Редакция №3 от «9» декабря 2024г.

РЕГЛАМЕНТ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ЮРИДИЧЕСКИХ ЛИЦ И ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ В АО «БАНК 131» С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДБО

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Регламенте дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с

Version No.3 of December, 09 2024

REGULATIONS ON REMOTE BANKING SERVICE IN THE BANKING APP SYSTEM FOR BANK 131 JSC CORPORATE CLIENTS AND INDIVIDUAL ENTREPRENEURS

1. TERMS AND DEFINITIONS

Regulations on Remote Banking Service in the ‘Banking App’ system for Bank 131 JSC Corporate

использованием Системы ДБО (далее - Регламент) используются термины и определения, указанные в Правилах комплексного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» (и приложениях к ним), далее – Правила, если иное не указано в настоящем Регламенте.	Clients and individual entrepreneurs (hereinafter referred to as Regulations) conform the terms and definitions specified in the Rules on Integrated Banking Service for Bank 131 JSC Corporate Clients (and their annexes), hereinafter referred to as the Rules, unless otherwise stated in these Regulations.
Активация ключа Мобильной подписи – процедура установления доверия мобильного устройства, используемого для доступа к подтверждению операций в Системе ДБО.	**Activation of the Mobile Signature Key** is a procedure for establishing the trust of a mobile device used to access confirmation of operations in the RBS System.
Временный пароль – пароль, который присваивается Банком Уполномоченному Представителю Клиента при его регистрации в Системе ДБО или смене аутентификационных данных, 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 or for authentication data changing 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 АО «Банк 131» с использованием Системы ДБО.	**Application** denotes application on joining the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC 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	**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 Regulations 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;

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).	- 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).
Клиент - юридическое лицо, за исключением кредитных организаций, зарегистрированное в соответствии с законодательством Российской Федерации или законодательством иностранного государства, индивидуальный предприниматель, занимающийся в установленном законодательством РФ порядке частной практикой, принимаемый на обслуживание и/или обслуживающийся в Банке в рамках договоров, предусматривающих обмен электронными документами.	**Client** is a legal entity, with the exception of credit institutions, registered in accordance with the legislation of the Russian Federation or the legislation of a foreign state, an individual entrepreneur engaged in private practice in accordance with the procedure established by the legislation of the Russian Federation, accepted for service and/or serviced by a Bank under agreements providing for the exchange of electronic documents.
Ключ Электронной подписи - уникальная последовательность символов, предназначенная для создания усиленной неквалифицированной Электронной подписи.	**The Electronic Signature key** is a unique sequence of symbols designed to create an enhanced non-certified Electronic Signature.
Ключ проверки Электронной подписи - уникальная последовательность символов, однозначно связанная с Ключом Электронной подписи и предназначенная для проверки подлинности усиленной неквалифицированной Электронной подписи.	**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.
Ключ Мобильной подписи – ключ Электронной подписи, используемый при подписании документов в Мобильной подписи.	**Mobile Signature Key -** the Electronic Signature key used when signing documents in the Mobile Signature.
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).	**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).
Мобильная подпись – мобильное приложение Банка, доступное для установки на мобильном устройстве (смартфон, планшет) с операционной системой Android или iOS, позволяющее Клиенту просматривать Электронные документы, подписанные усиленной неквалифицированной Электронной подписью в Системе ДБО, а также подтверждать совершенные Клиентом в Системе ДБО действия и операции. Создание, хранение ключей ЭП Мобильной подписи и формирование ЭП под Электронными документами выполняется на удаленном сервере Банка.	**Mobile Signature** is a mobile application of the Bank, available for installation on a mobile device (smartphone, tablet) with Android or iOS operating system, which allows the Client to view Electronic Documents signed by an enhanced unqualified Electronic Signature in the RBS System, as well as to confirm the actions and operations performed by the Client in the RBS System. The creation and storage of the Electronic signature keys of the Mobile Signature and the formation of the Electronic signature under the Electronic Documents is performed on a remote server of the Bank.

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 подписания Электронных документов простой Электронной подписью.	**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 signings of Electronic Documents using a simple electronic signature.
Оператор Удостоверяющего центра – работник Банка, уполномоченный на выдачу и отзыв сертификатов ключей Электронной подписи (усиленной неквалифицированной).	**Certification Centre Operator** is an employee of the Bank authorized to issue and recall Electronic Signature (Enhanced Non-Certified) Key Certificates.
Оператор Центра регистрации – работник Банка, уполномоченный на регистрацию Клиента/уполномоченного Представителя Клиента в Системе ДБО.	**Registration Centre Operator** is an employee of the Bank authorized to register the Client/Authorized Person of the Client in the RBS System.
Оператор ЭДО - российская организация, соответствующая требованиям, утвержденных Приказом ФНС России от 08.06.2021 N ЕД-7-26/546@ "Об утверждении Требований к оператору электронного документооборота", и осуществляющая деятельность по обеспечению электронного документооборота между Банком и Клиентом.	**EDM operator** is a Russian organization that meets the requirements established by the Order of the Federal Tax Service of Russia dated June 8, 2021, No. ED-7-26/546@ "On Approval of Requirements for the Electronic Document Management Operator" and is engaged in activities to ensure electronic document management between the Bank and the Client
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.	**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.
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 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 и Мобильной подписи.	**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 to be changed upon the first login to the RBS System. Static password shall be applied when using Simple Electronic Signature and Mobile Signature.
Простая электронная подпись (Простая ЭП, ПЭП) - аналог собственноручной подписи Клиента, представленный в виде Одноразового пароля	**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

(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.	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.
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.	**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.
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).	**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).
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.	**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.
Уполномоченный Представитель Клиента/Уполномоченное лицо – Представитель Клиента, в том числе Клиент - индивидуальный предприниматель, 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), или имеющий право на просмотр и получение Электронных документов, в том числе выписок по Счету (без права распоряжаться денежными средствами/совершения сделок от имени Клиента).	**Client Authorized Person/Authorised person** is the Client's representative including individual entrepreneurs 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) or or having the right to view and receive Electronic documents, including Account statements (without the right to dispose of funds/make transactions on behalf of the Client).
УНЭП (Усиленная неквалифицированная Электронная подпись) - Электронная подпись, которая:	**ENCES (Enhanced Non-Certified Electronic Signature)** is an electronic signature that:

- 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.

УКЭП – усиленная квалицированная электронная подпись, которая соответствует всем признакам УНЭП и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

Настоящий Регламент предусматривает направление заявлений, сообщений, необходимых для получения (восстановления) доступа, изменения условия использования Системы ДБО с использованием УКЭП внешнего аккредитованного удостоверяющего центра. УКЭП внешнего аккредитованного удостоверяющего центра используется в рамках обмена электронными документами через Оператора ЭДО.

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.

Утилита MobileSignVerify – программное обеспечение для проверки Мобильной подписи, разработчик ООО «Информационные системы».

PIN-код – четырехзначный код, используемый для доступа к Мобильной подписи. PIN-код устанавливается Уполномоченным Представителем Клиента при активации ключа Мобильной подписи.

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 Правил и Общих условий осуществления информационного взаимодействия с

-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.

EQES is enhanced qualified electronic signature that meets all the features of ENCES and the following additional features:

1) the electronic signature verification key is specified in the qualified certificate;

2) to create and verify an electronic signature, electronic signature tools are used that have received confirmation of compliance with the requirements established by Federal Law No. 63-FZ of 06.04.2011 "On Electronic Signature".

This Regulation provides for the sending of applications, messages necessary for registration, access, changes to the terms of use of the RBS System with using of the EQES of an external accredited certification center. The EQES of an external accredited certification center is used as part of the exchange of electronic documents through the EDM operator.

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.

The MobileSignVerify utility is software for verifying a Mobile signature, developed by Information Systems LLC.

PIN is a four-digit code used to access the Mobile Signature. The PIN is set by the Authorized Representative of the Client when activating the Mobile Signature key.

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 and essential part of the Rules and General Conditions for the implementation of information interaction using the

использованием Системы информационного обмена (Приложение №2 к Правилам).	Information Exchange System (Appendix No. 2 to the Rules)
2.3 Для подключения Клиента и Уполномоченного Представителя Клиента к Системе ДБО и ее использования Уполномоченный Представитель Клиента должен присоединиться к Правилам и Общим условиям осуществления информационного взаимодействия с использованием Системы информационного обмена, а также к настоящему Регламенту путем подписания Заявления, форма которого определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка.	2.3. In order for the Client and the Authorized Representative of the Client to connect to the Remote Banking System (RBS) and use it, the Authorized Representative of the Client must agree to the Rules and General Conditions for the implementation of information interaction using the Information Exchange System, as well as to this Regulation, by signing the Application, the form of which is determined by the Bank and is available on the website https://131.ru/contracts and at the Bank's office.
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.	2.4. 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 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.	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 Regulations (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 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.	2.6. The Client agrees that the Electronic Documents of the Parties within the framework of the 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 recognize 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 Клиент обязуется обеспечить допуск к работе и работу в Системе ДБО только Уполномоченных Представителей Клиента. 2.10 Используя Систему ДБО Клиент приобретает	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

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. права распоряжения денежными средствами (проверка ЭП, запрос по отдельным платежам клиента дополнительного подтверждения, получение от клиента подтверждения совершаемой операции в случае использования Мобильной подписи); 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. 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	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. the right to cash dispose (ES verification, request for individual client's payments of additional confirmation, receipt of confirmation from the client of the operation being performed in case of using the Mobile signature); 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. 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

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.	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:	2.15. The system assigns the following statuses to Electronic Documents:
• **«2-я картотека»** - присваивается Электронному документу, если при обработке платежа на счете Клиента оказалось недостаточно средств для совершения операции.	• **List 2** is assigned to the Electronic Document, if during the processing of the payment on the Client's account there were not enough funds to complete the transaction.
• **«Создан»** - присваивается при создании и сохранении нового Электронного документа Клиентом.	• **Created** is assigned when a new Electronic document is created and saved by the Client.
• **«Запланирован»** - Электронный документ создан и подписан клиентом, но не отправлен в Банк. Отправка Электронного документа в Банк будет выполнена в назначенную клиентом дату.	• **Planned** - the Electronic document was created and signed by the client, but not sent to the Bank. The Electronic Document will be sent to the Bank on the date specified by the client.
• **«На подписи»** - присваивается Электронному документу после установки подписи и непрохождении контроля соответствия количества подписей, заявленного в банке.	• **Under Signature** is assigned to the Electronic Document after setting the signature and not passing the control of compliance with the number of signatures declared in the bank.
• **«Отправлен»** - Электронный документ отправлен в Банк, но еще не принят к исполнению.	• **Sent** - the Electronic Document has been sent to the Bank, but has not yet been accepted for execution.
• **«Отправлен в банк»** - присваивается Электронному документу при прохождении процедуры приема к исполнению, в том числе при запросе Банком от Клиента подтверждения совершаемой операции в случае использования Мобильной подписи.	• **Sent to the Bank** is assigned to the Electronic Document when passing the procedure of acceptance for execution, including when the Bank requests from the Client confirmation of the transaction in case of using the Mobile signature.
• **«Принят»** - присваивается документу после его принятия Банком к исполнению.	

• **«Исполнено»** - присваивается документу после его исполнения Банком (в том числе после списания денежных средств со Счета Клиента на основании данного документа). • **«Отказ»** - присваивается Электронному документу, если он не может быть принят к исполнению в Банке. Для уточнения причины необходимо обратиться в Банк. • **«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 Клиента на отзыв документа. • **«Требуется подтверждение»** - обработка Электронного документа приостановлена до уточнения деталей платежа сотрудником Банка.	• **Accepted** is assigned to a document after it has been accepted by the Bank for execution. • **Executed** is assigned to a document after its execution by the Bank (including after debiting the Client's Account based on this document). • **Rejection** is assigned to the Electronic Document if it cannot be accepted for execution in the Bank. To clarify the reason, you need to contact the Bank. • **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, Regulations 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 the Client's request to withdraw a document has been made. • **Confirmation required** - the processing of the Electronic Document is suspended until the details of the payment are clarified by the Bank's employee
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 корректность.	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 Regulations; • 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 for correctness. 2.19. Electronic documents executed in violation of

2.19 Электронные документы, оформленные с нарушением требований, приему не подлежат, таким Электронным документам присваивается статус в Системе ДБО «Аннулирован».	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 Regulations 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; - документы для совершения валютных операций (заявления на перевод иностранной валюты, распоряжения на покупку/продажу валюты и т.п.) - документы валютного контроля; - заявления о смене Абонентского номера; - заявления на изменение БП.	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; - documents for performing currency transactions (applications for the transfer of foreign currency, orders for the purchase/sale of currency, etc.) - currency control documents; - applications for changing the subscriber number; applications for changing the BP.
2.23 Уполномоченному Представителю Клиента может быть предоставлен доступ к Системе ДБО, с возможностью получения сведений о Клиенте, его операциях, открытых в Банке банковских счетах Клиента, с правом просмотра и получения Электронных документов, в том числе выписок по счетам, без выдачи такому Представителю Электронной подписи.	2.23 Access to the RBS System can be provided to The Client's Authorized Person, with access to the Client`s information, information of it`s transactions, and information of the Client's bank accounts opened in the Bank, with access to reading and receiving electronic documents, including account statements, without issuing an Electronic signature to the Client's Authorized Person.
2.24 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), подписавшего и направившего Электронный документ.	2.24 Electronic Documents signed with a simple Electronic Signature contain information indicating the Authorized Representative of the Client (full name, application number assigned upon registration of such person in the RBS System), who signed and sent the Electronic Document.

3 ПОРЯДОК ПОДКЛЮЧЕНИЯ КЛИЕНТА К СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

3.1 Порядок регистрации Уполномоченного Представителя Клиента в Системе ДБО:

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 и Заявления о присоединении к настоящему Регламенту.

3.1.2. Подача Уполномоченным Представителем Клиента Заявления о присоединении к настоящему Регламенту осуществляется каждым таким лицом, путем обращения к Ответственному работнику по юридическому адресу Банка в течение Операционного времени Банка.

3.1.3 При приеме Заявления Ответственный работник идентифицирует Уполномоченного Представителя Клиента, с использованием документа, удостоверяющего 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;

3.2 При выборе Клиентом метода работы в Системе ДБО с использованием простой Электронной подписи/ правом просмотра (без использования Электронной подписи) Оператор Центра регистрации направляет на указанный в Заявлении на приобретение/изменение БП Абонентский номер Уполномоченного Представителя Клиента данные для первого входа в Систему ДБО – Логин и Временный пароль.

3.3 Порядок активации ключа Мобильной подписи:

3. PROCEDURE FOR CONNECTING THE CLIENT TO THE REMOTE BANKING SERVICE SYSTEM

3.1. Registration procedure Authorized Person of the Client in the RBS System:

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 and Application on joining these Regulations.

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. 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 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;

3.2 When the Client chooses a method of working in the RBS System using a simple Electronic Signature/view right (without using an Electronic Signature), the Registration Center Operator sends to the Subscriber Number of the Client's Authorized Representative specified in the Application for Purchase/Change of BP data for the first log on the

3.3.1 После проведения регистрации уполномоченного Представителя Клиента Ответственный работник Банка: a) подготавливает средствами Системы ДБО ключ проверки Мобильной подписи для передачи и активации уполномоченному Представителю Клиента; b) направляет на Абонентский номер уполномоченного Представителя Клиента, указанный в Заявлении о присоедини к настоящему регламенту, данные для активации ключа проверки Мобильной подписи – Логин и Временный пароль c) направляет на адрес электронной почты, указанный в Заявлении о присоедини к настоящему регламенту, Акт признания ключа проверки Мобильной подписи. 3.3.2 Для получения ключа Мобильной подписи уполномоченный Представитель Клиента должен лично: a) активировать ключ Мобильной подписи в приложении Банка, используя предоставленные в SMS/email - сообщении Логин и Временный пароль. b) подписать и направить в Банк сканированную копию Акта признания ключа проверки Мобильной подписи, форма которого определяется Банком и размещена на ресурсе https://131.ru/contracts. c) предоставить в Банк в течении 40 календарных дней с момента активации Ключа Мобильной подписи Акт признания ключа проверки Мобильной подписи на бумажном носителе, заверенный собственноручной подписью такого Уполномоченного Представителя Клиента. 3.3.3 Инструкция по активации ключа проверки Мобильной подписи размещена на ресурсе https://131.ru/contracts и в офисе Банка. 3.4 При выборе Клиентом метода работы в Системе ДБО с использованием усиленной неквалифицированной Электронной подписи, хранящейся на ФКН: 3.4.1 Оператор Удостоверяющего центра: ● после выполнения указанных в разделе 4 Регламента действий, подготавливает Функциональный ключевой носитель, формирует карточку первоначальных PIN-кодов для Функционального ключевого носителя, «Инструкцию по управлению PIN-кодами Функционального ключевого носителя» (размещена также на https://131.bank/contracts) и помещает их 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	RBS System - Login and temporary password. 3.3 How to activate the Mobile Signature key: 3.3.1 After the registration of the authorized Representative of the Client, the Responsible employee of the Bank: a) prepares the Mobile signature verification key by means of the RBS System for transfer and activation to an authorized Representative of the Client; b) sends to the Subscriber number of the authorized Representative of the Client, specified in the Application for accession to this regulation, the data for activating the Mobile signature verification key - Login and Temporary password. c) sends to the e-mail address specified in the Application for accession to this regulation, the act of recognition of the Mobile signature verification key. 3.3.2 To obtain the Mobile Signature key, the authorized Representative of the Client must personally: a) activate the Mobile Signature key in the Bank's application using the Login and Temporary password provided in the SMS/email message. b) sign and send to the Bank a scanned copy of the Mobile Signature Verification Key Recognition Act, the form of which is determined by the Bank and posted at https://131.ru/contracts. c) submit to the Bank, within 40 calendar days from the date of activation of the Mobile Signature Key, the Certificate of Recognition of the Mobile Signature Verification Key on paper, certified by the handwritten signature of such Authorized Representative of the Client. 3.3.3 Instructions for activating the Mobile signature verification key are available at https://131.ru/contracts and at the Bank's office. 3.4 When the Client chooses a method of working in the RB System using an enhanced unqualified Electronic Signature stored on the FKM: 3.4.1 Operator of the Certification Centre: ● prepares the Functional Key Carrier, generates a card of the initial PIN-codes, «Instructions for managing the PIN-codes of 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 Regulations; ● hands over a properly packaged Functional

[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.

Клиента. ● Уполномоченный Представитель Клиента в праве отказаться от получения Функционального ключевого носителя при наличии у него собственного Функционального ключевого носителя, поддерживающего аппаратные криптографические функции -Рутокен ЭЦП 2.0. Банк не несет ответственности за возможные проблемы использования Функционального ключевого носителя, полученного не в Банке. 3.4.2 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 https://131.ru/contracts и в офисе Банка. В случае нарушения целостности упаковки Функционального ключевого носителя Уполномоченный Представитель Клиента должен 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. 3.5. Уполномоченный Представитель Клиента при использовании Системы ДБО и обмене Электронными документами через нее вправе использовать указанный в Заявлении на приобретение/изменение БП метод работы (способ подписания Электронных документов, с учетом функциональных возможностей Системы ДБО): с использованием простой Электронной подписи, либо усиленной неквалифицированной Электронной подписи, в том числе с использованием Мобильной подписи, с учетом установленных в Системе ДБО ограничений для отдельных категорий Электронных документов. В рамках обмена электронными документами с использованием Системы ДБО информационное взаимодействие между Банком и Клиентом осуществляется с использованием Электронных подписей, выпущенных Банком. 3.6. Клиент (его уполномоченный Представитель) считается подключенным к Системе ДБО, а Уполномоченный Представитель Клиента имеет возможность пользоваться Системой ДБО при наступлении следующих событий: - с момента регистрации Уполномоченного Представителя Клиента в Системе ДБО, и направлении на Абонентский номер/адрес электронной почты такого Уполномоченного Представителя Клиента SMS/email-сообщения с данными для первоначального входа в Систему ДБО (логин и временный пароль). Указанное условие применяется в отношении уполномоченных Представителей Клиента, наделенных правом распоряжаться денежными средствами/совершения сделок (при использовании простой Электронной подписи), а также в отношении	Key Carrier to the Responsible Officer for handing it over to the Client's Authorized Person. • The Client's Authorized Person has the right to refuse to receive a Functional Key Carrier if he has his own Functional Key Carrier that supports hardware cryptographic functions-Rutoken EDS 2.0. The Bank is not responsible for possible problems with the use of a Functional Key Carrier that is not received from the Bank. 3.4.2. 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 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. 3.5. 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, including using Mobile Signature, taking into account the limitations set in the RBS System for certain categories of Electronic Documents. As part of the exchange of electronic documents using the RBS System, information interaction between the Bank and the Client is carried out using Electronic Signatures issued by the Bank. 3.6. The Client (The Client's Authorized Representative) 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: - from the moment of registration of the Client's Authorized Representative in the RBS System and sending an SMS/E-mail message with data for initial login to the Client's Subscriber number/E-mail address of such Authorized Representative (login and temporary password). This condition applies to the Client's Authorized Person who have the right to

уполномоченных Представителей Клиента, наделенных полномочиями (роль в Системе ДБО) на просмотр и получение Электронных документов, в том числе выписок по Счету (без права распоряжаться денежными средствами/совершения сделок от имени Клиента); - при использовании Мобильной подписи после активации ключа ЭП в мобильном приложении и подписания Акта признания ключа ЭП Мобильной подписи; - при использовании усиленной неквалифицированной Электронной подписи на ФКН после получения уведомления о выпуске Сертификата ключа проверки Электронной подписи и завершения процедуры формирования Электронной подписи средствами Системы ДБО Уполномоченным Представителем Клиента. 3.7. По истечении срока полномочий Уполномоченного Представителя Клиента Банк блокирует доступ такого Уполномоченного Представителя Клиента к Системе ДБО. 3.8. Клиент вправе установить ограничения по параметрам операций, которые могут осуществляться Клиентом с использованием системы ДБО в заявлении, форма которого определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка. Прием заявления осуществляется путем передачи оригинала заявления Ответственному работнику Банка. При приеме Заявления Ответственный работник идентифицирует Уполномоченного Представителя Клиента, с использованием документа, удостоверяющего личность последнего[2]. 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. 3.9. Для получения Средств подтверждения Электронного документа для создания простой Электронной подписи или ключа Мобильной 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. В случае невыполнения указанного условия доступ и использование Системы ДБО не допускается. 3.10. Рекомендуется осуществлять смену Статического пароля для доступа к Системе ДБО не реже	dispose of funds/make transactions (when using a simple Electronic signature), as well as to the Client's Authorized Representative who have the right (role in the RBS System) to view and receive Electronic Documents, including account statements (without the right to dispose of funds/make transactions on behalf of the Client); - when using the Mobile Signature after activating the ES key in the mobile application and signing the Certificate of Recognition of the ES Key of the Mobile Signature; - when using an enhanced non-certified Electronic Signature on the FKM 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. 3.7 Upon the expiration of the term of office of the Client's Authorized Representative, the Bank blocks the access of such the Client's Authorized Representative to the RBO System. 3.8 The Client has the right to set restrictions on the parameters of operations that can be carried out by the Client using the RBO system in the application, the form of which is determined by the Bank and posted on the resource https://131.ru/contracts and in the Bank's office. Acceptance of the application is carried out by transferring the original application to the Responsible employee of the Bank. When accepting the Application, the Responsible Employee identifies the Authorized Representative of the Client, using the identity document of the latter. The Responsible Employee has the right to request, and the Authorized Representative of the Client must submit, other documents necessary for his Identification, including documents confirming the information submitted to the Bank. 3.9 In order to receive the Electronic Document Confirmation Tools for creating a simple Electronic Signature or a Mobile Signature key, the Authorized Representative of the Client must complete the registration procedure in accordance with Section 3 of these Regulations and change the initial Authentication Data in the RBS System (Temporary Password). After entering the RBS System in order to use it and exchange Electronic Documents, the Authorized Representative of the Client must change the Temporary Password to a Static Password. In case of failure to fulfill the specified condition, access and use of the RBS System is not allowed.

[2] 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.

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. 3.11. 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 подписания Электронного документа. Уполномоченный Представитель Клиента должен ввести полученный Одноразовый пароль для прохождения процедуры аутентификации и/или подписания Электронного документа. 3.12. 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 или Заявлении о смене абонентского номера мобильной связи. 3.13. Порядок смены Логина и Статического пароля в Системе ДБО. 3.13.1. Уполномоченный Представитель Клиента может самостоятельно изменить Логин и Статический пароль в Системе ДБО, за исключением случая их утраты. В случае утраты Статического пароля или/и Логина уполномоченный Представитель Клиента обязан незамедлительно обратиться в Банк для блокирования доступа, в соответствии с разделом 8 настоящего Регламента. Для восстановления доступа в Систему ДБО уполномоченный Представитель Клиента может лично обратиться в Банк с Заявлением о смене логина и/или пароля /разблокировке 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, либо провести смену дистанционным способом. 3.13.2. Для дистанционной смены Логина и Статического пароля уполномоченный Представитель Клиента должен направить с адреса электронной почты, указанного в Заявлении на приобретение/изменение БП, Заявлении в Банк сканированную копию подписанного Заявления о смене логина и статического пароля по следующим контактным данным: dbo@131.ru. Для обработки Заявления о смене логина и статического пароля уполномоченный работник Банка связывается с Уполномоченным Представителем Клиента с использованием контактных данных, указанных Уполномоченным Представителем Клиента в Заявлении на приобретение/изменение БП и Заявлении. При этом, Уполномоченный Представитель Клиента должен сообщить уполномоченному работнику Банка следующую информацию: • свои идентификационные данные; • специальную парольную фразу.	3.10 It is recommended to change the Static password for access to the RBS System at least once every 3 (Three) months. The Bank shall not be liable if the Authorized Representative of the Client fails to comply with the said recommendation, including in the event of negative events. 3.11 A one-time password is automatically generated by the RBS System, including for the purpose of additional authentication of the Authorized Representative of the Client when granting him access to the RBS System and/or signing the Electronic Document. The Authorized Representative of the Client must enter the received One-Time Password in order to pass the authentication procedure and/or sign the Electronic Document. 3.12 The one-time password is sent by the Bank to the Subscriber Number of the Authorized Representative of the Client, specified in the Bank's software and hardware complex based on the information contained in the Application for the purchase / change of the BP, the Application or the Application for changing the mobile subscriber number. 3.13 Procedure for changing the Login and Static password in the RBS System. 3.13.1 The Authorized Representative of the Client may independently change the Login and Static Password in the RBS System, except for the case of their loss. In case of loss of the Static password and/or Login, the authorized Representative of the Client is obliged to immediately apply to the Bank to block access, in accordance with Section 8 of these Regulations. To restore access to the RBS System, the authorized Representative of the Client may personally apply to the Bank with an Application to change the login and/or password / unlock access to the RBS System, the form of which is determined by the Bank and posted on the resource https://131.ru/contracts and in the office Bank, and a document proving his identity, or carry out the change remotely. 3.13.2 In order to remotely change the Login and Static Password, the authorized Representative of the Client must send a scanned copy of the signed Application for changing the login and static password from the email address specified in the Application for the purchase/change of the BP, the Application to the Bank to the following contact details: dbo@131.ru. To process the Application for changing the login and static password, an authorized employee of the Bank contacts the Authorized Representative of the Client using the contact details specified by the Authorized Representative of the Client in the Application for the purchase/change of the BP and the Application. In this case, the Authorized Representative of the Client must provide the authorized employee of the Bank with the following information:

Аутентификация заявителя при подаче запроса на смену Логина и Статического пароля Системе ДБО - Уполномоченного Представителя Клиента осуществляется по специальной парольной фразе, содержащейся в реестрах Системы ДБО. После успешной аутентификации уполномоченный работник Банка направляет на контактные данные Уполномоченного лица Клиента ссылку-приглашение на видеозвонок, в целях проведения дополнительной аутентификации. В случае проведения успешных процедур идентификации и аутентификации на Абонентский номер и/или адрес электронной почты Уполномоченного лица Клиента направляется SMS/email-сообщение с новыми Логином и временным Паролем. Банк вправе отказать Уполномоченному лицу Клиента в дистанционной смене Логина и Пароля без объяснения причин такого отказа. В случае отказа в смене Логина и Пароля дистанционным способом Уполномоченный представитель Клиента проводит смену в соответствии с п.5.6.1 настоящего Регламента.	• his identification data; • a special passphrase. Authentication of the applicant when submitting a request to change the Login and Static password to the RBS System - the Authorized Representative of the Client is carried out using a special password phrase contained in the RBS System registers. After successful authentication, an authorized employee of the Bank sends a video call invitation link to the contact details of the Client's Authorized Person in order to conduct additional authentication. In case of successful identification and authentication procedures, an SMS/email message with a new Login and temporary Password is sent to the Subscriber number and/or e-mail address of the Client's Authorized Person. The Bank has the right to refuse the Client's Authorized Person to remotely change the Login and Password without explaining the reasons for such refusal. In case of refusal to change the Login and Password remotely, the authorized representative of the Client shall carry out the change in accordance with clause 5.6.1 of these Regulations.
3.14. Порядок смены Абонентского номера используемого для получения Одноразового пароля/ использования Мобильной подписи.	3.14 The procedure for changing the Subscriber number used to obtain the One-Time Password / use enhanced unqualified Electronic Signature / use Mobile Signature key.
3.14.1. Для изменения Абонентского номера Уполномоченного Представителя Клиента, используемого для получения Одноразового пароля/Мобильной подписи такой Уполномоченный Представитель Клиента должен обратиться в Банк и предоставить Заявление на изменение Условий осуществления информационного взаимодействия с использованием Системы информационного обмена и Заявление на изменение абонентского номера мобильной связи, с предоставлением удостоверяющих личность документов. Если Абонентский номер меняет Уполномоченный представитель клиента, уполномоченный подписывать договоры/заявления, он может подписать только Заявление на изменение Условий осуществления информационного взаимодействия с использованием Системы информационного обмена, указав в нем, что подтверждает принадлежность ему абонентского номера.	3.14.1 In order to change the Subscriber Number of the Authorized Representative of the Client used to obtain the One-Time Password/Mobile Signature, such Authorized Representative of the Client must apply to the Bank and submit an Application for changing the banking product "Remote banking service using the RBS System" and an Application for changing the subscriber number of the mobile connection with the provision of identity documents. If the Subscriber Number is changed by the Authorized Representative of the Client, authorized to sign agreements/applications, he can only sign the Application for changing the banking product "Remote Banking Services Using the RBS System", indicating in it that confirms that the subscriber number belongs to him.
3.14.2. Для дистанционной смены Абонентского номера Уполномоченный Представитель Клиента направляет Заявление на изменение абонентского номера мобильной связи посредством Системы ДБО, выбрав необходимый шаблон документа и Заявление на изменение Условий осуществления информационного взаимодействия с использованием Системы информационного обмена. Заявления должны быть подписаны простой электронной подписью/ усиленной неквалифицированной Электронной подписью / ключом Мобильной подписи обратившегося Уполномоченного Представителя Клиента. Дистанционная смена Абонентского номера возможна при наличии полномочий Уполномоченного Представителя Клиента подписывать и подать в Банк документы, заявления, сообщения,	3.14.2 In order to remotely change the Subscriber Number, the Client's Authorized Representative sends an Application for changing the mobile subscriber number via the RBS System, selecting the required document template and the Application for changing the banking product "Remote Banking Service Using the RBS System". Applications must be signed with a simple electronic signature/Mobile signature of the Client's Authorized Representative. Remote change of the Subscriber Number is possible if the Authorized Representative of the Client has the authority to sign and submit to the Bank documents, applications,

необходимые для регистрации, получения доступа, изменения условия использования Системы ДБО. Дистанционная смена Абонентского номера невозможна в случае Компрометации Электронной подписи или подозрений на Компрометацию Электронной подписи.	messages necessary for registration, gaining access, changing the conditions for using the RBS System. Remote change of the Subscriber number is not possible in case of Compromise of the Electronic Signature or suspicions of Compromise of the Electronic Signature.
3.14.3. 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.	3.14.3 The change of the Subscriber number of the Authorized Representative of the Client is carried out only after the positive completion of the verification of the submitted information and documents. The Bank has the right to refuse the Client to change the Subscriber Number of the Authorized Representative of the Client without explaining the reasons for such refusal.
3.15. При наличии технической возможности Банка и Клиента допускается направление Заявления о смене логина и/или статического пароля, Заявления на изменение абонентского номера мобильной связи, Заявления на приобретение/изменение БП через Оператора ЭДО, согласованного Банком. Заявление о смене логина и статического пароля и Заявление на изменение абонентского номера мобильной связи должны быть подписаны УКЭП Уполномоченного Представителя Клиента, указанного в этих заявлениях. Заявление на приобретение/изменение БП должно быть подписано УКЭП Уполномоченного Представителя Клиента, указанного в Заявлении на приобретение/изменение БП и имеющего полномочия подписывать и подавать в Банк документы, заявления, сообщения, необходимые для регистрации, получения доступа, изменения условия использования Системы ДБО. В случае предоставления Клиентом через Оператора ЭДО Заявления о смене логина и/или статического пароля или Заявления на изменение абонентского номера мобильной связи проводится аутентификация Уполномоченного Представителя Клиента в соответствии с п.5.6.2.	3.15 If there is a technical capability of the Bank and the Client, it is allowed to send an Application for changing the login and / or static password, an Application for changing the mobile phone subscriber number, an Application for purchasing / changing a BP through the EDM operator agreed by the Bank. The application for changing the login and static password and the Application for changing the mobile subscriber number must be signed by the EQES of the Authorized Representative of the Client specified in these applications. The Application for the acquisition/change of BP must be signed by the EQES of the Authorized Representative of the Client specified in the Application for the purchase/change of BP and having the authority to sign and submit to the Bank documents, applications, messages necessary for registration, access, change of the terms of use of the RBS System. If the Client, through the EDM operator, submits the Application for changing the login and / or static password or an Application for changing the mobile phone number, the Authorized Representative of the Client is authenticated in accordance with clause 5.6.2.
3.16 Для изменения специальной парольной фразы Уполномоченный представитель Клиента должен лично обратится в Банк с заявлением, форма которого размещена на ресурсе https://131.ru/contracts и в офисе Банка с предоставлением удостоверяющих личность документов.	3.16 To change the special password phrase, the Client's authorized representative must personally apply to the Bank with an application, the form of which is posted on the https://131.ru/contracts resource and at the Bank's office, providing identification documents.
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[3], должен лично:	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

[3] The Client's Authorized Persons entitled to dispose of the funds must also be indicated in such Card accepted by the

- создать с помощью средств Системы ДБО запрос на выпуск Сертификата ключа проверки электронной подписи, в электронном виде и на бумажном носителе; - подписать и направить в Банк сканированную копию данного запроса на электронный почтовый ящик dbo@131.ru; - предоставить в Банк данный запрос на бумажном носителе, заверенный собственноручной подписью такого Уполномоченного Представителя Клиента; - подписать Акт признания ключа проверки электронной подписи используемого для обмена сообщениями в системе ДБО АО «Банк 131», форма которого определяется Банком и размещена на ресурсе https://131.ru/contracts. 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 электронный почтовый ящик dbo@131.ru. 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	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 Application shall personally to: - create a request to issue an electronic signature verification key certificate, electronically and on paper using the RBS System tools; - sign and send a scanned copy of this request to the Bank by e-mail dbo@131.ru ; - submit this request to the Bank in hard copy, certified by the handwritten signature of such Authorized Person of the Client; - sign the Certificate of recognition of the electronic signature verification key used for message exchange in the DBO system of Bank 131 JSC, the form of which is determined by the Bank and posted on the resource https://131.ru/contracts. 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. When the Bank receives a request to issue an electronic signature verification key Certificate in electronic form, the Registration Center Operator checks the data contained in the specified request in electronic form with the data specified in the request submitted by the Client to the electronic mailbox dbo@131.ru. 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

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.

проверки электронной подписи, последний должен обратится к Ответственному работнику Банка и представить документы, удостоверяющие личность.[4] Выдача сгенерированного Сертификата проверки электронной подписи осуществляется по Акту признания ключа проверки электронной подписи используемого для обмена сообщениями в системе ДБО АО «Банк 131», и только на основании оригинала 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 «Акт признания ключа проверки электронной подписи используемого для обмена сообщениями в системе ДБО АО «Банк 131» и сертификат в момент его получения.	certificate.
4.5. Выпущенный Сертификат ключа проверки электронной подписи подписывается Уполномоченным Представителем Клиента и после этого размещается в Системе ДБО.	4.4. In order for the Client's Authorized Person to receive the generated Certificate of the electronic signature verification key, the latter must contact the Responsible Employee of the Bank and submit identity documents. The issue of the generated Electronic Signature Verification Certificate is carried out according to the Act of Recognition of the electronic signature verification key used for messaging in the RBS system of Bank 131 JSC, and only on the basis of the original request for the issuance of the Electronic Signature verification key certificate and with a positive result of verification of the submitted documents and the information contained therein. The Client's Authorized Person must sign the "Certificate of recognition of the electronic signature verification key used for the exchange of messages in the RBS system of Bank 131 JSC " and the certificate at the time of its receipt .
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. – 4.4. Регламента.	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. 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. - 4.4 of the Regulation.
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.	4.7. 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. 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;	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;

[4] 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.

● 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, равный сроку полномочий, но не более 1 года с момента его выпуска.

4.9. 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.

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

● 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 equal to the term of office, but not more than 1 year from the date of its issue.

4.9. 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. 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

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 текстом SMS сообщения подписать простой Электронной подписью Электронный документ. В случае несогласия с текстом SMS сообщения 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 Представителем Клиента специальной функциональной кнопки в веб-интерфейсе системы ДБО Электронный документ считается подписанным Клиентом и 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. •	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 text of the SMS message, 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 text of the SMS message. 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 Electronic Document by means of a simple Electronic Signature. h) The Electronic Document shall be deemed signed by the Client and 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,

6. ПОРЯДОК ИСПОЛЬЗОВАНИЯ КЛЮЧА МОБИЛЬНОЙ ПОДПИСИ

6.1. В качестве средства подтверждения Электронного документа, подписанного ключом Мобильной подписи, используется Логин, Статический пароль, а также подтверждение операции в мобильном приложении Банка.

6.2. 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.

d) На Мобильное устройство Уполномоченного Представителя Клиента направляется PUSH сообщение о необходимости подтвердить подписание Электронного документа.

e) Уполномоченный Представитель Клиента использует PIN-код приложения, или встроенную систему биометрической авторизации для входа в мобильное приложение Банка и подтверждения подписания Электронного документа.

f) Перед подтверждением подписания Электронного документа Уполномоченный Представитель Клиента обязан ознакомиться с информацией, поступившей в мобильном приложении Банка, и в случае согласия с текстом сообщения подтвердить подписание Электронного документа. В случае несогласия с текстом сообщения Уполномоченный Представитель Клиента должен отказаться от подтверждения подписания Электронного документа.

g) Для подтверждения подписания сформированного Электронного документа посредством Мобильной подписи Уполномоченный Представитель Клиента нажимает соответствующую электронную кнопку в мобильном приложении Банка.

h) С момента нажатия Уполномоченным Представителем Клиента специальной функциональной кнопки в мобильном приложении Банка Электронный

(2) The Electronic document contains the Client's simple Electronic signature, the verification result of which coincides with the One-time password.

6 PROCEDURE FOR USING THE MOBILE SIGNATURE KEY

6.1 As a means of confirming the Electronic Document signed with a Mobile Signature key, the Login, Static Password, as well as confirmation of the operation in the Bank's mobile application are used.

6.2 In order to send the Electronic Document by the Authorized Representative of the Client to the Bank, the Authorized Representative of the Client, following the instructions in the screen forms of the web interface of the RBS System, using the function buttons, initiates the signing of the corresponding Electronic Document:

a) The Authorized Representative of the Client enters the necessary data requested by the web interface of the RBS system using the functional buttons and fields for entering information.

b) Before signing the Electronic Document, the Client's Authorized Representative must review it and agree with its content in full.

c) To sign the generated Electronic Document via the web interface of the RBS system, the Authorized Representative of the Client initiates the process of signing the Electronic Document after checking its content.

d) A PUSH message is sent to the Mobile Device of the Authorized Representative of the Client to confirm the signing of the Electronic Document.

e) The Authorized Representative of the Client uses the Application PIN or the built-in biometric authorization system to enter the Bank's mobile application and confirm the signing of the Electronic Document.

f) Before confirming the signing of the Electronic Document, the Authorized Representative of the Client is obliged to familiarize himself with the information received in the Bank's mobile application and, if he agrees with the text of the message, confirm the signing of the Electronic Document. In case of disagreement with the text of the message, the Authorized Representative of the Client must refuse to confirm the signing of the Electronic Document.

g) To confirm the signing of the generated Electronic Document using the Mobile Signature, the Authorized Representative of the Client presses the appropriate electronic button in the Bank's mobile application.

h) From the moment the Authorized Representative of

документ считается подписанным Клиентом и направленным в Банк.

6.3. Для смены ключа Мобильной подписи Уполномоченному Представителю Клиента необходимо провести активацию ключа Мобильной подписи в соответствии с п.3.3.2 и п.3.3.3.

6.4. Смена ключа Мобильной подписи производится в случаях:

- Компрометации Мобильной подписи;
- утраты Логина и/или Временного/Статического пароля;
- утраты PIN-кода Мобильного приложения;
- утраты или смены мобильного устройства;
- переустановки Мобильного приложения.

7. ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

7.1. 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.

7.2. До истечения срока действия Сертификатов ключей проверки Электронной подписи Уполномоченный Представитель Клиента имеет возможность провести плановую процедуру смены Ключей Электронной подписи с использованием Системы ДБО и ее средств.

7.3. 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.

7.4. 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. При истечении срока полномочий Уполномоченный представитель Клиента одновременно с запросом должен предоставить документы, подтверждающие его полномочия.

7.5. 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. Банк направляет посредством Системы ДБО Акт признания ключа проверки электронной подписи и Сертификат Уполномоченному

the Client presses a special functional button in the Bank's mobile application, the Electronic Document is considered signed by the Client and sent to the Bank.

6.3 To change the Mobile Signature key, the Authorized Representative of the Client must activate the Mobile Signature key in accordance with clauses 3.3.2 and 3.3.3.

6.4 The Mobile Signature key is changed in the following cases:

- Compromises of the Mobile signature;
- loss of Login and/or Temporary/Static password;
- loss of the PIN-code of the Mobile application;
- loss or change of a mobile device;
- reinstallation of the Mobile application.

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

7.1. 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.

7.2. 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 Signature Key Certificates.

7.3. 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.

7.4. 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. At the end of the term of office, the Client's Authorized Person must provide documents confirming his / her authority at the same time as the request.

7.5. The Certification Authority Operator issues a Certificate of the electronic signature verification Key. The Bank has the right to refuse to issue a Certificate of the electronic signature verification key, the request for which was received using the RBS System, without explaining the reason. If the Bank refuses to issue an Electronic Signature Verification Key Certificate, the Client's Authorized Person has the right to personally

Представителю Клиента, от которого поступил запрос, для его подписания. Уполномоченный Представитель Клиента должен распечатать, подписать и передать в Банк два экземпляра Акта признания ключа проверки электронной подписи и Сертификаты. После получения Банком подписанных экземпляров Актов признания ключа проверки электронной подписи и Сертификатов, такой сертификат размещается в Системе ДБО.

apply to the Bank for issuing such a certificate, in accordance with the procedure specified in Section 4 of these Regulations. The Bank sends the Certificate of Recognition of the electronic signature verification Key and the Certificate to the Client's Authorized Person from whom the request was received, for its signature, via the RBS System. The Client's Authorized Person must print, sign and hand over to the Bank two copies of the Certificate of Recognition of the Electronic Signature Verification Key and Certificates. After the Bank receives the signed copies of the Acts of Recognition of the electronic Signature Verification Key and Certificates, such a certificate is placed in the RBS System.

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

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

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

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

8. ПОРЯДОК БЛОКИРОВКИ И ВОССТАНОВЛЕНИЯ ДОСТУПА К СИСТЕМЕ ДБО

8 PROCEDURE FOR BLOCKING AND RESTORING ACCESS TO THE RBS SYSTEM

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

8.1.1. 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 Клиента), запроса о приостановлении доступа к Системе ДБО, с указанием причин такого приостановления;

8.1.2. компрометация Электронной подписи и/или использование Электронной подписи без согласия Уполномоченного Представителя Клиента;

8.1.3. замена Карточки с образцами подписей и оттиска печати и/или Соглашения о сочетании электронных подписей, при их оформлении в соответствии с Правилами;

8.1.4. прекращение или изменение полномочий или данных Уполномоченного Представителя Клиента;

8.1.5. смена Абонентского номера Уполномоченного Представителя Клиента;

8.1.6. утраты Аутентификационных данных, Временного, Одноразового, Статического паролей;

8.1.7. непредставление или представление недостоверных сведений и документов, запрашиваемых Банком, в том числе в целях выполнения требований

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

8.1.1. 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;

8.1.2. Compromising the Electronic Signature and/or using the Electronic Signature without the consent of the Client's Authorized Person;

8.1.3. 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;

8.1.4. termination or change of powers or data of the Client's Authorized Person;

8.1.5 change of the Subscriber number of the Client's Authorized Person;

8.1.6. loss of Authentication Data, Temporary, One-

законодательства Российской Федерации и нормативных актов Банка России; 8.1.8. выявление Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, установленным Банком России или подозрений на их совершение; 8.1.9. направление Клиентом Заявления на блокировку доступа к Системе ДБО. 8.2. При наступлении событий, указанных в пп. 8.1.3, 8.1.7, 8.1.8 доступ в Систему ДБО блокируется всем Уполномоченным Представителям Клиента. 8.3. Клиент вправе осуществить блокировку доступа к Системе ДБО, в случаях, не связанных с компрометацией, или подозрении на компрометацию электронной подписи. 8.3.1. Порядок блокировки доступа к Системе ДБО дистанционным способом: 8.3.1.1. Для дистанционной блокировки доступа к Системе ДБО Уполномоченному Представителю Клиента необходимо обратиться в Банк с соответствующим запросом по следующим контактным данным: **dbo@131.ru** или с использованием Системы ДБО, с указанием данных Уполномоченного Представителя Клиента, позволяющих установить его личность. Для обработки запроса на дистанционную блокировку уполномоченный работник Банка связывается с Уполномоченным Представителем Клиента с использованием контактных данных такого лица, указанных Уполномоченным Представителем Клиента в Заявлении на приобретение/изменение БП и Заявлении о присоединении к Регламенту, при этом, Уполномоченный Представитель Клиента должен сообщить уполномоченному работнику Банка сведения, необходимые для аутентификации Уполномоченного представителя Клиента. 8.3.2. Порядок блокировки доступа к Системе ДБО при личном обращении Уполномоченного Представителя Клиента в Банк: 8.3.2.1. Уполномоченному Представителю Клиента необходимо обратиться непосредственно в офис Банка, по 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. 8.3.2.2. Подача запроса на блокировку доступа к Системе ДБО Уполномоченного Представителя Клиента возможна только в течение Операционного времени Банка. 8.4. Блокировка доступа осуществляется незамедлительно после получения соответствующего запроса и аутентификации Уполномоченного Представителя Клиента Банком, при условии его получения	time and Static passwords; 8.1.7. 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; 8.1.8. 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; 8.1.9 sending an Application by the Client to block access to the RBS System. 8.2. Access to the RBS System is blocked to all Authorized Persons of the Client upon occurrence of the events specified in subclauses 8.1.3, 8.1.7, 8.1.8. 8.3. The Client has the right to block access to the RBS System, in cases not related to compromise, or suspected of compromising the electronic signature. 8.3.1 Procedure for blocking access to the RBS System by remote means: 8.3.1.1 In order to remotely block access to the RBS System, the Client's Authorized Person must contact the Bank with a corresponding request using the following contact details: **dbo@131.ru** or using the RBS System, with the indication of the data of the Client's Authorized Person, allowing to establish his identity. To process the request for remote blocking, the authorized employee of the Bank contacts the Client's Authorized Person using the contact details of such a person specified by the Client's Authorized Person in the Application for the purchase/Modification of the PS and the Application for joining the Regulations, and the Client's Authorized Person must inform the authorized employee of the Bank of the information necessary for authentication of the Client's Authorized Person. 8.3.2. Procedure for blocking access to the RBS System when the Client's Authorized Person addresses the Bank in person: 8.3.2.1. 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. Simultaneously with the request, the Client's Authorized Person provides documents proving his/her identity and authority. 8.3.2.2. 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. 8.4. Access blocking is carried out immediately

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.	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.
8.5. Порядок восстановления доступа к Системе ДБО: В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п.8.1.2-8.1.6, 8.1.9 разблокировка возможна после 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 и:	8.5. Procedure for restoring access to the RBS System: If the reason for blocking access to the RBS System is due to the circumstances specified in clauses 8.1.2-8.1.6, 8.1.9, unlocking is possible after 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 and:
a) При использовании УНЭП проведенной процедуры внеплановой смены сертификата ключа проверки Электронной подписи в соответствии с разделом 9 настоящего Регламента;	a) In the case of an unscheduled change of the electronic signature verification key certificate in accordance with Section 9 of these Regulations;
b) При использовании простой Электронной подписи: смены Статического пароля Уполномоченного Представителя Клиента в соответствии с п.3.13 Регламента; смены Абонентского номера Уполномоченного Представителя Клиента в случае утери и/или прекращения доступа к нему.	b) When using a simple Electronic Signature: change of the static password of the Client's Authorized Person in accordance with Clause 3.13 of the Regulations; change of the Client's Authorized Person Subscriber Number in case of loss and/or termination of access to the Client.
c) При использовании Мобильной подписи проведенной смены Статического пароля в соответствии с п.3.13 и смене ключа Мобильной подписи Уполномоченного Представителя Клиента в соответствии с п.6.3 Регламента.	c) When using the Mobile Signature of the carried out change of the Static password in accordance with clause 3.13 and the change of the Mobile Signature key of the Authorized Representative of the Client in accordance with clause 6.3 of the Regulations.
8.6. В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п. 8.1.6 разблокировка возможна в соответствии с п. 3.13 Дистанционная разблокировка в соответствии с п. 3.13 возможна при отсутствии у Банка оснований полагать, что Средства подтверждения Электронного документа стали известны неуполномоченным третьим лицам.	8.6 If the circumstances specified in clause 8.1.6 serve as the basis for blocking access to the RBS System, unlocking is possible in accordance with clause 3.13 Remote unlocking in accordance with clause 3.13 is possible if the Bank has no reason to believe that the Means of confirming the Electronic Document have become known to unauthorized third parties.
8.7. В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п.8.1.8 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.	8.7. If the reason for blocking access to the RBS System is due to circumstances specified in clause 8.1.8, 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

8.8. В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п.8.1.7, доступ к Системе ДБО возобновляется после представления сведений и документов, запрашиваемых Банком. Документы предоставляются Клиентом Ответственному работнику по юридическому адресу Банка в течение Операционного времени Банка.

9. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ КОМПРОМЕТАЦИИ ИЛИ ПОДОЗРЕНИИ НА КОМПРОМЕТАЦИЮ ЭЛЕКТРОННОЙ ПОДПИСИ

9.1. При выявлении одной из Сторон Компрометации Электронной подписи или ее признаков (подозрений), выявившая Сторона уведомляет об этом другую Сторону.
9.2. 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.

9.3. 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.

9.4. С момента получения Банком уведомления Клиента или выявления Банком обстоятельств, указанных в п. 9.1 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.

9.5. С момента направления Клиентом Банку или получения Клиентом от Банка уведомления о наступлении указанных в п. 9.1 Регламента обстоятельствах, Клиент не

established by the Bank of Russia, or two business days after the day of suspension when such confirmation is not received.

8.8. In the event that the reason for blocking access to the RBS System is due to the circumstances specified in 8.1.7 access to the RBS System is resumed after the submission of the information and documents requested by the Bank. The documents are provided by the Client to the Responsible Employee at the Bank's legal address during the Bank's Operating Time.

9. THE PROCEDURE IN THE EVENT OF COMPROMISE OR SUSPICION OF COMPROMISE OF AN ELECTRONIC SIGNATURE

9.1. The identified Party notifies the other Party if one of the Parties identifies the Electronic Signature Compromise, or its signs (suspicions).
9.2. The Bank notifies the Client of the occurrence of the circumstances specified in clause 8.1 of these Regulations by any means available to the Bank, using the contact details of the Client previously provided by the Client.

9.3. The Client notifies the Bank of the occurrence of the circumstances specified in clause 8.1 of the Regulations 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.
9.4. 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 9.1 of these Regulations. 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.

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 неблагоприятных последствий для него, в том числе правовых и финансовых.

9.6. Разблокировка доступа к Системе ДБО осуществляется в соответствии с п. 8.6 настоящего Регламента при получении Банком Уведомления о компрометации на бумажном носителе.

10. ПОРЯДОК ПРОВЕДЕНИЯ ВНЕПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

10.1. 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;
- изменения регистрационных данных Уполномоченного Представителя Клиента;
- истечения срока действия сертификата ключа проверки электронной подписи;
- выхода из строя ФКН.

10.2. После получения Банком Уведомления о компрометации Банк отзывает Сертификат скомпрометированного ключа проверки электронной подписи, путем помещения его в список отозванных сертификатов Системы ДБО.

10.3. 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.

9.5. 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 9.1 of the Regulations. 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.

9.6. RBS System access unblocking is performed in accordance with cl. 8.6 of these Regulations upon receipt by the Bank of a Notice of Compromising on Paper.

10. PROCEDURE FOR UNPLANNED CHANGE OF THE ELECTRONIC SIGNATURE VERIFICATION KEY CERTIFICATE

10.1. 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:

- the established fact of Compromising the Electronic Signature or suspicion of it;
- changes to the registration data of the Client's Authorized Person;
- expiration of the electronic signature verification key certificate;
- failure of the FKM.

10.2. 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.

10.3. 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 Regulations, 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.

11. ПОРЯДОК РАССМОТРЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

11.1. 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.

11.2. 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 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.11.11 настоящего Регламента.

11.3. 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.11.10 настоящего Регламента.

11.4. 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.

11. THE PROCEDURE FOR DEALING WITH CONFLICT SITUATIONS

11.1. 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.

11.2. 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 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 11.11 of these Regulations.

11.3. 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 11.10 hereof.

11.4. 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

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

11.6. 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.

11.7. 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.

11.8. 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.

11.9. Порядок разрешения конфликтной ситуации.

11.9.1. 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

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.

11.5. 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.

11.6. The Bank ensures the request for the electronic 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.

11.7. 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.

11.8. 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.

11.9. Procedure for resolving a conflict situation.

11.9.1 If there is a need to carry out the procedure for verifying the authenticity of an Electronic Signature, when exchanging Electronic Documents using the RBS

он оспаривает. 11.9.2 Банк и Клиент должны в течение не более пяти рабочих дней от даты приема Банком заявления Клиента сформировать Согласительную комиссию для его рассмотрения. 11.9.3 Согласительная комиссия должна закончить свою работу в течение 14 рабочих дней с момента ее создания. 11.9.4 Решение Согласительной комиссии принимается большинством голосов ее участников, оформляется актом и подписывается всеми членами комиссии. 11.9.5 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. 11.9.6 При использовании Уполномоченным Представителем Клиента двух видов подписи, усиленной неквалифицированной Электронной подписи и простой Электронной подписи одновременно, или в разные периоды, определятся вид подписи под оспариваемы документом из системных журналов Системы ДБО. **11.10. Процедура проверки усиленной неквалифицированной Электронной подписи.** 11.10.1 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 Сертификата ключа проверки электронной подписи, использованный при создании усиленной неквалифицированной Электронной подписи под оспариваемым Электронным документом. 11.10.2 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 Сертификате 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	System, the Client's Authorized Person submits to the Bank a written statement containing the substance of the claim with an indication of the Electronic Document that he (she) disputes. 11.9.2 The Bank and the Client must, within no more than five working days from the date of the Bank's acceptance of the Client's application, form a Conciliation Commission for its consideration. 11.9.3 The Conciliation Commission must complete its work within 14 working days of its establishment. 11.9.4 The decision of the Conciliation Commission is adopted by a majority of the votes of its participants, is drawn up by an act and signed by all members of the commission. 11.9.5 If the parties have not reached a mutual agreement or if they refuse to voluntarily execute the decision of the Conciliation Commission, the parties shall resolve the conflict situation in court. 11.9.6 If the Client's Authorized Person uses two types of signature, an enhanced unqualified Electronic signature and a simple Electronic signature at the same time, or at different periods, the type of signature under the disputed document will be determined from the system logs of the RBS System. **11.10. Enhanced Non-Certified Electronic Signature verification procedure.** 11.10.1 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 Electronic Signature Validation Key Certificate file of the Authorized Person of the Client is not distorted in the Electronic Document. 11.10.2 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

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.

11.10.3 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.

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.

11.10.3 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

11.10.4 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. 11.10.5 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. 11.10.6 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 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. **11.11. 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:	owner of the Key Certificate of Electronic Signature Verification, shall be deemed valid. 11.10.4 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. 11.10.5 The Bank's reference hardware and software tools are used to analyze conflict situations. Special certified software is used to verify an enhanced non-certified Electronic Signature under an Electronic Document. 11.10.6.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 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. **11.11. 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

● 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.
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

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 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

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.	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.
11.12. **Процедура проверки Мобильной подписи** 11.12.1.Для проверки принадлежности Мобильной подписи Уполномоченному Представителю Клиента и отсутствия искажений в Электронном документе из базы данных Банка уполномоченным работником Банка извлекается оспариваемое Электронное сообщение, файл подписи к оспариваемому Электронному сообщению и файл с идентификатором ключ Мобильной подписи. 11.12.2.Для разбора конфликтной ситуации используются эталонные программно-аппаратные средства Банка. Используется специальное программное обеспечение, предназначенное для проверки Мобильной подписи под Электронным документом. 11.12.3.Устанавливается принадлежность ключа проверки Мобильной подписи, содержащегося в извлеченном файле, Уполномоченному Представителю Клиента по следующей процедуре: сравнивается номер ключа Мобильной подписи, извлеченный из базы данных Банка с номером ключа указанного в «Акте признания ключа проверки мобильной подписи для обмена сообщениями в системе ДБО АО «Банк 131» хранящегося в досье Клиента, или в базе данных Банка. В случае, если принадлежность ключа установлена Комиссия переходит к следующему этапу. При несовпадении информации оспариваемый документ признается некорректным. 11.12.4.Проверка Мобильной подписи оспариваемого Электронного документа производится программой MobileSignVerify (разработчик ООО «Информационные системы»). По результатам проверки подпись под оспариваемым Электронным документом признается принадлежащей Уполномоченному Представителю Клиента, если в протоколе проверки, выдаваемом указанной в настоящем пункте программой, сформирована запись о том, что «Результат проверки: «Подпись подтверждена» (signature correct), и не принадлежащей Уполномоченному Представителю Клиента, в случае Результата проверки: «Подпись не подтверждена». Протокол проверки Мобильной подписи распечатывается и подписывается всеми членами Согласительной комиссии.	11.12 **Mobile signature verification procedure** 11.12.1 To verify that the Mobile signature belongs to the Authorized Representative of the Client and that there are no distortions in the Electronic Document, the disputed Electronic Message, the signature file for the disputed Electronic Message and the file with the Mobile Signature key identifier are extracted from the Bank's database by an authorized employee of the Bank. 11.12.2 To resolve a conflict situation, the reference software and hardware of the Bank is used. Special software is used to verify the Mobile signature under the Electronic Document. 11.12.3 The ownership of the Mobile signature verification key contained in the extracted file to the Client's Authorized Representative is established according to the following procedure: the Mobile signature key number extracted from the Bank's database is compared with the key number specified in the "Acknowledgement Act of the mobile signature verification key for messaging in the RBS system Bank 131 JSC stored in the Client's file or in the Bank's database. If the ownership of the key is established, the Commission proceeds to the next stage. If the information does not match, the disputed document is recognized as incorrect. 11.12.4 Verification of the Mobile Signature of the disputed Electronic Document is carried out by the MobileSignVerify program (developer is Information Systems LLC). Based on the results of the verification, the signature under the disputed Electronic Document is recognized as belonging to the Authorized Representative of the Client, if the verification protocol issued by the program specified in this clause contains an entry stating that “Verification result: “Signature is confirmed” (signature correct), and does not belong to the Authorized Representative Client, in case of Verification Result: "Signature not confirmed". The Mobile signature verification protocol is printed out and signed by all members of the Conciliation Commission.
11.13. Ответственность сторон при оспаривании Электронных документов, обмен которыми осуществляется с использованием Системы ДБО, подписанных усиленной неквалифицированной Электронной подписью.	**11.13. Responsibility of the parties in contesting Electronic Documents exchanged with the use of the**

• 11.13.1 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 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 получения Банком оспариваемого Электронного документа.

11.13.2 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.

11.13.3 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.

11.14. Ответственность сторон при оспаривании Электронных документов, обмен которыми осуществляется с использованием Системы ДБО, подписанных простой Электронной подписью.

11.14.1 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

RBS System and signed by an enhanced non-certified Electronic Signature.

11.13.1. 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 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.

11.13.2.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.

11.13.3.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 Regulations (including their annexes), these Regulations, 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.

11.14. Responsibility of the parties in contesting Electronic Documents exchanged using the RBS System and signed with a simple electronic signature.

11.14.1.The Bank shall not be liable to the Client in the

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.

11.14.2 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.

11.14.3 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.

11.15. Ответственность сторон при оспаривании Электронных документов, обмен которыми осуществляется с использованием Системы ДБО, подписанных Мобильной подписью.

11.15.1. 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 Мобильной подписи 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

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.

11.14.2.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.

11.14.3.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 Regulations (including their annexes), these Regulations, 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 unfavorable for the Client, the Bank and other persons, related to such violation/ improper fulfillment.

11.15 Responsibility of the parties when disputing Electronic Documents exchanged using the RBS System, signed by the Mobile Signature.

11.15.1 The Bank shall not be liable to the Client in the cases specified in the Rules (including annexes thereto), as well as if the Conciliation Commission establishes the totality of the following facts when verifying the Mobile Signature by the disputed Electronic Document:

• it has not been established that the Bank received from the Client a Notification of the compromise of the Electronic Signature key and/or an application to block access to the RBS System of the Authorized Representative of the Client using the Electronic

Систему ДБО позже или равна моменту получения Банком оспариваемого Электронного документа.

- Установлен факт подтверждения Клиентом операции в мобильном приложении.

11.15.2. 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.

11.15.3. 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.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

12.2. 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.

Document Confirmation Tool that signed the disputed Electronic Document, or the moment the Bank received the Notification of the compromise of the key Electronic signature and/or application for blocking access to the RBS System is later or equal to the moment of receipt by the Bank of the disputed Electronic Document.

• The fact of the Client's confirmation of the operation in the mobile application has been established.

11.15.2 The Bank is not liable to the Client and does not compensate the Client for the lost profit of the latter. The Bank's liability arises only if the latter is proven guilty and there is a direct causal relationship between the events that have occurred, the Bank's proven fault and negative consequences for the Client.

11.15.3 The Client/Authorized Representative of the Client shall be liable to the Bank in all and any cases of non-fulfillment and/or improper fulfillment of the Rules (including annexes thereto), these Regulations, the provisions of the legislation of the Russian Federation and the requirements of the Bank, and also bear the risk of any legal and /or financial consequences, including those unfavorable for the Client, the Bank, other persons, associated with such violation/improper performance.

12 FINAL PROVISIONS

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

12.2. Legal relations of the Parties settled by these Regulations, as well as any other legal relations of the Parties related to the implementation of these Regulations, 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 Regulations 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 Regulations is mandatory. The deadline for replying to a pre-trial

12.3. 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. 12.4. 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 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 настоящим 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.	claim is 30 (thirty) days from the date of its receipt by the Bank. 12.3. In the event of changes in the provisions of the legislation of the Russian Federation in which the provisions of these Regulations 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 Regulations as a whole and/or any other provisions of the Regulations in the event of invalidity of any provision of these Regulations. The provisions of the Russian Federation legislation shall be applied to the legal relations of the Parties in lieu of the invalid provision. 12.4. The Bank may unilaterally and extrajudicially amend these Regulations and/or their annexes. Amendments to these Regulations 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 Regulations 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 the Bank, and at least once every 10 (ten) calendar days, the Client and its Authorized Persons are obliged to familiarize themselves with these Regulations, 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 Regulations 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 Regulations, 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 Regulations. 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 Regulations, 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 и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО

АО «Банк 131»
420012, РФ, Республика Татарстан,
г. Казань, ул. Некрасова, д. 38
ИНН/ОГРН 1655505780/1241600056390

_____ _____202_

Заявление[1] №_____
о присоединении к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО

ФИО	
Серия и номер паспорта	
Орган и дата выдачи паспорта	
Действующий на основании _	
От имени Клиента	
ОГРН	
Адрес электронной почты[2]	
Абонентский номер[3]	

Настоящим сообщаю АО «Банк 131» что полностью и безусловно соглашаюсь с Регламентом дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «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 АО «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, указанный в настоящем заявлении, для направления Логина и Временного Пароля для доступа в Систему ДБО, а также Средств подтверждения.
☐ выдать Мобильную подпись и установить Абонентский номер, указанный в настоящем заявлении, для направления Логина и Временного Пароля для доступа в Систему ДБО и активации ключа Мобильной подписи.
☐ ***(используется для Уполномоченных Представителей Клиента с правом просмотра)*** установить Абонентский номер, указанный в настоящем заявлении, для направления Логина и Временного Пароля для доступа в Систему ДБО, а также Одноразовых кодов для аутентификации.
☐Уведомления о совершенных операциях прошу направлять:
☐ по адресу электронной почты
☐ на Абонентский номер

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

Настоящим подтверждаю, что указанные в настоящем заявлении Абонентский(-ие) номер (-а) 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 и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО ознакомлен и согласен, обязуюсь выполнять требования, указанные в них.

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

[1] Номер Заявления присваивается после регистрации Уполномоченного Представителя Клиента в реестрах Системы ДБО.
[2] Указывается адрес электронной почты уполномоченного лица. Поле обязательно для заполнения.
[3] Указывается Абонентский номер уполномоченного лица. Поле обязательно для заполнения.

To be filled in by the Bank / Заполняется Банком

Идентификация Уполномоченного лица Клиента проведена, полномочия и документы проверены, Заявление зарегистрировано в Банке «____» _____ 20____ г.

_____ _____ _____ « ___» ___ 20 __ г.
(должность) (подпись) (расшифровка подписи.)

Отметка об исполнении:
Заявление выполнено, присвоен № _____ **:**

_____ _____ _____ « ___» ___ 20 __ г.
(должность) (подпись) (расшифровка подписи.)

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

_____ _____202_

Заявление №/ Application[1] No. _____

о присоединении к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО

on joining the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs

ФИО / Full name	
Серия и номер паспорта / Passport series and number	
Орган и дата выдачи паспорта / Authority issued the passport and date of the issue	
Действующий на основании/ Acting on the basis of	
От имени Клиента / On behalf of the Client	
Регистрационный № / Registration No.	
Адрес электронной почты[2] / e-mail address	
Абонентский номер[3] / Subscriber Number	

Настоящим сообщаю АО «Банк 131» что полностью и безусловно соглашаюсь с Регламентом дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «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.

I hereby inform Bank 131 JSC that I fully and unconditionally agree with the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs (hereinafter referred to as the Regulations), have read and agree with the Regulations, including their annexes, and will comply with all the provisions of the Regulations when using the RBS system.

Прошу зарегистрировать меня в Системе ДБО АО «Банк 131» и: / I hereby request to register me in the RBS System of Bank 131 JSC and:

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

☐ выдать простую Электронную подпись и установить Абонентский номер, указанный в настоящем заявлении, для направления Логина и Временного Пароля для доступа в Систему ДБО, а также Средств подтверждения / issue a simple Electronic Signature and set the Subscriber Number specified in this application to send the Login and Temporary Password for access to the RB System, as well as Confirmation Tools

☐ выдать Мобильную подпись и установить Абонентский номер, указанный в настоящем заявлении, для направления Логина и Временного Пароля для доступа в Систему ДБО и активации ключа Мобильной подписи. / issue a Mobile Signature and set the Subscriber Number specified in this application to send a Login and a Temporary Password to access the RB System and activate the Mobile Signature key. /

☐***(используется для Уполномоченных Представителей Клиента с правом просмотра)*** установить Абонентский номер, указанный в настоящем заявлении, для направления Логина и Временного Пароля для доступа в Систему ДБО, а также Одноразовых кодов для аутентификации. / set the Subscriber number specified in this application for sending the Login and Temporary Password for access to the RBS System, as well as One-Time Codes for authentication/

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

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

[2] Указывается адрес электронной почты уполномоченного лица. Поле обязательно для заполнения / The e-mail address of the authorized person is indicated. Required field.

[3] Указывается Абонентский номер уполномоченного лица. Поле обязательно для заполнения / The subscriber number of the authorized person is indicated. Required field.

☐ по адресу электронной почты / at e-mail address:
☐ на Абонентский номер / to the Subscriber number:

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

Question / вопрос: _____ _ answer / ответ: _____

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 и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО ознакомлен и согласен, обязуюсь выполнять требования, указанные в них.

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 Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs have been read and agreed.

Authorised Represent 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 зарегистрировано в Банке «____» _____ 20____ г.

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:
Заявление выполнено, присвоен № _____ **:**

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Приложение №2 к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО

АКТ № ___
приема-передачи ФКН Системы ДБО

г. Казань «___» _____20__ г.

АО «Банк 131», именуемое в дальнейшем Банк в лице _____, действующего(-ей) на основании _____ с одной стороны, и _____ , именуемый в дальнейшем «Клиент», в лице____
_____, действующего(-ей) на основании _____, с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», в рамках Регламента дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» (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 и индивидуальных предпринимателей в АО «Банк 131» и Регламентом дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО:

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

Передал
АО «Банк 131»
420012, Республика Татарстан,
г. Казань, ул. Некрасова, д. 38
ИНН/ОГРН 1655505780/1241600056390

от Банка:
_____
(должность)

_____ _____
(подпись) (расшифровка подписи)

Принял
Наименование
Адрес
ИНН/ОГРН

от Клиента:
_____
(должность) М.П.

_____ _____
(подпись) (расшифровка подписи)

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

Kazan _____20 _

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

Bank 131 JSC, hereinafter referred to as the Bank represented by _____
acting under _____
on the one part, and _____
hereinafter referred to as the Client`s Authorized person
represented by _____
acting under _____
on the other part, referred together herein as Parties and individually as a Party, within the scope of the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs (Application on joining
No. _____ dated _____ _____20__), have drawn up this Act as follows:

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 и индивидуальных предпринимателей в АО «Банк 131» и Регламентом дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО:

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 Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs and the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC corporate clients:

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

Transferred to Bank 131 JSC (Bank) Nekrasova 38, Kazan, Republic of Tatarstan, 420012 INN/OGRN 1655505780/1241600056390 from the Bank: (title) (signature)	Accepted Name _____ Address _____ Reg. No._____ from the Client: (title) (signature)

Приложение №3 к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО

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

г. Казань **«___» _____20__ г.**

ФИО	
Серия и номер паспорта	
Орган и дата выдачи паспорта	
Действующий на основании _	
От имени Клиента	
ОГРН	
Адрес электронной почты[1]	
Абонентский номер[2]	

В соответствии с Регламентом дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «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 АО «Банк 131» не имею);

☐ – произвести смену логина и статического пароля и направить данные для входа в систему ДБО на мой Абонентский номер, указанный в Заявление на приобретение/изменение БП.

☐ – произвести смену ключа Мобильной подписи и направить данные для активации ключа Мобильной подписи на Абонентский номер;

☐ - установить новый Абонентский номер, на который прошу направлять Логин и Временный пароль для доступа в Систему ДБО, прохождения процедуры аутентификации и подписания Электронных документов при ее использовании, для указанных Уполномоченных лиц: + (___)_____;

☐Уведомления о совершенных операциях прошу направлять:

☐ по адресу электронной почты

☐ на Абонентский номер:

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.

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

[1] The e-mail address of the authorized person is indicated. Required field.

[2] The subscriber number of the authorized person is indicated. Required field

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

Application
on login and static password change / unlocking RBS system access / subscriber number of mobile communication change

Kazan **___ _____ 20___**

Full name / ФИО	
Passport series and number/Серия и номер паспорта	
Authority issued the passport and date of the issue/Орган и дата выдачи паспорта	
Acting on the basis of / Действующий на основании _	
On behalf of the Client / От имени Клиента	
Registration No. / Регистрационный №	
e-mail address/Адрес электронной почты[1]	
Subscriber Number/ Абонентский номер[2]	

В соответствии с Регламентом дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО прошу:

In accordance with the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs, I hereby request to:

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

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

☐ – change the Mobile Signature key and send and send the data for activating the Mobile Signature key to the Subscriber number /произвести смену ключа Мобильной подписи и направить и направить данные для активации ключа Мобильной подписи на Абонентский номер;

☐ - 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: /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: + (___)_____;

☐ 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: + (____)_____.

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 исключительнс и только мне, иные лица не имеют доступа к нему.

_____/_____ /_____ _____202_ /

(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.:

_____/_____/_____ «___» _____20___г

[1] The e-mail address of the authorized person is indicated. Required field.

[2] The subscriber number of the authorized person is indicated. Required field.

(должность) (подпись) (расшифровка подписи) (дата)

Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г

(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:

Ответственный работник Банка**:**

_____/_____/_____ «___» _____20___г

(должность) (подпись) (расшифровка подписи) (дата)

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.

ФИО	
Серия и номер паспорта	
Орган и дата выдачи паспорта	
Действующий на основании	
От имени Клиента	
ОГРН	

в соответствии с Регламентом дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО, настоящим уведомляю АО «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 и индивидуальных предпринимателей в АО «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:

№	Ф.И.О. владельца – Уполномоченного лица	Серийный номер Сертификата ключа Электронной подписи
1		

☐Простую ЭП и Абонентский номер мобильной связи:

№	Ф.И.О. владельца-Уполномоченного лица	Абонентский номер мобильного устройства
1		

☐Ключ мобильной подписи:

№	Ф.И.О. владельца-Уполномоченного лица	Абонентский номер мобильного устройства
1		

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

М.П.

Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены, Заявление зарегистрировано в Банке «____» _____:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

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)

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)

Kazan ___ _____20__

Full name / ФИО	
Passport series and number/Серия и номер паспорта	
Authority issued the passport and date of the issue/Орган и дата выдачи паспорта	
Acting on the basis of / Действующий на основании	
On behalf of the Client / От имени Клиента	
Registration No. / Регистрационный №	

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

In accordance with the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs hereby notifies Bank 131 JSC on the Electronic Signature Compromise in connection with

_____

_____

_____

_____

(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)

(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)

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

I hereby request to block Means of Confirmation noted below that were used within the scope of the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs according to Application on joining

No. _____ dated _____20__
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:

☐Сертификаты ключей Электронной подписи/ Certificate of the electronic signature verification key:

№	Full name of the owner - Authorized person / Ф.И.О. владельца – Уполномоченного лица	Certificates of the electronic signature verification key Serial number / Серийный номер Сертификата ключа Электронной подписи
1		

☐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
1		

☐Mobile Signature Key/ Ключ мобильной подписи:

№	Full name of the owner - Authorized person /Ф.И.О. владельца-Уполномоченного лица	Subscriber number of the mobile device / Абонентский номер мобильного устройства
1		

_____/_____ /_____202_ /
(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:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Приложение №5 к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «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 АО «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. При использовании Мобильной подписи/Простой Электронной подписи внимательно проверять информацию об Операции, полученную в СМС-сообщении с Одноразовым паролем или в PUSH-сообщении.
3. Использовать процедуру аутентификации доступа к Мобильному устройству (ввод пароля для разблокировки Мобильного устройства), вход по отпечатку пальца, Face-ID.
4. Своевременно устанавливать доступные обновления операционной системы и приложений на ваш телефон.
5. Мобильное устройство не должно быть подвергнуто операциям повышения привилегий / взлома операционной системы устройства (jail-break, rooting).
6. Использовать антивирус для Мобильного устройства, своевременно устанавливать на него обновления вирусных баз.
7. Никогда не передавайте свое Мобильное устройство и sim-карту третьим лицам.
8. Ключи Усиленной неквалифицированной Электронной подписи (далее по тексту – УНЭП) хранить только на ФКН (Функциональный ключевой носитель) в недоступном для посторонних и неуполномоченных лиц месте (запирающиеся персональный сейф, металлический шкаф).
9. Не допускается:
- снимать копии с ФКН;
- передавать ФКН лицам, к ним не допущенным;
- записывать на ФКН постороннюю информацию.

Annex 5 to the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs

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 JSC, 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. When using a Mobile signature/Simple Electronic Signature, carefully check the information about the Operation received in an SMS message with a One-time password or in a PUSH message..
3. Use the procedure for authenticating access to the Mobile Device (entering a password to unlock the Mobile device), entering by fingerprint, Face-ID.
4. Install available operating system and app updates on your phone in a timely manner.
5. The mobile device must not be subjected to operations of privilege escalation / hacking of the device's operating system (jail-break, rooting).
6. Use an antivirus for a mobile device, install virus database updates on it in a timely manner.
7. Never transfer your Mobile Device and SIM Card to third parties.
8. The Enhanced Non-Certified Electronic Signature (ENCES) 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).
9. 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.

10. 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.	10. 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.
11. Статический пароль должен: - быть не менее 8 символов; - содержать цифры, строчные и заглавные буквы; - содержать хотя бы 1 символ, не являющийся буквой или цифрой.	11. 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.
12. На персональном компьютере (ноутбуке) должна быть установлена парольная защита на вход в Операционную систему.	12. A password protection for accessing the Operating System must be installed on the personal computer (laptop).
13. Рекомендуется менять пароль пользователя в операционной системе, а также в Системе ДБО не реже одного раза в 3 месяца.	13. 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.
14. Пароль доступа к ключу УНЭП хранить отдельно от ФКН.	14. The password for accessing the ENCES key should be stored separately from the FCN .
15. Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в доступных третьим лицам местах, передавать неуполномоченным лицам.	15. It is strictly prohibited to write down passwords on paper or in text files at the workplace, to leave them available to third parties or to pass them on to unauthorised persons.
16. 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.	16. 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.
17. 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.	17. 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.
18. Не копировать содержимое ФКН, содержащего ключ ЭП, и не передавать его никому даже на короткое время.	18. Do not copy the contents of the FKM containing the ES key or pass it on to anyone, even for a short time.
19. Закончив работу в Системе ДБО или прервав её (даже на несколько минут), извлечь ФКН, содержащий ключ УНЭП, и убрать его в недоступное другим лицам место.	19. After completing or interrupting work in the RBS system (even for a few minutes), extract the FKM containing the ENCES key and remove it to an area inaccessible to others.
20. Применять на рабочем месте лицензионные средства защиты от вредоносного кода с возможностью автоматического обновления баз данных сигнатур вредоносного кода.	20. Apply licensed anti-malware at the workplace with the possibility of automatically updating malware signature databases.
21. Если в качестве компьютера для работы в Системе ДБО используется переносной компьютер	21. If a portable computer (laptop) is used as a computer for work in the RBS System, its

(ноутбук), должно быть исключено его подключение к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.)	connection to public networks in places with free Internet access (office centres, cafes, etc.) must be excluded.
22. Осуществлять постоянный контроль отправляемых платежных (расчетных) документов при работе с Системой ДБО, а также за состоянием расчетных (банковских) счетов, операциям по ним и остаткам.	22. 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.
23. 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) 5983131 с 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 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	23. 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 Regulations 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; - 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).

ключевой информации).	
24. 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 и индивидуальных предпринимателей в АО «Банк 131», а также обратиться с соответствующим заявлением в правоохранительные органы.	24. 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 JSC using the RBS system, as well as to apply to law enforcement agencies.
25. 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.	25. 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.
26. Использовать комбинации клавиш «Ctrl + Alt + Del» для идентификации пользователя в операционной системе.	26. Use the key Ctrl + Alt + Del combination to identify the user in the operating system.
27. Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы по Системе ДБО, заблокировать 3389 (RDP Remote desktop).	27. Disable the possibility of remote and terminal connection to computers used for RBS System, block 3389 (RDP Remote desktop).
28. Включить в операционной системе журнал безопасности Windows.	28. Enable the Windows security log in the operating system.
29. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д. (далее по тексту – ПО).	29. Use only licensed such software as operating systems, anti-malware, office packages, etc. (hereinafter referred to as software).
30. Обеспечить возможность своевременного обновления системного и прикладного ПО.	30. Ensure that system and application software can be updated in a timely manner.
31. Доступ в помещение, где размещен компьютер с Системой ДБО, предоставлять только Уполномоченным лицам.	31. Access to the premises where the computer with the RBS System is located shall be granted only to the Authorised Persons.
32. 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.	32. 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.
33. Исключить доступ к компьютерам, используемым для работы по Системе ДБО, посторонних лиц и персонала, неуполномоченных на работу в Системе ДБО и/или обслуживание компьютеров.	33. 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.

34. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.	34. IT staff must ensure that they have control over the actions they take when servicing the computer.
35. АО «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.	35. Bank 131 JSC does not send e-mails requesting to send ES keys and/or password to the RBS System and never asks you for this information.
36. 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.	36. 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.
37. Запрещено передавать логины и пароли третьим лицам в том числе иным Уполномоченным Представителям Клиента.	37. It is prohibited to transfer usernames and passwords to third parties, including other the Client's Authorized Person.

Приложение №6 к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО

Annex 6 to the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs

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[1];

- 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.

1.3 При использовании Мобильной подписи:

-устройство с iOS (три последние версии системы);

- устройство Android — с версии 5.0 и более поздние версии.

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:

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[1];

- 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.

1.3. When using Mobile Signature:

- device with iOS (three latest versions of the system);

- Android device - from version 5.0 and later.

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:

● Установка программного обеспечения сторонних фирм, а также сознательное внесение изменений в файлы программного и информационного обеспечения Системы ДБО; ● Доступ к Системе ДБО неуполномоченных лиц; 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.	● 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; 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.
[1]Инструкция по работе с MacOS размещена на официальном сайте Банка.	[1]Instructions on working with MacOS are available on the Bank's official website.

Приложение №7 к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием системы ДБО

Заявление № _____
на установление ограничений по параметрам операций с использованием Системы дистанционного банковского обслуживания АО «Банк 131»

ФИО	
Серия и номер паспорта	
Орган и дата выдачи паспорта	
Действующий на основании _	
От имени Клиента	
ОГРН	

В соответствии с условиями Договора ДБО прошу установить ограничения по параметрам Операций по Счету(-ам) №: _____

<table>
<tr><td>☐</td><td colspan="2">На максимальные лимиты на операции и за период в разрезе счетов/способов подписания
<table>
<tr><th>Номер счета</th><th>Тип подписи (ПЭП/УНЭП/Мобильная подпись)</th><th>Период (1 операция/1 день/1 неделя/1 месяц)</th><th>Максимальная сумма перевода денежных средств в валюте Счета</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>☐</td><td>перечень разрешенных получателей денежных средств (указываются наименование, реквизиты получателей денежных средств)</td><td>1. Наименование получателя _____
Номер счета _____
БИК_____
ИНН(если есть)_____
2. …</td></tr>
<tr><td>☐</td><td>разрешенный временной период для совершения операций (указывается временной период приема Распоряжений о переводе денежных средств в часовом поясе UTC+3)</td><td></td></tr>
<tr><td>☐</td><td>страны, находясь в которых Клиент может совершать переводы денежных средств (используется определение географического расположения по IP адресу [1]устройства, с которого осуществляется доступ в Систему ДБО)</td><td></td></tr>
<tr><td>☐</td><td>перечень разрешенных категорий операций</td><td>☐ Платеж по шаблону, сохраненному в Системе ДБО
☐ Внутренний платеж (счет получателя открыт в АО «Банк 131»)
☐ Внешний платеж (счет получателя открыт в другой кредитной организации)
☐ Платежи в бюджет РФ</td></tr>
</table>

[1] При использовании VPN сервисов, или анонимайзеров будет определяться конечный IP адрес устройства, с которого будет осуществлён доступ в Систему ДБО, что может повлечь недоступность Системы ДБО.

		☐ Валютный перевод

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

М.П.

Заполняется Банком

Заявление принял ___ часов____ минут «__» _____20__г.
Работник Банка, принявший заявление:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
(расшифровка подписи.)
Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
(расшифровка подписи.)

Ограничения установлены «__» _____20__г. (проставляется дата установки ограничений).
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Application No. _____ for
the establishment of restrictions on the parameters of operations
using the Remote Banking Service System of Bank 131 JSC»
/Заявление № _____
на установление ограничений по параметрам операций
с использованием Системы дистанционного банковского обслуживания АО «Банк 131»

Full name / ФИО	
Passport series and number/Серия и номер паспорта	
Authority issued the passport and date of the issue/Орган и дата выдачи паспорта	
Acting on the basis of / Действующий на основании _	
On behalf of the Client / От имени Клиента	
Registration No. / Регистрационный №	

In accordance with the terms of the RBS System Agreement, please set restrictions on the parameters of Operations on the Account (s)
No.:_____

<table>
<tr><td>☐</td><td colspan="2">For the maximum limits on transactions and for the period in the context of accounts/signing methods /
На максимальные лимиты на операции и за период в разрезе счетов/способов подписания
<table>
<tr><th>Account No.
Номер счета</th><th>Signature Type
(SES / ENCES/ Mobile Signature)/
Тип подписи
(ПЭП/УНЭП/Мобильная подпись)</th><th>Period (1 operation/1 day/1 week/1 month)
/Период (1 операция/1 день/1 неделя/1 месяц)</th><th>Maximum amount of money transfer in the Account currency /
Максимальная сумма перевода денежных средств в валюте Счета</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>☐</td><td>list of authorized recipients of funds (specify the name and details of the recipients of funds) / перечень разрешенных получателей денежных средств (указываются наименование, реквизиты получателей денежных средств)</td><td>1. Наименование получателя _____
Номер счета _____
БИК_____
ИНН (если есть)_____
2. …</td></tr>
<tr><td>☐</td><td>the allowed time period for making transactions (the time period for accepting Money transfer Orders in the UTC+3 time zone is specified) / разрешенный временной период для совершения операций (указывается временной период приема Распоряжений о переводе денежных средств в часовом поясе UTC+3)</td><td></td></tr>
</table>

☐	countries where the Client can make money transfers (the geographical location is determined by the IP address of the device from which the RBO System is accessed) / страны, находясь в которых Клиент может совершать переводы денежных средств (используется определение географического расположения по IP адресу [1]устройства, с которого осуществляется доступ в Систему ДБО)	
☐	list of permitted categories of operations / перечень разрешенных категорий операций	☐ Payment based on a template saved in the RBS System / Платеж по шаблону, сохраненному в Системе ДБО ☐ Internal payment (the recipient's account is opened with Bank 131 JSC) / Внутренний платеж (счет получателя открыт в АО «Банк 131») ☐ External payment (the recipient's account is opened with another credit institution) / Внешний платеж (счет получателя открыт в другой кредитной организации) ☐ Payments to the budget of the Russian Federation / Платежи в бюджет РФ ☐ Currency transfer / Валютный перевод

_____/_____ /_____202_ /
(Signature) (Full name) (Date)

Seal (if any)

To be filled in by the Bank / Заполняется Банком

Заявление принял ___ часов____ минут «__» _____20__г.
Работник Банка, принявший заявление:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
(расшифровка подписи.)

Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
(расшифровка подписи.)

Ограничения установлены «__» _____20__г. (проставляется дата установки ограничений).
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

[1] При использовании VPN сервисов, или анонимайзеров будет определяться конечный IP адрес устройства, с которого будет осуществлён доступ в Систему ДБО, что может повлечь недоступность Системы ДБО.

Приложение №8 к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО

АКТ
признания ключа проверки электронной подписи
юридического лица или индивидуального предпринимателя
для обмена сообщениями в системе ДБО АО «Банк 131»

Город Казань «___» _____ 20__ года

АО «Банк 131», именуемое в дальнейшем Банк в лице _____, действующего(-ей) на основании _____ с одной стороны, и _____ , именуемый в дальнейшем «Клиент», в лице_____, действующего(-ей) на основании _____, с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», составили настоящий Акт о нижеследующем:

1. Владелец Сертификата с использованием программного обеспечения, в соответствии с предоставленным Банком дистрибутивом, самостоятельно создал ключи Усиленной неквалифицированной электронной подписи (далее - УНЭП), позволяющие Владельцу Сертификата подписывать электронные документы УНЭП в Системе ДБО АО «Банк 131» и передал Банку запрос на выпуск Сертификата ключа проверки электронной подписи для регистрации в УЦ Банка. При этом ключ УНЭП хранится и используется Владельцем Сертификата в соответствии с «Инструкцией по обеспечению информационной безопасности при работе в Системе ДБО».

2. Подписание Акта означает взаимное признание УНЭП Клиента с момента регистрации ключа проверки УНЭП Владельца Сертификата в реестре Удостоверяющего Центра Банка и формирования сертификата.

3. Подписание Акта означает, что Владелец сертификата ключа проверки ЭП получил сертификат ключа проверки электронной подписи на бумажном носителе в соответствии с Приложением настоящему Акту и в электронном виде посредством Системы ДБО АО «Банк 131».

АО «Банк 131»: _____/_____
Подпись/Фамилия И.О

Владелец сертификата _____/_____
Подпись/Фамилия И.О
М.П. (при наличии)

АКТ
признания ключа проверки электронной подписи юридического лица или индивидуального предпринимателя
для обмена сообщениями в системе ДБО

АО «Банк 131»

The CERTIFICATE of

recognition of the electronic signature verification key

of a legal entity or individual entrepreneur

for the exchange of messages in the DBO system

of Bank 131 JSC

Kazan ___ _____20__

АО «Банк 131», именуемое в дальнейшем Банк в лице _____,
Действующего(-ей) на основании _____
с одной стороны, и _____
именуемое в дальнейшем Клиент,
в лице _____,
действующего(-ей) на основании _____
с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона»,
составили настоящий Акт о нижеследующем:

Bank 131 JSC, hereinafter referred to as the Bank represented by _____
acting under _____
on the one part, and _____
hereinafter referred to as the Client`s Authorized person
represented by _____
acting under _____
on the other part, referred together herein as Parties and individually as a Party,
have drawn up this Act as follows:

1. Владелец Сертификата с использованием программного обеспечения, в соответствии с предоставленным Банком дистрибутивом, самостоятельно создал ключи Усиленной неквалифицированной электронной подписи (далее - УНЭП), позволяющие Владельцу Сертификата подписывать электронные документы УНЭП в Системе ДБО АО «Банк 131» и передал Банку запрос на выпуск Сертификата ключа проверки электронной подписи для регистрации в УЦ Банка. При этом ключ УНЭП хранится и используется Владельцем Сертификата в соответствии с «Инструкцией по обеспечению информационной безопасности при работе в Системе ДБО».

1. The Certificate Holder, using the software, in accordance with the distribution package provided by the Bank, independently created the keys of the Enhanced Non-Certified Electronic Signature (ENCES), which allow the Certificate Holder to sign the electronic documents of the ENCES in the System of RBS of Bank 131 JSC and submitted to the Bank a request for issuing a Certificate of the electronic signature verification key for registration in the Bank's UC. At the same time, the ENCES key is stored and used by the Certificate Holder in accordance with the "Instructions for ensuring information security when working in the RBS System".

2. Подписание Акта означает взаимное признание УНЭП Клиента с момента регистрации ключа проверки УНЭП Владельца Сертификата в реестре Удостоверяющего Центра Банка и формирования сертификата.

2. The signing of the Act means the mutual recognition of the Client's ENCES from the moment of registration of the Certificate Holder's ENCES verification key in the register of the Bank's Certification Center and the formation of the certificate.

3. Подписание Акта означает, что Владелец сертификата ключа проверки ЭП получил сертификат ключа проверки электронной подписи на бумажном носителе в соответствии с Приложением настоящему Акту и в электронном виде посредством Системы ДБО АО «Банк 131».

3. The signing of the Certificate means that the Holder of the certificate of the electronic signature verification key has received the certificate of the electronic signature verification key on paper in accordance with the Annex to this Act and in electronic form through the RBS System of Bank 131 JSC.

Bank 131 JSC / АО «Банк 131»: _____/_____
Подпись/Фамилия И.О
Signature/Printed

Certificate Holder / Владелец сертификата : _____/_____
Подпись/Фамилия И.О
Signature/Printed
Seal / М.П. (при наличии)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:01:01:08:01:01:01:0a
        Signature Algorithm: gost3410-2012-256 (1.2.643.7.1.1.3.2)
        Issuer: C=RU, SP=116 Казань, L=Казань, O="АО "Банк 131"", CN="Тестовый УЦ АО"Банк 131"", Email=ca@131.ru,
OGRN=1191690025746
        Validity
            Not Before: Oct 20 09:51:18 2020 GMT
            Not After : Oct 20 09:51:18 2021 GMT
        Subject: C=RU, O="ООО "Барбариска"", T=директор, CN=Пользователь ДБО 1sfront, STREET="*Казань, ул.Некрасова, 38"
        Subject Public Key Info:
            Public Key Algorithm: gost3410-2012-256 (1.2.643.7.1.1.1.1)
            Public Key:
                pub:
                    b4:7f:6d:d0:62:22:7d:20:fc:05:bd:7f:f7:18:94:
                    96:26:b2:2c:e0:66:9e:54:39:fd:a3:0c:3c:c5:af:
                    83:77:d2:75:f5:88:15:46:99:46:c[illegible]:c:f9:9e:11:
                    7d:a4:40:6a:f5:1a:5c:21:38:05:11:00:f2:d5:69:
                    d3:39:e6:e7
                Parameters OID: 1.2.643.2.2.35.1
        X509v3 extensions:
            Subject Key Identifier:
                cc:a7:0a:f0:b4:b9:d6:a6:16:e0:12:15:a2:01:a6:ca:1b:2d:20:22
            Authority Key Identifier:
                keyid:a6:7a:61:07:27:b4:4b:6b:d1:f4:9c:02:9b:d2:e4:7a:49:04:2e:a8

            Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
            Extended Key Usage:
                TLS Web Client Authentication
                E-mail Protection

    Signature Algorithm: gost3410-2012-256 (1.2.643.7.1.1.3.2)
        b8:d5:9d:2f:8e:2f:a1:7e:5b:4c:de:5a:f6:cb:a9:2f:c4:d2:
        86:53:a6:96:0f:db:c3:02:7d:cf:ca:82:ae:0b:71:b7:c3:4f:
        19:a9:e3:11:05:7c:9d:b3:60:1e:50:e0:71:aa:6f:5b:5f:d1:
        08:3e:87:3a:8d:93:4b:71:0b:f2
```

ОБРАЗЕЦ

АО «Банк 131»: _____/_____
Подпись/Фамилия И.О

Владелец сертификата _____/_____
Подпись/Фамилия И.О
М.П. (при наличии)

Приложение №9 к Регламенту дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Банк 131» с использованием Системы ДБО

АКТ
признания ключа проверки мобильной подписи
для обмена сообщениями в системе ДБО АО «Банк 131»

Город Казань «___» _____ 20__ года

АО «Банк 131», именуемое в дальнейшем Банк в лице _____, действующего(-ей) на основании _____ с одной стороны, и _____ , именуемый в дальнейшем «Клиент», в лице_____, действующего(-ей) на основании _____, с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», составили настоящий Акт о нижеследующем:

Владелец ключа Мобильной подписи с использованием программного обеспечения, в соответствии с предоставленным Банком дистрибутивом, самостоятельно провел активацию ключа Мобильной подписи, позволяющий Владельцу подписывать электронные документы в Системе ДБО АО «Банк 131». При этом ключ Мобильной подписи хранится на сервере Банка и используется Владельцем ключа в соответствии с «Инструкцией по обеспечению информационной безопасности при работе в Системе ДБО».

Владелец ключа проверки электронной подписи: **Иванов Иван Иванович**
Организация: **ООО «Лучшая компания»**
Номер договора об ЭП: **260853**
Идентификатор ключа: **ADBCDEFG1234567890XADBCDEFG1234567890X**

Представление ключа проверки электронной подписи в шестнадцатеричном виде:
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234

ОБРАЗЕЦ

АО «Банк 131»: _____/_____
Подпись/Фамилия И.О

Владелец сертификата _____/_____
Подпись/Фамилия И.О
М.П. (при наличии)

Annex 9 to the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs

The CERTIFICATE of
recognition of the mobile signature verification key
for the exchange of messages in the DBO system

of Bank 131 JSC

Kazan ___ _____20

Bank 131 JSC, hereinafter referred to as the Bank represented by _____ acting under _____
on the one part, and hereinafter referred to as the Client`s Authorized person represented by _____ acting under _____ on the other part, referred together herein as Parties and individually as a Party, have drawn up this Act as follows:

The mobile signature key Holder, using the software, in accordance with the distribution package provided by the Bank, independently activated the Mobile Signature key which allow the Holder to sign the electronic documents in the System of RBS of Bank 131 JSC. In this case, Mobile Signature key is stored on the Bank's server and used by the key Holder in accordance with the "Instructions for ensuring information security when working in the RBS System".

The Holder of the electronic signature verification key: **Ivanov Ivan Ivanovich**
Company: **Best Company LLC**
Electronic signature Agreement number: **260853**
Key identifier: **ADBCDEFG1234567890XADBCDEFG1234567890X**

SAMPLE

Representation of the electronic signature verification key in hexadecimal form:
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234
XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234 XYXY 1234

Bank 131 JSC: _____/_____
Signature/Printed

Certificate Holder _____/_____
Signature/Printed
Seal (if any)