ г.), составили настоящий Акт о нижеследующем:

The Bank has transferred, and the Client has accepted an Envelope with the personal alienated carrier(s) intended for storage and use of the enhanced non-certified Electronic Signature (hereinafter referred to as the FKM), the integrity of which has not been violated, for the purpose of using the RBS system in accordance with the Rules of Integrated Banking Service for Bank 131 LLC corporate clients and the Rules of remote banking service for Bank 131 LLC corporate clients: / Банком передан, а Клиентом принят Конверт с персональным (-и) отчуждаемым (-и) носителем (-ми), предназначенным (-ми) для хранения и использования усиленной неквалифицированной Электронной подписи (далее- ФКН), целостность которого не нарушена, с целью использования Системы ДБО в соответствии с Правилами комплексного банковского обслуживания юридических лиц в ООО «Банк 131» и Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО:

n/a	Full name (Client Authorized person) / ФИО (Уполномоченного лица клиента)	FKM / ФКН
1.		Rutoken ES 2.0 electronic key No. _____
2.		Rutoken ES 2.0 electronic key No. _____
…		

Transferred to
Bank 131 LLC (Bank)
Nekrasova 38, Kazan, Republic of Tatarstan, 420012
INN/OGRN 1655415696/1191690025746

from the Bank:

_____
(title)

_____
(signature)

Accepted
Name
Address
INN/OGRN (reg. No.)

from the Client:

_____
(title)_ Seal (if any)

_____
(signature)

Приложение №3 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

Заявление
о смене логина и/или статического пароля /разблокировку доступа в системе ДБО

г. Казань **«___» _____20__ г.**

Наименование Клиента: _____
(полное фирменное наименование юридического лица)
в лице _____
(должность, ФИО полностью)
действующего на основании _____
(устава, доверенности или иного документа с указанием реквизитов)
ИНН: _____, ОГРН/регистрационный № _____

В соответствии с Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО прошу:

☐ – разблокировать доступ в Систему ДБО, с использованием ранее предоставленных данных для доступа (с условиями и причинами блокировки согласен, претензий к ООО «Банк 131» не имею);

☐ – произвести смену ☐логина ☐ статического пароля и направить данные для входа в систему ДБО на мой Абонентский номер

для указанных Уполномоченных Представителей Клиента:

Ф.И.О. Уполномоченного лица	Данные документа, удостоверяющего личность

Настоящим подтверждаю, что указанный в настоящем заявлении Абонентский номер принадлежит исключительно и только мне, иные лица не имеют доступа к нему.

_____ /_____/«___» _____20___г /
(Подпись) (ФИО) (Дата)

М.П.

Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены, Заявление зарегистрировано в Банке «____» _____ 20__ г. № _____
Работник Банка, принявший заявление:

_____ _____ _____
(должность) (подпись) (расшифровка подписи.)
Отметка об исполнении:
Ответственный работник Банка**:**

_____ _____ _____
(должность) (подпись) (расшифровка подписи.)
М.П.

Appendix 3 to the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients / Приложение №3 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

Application
on login and/or static password change / unlocking RBS system access
/ Заявление
о смене логина и/или статического пароля /разблокировку доступа в системе ДБО

Kazan **_____ _____ 20____**

Name of the Client: / Наименование Клиента: _____
(full corporate name of the legal entity)
presented by / в лице _____
(title, full name)
acting under / действующего на основании _____
(articles of association, power of attorney or other document with reference details)
registration No. / регистрационный № _____

In accordance with the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients, I hereby request to: / В соответствии с Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО прошу:

☐ - unblock access to the RBS System using previously provided access data (agree with the terms and ground for the blocking, no claims against Bank 131 LLC); / – разблокировать доступ в Систему ДБО, с использованием ранее предоставленных данных для доступа (с условиями и причинами блокировки согласен, претензий к ООО «Банк 131» не имею);

☐ - switch ☐login ☐ static password and send the RBS system login data to my Subscriber number / произвести смену ☐логина ☐ статического пароля и направить данные для входа в систему ДБО на мой Абонентский номер

for these Authorized Persons of the Client:

Full name of the Authorized Person / Ф.И.О. Уполномоченного лица	Identity document data / Данные документа, удостоверяющего личность

I hereby confirm that the Subscriber number specified in this application belongs exclusively and only to me, other persons have no access to it. / Настоящим подтверждаю, что указанный в настоящем заявлении Абонентский номер принадлежит исключительно и только мне, иные лица не имеют доступа к нему.

_____/_____ /____ _____20___ /
(Signature) (Full name) (Date)

Seal (if any)

To be filled in by the Bank / Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены, Заявление

зарегистрировано в Банке «____» _____ 20__ г. № _____

Работник Банка, принявший заявление:

_____ _____ _____

(должность) (подпись) (расшифровка подписи.)

Отметка об исполнении:

Ответственный работник Банка**:**

_____ _____ _____

(должность) (подпись) (расшифровка подписи.)

М.П.

Приложение №4 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

ЗАЯВЛЕНИЕ
на изменение абонентского номера мобильной связи

Наименование Клиента: _____
(полное фирменное наименование юридического лица)
в лице _____
(должность, ФИО полностью)
действующего на основании _____
(устава, доверенности или иного документа с указанием реквизитов)
ИНН: _____, ОГРН/регистрационный № _____

В соответствии с Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО прошу установить новый Абонентский номер, на который прошу направлять Логин и Временный пароль для доступа в Систему ДБО, прохождения процедуры аутентификации и подтверждения Электронных документов при ее использовании, для указанных Уполномоченных лиц:

Ф.И.О. Уполномоченного лица	Данные документа, удостоверяющего личность	Абонентский номер мобильного устройства
		+7 (____) _____

Настоящим подтверждаю, что указанный в настоящем заявлении Абонентский номер принадлежит исключительно и только мне, иные лица не имеют доступа к нему._

_____ /_____/«___» _____20___г /
(Подпись) (ФИО) (Дата)

М.П.

Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены
Заявление зарегистрировано в Банке «____» _____ 20__ г. № _____
Работник Банка, принявший заявление:

_____ _____ _____
(должность) (подпись) (расшифровка подписи.)

Отметка об исполнении:
Ответственный работник Банка**:**

_____ _____ _____
(должность) (подпись) (расшифровка подписи.)

М.П.

Annex 4 to the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients / Приложение №4 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

NOTICE
on subscriber number of mobile communication change /
ЗАЯВЛЕНИЕ
на изменение абонентского номера мобильной связи

Name of the Client: / Наименование Клиента: _

_____

(full corporate name of the legal entity)
presented by / в лице

_____

(title, full name)
acting under / действующего на основании

_____

(articles of association, power of attorney or other document with reference details)
registration No. / регистрационный № _____

In accordance with the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients, I hereby request to establish a new Subscriber number with its Login and Temporary password for access to the RBS System, for passing the procedure of authentication and confirmation of Electronic documents when using it, for the specified Authorized persons: / В соответствии с Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО прошу установить новый Абонентский номер, на который прошу направлять Логин и Временный пароль для доступа в Систему ДБО, прохождения процедуры аутентификации и подтверждения Электронных документов при ее использовании, для указанных Уполномоченных лиц:

Full name of the Authorized Person / Ф.И.О. Уполномоченного лица	Identity document data / Данные документа, удостоверяющего личность	Mobile device subscriber Number / Абонентский номер мобильного устройства
		+7 (____)

I hereby confirm that the Subscriber number specified in this application belongs exclusively and only to me, other persons have no access to it. / Настоящим подтверждаю, что указанный в настоящем заявлении Абонентский номер принадлежит исключительно и только мне, иные лица не имеют доступа к нему._

_____/_____/ ___ _____ 20__
(Signature) (Full name) (Date)

Seal (if any)

To be filled in by the Bank / Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены Заявление зарегистрировано в Банке «____» _____ 20__ г. № _____

Работник Банка, принявший заявление:

_____ _____ _____
(должность) (подпись) (расшифровка подписи.)

Отметка об исполнении:

Ответственный работник Банка**:**

_____ _____ _____
(должность) (подпись) (расшифровка подписи.)

М.П.

Приложение №5 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

УВЕДОМЛЕНИЕ

о компрометации ключа Электронной подписи

(прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании Системы ДБО без согласия Клиента)

г. Казань «__»_____20__г.

Наименование Клиента: _____

(полное фирменное наименование юридического лица)

в лице _____

(должность, ФИО полностью)

действующего на основании _____

(устава, доверенности или иного документа с указанием реквизитов)

ИНН: _____, ОГРН/регистрационный № _____

в соответствии с Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО, настоящим уведомляет ООО «Банк 131» о Компрометации Электронной подписи в связи с

_____

_____

_____

_____

(*дата Компрометации ЭП/утраты ЭСП и (или) его использования без согласия Клиента, обстоятельства такой компрометации/утраты и (или) такого использования, подтверждения (при наличии) такой компрометации/утраты и (или) такого использования*)

Прошу с «____» _____20__г. заблокировать указанные ниже Средства подтверждения, использовавшиеся в рамках «Регламента дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО» согласно заявлению о присоединении № _____ от «__»_____20__г., и остановить обработку Электронных документов, подписанных/подтвержденных указанными средствами:

Сертификаты ключей Электронной подписи, содержащие следующие ключи Электронной подписи :

Ф.И.О. владельца – Уполномоченного лица	Идентификатор ключа проверки Электронной подписи	Номер Рутокена

Абонентский номер мобильной связи:

Ф.И.О. владельца-Уполномоченного лица	Абонентский номер мобильного устройства

_____ _____ (_____)
(должность) (подпись) (Ф.И.О.)

М.П.

Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены
Заявление зарегистрировано в Банке «____» _____ 20__ г. № _____
Работник Банка, принявший заявление:

_____ _____ _____
(должность) (подпись) (расшифровка подписи.)

Отметка об исполнении:
Ответственный работник Банка**:**

_____ _____ _____
(должность) (подпись) (расшифровка подписи.)

М.П.

Annex No. 5 to the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients / Приложение №5 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

NOTICE
on compromising the key of the Electronic Signature (termination of the means of confirmation and/or loss of the means of confirmation and/or use of the RBS System without the consent of the Client) / УВЕДОМЛЕНИЕ
о компрометации ключа Электронной подписи (прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании Системы ДБО без согласия Клиента)

Kazan ___ _____20__

Name of the Client: / Наименование Клиента:

_____

(full corporate name of the legal entity)
presented by / в лице

_____

(title, full name)
acting under / действующего на основании

_____

(articles of association, power of attorney or other document with reference details)
registration No. / регистрационный № _____

In accordance with the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients hereby notifies Bank 131 LLC on the Electronic Signature Compromise in connection with / в соответствии с Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО, настоящим уведомляет ООО «Банк 131» о Компрометации Электронной подписи в связи с

_____
_____
_____
_____

(*date of ES Compromising/Loss of ES and/or its use without the Client's consent, circumstances of such Compromising/Loss and/or such use, confirmation (if any) of such Compromising/Loss and/or such use) / (дата Компрометации ЭП/утраты ЭСП и (или) его использования без согласия Клиента, обстоятельства такой компрометации/утраты и (или) такого использования, подтверждения (при наличии) такой компрометации/утраты и (или) такого использования)*

I hereby request to block Means of Confirmation noted below that were used within the scope of Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients since ____ _____ 20__ and stop the Electronic Documents processing that were signed/confirmed by the mentioned means:

Electronic Signature Key Certificates containing the following Electronic Signature Keys:

/ Прошу с «____» _____20__г. заблокировать указанные ниже Средства подтверждения, использовавшиеся в

рамках «Регламента дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО» согласно заявлению о присоединении № _____ от «__»_____20__г., и остановить обработку Электронных документов, подписанных/подтвержденных указанными средствами: Сертификаты ключей Электронной подписи, содержащие следующие ключи Электронной подписи :

Full name of the owner - Authorized person / Ф.И.О. владельца – Уполномоченного лица	Identifier of the electronic signature verification key / Идентификатор ключа проверки Электронной подписи	Rutoken No. / Номер Рутокена

Subscriber mobile phone number: / Абонентский номер мобильной связи:

Full name of the owner, the authorized person / Ф.И.О. владельца-Уполномоченного лица	Subscriber number of the mobile device / Абонентский номер мобильного устройства

(title) (signature) (printed)

Seal (if any)

To be filled in by the Bank / Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены Заявление зарегистрировано в Банке «____» _____ 20__ г. № _____

Работник Банка, принявший заявление:

_____ _____ _____

(должность) (подпись) (расшифровка подписи.)

Отметка об исполнении:

Ответственный работник Банка:

_____ _____ _____

(должность) (подпись) (расшифровка подписи.)

М.П.

Приложение №6 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

Инструкция по обеспечению информационной безопасности при работе в Системе ДБО

В целях обеспечения информационной безопасности при работе в Системе дистанционного банковского обслуживания ООО «Банк 131», Клиент обязан:

1. При осуществлении доступа к Системе ДБО, необходимо удостовериться в правильности указанного адреса в адресной строке браузера (https://online.131.ru/) и наличии значка защищенного соединения (замок), исключая выход на сайты, внешне маскирующиеся под Систему ДБО.
2. Ключи Электронной подписи (далее по тексту – ЭП) хранить только на ФКН (Функциональный ключевой носитель) в недоступном для посторонних и неуполномоченных лиц месте (запирающиеся персональный сейф, металлический шкаф).
3. Не допускается:
- снимать копии с ФКН;
- передавать ФКН лицам, к ним не допущенным;
- записывать на ФКН постороннюю информацию.
4. Не использовать в качестве Статического 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/Уполномоченного Представителя Клиента.
5. Статический пароль должен:
- быть не менее 8 символов;
- содержать цифры, строчные и заглавные буквы;
- содержать хотя бы 1 символ, не являющийся буквой или цифрой.
6. На персональном компьютере (ноутбуке) должна быть установлена парольная защита на вход в Операционную систему.
7. Рекомендуется менять пароль пользователя в операционной системе, а также в Системе ДБО не реже одного раза в 3 месяца.
8. Пароль доступа к ключу ЭП хранить отдельно от ФКН .

Annex 6 to the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients

Instruction to ensure information security when working in the RBS System

In order to ensure information security when working in the Remote Banking System of Bank 131 LLC, the Client shall:

1. When accessing the RBS System, it is necessary to make sure that the address specified in the browser address bar (https://online.131.ru/) is correct and that the secure connection icon (lock) is present, excluding access to sites externally masquerading as RBS.
2. The Electronic Signature Keys (hereinafter referred to as ESK) shall only be stored on the FKM (Functional Keystock Medium) in a place that is inaccessible to unauthorized and unauthorized persons (lockable personal safe, metal cabinet).
3. Not allowed:
   - take copies from the FKM;
   - to hand over the FKM to persons who are not allowed to access them;
   - to write down relevant information to the FKM.
4. Do not use as a Static Password:
   - character sequences consisting of the same digits (including dates, phone numbers, car numbers, etc.);
   - sequences of repetitive letters or numbers;
   - consecutive keyboard layouts or alphabetical characters;
   - names and surnames;
   - INN or other details of the Client/Authorized Representative of the Client.
5. Static password must:
   - be at least 8 symbols;
   - contain numbers, lowercase and uppercase letters;
   - contain at least 1 symbol, which is not a letter or number.
6. A password protection for accessing the Operating System must be installed on the personal computer (laptop).
7. It is recommended to change the user password in the operating system as well as in the RBS System at least once every 3 months.
8. The password for accessing the ES key should be stored separately from the FCN .
9. It is strictly prohibited to write down passwords on

9. Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в доступных третьим лицам местах, передавать неуполномоченным лицам.
10. Подключать ФКН, содержащий ключ ЭП, только в момент использования Системы ДБО и подписания Электронных документов. Не оставлять ФКН, содержащий ключ ЭП, постоянно подключенным к компьютеру.
11. Не использовать ФКН, содержащий ключ ЭП, для каких-либо других целей, в частности, не хранить на нём информацию произвольного содержания, не относящегося к работе с Системой ДБО.
12. Не копировать содержимое ФКН, содержащего ключ ЭП, и не передавать его никому даже на короткое время.
13. Закончив работу в Системе ДБО или прервав её (даже на несколько минут), извлечь ФКН, содержащий ключ ЭП, и убрать его в недоступное другим лицам место.
14. Применять на рабочем месте лицензионные средства защиты от вредоносного кода с возможностью автоматического обновления баз данных сигнатур вредоносного кода.
15. Если в качестве компьютера для работы в Системе ДБО используется переносной компьютер (ноутбук), должно быть исключено его подключение к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.)
16. Осуществлять постоянный контроль отправляемых платежных (расчетных) документов при работе с Системой ДБО, а также за состоянием расчетных (банковских) счетов, операциям по ним и остаткам.
17. В случае выявления признаков Компрометации ЭП или выявления вредоносного кода в компьютере, используемом для работы в Системе ДБО, необходимо немедленно уведомить Банк по телефонам: 8 (843) 5983131с 9 часов 00 минут до 18 часов 00 минут (в рабочие дни), либо лично явиться в Банк с целью блокирования скомпрометированных ключей ЭП с последующей их заменой. К событиям, связанным с Компрометацией ЭП, в том числе, относятся:

– утрата функциональных ключевых носителей, с последующим обнаружением или без такового;

– нарушение правил хранения, использования и уничтожения (в том числе после окончания срока действия) ключа Электронной подписи (усиленной неквалифицированной);

– утеря, передача и/или предоставлением доступа неуполномоченным третьим лицам к аппаратным средствам (в том числе мобильным

paper or in text files at the workplace, to leave them available to third parties or to pass them on to unauthorised persons.
10. Connect the FCN containing the ES key only at the moment when the RBS System is used and the Electronic Documents are signed. Do not leave the FKM containing the ES key permanently connected to the computer.
11. Do not use the FKM containing the ES key for any other purposes, in particular, do not store any arbitrary information on it that does not relate to the operation of the RBS system.
12. Do not copy the contents of the FKM containing the ES key or pass it on to anyone, even for a short time.
13. After completing or interrupting work in the RBS system (even for a few minutes), extract the FKM containing the ES key and remove it to an area inaccessible to others.
14. Apply licensed anti-malware at the workplace with the possibility of automatically updating malware signature databases.
15. If a portable computer (laptop) is used as a computer for work in the RBS System, its connection to public networks in places with free Internet access (office centres, cafes, etc.) must be excluded.
16. Constantly monitor the payment (settlement) documents sent out when working with the RBS System, as well as the status of settlement (bank) accounts, transactions and balances.
17. In the event of signs of ES Compromisation or detection of malicious code in the computer used to operate the RBS System, the Bank must be notified immediately by telephone: 8 (843) 5983131 from 9:00 AM to 6:00 PM (on business days), or to come to the Bank in person to block compromised ES keys with their subsequent replacement. Among other things, events related to ES Compromised include:

- loss of functional keystock media, with or without subsequent detection;

- violation of the rules for storage, use and destruction (including after the expiry date) of the Electronic Signature key (enhanced non-certified);

- loss, transfer and/or granting access to hardware (including mobile phones or other) and/or a SIM card with a Subscriber number to unauthorised third parties, including that used to send the Temporary and/or One-time password;

- there are suspicions that the Electronic Document Validation Tools have become known to unauthorised third parties;

телефонам или иным) и/или SIM-карте с Абонентским номером, в том числе который используется для направления Временного и/или Одноразового пароля; – наличие подозрений, что Средства подтверждения Электронного документа стали известны неуполномоченным третьим лицам; – возникновение подозрений на утечку информации или ее искажение; – несанкционированное копирование или подозрение на копирование Временного, Статического и/или Одноразового пароля, функционального ключевого носителя, аппаратного средства и/или SIM-карты с Абонентским номером; – прекращение полномочий или увольнение Уполномоченных лиц, имеющих доступ к Средству подтверждения; – случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц, другие виды разглашения ключевой информации).	- suspicion of information leakage or misrepresentation; - unauthorised copying or suspicion of copying a Temporary, Static and/or One-time password, functional key media, hardware and/or SIM card with a Subscriber number; - termination of powers or dismissal of the Authorised Persons who have access to the Confirmation Tool; - cases where it is impossible to establish reliably what happened to the media containing key information (including cases where the media failed and the possibility that this fact occurred as a result of unauthorised actions of third parties and other types of disclosure of key information was not proved).
18. При обнаружении несанкционированных доступов в Систему ДБО, платежных и иных операций в Системе ДБО, Компрометации или подозрении на Компрометацию ЭП немедленно уведомить Банк и направить «Уведомление о компрометации» в порядке, установленном «Регламентом дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием Системы ДБО», а также обратиться с соответствующим заявлением в правоохранительные органы.	18. In case of detection of unauthorized access to the RBS System, payment and other transactions in the RBS System, compromise or suspicion of ES Compromise, immediately notify the Bank and send the Notice of Compromise in accordance with the procedure established by the Regulation on remote banking service of legal entities in Bank 131 LLC using the RBS system, as well as to apply to law enforcement agencies.
19. Запрещено восстанавливать работоспособность поврежденного компьютера до проведения технической экспертизы. Работу с Системой ДБО разрешено проводить только после новой установки операционной системы с форматированием жестких дисков и после смены всех ключей ЭП клиента.	19. It is forbidden to restore the functionality of a damaged computer before a technical examination is carried out. Work with the RBS System may only be performed after a new installation of the operating system with hard disk formatting and after all the client's ES keys have been changed.
20. Использовать комбинации клавиш «Ctrl + Alt + Del» для идентификации пользователя в операционной системе.	20. Use the key Ctrl + Alt + Del combination to identify the user in the operating system.
21. Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы по Системе ДБО, заблокировать 3389 (RDP Remote desktop).	21. Disable the possibility of remote and terminal connection to computers used for RBS System, block 3389 (RDP Remote desktop).
22. Включить в операционной системе журнал	22. Enable the Windows security log in the operating system.

безопасности Windows. 23. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д. (далее по тексту – ПО). 24. Обеспечить возможность своевременного обновления системного и прикладного ПО. 25. Доступ в помещение, где размещен компьютер с Системой ДБО, предоставлять только Уполномоченным лицам. 26. 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. 27. Исключить доступ к компьютерам, используемым для работы по Системе ДБО, посторонних лиц и персонала, неуполномоченных на работу в Системе ДБО и/или обслуживание компьютеров. 28. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями. 29. ООО «Банк 131» не осуществляет рассылку электронных писем с просьбой прислать ключи ЭП и/или пароль к Системе ДБО и никогда не запрашивает у вас эту информацию. 30. Банк не осуществляет звонков, рассылку сообщений по электронной почте, СМС сообщений, или иными способами, с просьбой сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.). При получении такого запроса ни при каких обстоятельствах не сообщайте данную информацию и немедленно сообщите об этом в Банк.	23. Use only licensed such software as operating systems, anti-malware, office packages, etc. (hereinafter referred to as software). 24. Ensure that system and application software can be updated in a timely manner. 25. Access to the premises where the computer with the RBS System is located shall be granted only to the Authorised Persons. 26. It is recommended the computer from which electronic documents are prepared and sent to the Bank be singled out as a separate network segment with obligatory exclusion of the computer from the customer's common local network. 27. Exclude access to computers used to operate the RBS system, unauthorised persons and personnel not authorized to work in the RBS system and/or maintain computers. 28. IT staff must ensure that they have control over the actions they take when servicing the computer. 29. Bank 131 LLC does not send e-mails requesting to send ES keys and/or password to the RBS System and never asks you for this information. 30. The Bank does not make calls, send e-mails, SMS messages or any other means requesting confidential information (passwords, code words, etc.). If you receive such a request, do not provide this information under no circumstances and report it to the Bank immediately.

Приложение №7 к Регламенту дистанционного банковского обслуживания юридических лиц в ООО «Банк 131» с использованием системы ДБО

Требования к программно-техническим средствам для проведения расчетных операций в электронной форме

1. Требования к программно-техническим средствам (приобретаются Клиентом за собственный счет у третьих лиц):

1.1. При использовании ПЭП:

- Персональный компьютер с предустановленной операционной системой (ОС): Windows 7 и выше, MacOS, Linux;

- Интернет-браузер актуальной версии: Chrome 47 и выше / Firefox 44.0 и выше / Internet Explorer 10 и выше / Opera 36 и выше / Safari 9 и выше;

- доступ в сеть Интернет;

1.2. При использовании УНЭП:

- Персональный компьютер с портом USB и предустановленной операционной системой (ОС) Windows 7 и выше, MacOS[5];

- Интернет-браузер актуальной версии: Chrome 47 и выше / Firefox 44.0 и выше / Internet Explorer 10 и выше / Opera 36 и выше / Safari 9 и выше;

- доступ в сеть Интернет;

- принтер.

2. Для использования Системы ДБО с применением УНЭП необходим выделенный компьютер с предустановленной операционной системой семейства Microsoft Windows. Если, по желанию Клиента, установка Системы ДБО производится на компьютер с предустановленными ОС сторонних производителей, Банк не несет ответственности за работоспособность Системы ДБО.

При эксплуатации Системы ДБО запрещается:

- Установка программного обеспечения сторонних фирм, а также сознательное внесение изменений в файлы программного и информационного обеспечения Системы ДБО;
- Доступ к Системе ДБО неуполномоченных лиц;

Annex 7 to the Rules on Remote Banking Service in the 'Banking App' system for Bank 131 LLC corporate clients

Requirements for software and hardware tools to perform settlement operations electronically

1. Requirements for software and hardware (purchased by the Client at its own expense

from third parties):

1.1. When using Simple Electronic Signature:

- Personal computer with pre-installed operating system (OS): Windows 7 and newer, MacOS, Linux;

- Internet browser current version: Chrome 47 and newer / Firefox 44.0 and newer / Internet Explorer 10 and newer / Opera 36 and newer / Safari 9 and newer;

- Internet access;

1.2. When using ENCES:

- Personal computer with USB port and pre-installed operating system (OS) Windows 7 and newer, MacOS[5];

- Internet browser current version: Chrome 47 and newer / Firefox 44.0 and newer / Internet Explorer 10 and newer / Opera 36 and newer / Safari 9 and newer;

- Internet access;

- printer.

2. In order to use the RBS System with the use of ENCES, a dedicated computer with a pre-installed operating system of the Microsoft Windows family is required. If, at the Client's request, the RBS System is installed on a computer with pre-installed third-party operating systems, the Bank shall not be liable for the performance of the RBS System.

When operating the RBS System the following is prohibited:

- Installation of third-party software as well as conscious changes to the RBS system software and information files;
- Access to the RBS System by unauthorised persons;

При эксплуатации Системы ДБО Клиент обязан: ● Использовать систему ДБО только на исправном и проверенном на отсутствие компьютерных вирусов персональном компьютере (ноутбуке); ● Исключить возможность заражения компьютера с установленной Системой ДБО программными вирусами или другими вредоносными программами; ● Использовать только легальное и лицензионное программное обеспечение; ● Обеспечить техническую исправность оборудования, входящего в состав рабочего места Системы ДБО; ● Применять средства антивирусной защиты и обеспечить регулярное обновление антивирусных баз. Необходимость резервного копирования рабочего места пользователя Системы ДБО определяет Клиент и при необходимости осуществляет его собственными силами.	When operating the RBS System, the Client shall: ● Use the RBS system only on a personal computer (laptop) that is in good order and has been checked for absence of computer viruses; ● Eliminate the possibility of infecting a computer with software viruses or other malicious programs installed in the RBS System; ● Use only legal and licensed software; ● Ensure the technical serviceability of the equipment included in the RBS system workstation; ● Use anti-virus protection tools and ensure that the anti-virus databases are regularly updated. The need to back up the user workplace of the RBS System shall be determined by the Client and, if necessary, performed by the Client himself.
[5]Инструкция по работе с MacOS размещена на официальном сайте Банка.	[5]Instructions on working with MacOS are available on the Bank's official website.