

**РЕГЛАМЕНТ ДИСТАНЦИОННОГО
БАНКОВСКОГО ОБСЛУЖИВАНИЯ
ЮРИДИЧЕСКИХ ЛИЦ, ИНДИВИДУАЛЬНЫХ
ПРЕДПРИНИМАТЕЛЕЙ, ФИЗИЧЕСКИХ ЛИЦ,
ЗАНИМАЮЩИХСЯ В УСТАНОВЛЕННОМ
ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ
ФЕДЕРАЦИИ ПОРЯДКЕ ЧАСТНОЙ
ПРАКТИКОЙ В АО «БАНК 131» С
ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДБО
ФАКТУРА.RU**

**REGULATIONS ON REMOTE BANKING
SERVICES FOR LEGAL ENTITIES,
INDIVIDUAL ENTREPRENEURS, AND
INDIVIDUALS ENGAGED IN PRIVATE
PRACTICE AT BANK 131 JSC IN THE
MANNER ESTABLISHED BY THE
LEGISLATION OF THE RUSSIAN
FEDERATION USING FAKTURA.RU RBS
SYSTEM**

1.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 2

1.TERMS AND DEFINITIONS 2

2.ОБЩИЕ ПОЛОЖЕНИЯ 9

2.GENERAL PROVISIONS 9

3..ПОРЯДОК АККРЕДИТАЦИИ И ПОДКЛЮЧЕНИЯ
КЛИЕНТА К СИСТЕМЕ ДИСТАНЦИОННОГО
БАНКОВСКОГО ОБСЛУЖИВАНИЯ 176

3. PROCEDURE FOR ACCREDITATION AND
CONNECTING THE CLIENT TO THE REMOTE
BANKING SERVICE SYSTEM 16

4.ПОРЯДОК ВЫПУСКА СЕРТИФИКАТОВ
ПРОВЕРКИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ
ПОДПИСИ/РЕГИСТРАЦИИ СЕРТИФИКАТОВ КЭП
ФНС 223

4. PROCEDURE FOR ISSUING ELECTRONIC
SIGNATURE VERIFICATION KEY
CERTIFICATES / QES FTS CERTIFICATES
REGISTRATION 21

5.ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВОЙ СМЕНЫ
СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ
ЭЛЕКТРОННОЙ ПОДПИСИ/СЕРТИФИКАТА КЭП
ФНС **Ошибка! Закладка не определена.**

5. PROCEDURE FOR SCHEDULED
REPLACEMENT OF THE ELECTRONIC
SIGNATURE VERIFICATION KEY CERTIFICATE
/ CERTIFICATE OF QUALIFIED ELECTRONIC
SIGNATURE OF FEDERAL TAX SERVICE 253

6. ПОРЯДОК БЛОКИРОВКИ И ВОССТАНОВЛЕНИЯ
ДОСТУПА К СИСТЕМЕ ДБО 254

6. PROCEDURE FOR BLOCKING AND
RESTORING ACCESS TO RBS SYSTEM 24

7.ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ
КОМПРОМЕТАЦИИ ИЛИ ПОДОЗРЕНИЯ НА
КОМПРОМЕТАЦИЮ ЭЛЕКТРОННОЙ ПОДПИСИ
258

7. PROCEDURE FOR ACTIONS IN CASE OF
COMPROMISE OR SUSPICION OF COMPROMISE
OF THE ELECTRONIC SIGNATURE 308

8.ПОРЯДОК ПРОВЕДЕНИЯ ВНЕПЛАНОВОЙ
СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ
ЭЛЕКТРОННОЙ
ПОДПИСИ/КВАЛИФИЦИРОВАННОГО
СЕРТИФИКАТА КЭП ФНС 30

8.PROCEDURE FOR UNSCHEDULED
REPLACEMENT OF THE ELECTRONIC
SIGNATURE VERIFICATION KEY CERTIFICATE
/ QES FTS QUALIFIED CERTIFICATE 30

9.ПОРЯДОК ПРОВЕРКИ ПОДЛИННОСТИ
ЭЛЕКТРОННОЙ ПОДПИСИ. ПОРЯДОК
РАССМОТРЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ 31

9. PROCEDURE FOR VERIFYING THE
AUTHENTICITY OF AN ELECTRONIC
SIGNATURE. PROCEDURE FOR RESOLVING
DISPUTES 31

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ 34

10. FINAL PROVISIONS 34

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Регламенте дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru (далее - Регламент) используются термины и определения, указанные в Правилах комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» (и приложениях к ним), далее – Правила, если иное не указано в настоящем Регламенте.

Аутентификационные данные – Логин, Пароль, а также иные данные Клиента, используемые для доступа в Систему ДБО.

Аккредитация – предоставление Банком возможности Клиенту обслуживаться в Системе ДБО с целью обмена информацией и ЭД в соответствии с Правилами Сервиса Faktura.ru.

Веб-приложение – веб-приложение «Интернет-банк», предоставляющее Клиенту и/или Уполномоченному Представителю Клиента возможность удалённого доступа к функционалу Системы ДБО.

Владелец квалифицированного сертификата КЭП ФНС – Клиент, которому Удостоверяющим центром ФНС России выдан квалифицированный сертификат ключа проверки электронной подписи ФНС и которое владеет соответствующим ключом КЭП ФНС, позволяющим с помощью средств криптографической защиты информации, сертифицированных ФСБ России, создавать квалифицированную электронную подпись в Электронных документах (подписывать Электронные документы), а также расшифровывать Электронные документы, адресованные Владелецу квалифицированного сертификата КЭП ФНС.

Владелец Сертификата ключа проверки электронной подписи – физическое лицо (Уполномоченный Представитель Клиента), на имя которого Удостоверяющим центром выдан Сертификат ключа проверки ЭП и которое владеет

1.TERMS AND DEFINITIONS

The terms and definitions specified in the Comprehensive Banking Services Rules for legal entities, individual entrepreneurs, and individuals engaged in private practice at Bank 131 JSC in accordance with the legislation of the Russian Federation (and its appendices), hereinafter – the Rules, shall apply in the Regulation on Remote Banking Services for legal entities, individual entrepreneurs, and individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System (hereinafter – the Regulation), unless otherwise stipulated in this Regulation.

Authentication Data are Login, Password, and other Client's data used to access RBS System.

Accreditation is enabling the Client by the Bank to be serviced in the RBS System for the purpose of exchanging information and electronic documents in accordance with the Faktura.ru Service Rules.

Web Application is Online Bank web application that provides the Client and/or the Client's Authorized Representative with remote access to the functionality of the RBS System.

Holder of the Qualified Certificate of Qualified Electronic Signature of the Federal Tax Service is a Client who has been issued a Qualified Electronic Signature Verification Key Certificate of the Federal Tax Service by the Certification Authority of the Federal Tax Service of Russia and who holds the corresponding Qualified Electronic Signature of the Federal Tax Service Key, which allows the creation of a Qualified Electronic Signature in Electronic Documents (signing Electronic Documents) and the decryption of Electronic Documents addressed to the Holder of the Qualified Certificate of Qualified Electronic Signature of the Federal Tax Service by means of data cryptographic protection facilities certified by the Federal Security Service of the Russian Federation.

The Holder of the Electronic Signature Verification Key Certificate is an individual (the Client's Authorized Representative) in whose name the Certification Authority has issued an ES Verification

соответствующим Ключом ЭП, позволяющим с помощью средств ЭП создавать Электронную подпись в Электронных документах (подписывать Электронные документы).

Имитовставка – последовательность данных фиксированной длины, вычисленная на основе сообщения и секретного (симметричного) ключа с целью обеспечения возможности обнаружения подмены и/или имитации Простого ЭД. Позволяет обеспечить целостность Простого ЭД.

Квалифицированный сертификат ключа проверки КЭП ФНС (КС КЭП ФНС, Сертификат КЭП ФНС) – сертификат ключа проверки КЭП ФНС, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» (далее – «Закон об электронной подписи») и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный Удостоверяющим центром ФНС России.

Квалифицированная электронная подпись ФНС (КЭП ФНС) – электронная подпись, квалифицированный сертификат которой выдан Клиенту Удостоверяющим центром ФНС России.

Клиент - юридическое лицо (за исключением кредитных организаций), индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, обладающее полной право- и дееспособностью, обратившееся в Банк в собственных интересах, которому Банк оказывает услугу на разовой основе либо которое принимается на обслуживание, предполагающее длящийся характер отношений, при осуществлении банковских операций и других сделок, указанных в статье 5 Федерального закона "О банках и банковской деятельности", в рамках заключенного с Банком Договора Продукта, предусматривающего обмен Электронными документами, и присоединившееся к Правилам.

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

Ключ КЭП ФНС – уникальная последовательность символов, предназначенная для создания КЭП ФНС.

Ключ проверки КЭП ФНС – уникальная последовательность символов, однозначно связанная с ключом КЭП ФНС и предназначенная для проверки подлинности КЭП ФНС.

Key Certificate and who holds the corresponding ES Key, which allows the creation of an Electronic Signature in Electronic Documents (signing Electronic Documents) using ES tools.

Message Authentication Code is a fixed-length data sequence calculated based on a message and a secret (symmetric) key to ensure the detection of Simple ED substitution and/or imitation. It ensures the integrity of a Simple ED.

Qualified Verification Key Certificate of Qualified Electronic Signature of the Federal Tax Service (QC QES FTS, QES FTS Certificate) is a Verification Key Certificate of Qualified Electronic Signature of the Federal Tax Service that meets the requirements established by Federal Law No. 63-ФЗ "On Electronic Signatures" dated 06/04/2011, (hereinafter referred to as the "Electronic Signature Law") and other regulatory legal acts adopted in accordance therewith, created by the Certification Authority of the Federal Tax Service of Russia.

Qualified Electronic Signature of the Federal Tax Service (QES FTS) is an electronic signature, which qualified certificate is issued to the Client by the Certification Authority of the Federal Tax Service of Russia.

Client is a legal entity (excluding credit institutions), individual entrepreneur, or individual engaged in private practice in the manner established by the legislation of the Russian Federation, possessing full legal capacity, who has applied to the Bank in his/her own interests, to whom the Bank provides a service on a one-time basis, or who is accepted for services implying an ongoing relationship, by performing banking operations and other transactions specified in Article 5 of the Federal Law "On Banks and Banking Activities," under a Product Agreement concluded with the Bank, providing for the exchange of Electronic Documents, and who has acceded to the Rules.

Electronic Signature Verification Key is a unique sequence of characters, uniquely linked to the Electronic Signature Key and used to verify the authenticity of an enhanced unqualified Electronic Signature.

Key of the Qualified Electronic Signature of the Federal Tax Service is a unique sequence of characters used to create the Qualified Electronic Signature of the Federal Tax Service.

Verification Key of the Qualified Electronic Signature of the Federal Tax Service is a unique sequence of characters, uniquely linked to the Key of the Qualified Electronic Signature of the Federal Tax Service and used to verify the authenticity of the

Ключ Электронной подписи (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания усиленной неквалифицированной Электронной подписи.

Компрометация ключа КЭП ФНС – нарушение конфиденциальности Ключа КЭП ФНС, констатация Владельцем квалифицированного сертификата КЭП ФНС обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование Ключа КЭП ФНС неуполномоченными лицами. Действия при компрометации КЭП ФНС регламентируются нормативными и инструктивными документами ФНС России.

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 Разового пароля;
- наличие подозрений, что Ключ ЭП стал известен неуполномоченным третьим лицам;
- возникновение подозрений на утечку информации или ее искажение;
- несанкционированное копирование или подозрение на копирование Разового пароля, функционального ключевого носителя, аппаратного средства и/или SIM-карты с Абонентским номером;
- прекращение полномочий или увольнение уполномоченных лиц, имеющих доступ к Ключу ЭП и(или) Системе ДБО;
- случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими

Qualified Electronic Signature of the Federal Tax Service.

Electronic Signature Key (ES Key) is a unique sequence of characters used to create an enhanced unqualified Electronic Signature.

Compromise of the Key of the Qualified Electronic Signature of the Federal Tax Service is a breach of confidentiality of the Key of the Qualified Electronic Signature of the Federal Tax Service, the recognition of circumstances by the Holder of the Qualified Certificate of Qualified Electronic Signature of the Federal Tax Service, or the occurrence of circumstances that allow unauthorized use of the Key of the Qualified Electronic Signature of the Federal Tax Service by unauthorized persons. Actions in the event of a compromise the Qualified Electronic Signature of the Federal Tax Service are regulated by regulatory and instructional documents of the Federal Tax Service of Russia.

Compromise of an Electronic Signature – The existence of grounds to believe that the trust in the electronic signature keys/tools, authentication data, subscriber number, and/or the electronic signatures themselves or their carriers has been compromised, lost/accessed by unauthorized persons, or may be used without the consent of authorized persons. Events related to the compromise of an electronic signature include, but are not limited to, the following:

- Loss of functional key carriers, with or without subsequent discovery;
- Violation of the rules for storage, use, and destruction (including after expiration) of the electronic signature key (enhanced unqualified);
- Loss, transfer, and/or provision of access to unauthorized third parties to hardware (including mobile phones or other devices) and/or SIM cards with a subscriber number, including those used for sending a One-Time Password;
- Suspicion that the Electronic Signature Key has become known to unauthorized third parties;
- Suspicion of information leakage or distortion;
- Unauthorized copying or suspicion of copying of Static and/or One-Time Passwords, functional key carriers, hardware, and/or SIM cards with a subscriber number;
- Termination of authority or dismissal of authorized persons with access to the Electronic Signature Key and/or RBS System;
- Cases where it is impossible to reliably determine what happened to the carriers containing key information (including cases where the carrier has malfunctioned, and it cannot be conclusively disproven that this occurred as a result of unauthorized actions by third parties, or other types of disclosure of key information).

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).

Корпоративная информационная система «BeSafe» (КИС «BeSafe») – система, организованная Закрытым акционерным обществом «Центр Цифровых Сертификатов» (ИНН 5407187087) и представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот в Системе ДБО в соответствии с «Правилами электронного документооборота корпоративной информационной системы «Besafe», размещенным в сети Интернет по адресу: www.besafe.ru.

Логин – уникальная последовательность символов, состоящая из латинских букв и цифр, которая позволяет Банку однозначно идентифицировать (установить) Клиента/Уполномоченного Представителя Клиента при доступе и работе в Системе ДБО.

Мобильная подпись — технология, позволяющая обеспечивать целостность Простых ЭД с помощью реализации механизма установки Имитовставки на Простой ЭД на мобильном устройстве/ Клиента/Уполномоченного Представителя Клиента.

Мобильное приложение – программное обеспечение для мобильного устройства (смартфона, планшета, функционирующего на системе Android), разработанное Банком или по поручению Банка третьими лицами, предоставляющее Клиенту и/или Уполномоченному Представителю Клиента возможность удалённого доступа к функционалу Системы ДБО. Мобильное приложение содержит элементы СКЗИ, обеспечивающиеся на стороне КИС «Besafe».

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.

Оператор – Закрытое акционерное общество «Биллинговый центр» (ИНН 5401152049), осуществляющее информационное и технологическое взаимодействие между Банком и Клиентом в рамках дистанционного банковского обслуживания согласно Правилам сервиса «FAKTURA.RU» (размещенным в сети Интернет по адресу: www.faktura.ru). В терминологии Правил КИС «BeSafe» Оператор именуется Организатором Сервиса Faktura.ru.

BeSafe Corporate Information System (BeSafe CIS) is a system that is organized by the Digital Certificate Center Closed Joint-Stock Company (INN (Taxpayer Identification Number 5407187087) and represents a combination of software, information, and hardware that implements electronic document management in RBS System in accordance with the "Rules for Electronic Document Management of BeSafe Corporate Information System" at www.besafe.ru.

Login is a unique sequence of characters consisting of Latin letters and numbers, which allows the Bank to uniquely identify (establish) the Client / Authorized Representative of the Client when accessing and working in RBS System.

Mobile signature is a technology that ensures the integrity of simple ED by implementing a mechanism for installing a Message Authentication Code on a simple ED on the mobile device of the Client / Authorized Representative of the Client.

Mobile Application is a software for a mobile device (smartphone, Android tablet), developed by the Bank or by third parties on behalf of the Bank, providing the Client and/or the Client's Authorized Representative with remote access to the functionality of RBS System. The Mobile Application contains elements of the cryptographic information protection system provided on Besafe CIS side.

Responsible Employee is a Bank employee authorized to identify the Client and its Authorized Representative, as well as to accept documents from the Client, including Applications from the Authorized Representatives of the Client, for the purpose of registration, granting access, and use of RBS System by the Client and its Authorized Representatives.

Operator is Billing Center Closed Joint-Stock Company (INN (Taxpayer Identification Number) 5401152049), which facilitates information and technological interaction between the Bank and the Client within the framework of remote banking services in accordance with FAKTURA.RU Service Rules (available at www.faktura.ru). For the purposes of BeSafe CIS Rules, the Operator is referred to as Faktura.ru Service Organizer.

Оператор ЭДО - оператор электронного документооборота (отличный от ЗАО «Биллинговый центр»), соответствующий требованиям, утвержденным Приказом ФНС России от 08.06.2021 N ЕД-7-26/546@ «Об утверждении Требований к оператору электронного документооборота», и осуществляющий деятельность по обеспечению электронного документооборота между Банком и Клиентом через систему электронного документооборота Оператора ЭДО.

Подтверждение подлинности КЭП ФНС в Электронном документе (проверка КЭП ФНС документа) – положительный результат проверки принадлежности Электронной подписи в Электронном документе Владелец квалифицированного сертификата КЭП ФНС и отсутствия искажений в данном Электронном документе. Подтверждение подлинности КЭП ФНС должно осуществляться соответствующим средством Электронной подписи с использованием КС КЭП.

Пароль – секретная последовательность символов, которая известна только Клиенту/Уполномоченному представителю Клиента, при использовании ПЭП.

Простой электронный документ, Простой ЭД - документ, в котором информация представлена в электронной форме, подписанный ПЭП. Простой ЭД считается подписанным Клиентом, если он содержит ПЭП, принадлежащую Клиенту.

Простая электронная подпись, ПЭП – электронная подпись, с помощью которой Клиент подписывает Простые электронные документы путем ввода Разового пароля в Мобильном приложении с использованием технологии Мобильной подписи.

Разовый пароль – уникальный набор символов, используемый для подписания ПЭП Простого ЭД/ группы Простых ЭД, а также для совершения иных действий, предусмотренных в рамках Системы ДБО.

Регистрация квалифицированного сертификата ключа проверки КЭП ФНС (Регистрация КС КЭП ФНС) – осуществляемая Банком процедура регистрации в Системе ДБО Владельца квалифицированного сертификата ключа проверки КЭП ФНС, позволяющая предоставить Владелец квалифицированного сертификата КЭП ФНС права на подписание электронных документов от имени Клиента.

EDI Operator is an electronic document interchange operator (different from Billing Center JSC) that meets the requirements approved by Order No. ЕД-7-26/546@ of the Federal Tax Service of Russia "On Approval of Requirements for Electronic Document Interchange Operators" dated 08/06/2021 and carries out activities to ensure electronic document interchange between the Bank and the Client through the EDI Operator's system.

Confirmation of the authenticity of the Qualified Electronic Signature of the Federal Tax Service in an Electronic Document (verification of QES FTS document) is a positive result of verification that the Electronic Signature in the Electronic Document belongs to the Holder of the Qualified Certificate of the Qualified Electronic Signature of the Federal Tax Service and that the Electronic Document is free of distortions. Confirmation of the authenticity of the Qualified Electronic Signature of the Federal Tax Service should be performed using the appropriate Electronic Signature tool using the Qualified Certificate of the Qualified Electronic Signature.

Password is a secret sequence of characters known only to the Client / Authorized Representative of the Client using SES.

Simple Electronic Document, Simple ED is a document containing information in electronic form, signed by a SES. A Simple ED is considered signed by the Client if it contains SES belonging to the Client.

Simple Electronic Signature, SES is an electronic signature used by the Client to sign Simple Electronic Documents by entering a One-Time Password in the Mobile Application using Mobile Signature technology.

One-Time Password is a unique set of characters used to sign a Simple ED/group of Simple ED by SES, as well as to perform other actions provided for within the RBS System.

Registration of a Qualified Verification Key Certificate of Qualified Electronic Signature of the Federal Tax Service (QC QES FTS Registration) is the procedure performed by the Bank to register the Holder of a Qualified Verification Key Certificate of Qualified Electronic Signature of the Federal Tax Service in the RBS System, which grants the Holder of a Qualified Verification Key Certificate of Qualified Electronic Signature of the Federal Tax Service the right

Сертификат ключа проверки электронной подписи – электронный документ, выданный Удостоверяющим центром либо агентом Удостоверяющего центра и подтверждающие принадлежность Ключа проверки электронной подписи Владелец Сертификата ключа проверки электронной подписи.

Система дистанционного банковского обслуживания «ФАКТУРА.RU» (Система ДБО) – Система информационного обмена, организованная Оператором согласно Правилам Сервиса Faktura.ru, обеспечивающая информационное и технологическое взаимодействие между Банком и Клиентом в рамках дистанционного банковского обслуживания с использованием Мобильного приложения и Веб-приложения.

Средства криптографической защиты информации (СКЗИ) – аппаратные и (или) программные средства, обеспечивающие использование Электронной подписи и шифрования при организации Электронного документооборота. Средства криптографической защиты информации могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Средства криптографической защиты информации КЭП ФНС (СКЗИ КЭП ФНС) – аппаратные, программные или аппаратно-программные средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание Электронной подписи, проверка Электронной подписи, создание Ключа Электронной подписи и Ключа проверки Электронной подписи.

Удостоверяющий центр (УЦ) - удостоверяющий центр «Authority», созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов» (ИНН 5407187087), который осуществляет выдачу Сертификатов ключей проверки электронных подписей для Клиентов с целью осуществления электронного документооборота в рамках КИС «BeSafe» в соответствии с Правилами работы Удостоверяющего Центра (AUTHORITY), размещенными на www.authority.ru. В рамках настоящего Регламента Банк выступает агентом Удостоверяющего центра.

Удостоверяющий центр ФНС России («УЦ ФНС») – Федеральная налоговая служба Российской Федерации (далее также «ФНС России»),

to sign electronic documents on behalf of the Client.

Electronic Signature Verification Key Certificate is the electronic document issued by the Certification Authority or by an agent of the Certification Authority and confirming the ownership of the Electronic Signature Verification Key to the Holder of the Electronic Signature Verification Key Certificate.

ФАКТУРА.RU Remote Banking System (RBS System) is an information exchange system organized by the Operator in accordance with Faktura.ru Service Rules, providing information and technological interaction between the Bank and the Client within the framework of remote banking services using the Mobile Application and Web Application.

Cryptographic information protection facilities (CIPF) are hardware and/or software that enable the use of Electronic Signatures and encryption in the organization of Electronic Document Management. Cryptographic information protection facilities can be used both as standalone software modules and as facilities embedded in application software.

Cryptographic information protection facilities of Qualified Electronic Signature of the Federal Tax Service (CIPF of QES FTS) are hardware, software, or hardware and software that perform cryptographic transformation of information to ensure its security.

Electronic Signature Tools are cryptographic tools used to implement at least one of the following functions: creation of an Electronic Signature, verification of an Electronic Signature, creation of an Electronic Signature Key and an Electronic Signature Verification Key.

Certification Authority (CA) - Authority, a certification authority established by Digital Certificate Center Closed Joint-Stock Company (TIN 5407187087), which issues Electronic Signature Verification Key Certificates to Clients for the purpose of electronic document management within the BeSafe CIS in accordance with the Certification Authority (AUTHORITY) Operating Rules posted at www.authority.ru. Under these Regulations, the Bank acts as an agent for the Certification Authority.

Certification Authority of the Federal Tax Service of Russia (CA FTS Russia) is the Federal Tax Service of the Russian Federation (hereinafter also referred to as the "FTS Russia"), which performs the functions of an accredited certification authority. CA

осуществляющая функции аккредитованного удостоверяющего центра. УЦ ФНС работает согласно Регламенту Удостоверяющего центра Федеральной налоговой службы, утвержденного Приказом ФНС России (далее – «Регламент УЦ ФНС»).

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

- получена в результате криптографического преобразования информации с использованием Ключа Электронной подписи;

- позволяет обнаружить факт внесения изменений в Электронный документ после момента его подписания;

- создается с использованием средств электронной подписи;

при использовании в целях обеспечения целостности электронных сообщений создана с применением средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, при осуществлении регулирования в соответствии с пунктом «ш» части 1 статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности».

Уполномоченный Представитель Клиента/Уполномоченное лицо – лицо, действующее от имени Клиента в силу полномочий, предоставленных ему по доверенности, на основании распорядительного акта или на основании договора, закона, или акта государственного органа, или акта органа местного самоуправления, в том числе исполнительный орган Клиента (если применимо), надлежащим образом уполномоченное на совершение юридических действий от имени Клиента и обладающее всеми необходимыми полномочиями, разрешениями, согласиями, одобрениями на совершение соответствующих действий, указанное в Заявлении о заключении договора комплексного банковского обслуживания или в Заявлении о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена, в том числе, имеющее право распоряжаться денежными средствами Клиента на Счете(-ах), или имеющее право на просмотр и получение Электронных документов, в том числе выписок по Счету (без права распоряжаться денежными средствами/совершения сделок от имени Клиента).

Электронный документ (ЭД) – документ, в котором информация представлена в электронной форме, подписанный УНЭП или КЭП ФНС.

FTS operates in accordance with the Regulations of the Certification Authority of the Federal Tax Service, approved by the Order of the FTS Russia (hereinafter referred to as the "CA FTS Regulations").

Enhanced Unqualified Electronic Signature (EUES) is an electronic signature that:

- Is obtained as a result of cryptographic transformation of information using the Electronic Signature Key;

- Allows detection of changes made to the Electronic Document after the moment of its signing;

- Is created using electronic signature tools;

when used to ensure the integrity of electronic messages, it was created using electronic signature facilities and certification authority facilities that have confirmation of compliance with the requirements established by the federal executive body authorized in the field of security, when implementing regulations in accordance with paragraph "ш" of Part 1 of Article 13 of the Federal Law No. 40-ФЗ "On the Federal Security Service" dated April 3, 1995.

Authorized Representative of the Client/Authorized Person is a person acting on behalf of the Client by virtue of authority granted by a power of attorney, based on a directive, contract, law, or act of a state body or local government, including the executive body of the Client (if applicable), duly authorized to perform legal actions on behalf of the Client and possessing all necessary powers, permissions, consents, and approvals to perform the relevant actions, specified in the Application for concluding the Agreement or the Application for amending the terms of the Agreement, the Application, as well as in the Electronic Signature Verification Key Certificate (when using an enhanced unqualified electronic signature), including having the right to dispose of the Client's funds in the Account(s), or having the right to view and receive Electronic Documents, including account statements (without the right to dispose of funds/conduct transactions on behalf of the Client).

Electronic Document (ED) is a document containing information presented in electronic form, signed with a EUES or QES FTS.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

ФКН (Функциональный ключевой носитель, Рутокен) - защищенный носитель (физическое устройство) в формате USB-накопителя для хранения и использования Сертификата ключа проверки электронной подписи/Сертификата КЭП ФНС и Ключа ЭП/Криптографических ключей КЭП ФНС, имеющий встроенную криптографическую защиту и специальные механизмы безопасности.

FRAMOS (FRAud MOonitoring System) – технологическая платформа, разработанная и принадлежащая ЗАО «ЗОЛОТАЯ КОРОНА» (ИНН 5406119655) – далее ЗАО «ЗОЛОТАЯ КОРОНА», которая обеспечивает анализ информации (с учетом требований Банка России), в том числе Простых ЭД/ЭД, на предмет выявления признаков мошеннических операций, а также операций, соответствующих признакам перевода денежных средств без согласия Клиента, а именно без согласия Клиента или с согласия, полученного под влиянием обмана или злоупотребления доверием (далее – Операции без согласия Клиента).

Если иное прямо не предусмотрено Регламентом, КЭП ФНС, УНЭП и ПЭП совместно именуются Электронная подпись /ЭП.

Electronic Signature is information in electronic form that is attached to other electronic information (the information being signed) or otherwise linked to such information and is used to identify the person signing the information.

FKC (Functional Key Carrier, Rutoken) is a secure storage medium (physical device) in USB flash drive format for storing and using the Electronic Signature Verification Key Certificate / QES FTS Certificate and ES Key / QES FTS Cryptographic Keys, with built-in cryptographic protection and special security mechanisms.

FRAMOS (FRAud MOonitoring System) is a technological platform developed and owned by ZOLOTAYA KORONA CJSC (INN (Taxpayer Identification Number) 5406119655) (hereinafter referred to as ZOLOTAYA KORONA CJSC), which analyzes information (in accordance with Bank of Russia requirements), including Simple ED/ED, to identify indicators of fraudulent transactions, as well as transactions that meet the criteria for transferring funds without the Client's consent, namely, without the Client's consent or with consent obtained through fraud or breach of trust (hereinafter referred to as "Transactions without the Client's consent").

Unless otherwise expressly provided in the Regulations, QES FTS, EUES, and SES are collectively referred to as the Electronic Signature/ES.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Регламент регулирует отношения возникшие в процессе оказания Банком услуг в рамках Соглашения об осуществлении информационного взаимодействия с использованием Системы информационного обмена – Системы дистанционного банковского обслуживания [Faktura.ru](https://faktura.ru) (далее – Система ДБО), при подключении и использовании Клиентом и (или) Уполномоченными Представителями Клиента Системы ДБО и является соглашением между Банком и Клиентом, определяющим порядок и условия взаимодействия при выпуске и использовании Электронных подписей в рамках указанной корпоративной информационной системы электронного документооборота.

Настоящий Регламент предусматривает, в том числе, направление заявлений, сообщений, необходимых для получения (восстановления) доступа, изменения условий использования

2.GENERAL PROVISIONS

2.1. These Regulations govern the relations arising in the process of the Bank providing services under the Agreement on Information Interaction Using the Information Exchange System – Faktura.ru Remote Banking Service System (hereinafter referred to as the "RBS System"), during the connection and use of RBS System by the Client and the Authorized Representatives of the Client and constitute an agreement between the Bank and the Client, defining the procedure and terms of interaction for the issuance and use of Electronic Signatures within the specified corporate electronic document management system.

These Regulations provide, among other things, for the submission of applications and messages necessary for obtaining (restoring) access to, or changing the terms of use of, RBS System using QES FTS CA FTS. QES FTS CA FTS is used within the exchange of electronic documents through the RBS System.

Системы ДБО с использованием КЭП ФНС УЦ ФНС. КЭП ФНС УЦ ФНС используется в рамках обмена электронными документами через Систему ДБО.

2.2. Настоящий Регламент является неотъемлемой и составной частью Правил и Условий осуществления информационного взаимодействия с использованием Систем информационного обмена.

2.3. Для подключения к Системе ДБО Клиент должен присоединиться к Правилам и Условиям осуществления информационного взаимодействия с использованием Систем информационного обмена, а также к Регламенту путем подписания Заявления о заключении договора комплексного банковского обслуживания/Заявления о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена.

При подключении к Системе ДБО Клиент также присоединяется к Правилам КИС «BeSafe» (размещенным в сети Интернет по адресу: www.besafe.ru) путем подписания Заявления о заключении договора комплексного банковского обслуживания/Заявления о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена.

Клиент считается присоединившимся к Регламенту ДБО, Правилам КИС «Besafe» с даты подписания им Заявления о заключении договора комплексного банковского обслуживания/Заявления о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена.

Подавая заявления на получение Сертификата/Сертифицированного сертификата (иные заявления, предусмотренные Правилами работы Удостоверяющего Центра (AUTHORITY) (Правила УЦ), Клиент осуществляет акцепт условий Правил УЦ, размещенных на www.authority.ru, и присоединяется к Правилам УЦ в порядке статьи 428 Гражданского кодекса Российской Федерации. Факт подачи заявления подтверждает полное и безусловное (безоговорочное) согласие Клиента с условиями Правил УЦ.

2.4. Клиент признает, что используемая Система ДБО является достаточной для обеспечения надежной и эффективной работы при приеме,

2.2. These Regulations are an integral and constituent part of the Rules and the Terms of Information Interaction Using Information Exchange Systems.

2.3. To connect the Client to RBS System, the Client should join the Rules and the Terms of Information Interaction Using Information Exchange Systems, as well as these Regulations, by signing an Application to enter into Comprehensive Banking Services Agreement/Application to amend the Agreement on the Implementation of Information Interaction Using Information Exchange Systems.

By connecting to RBS System, the Client also subscribes to BeSafe CIS Rules (available online at www.besafe.ru) by signing the Application to enter into Comprehensive Banking Services Agreement/Application to amend the Agreement on the Implementation of Information Interaction Using Information Exchange Systems.

The Client is deemed to have subscribed to RBS Regulations and Besafe CIS Rules from the date they sign the Application to enter into Comprehensive Banking Services Agreement / Application to amend the Agreement on the Implementation of Information Interaction Using Information Exchange Systems.

By submitting an application for a Certificate/Certified Certificate (or other applications stipulated by the Certification Authority (AUTHORITY) Operating Rules (CA Rules), the Client accepts the terms of the CA Rules posted at www.authority.ru and accedes to the CA Rules in accordance with Article 428 of the Civil Code of the Russian Federation. Submitting an application confirms the Client's full and unconditional (irrevocable) agreement with the terms of the CA Rules.

2.4. The Client acknowledges that RBS System used is sufficient to ensure reliable and efficient operation in receiving, transmitting,

передаче, обработке и хранении информации, а используемые средства защиты информации, обеспечивающие разграничение доступа, шифрование, контроль целостности и формирование ЭП, являются достаточными для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых ЭД, обеспечения целостности информации, условий неотказуемости, неизменности, достоверности, отсутствия искажений, а также разрешения спорных ситуаций при условии соблюдения Сторонами мер безопасности, в том числе обеспечения Клиентом надлежащей защиты Клиентской части Системы ДБО от несанкционированного доступа.

Для обеспечения конфиденциальности ЭД, а также для обеспечения авторства и целостности ЭД в Системе ДБО используются программные средства защиты информации, реализующие алгоритмы шифрования, формирования и проверки ЭП.

2.5. Банк и Клиент соглашаются и подтверждают, что Электронные документы Сторон, обмен которыми осуществляется в рамках Системы ДБО и которые подписаны:

- УНЭП (размещена на ФКН);
- КЭП ФНС (размещена на сертифицированном USB-токене, требования к которому содержатся в Регламенте УЦ ФНС);
- ПЭП, признаются электронными документами, равнозначными документам на бумажных носителях, подписанным собственноручной подписью уполномоченного лица Стороны и скрепленными печатью (для УНЭП и КЭП ФНС) такой Стороны (при наличии), в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2.6. Стороны признают, что применяемая в Системе ДБО технология защиты информации, обеспечивающая шифрование, контроль целостности и создание Мобильной подписи, достаточна для защиты информации от несанкционированного доступа подтверждения подлинности и авторства Простого ЭД.

Стороны договорились считать, что Клиент отказался от передачи электронного документа на исполнение в Банк через Систему ДБО, если он не осуществил ввод Пароля при использовании технологии Мобильной подписи.

2.7. Стороны признают, что, в целях снижения риска совершения Операций без согласия Клиента, выявление которых осуществляется с помощью технологий FRAMOS, Клиент соглашается на передачу Банком Оператору и ЗАО «Золотая

processing, and storing information, and that the information security tools used, ensuring access control, encryption, integrity control, and ES generation, are sufficient to protect against unauthorized access, confirm authorship and authenticity of the information contained in the received ED, ensure the integrity of information, conditions of non-repudiation, immutability, reliability, absence of distortions, and resolution of disputes, provided that the Parties comply with security measures, including the Client ensuring proper protection of the Client's part of RBS System from unauthorized access.

To ensure ED confidentiality, as well as to ensure ED authorship and integrity, RBS System uses information security software that implements encryption algorithms, generation and verification of ES.

2.5. The Bank and the Client agree and confirm that the Electronic Documents of the Parties, exchanged within the Remote Banking System and signed by:

- EUES (located on FKC);
- QES FTS (located on a certified USB token, the requirements for which are contained in CA FTS Regulations);
- SES, are recognized as electronic documents equivalent to paper documents signed by the handwritten signature of an authorized representative of the Party and sealed (for EUES and QES FTS) of such Party (if any), in accordance with Federal Law No. 63-ФЗ "On Electronic Signatures" dated 06/04/2011.

2.6. The Parties acknowledge that the information security technology used in RBS System, which provides encryption, integrity control, and Mobile Signature generation, is sufficient to protect information from unauthorized access and to confirm the authenticity and authorship of a Simple ED.

The Parties agree that the Client has refused to submit an electronic document for execution to the Bank through RBS System if they fail to enter a Password when using Mobile Signature technology.

2.7. The Parties acknowledge that, in order to reduce the risk of Transactions being performed without the Client's consent, which are detected using FRAMOS technologies, the Client

Корона» и обработку ими информации об операциях (в том числе ЭД, Простых ЭД, отправленных Клиентом, и данных Клиента) для проведения соответствующего анализа.

2.8. Одной Электронной подписью могут быть подписаны несколько связанных между собой Электронных документов/Простых ЭД (пакет Электронных документов/Простых ЭД). 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.

2.9. 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.

2.10. Клиент обязуется обеспечить допуск к работе и работу в Системе ДБО только Уполномоченных Представителей Клиента, с учетом ролей таких лиц при использовании Системы ДБО. Клиент (его Уполномоченный представитель) обязуется сохранять конфиденциальность Ключей ЭП / ПЭП.

2.11. Клиент осознает повышенный риск несанкционированного использования Системы ДБО, включая компрометацию Ключей ЭП/Компрометацию ключа КЭП ФНС и несанкционированное удаленное управление Системой ДБО, при ненадлежащем соблюдении Клиентом мер безопасности.

2.12. Используя Систему ДБО (с учетом особенностей, обозначенных в п. 3.5. настоящего Регламента), Клиент приобретает возможность:

- Формировать, подписывать Электронной подписью и направлять в Банк расчетные (платежные) 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 расчетных (платежных) 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

consents to the Bank's transfer to the Operator and Zolotaya Korona CJSC and their processing of transaction information (including EDs, Simple EDs sent by the Client, and Client data) for appropriate analysis.

2.8. Several related Electronic Documents / Simple EDs (a package of Electronic Documents / Simple EDs) may be signed with one Electronic Signature. When signing a package of Electronic Documents with an Electronic Signature, each of the Electronic Documents included in this package is considered signed with the type of Electronic Signature used to sign the package of Electronic Documents.

2.9. The Parties recognize the local time at the location of the Bank's division servicing the Client as the unified time scale when working in RBS System. The control time is the system clock time of the Bank's hardware.

2.10. The Client undertakes to ensure access to and work in RBS System only for the Authorized Representatives of the Client, taking into account the roles of such persons when using RBS System. The Client (his/her Authorized Representative) undertakes to maintain the confidentiality of ES/SES Keys.

2.11. The Client acknowledges the increased risk of unauthorized use of RBS System, including the compromise of ES Keys / compromise of QES FTS Keys and unauthorized remote control of RBS System, in case of inadequate compliance by the Client with security measures.

2.12. By using RBS System (taking into account the features indicated in clause 3.5 of the Regulations), the Client gains the ability to:

- Prepare, sign with an Electronic Signature, and send to the Bank payment (settlement) documents in accordance with the legislation of the Russian Federation, including payment orders, for the purpose of conducting transactions on the Client's Accounts opened with the Bank;
- Prepare, sign with an Electronic Signature, and send to the Bank requests to revoke payment (settlement) documents, including payment orders, previously submitted to the Bank;
- Receive from the Bank account(s) statements in the form of Electronic Documents containing information on transactions conducted on the Client's Account(s) opened with the Bank;
- Prepare, send, and receive from the Bank free-format information in the form of Electronic

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 Правилами, Условиями, Правилами КИС "Besafe", Правилами УЦ, приобретенными Клиентом продуктами и услугами Банка, а также в соответствии с условиями отдельных заключенных Сторонами сделок (если использование Системы ДБО предусмотрено последними);
- Формировать, подписывать Электронной подписью и направлять в Банк заявления (если это предусмотрено Правилами и при наличии технической возможности).

2.13. При получении Электронного документа Банк производит процедуры приема к исполнению, отзыва, возврата (аннулирования) расчетного (платежного) документа, в соответствии с Банковскими правилами, в том числе проверку:

- Права распоряжения денежными средствами (проверка ЭП, запрос по отдельным платежам Клиента дополнительного подтверждения);
- Контроль целостности (неизменности) реквизитов расчетного (платежного) документа;
- Структурный контроль (проверка установленных реквизитов и максимального количества символов в реквизитах расчетного (платежного) документа);
- Контроль значений реквизитов;
- Контроль достаточности денежных средств.

При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный ЭД Системой ДБО Faktura.ru не принимается и данный результат (Электронный документ) автоматически направляется Клиенту, а поручение, содержащееся в нем, Банком не исполняется.

При получении Электронного документа/Простого ЭД Сервисом Faktura.ru производится проверка УНЭП/КЭП ФНС/ПЭП/. При положительном результате проверки электронный документ переходит из статуса «Принят банком» в статус «Исполнен». При отрицательном результате проверки электронный документ переходит в статус «Возвращен».

Обеспечение проверки защищенного

Documents (including service-information messages), in accordance with the functional and technical capabilities of RBS System;

- Prepare, sign with an Electronic Signature, send, and receive from the Bank Electronic Documents in accordance with the Rules, Terms, Besafe CIS Rules, CA Rules, products, and services acquired by the Client from the Bank, as well as in accordance with the terms of individual agreements concluded by the Parties (if the use of RBS System is provided for therein);
- Prepare, sign with an Electronic Signature, and send to the Bank applications (if provided for by the Rules and if technically possible).

2.13. Upon receipt of an Electronic Document, the Bank performs procedures for acceptance for execution, revocation, return (cancellation) of the payment (settlement) document, in accordance with the Bank's rules, including verification of:

- The right to dispose of funds (ES verification, request for additional confirmation for certain payments of the Client);
- Integrity (immutability) control of the payment (settlement) document details;
- Structural control (verification of the established details and the maximum number of characters in the payment (settlement) document details);
- Control of detail values;
- Control of the sufficiency of funds.

If a negative result of the verification of any of the above circumstances is identified, ED received by Faktura.ru RBS System is not accepted, and this result (Electronic Document) is automatically sent to the Client, and the instruction contained therein is not executed by the Bank.

Upon receipt of an Electronic Document / Simple ED, Faktura.ru Service verifies EUES/QES FTS/SES. If the verification result is positive, the Electronic Document transitions from the status "Accepted by the Bank" to the status "Executed." If the verification result is negative, the Electronic Document transitions to the status "Returned."

Secure access to RBS System is ensured by using the SSL protocol during the establishment of a connection between the

доступа к Системе ДБО достигается применением защищенного протокола SSL в процессе установления соединения между web-сервером банка и Клиентом. Для подтверждения подлинности web-сервера выполняется сравнение доменного имени загружаемого web-сервера с указанным в сертификате. Протокол SSL используется в форме протокола https (прикладной протокол http поверх криптографического протокола SSL).

2.14. 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 Уполномоченного Представителя Клиента, содержащаяся в Электронном документе Клиента, подтверждает авторство Уполномоченного Представителя Клиента и является средством проверки неизменности содержания Электронного документа, так как любое изменение Электронного документа, после его подписания Электронной подписью, нарушает целостность Электронной подписи.

2.15. Электронный документ должен быть подписан Электронной подписью только Уполномоченных Представителей Клиента, имеющих право распоряжения денежными средствами на Счете (для расчетных (платежных) Электронных документов), данные о которых указаны в Заявлении о заключении договора комплексного банковского обслуживания / Заявлении о заключении Договора Продукта / Заявлении о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена. Если Электронный документ должен быть подписан несколькими подписями Уполномоченных Представителей Клиента, в соответствии с Заявлениями, указанными в настоящем пункте /Карточкой с образцами подписей и оттиском печати, и Соглашением о сочетании подписей к КОП, Электронный документ должен быть подписан каждым из Уполномоченных Представителей Клиента, согласно вышеуказанным документам, по одной Электронной подписи из первой и второй группы подписей.

2.16. Система ДБО автоматически отображает сведения о текущем этапе обработки Клиентом и (или) Банком Электронного документа,

Bank's web server and the Client. To confirm the authenticity of the web server, the domain name of the loaded web server is compared with the one specified in the certificate. The SSL protocol is used in the form of the HTTPS protocol (application protocol HTTP over the cryptographic protocol SSL).

2.14. The format of Electronic Documents is determined by the functional and technical capabilities of RBS System and the screen form of the Client's part of RBS System. Each Electronic Document sent by the Client to the Bank using RBS System should contain the Electronic Signature of the Authorized Representative of the Client. The Electronic Signature of the Authorized Representative of the Client contained in the Electronic Document of the Client confirms the authorship of the Authorized Representative of the Client and is a means of verifying the immutability of the content of the Electronic Document, as any change to the Electronic Document after its signing with the Electronic Signature violates the integrity of the Electronic Signature.

2.15. The Electronic Document should be signed with the Electronic Signature only by the Authorized Representatives of the Client who have the right to dispose of funds in the Account (for payment (settlement) Electronic Documents), the data of which are specified in the Application to enter into Comprehensive Banking Services Agreement / Application to enter into Product Agreement / Application to amend the Agreement on the Implementation of Information Interaction Using Information Exchange Systems. If the Electronic Document should be signed with several signatures of the Authorized Representatives of the Client, in accordance with the Applications stated in the clause /Specimen Signature Card and Seal Impression, and the Agreement on the Combination of Signatures to the COP, the Electronic Document should be signed by each of the Authorized Representatives of the Client, according to the above documents, with one Electronic Signature from the first and second groups of signatures.

2.16. RBS System automatically displays information about the current stage of processing of the Electronic Document by the

посредством присвоения Электронному документу определенного статуса и его изменения.

2.17. Система присваивает Электронным документам следующие статусы:

- **«В картотеке»** - присваивается Электронному документу, если при обработке платежа на счете Клиента оказалось недостаточно средств для совершения операции.
- **«Подготовлен»** - присваивается при создании и сохранении нового Электронного документа Клиентом, который еще не отправлен в Банк и возможен к редактированию.
- **«Подписан»** - присваивается Электронному документу, подписанному одним из видов ЭП. Электронный документ остается в данном состоянии до момента завершения его подписания всеми Уполномоченными лицами (если требуется).
- **«Отправлен в банк»** - присваивается в случае, когда Система ДБО отправила Электронный документ, но он фактически еще не получен Банком.
- **«Доставлен в банк»** - присваивается в случае фактического поступления Электронного документа в Банк.
- **«Принят банком»** - присваивается Электронному документу при нахождении его в очереди на обработку.
- **«Исполнен»** - присваивается Электронному документу после его исполнения Банком (в том числе после списания денежных средств со Счета Клиента на основании данного документа).
- **«Возвращен»** - присваивается Электронному документу, если он не может быть принят к исполнению в Банке. Для уточнения причины необходимо обратиться в Банк любым доступным Клиенту способом.
- **«На контроле»** - присваивается Электронному документу в случае проведения со стороны Банка дополнительной проверки.

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

2.19. Банк осуществляет проверку полученного от Клиента Электронного документа и принимает его к исполнению при условии положительного результата проверки, в том числе положительного результата всех процедур контроля, предусмотренных пунктом 2.17 - 2.19 настоящего Регламента.

2.20. Результат проверки Электронного документа считается положительным, если он:

Client and/or the Bank by assigning a certain status to the Electronic Document and changing it.

2.17. The System assigns the following statuses to Electronic Documents:

- **"In File"** – assigned to an Electronic Document if, during the processing of the payment, there were insufficient funds in the Client's Account to complete the transaction.
- **"Prepared"** - assigned when the Client creates and saves a new Electronic Document that has not yet been sent to the Bank and is editable.
- **"Signed"** - assigned to an Electronic Document signed with one of ES types. The Electronic Document remains in this state until it is signed by all Authorized Persons (if required).
- **"Sent to the Bank"** - assigned when RBS System has sent the Electronic Document, but it has not yet been received by the Bank.
- **"Delivered to the Bank"** - assigned when the Electronic Document has actually been received by the Bank.
- **"Accepted by the Bank"** - assigned to the Electronic Document when it is queued for processing.
- **"Executed"** – assigned to an Electronic Document after its execution by the Bank (including after the debiting of funds from the Client's Account based on this document).
- **"Returned"** - assigned to an Electronic Document if it cannot be accepted for execution by the Bank. To clarify the reason, please contact the Bank by any means available to the Client.
- **"Under Control"** - assigned to an Electronic Document if the Bank conducts additional verification.

2.18. The Client sends the created and signed Electronic Document to the Bank using the BIFIT RBS.

2.19. The Bank verifies the Electronic Document received from the Client and accepts it for execution if the verification result is positive, including the positive result of all control procedures provided for in clauses 2.17 - 2.19 of the Regulations.

2.20. The verification result of the Electronic Document is considered positive if it:

- 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, Правилами КИС “Besafe”, Правилами УЦ, и настоящим Регламентом;
 - Подписан 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.
- 2.21.** 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. Отзываны могут быть только неисполненные Электронные документы, которые не перешли в статус «Исполнен».
- 2.22.** Клиент самостоятельно контролирует (отслеживает) этапы и результаты обработки отправленных в Банк Электронных документов в соответствующих разделах Системы ДБО.
- 2.23.** Банк и Клиент обмениваются по Системе ДБО следующими Электронными документами:
- платежные поручения;
 - запросы на отзыв документа;
 - 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;
 - Заявление об открытии Счета, Заявление на закрытие Счета, Заявление о внесении изменений в условия Договора, Заявление о расторжении Договора (при наличии технической возможности);
 - иные расчетные (платежные) документы, применимые в рамках предусмотренных законодательством Российской Федерации и заключенных между Сторонами сделок форм безналичных расчетов (в соответствии с функциональными и техническими возможностями Системы ДБО);
 - произвольные документы (иные
- Is prepared in accordance with the current legislation of the Russian Federation;
 - Is prepared in accordance with the regulatory documents of the Central Bank of Russia and the requirements of the Bank;
 - Is prepared in accordance with the requirements established by the agreements concluded by the Parties, in accordance with the Rules, Besafe CIS Rules, CA Rules, and the Regulations;
 - Is signed with the proper Electronic Signature(s) of the Authorized Representative(s) of the Client who have the right to dispose of funds in the Account (for payment (settlement) Electronic Documents), and the Electronic Signatures have been verified by the Bank.
- 2.21.** The Client may revoke an Electronic Document submitted to the Bank in accordance with the requirements of the legislation of the Russian Federation, agreements concluded by the Parties, and the rules for conducting transactions, using RBS System. Only unexecuted Electronic Documents that have not reached the status "Executed" may be revoked.
- 2.22.** The Client independently monitors (tracks) the stages and results of processing of Electronic Documents sent to the Bank in the relevant sections of RBS System.
- 2.23.** The Bank and the Client exchange the following Electronic Documents through RBS System:
- Payment orders;
 - Requests to revoke documents;
 - Statements containing information on the movement of funds in accounts;
 - Documents for conducting foreign exchange transactions (applications for foreign currency transfers, orders for the purchase/sale of currency, etc.);
 - Currency control documents;
 - Application for opening an Account, Application for closing an Account, Application for amending the terms of the Agreement, Application for termination of the Agreement (if technically possible);
 - Other payment (settlement) documents applicable within the framework of non-cash settlement forms provided for by the legislation of the Russian Federation and agreements concluded between the Parties (in accordance with the functional and technical capabilities of RBS System);
 - Optional documents (other documents or letters prepared in free form).
- Using Mobile Signature technology, only signing payment orders is available, including

документы или письма, составленные в произвольной форме).

С применением технологии Мобильной подписи доступно только подписание платежных поручений, включая совершаемые через Систему быстрых платежей.

- 2.24.** 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/Простых ЭД, в том числе выписок по счетам. В случае предоставления Уполномоченному Представителю Клиента указанного доступа в Систему ДБО, последний не вправе совершать операции по Счету(-ам), в т.ч. распоряжаться денежными средствами, подписывать расчетные (платежные) Электронные документы/Простые ЭД. Клиент самостоятельно осуществляет контроль за соблюдением Уполномоченными Представителями Клиента ограничений полномочий последних, неся при этом ответственность перед Банком и иными третьими лицами, а также риск возникновения неблагоприятных последствий, в том числе имущественного характера, при ненадлежащем исполнении указанной обязанности и(или) ее неисполнении.

При наличии технической возможности у Банка, Клиенту в Системе ДБО доступна функция установления лимитов на операции, а также формирование перечня запрещенных IP-адресов и счетов. Инструкция по использованию данного функционала размещается Банком на ресурсе: <https://corpdocs.131.ru/>.

3. ПОРЯДОК АККРЕДИТАЦИИ И ПОДКЛЮЧЕНИЯ КЛИЕНТА К СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Процедура Аккредитации и подключения Клиента проводится Банком после получения от Клиента согласия о присоединении к Правилам КИС «BeSafe».

В процессе Аккредитации и подключения Банк:

осуществляет проверку документов и полномочий Клиента и (или) Уполномоченного Представителя Клиента в объеме, достаточном для открытия Счета/заключении Договора на иной Продукт, а также управления Клиентом/Уполномоченным Представителем Клиента Счетом в Банке;

если необходимо, осуществляет

those made through the Faster Payments System.

- 2.24.** The Authorized Representative of the Client may be granted access to RBS System, with the ability to obtain information about the Client, his/her transactions, Client's bank accounts opened with the Bank, with the right to view and receive Electronic Documents / Simple ED, including account statements. If the Authorized Representative of the Client is granted such access to RBS System, the latter is not entitled to conduct transactions on the Account(s), including disposing of funds, signing payment (settlement) Electronic Documents / Simple ED. The Client independently monitors the compliance of the Authorized Representatives of the Client with the restrictions on their powers, bearing responsibility to the Bank and other third parties, as well as the risk of adverse consequences, including property consequences, in case of improper performance and / or non-performance of this obligation.

If the Bank has the technical capability, the Client can set transaction limits and create a list of prohibited IP addresses and accounts in RBS System. Instructions for using this functionality are posted by the Bank at <https://corpdocs.131.ru/>.

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

The Client Accreditation and Connection procedure is carried out by the Bank after receiving the Client's consent to join BeSafe CIS Rules.

During the Accreditation and Connection process, the Bank:

verifies the documents and authority of the Client and/or the Client's Authorized Representative to the extent sufficient to open an Account/conclude an Agreement for another Product, as well as manage the Client's/Client's Authorized Representative's Account with the Bank;

if necessary, registers the Electronic Signature Verification Key Certificate in RBS System for the exchange of Electronic Documents between the Client/Client's Authorized Representative and the

регистрацию Сертификата ключа проверки электронной подписи в Системе ДБО для осуществления Клиентом/Уполномоченным Представителем Клиента и Банком обмена Электронными документами;

если необходимо, осуществляет регистрацию КЭП ФНС Клиента в Сервисе Faktura.ru для осуществления Клиентом обмена Электронными документами;

если необходимо, обеспечивает получение Клиентом/Уполномоченным Представителем Клиента уникального Логина и Пароля для обмена Простыми Электронными документами с использованием ПЭП (Мобильной подписи).

Регистрирует Клиента/Уполномоченного Представителя Клиента, включая полученную в ходе Аккредитации информацию в Сервисе Faktura.ru.

В Заявлении о заключении договора комплексного банковского обслуживания / Заявлении о заключении Договора Продукта / Заявлении о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена Клиент/Уполномоченный Представитель клиента указывает кодовую информацию, которая в дальнейшем может быть использована для дополнительной идентификации Клиента/Уполномоченного Представителя Клиента.

При выборе Клиентом способа работы в Системе ДБО с использованием Мобильной подписи Клиенту/Уполномоченному Представителю Клиента необходимо:

- Установить Мобильное приложение (посредством скачивания через магазин мобильных приложений, например, RuStore), после чего вход в Мобильное приложение доступен с применением Логина (направляется Банком на адрес электронной почты Клиента, указанный в Заявлении о заключении договора комплексного банковского обслуживания) и Разового пароля (направляется Банком посредством СМС-оповещения на Абонентский номер Клиента/Уполномоченного Представителя Клиента, указанный в Заявлении о заключении договора комплексного банковского обслуживания / Заявлении о заключении Договора Продукта / Заявлении о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена). После первоначальной авторизации в

Bank;

- if necessary, registers QES FTS of the Client in Faktura.ru Service for the exchange of Electronic Documents by the Client;

- if necessary, ensures that the Client/Client's Authorized Representative receives a unique Login and Password for the exchange of Simple Electronic Documents using SES (Mobile Signature).

Registers the Client/Authorized Representative of the Client, including the information obtained during Accreditation, in Faktura.ru Service.

In the Application to enter into a Comprehensive Banking Services Agreement / Application to enter into a Product Agreement / Application to amend the Agreement on the Implementation of Information Interaction Using Information Exchange Systems, the Client/Authorized Representative of the Client specifies code information that may subsequently be used for additional identification of the Client/Authorized Representative of the Client.

When the Client chooses to use RBS System with a Mobile Signature, the Client/Authorized Representative should:

- Install the Mobile App (by downloading it from a mobile app store, such as RuStore). Access to the Mobile App is then available using the Login (sent by the Bank to the Client's email address specified in the Application to enter into a Comprehensive Banking Services Agreement) and the One-Time Password (sent by the Bank via SMS message to the Subscriber Number of the Client/Authorized Representative specified in the Application to enter into a Comprehensive Banking Services Agreement/Application to enter into a Product Agreement/Application to amend the Agreement on the Implementation of Information Interaction Using Information Exchange Systems). After initial authorization in the Mobile App, the One-Time Password may be changed independently by the Client/Authorized Representative.

- Issue a Mobile Signature in the Mobile App.

Мобильном приложении Разовый пароль подлежит самостоятельной замене Клиентом/Уполномоченным Представителем Клиента.

- Осуществить выпуск Мобильной подписи в Мобильном приложении.

- 3.1. При выборе Клиентом способа работы в Системе ДБО с использованием УНЭП, Ответственный работник передает должным образом упакованный ФКН Уполномоченному Представителю Клиента.
- 3.2. Факт передачи ФКН, а также целостность упаковки подтверждается собственноручной подписью Уполномоченного Представителя Клиента в Акте приема-передачи ФКН. Форма Акта определяется Банком в Приложении №2 к настоящему Регламенту. В случае нарушения целостности упаковки ФКН Уполномоченный Представитель Клиента должен указать об этом в Акте приема-передачи. При отсутствии соответствующей отметки в Акте приема-передачи, Стороны определили считать целостность упаковки ФКН не нарушенной, а сам ФКН надлежащим образом полученным Клиентом. После получения ФКН Клиенту/Уполномоченному Представителю Клиента доступна генерация Ключа ЭП и выпуск Сертификата ключа проверки электронной подписи (ссылка на выпуск Сертификата ключа проверки электронной подписи формируется автоматически и поступает на адрес электронной почты Клиента/Уполномоченного Представителя Клиента, указанный в Заявлении о заключении комплексного банковского обслуживания, после создания Ключа ЭП). Выпуск Сертификата ключа проверки электронной подписи осуществляется в порядке, установленном разделом 4 настоящего Регламента.

Клиент уведомлен и полностью согласен с тем, что Клиент несет единоличную и полную ответственность за любые последствия правового, имущественного или иного характера, в том числе, неблагоприятные для Клиента, Банка, иных лиц, чьи законные интересы будут (могут быть) затронуты, в случае хранения Клиентом Ключа ЭП способом, отличным от предоставленным ему Банком ФКН (Рутокен).

При выборе Клиентом метода работы в Системе ДБО с использованием КЭП ФНС Ключ КЭП ФНС создается средствами УЦ ФНС в соответствии с Регламентом УЦ ФНС. КС КЭП ФНС оформляется Уполномоченным

3.1. If the Client chooses the method of working in RBS System using EUES, the Responsible Employee transfers the properly packaged FKC to the Authorized Representative of the Client.

3.2. The fact of FKC transfer, as well as the integrity of the packaging, is confirmed by the handwritten signature of the Authorized Representative of the Client in the Act of Acceptance and Transfer of the FKC of RBS System. The form of the Act is determined by the Bank in Appendix No. 2 to the Regulations. If the integrity of FKC packaging is violated, the Authorized Representative of the Client should indicate this in the Act of Acceptance and Transfer. In the absence of such a note in the Act of Acceptance and Transfer, the Parties agree to consider the integrity of FKC packaging as not violated and FKC as properly received by the Client. After FKC receiving the Client/Authorized Representative of the Client can generate ES Key and issue an Electronic Signature Verification Key Certificate (a link to issue ES Key Certificate is generated automatically and sent to the Client/Client's Authorized Representative's email address specified in the Application to enter into a Comprehensive Banking Service after the ES Key is generated). The ES Key Certificate is issued in accordance with the procedure established in Section 4 of the Regulations.

The Client is aware of and fully agrees that the Client bears sole and full responsibility for any legal, property, or other consequences, including those adverse to the Client, the Bank, or other persons whose legitimate interests will (may) be affected, should the Client store the ES Key in a manner other than that provided to them by the FKC (Rutoken) Bank.

When the Client selects the method of working in RBS System using QES FTS, QES FTS Key is generated by the CA FTS in accordance with CA FTS Regulations. CK QES FTS is issued by the Client's Authorized Representative independently by contacting any FTS office/authorized person of CA FTS (authorized persons of CA FTS are defined by the relevant order of FTS of Russia; the list of such persons is posted on the official website of FTS of Russia in the section "Authorized Persons of CA FTS").

Представителем Клиента самостоятельно путем обращения в любое отделение ФНС/к доверенному лицу УЦ ФНС (доверенные лица УЦ ФНС определены соответствующим приказом ФНС России, перечень данных лиц размещен на официальном сайте ФНС России в разделе «Доверенные лица УЦ ФНС России».

3.3. Клиент/Уполномоченный Представитель Клиента считается подключенным к Системе ДБО и имеет возможность пользоваться Системой ДБО при наступлении следующих событий:

- при использовании УНЭП на ФКН - после получения (выпуска) Сертификата ключа проверки Электронной подписи, а также предоставления в Банк подписанного Клиентом Акта приема-передачи Сертификата ключа проверки электронной подписи.

- при использовании ПЭП - после выпуска Мобильной подписи в Мобильном приложении;

- при использовании КЭП ФНС - после регистрации Банком КС КЭП ФНС Клиента (в соответствии с разделом 4 настоящего Регламента) в Системе ДБО.

По истечении срока действия полномочий Уполномоченного Представителя Клиента Банк блокирует доступ такого Уполномоченного Представителя Клиента к Системе ДБО.

3.4. Клиент вправе установить ограничения по параметрам операций, которые могут осуществляться Клиентом с использованием Системы ДБО в заявлении, форма которого определяется Приложением № 6 к Регламенту и размещена на ресурсе <https://131.ru/contracts> и в офисе Банка. Прием заявления в Банк осуществляется с использованием Системы ДБО.

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

3.3. The Client / Authorized Representative of the Client is considered connected to RBS System and has the opportunity to use RBS System upon the occurrence of the following events:

- When using EUES on FKC - after receiving (issuance) of the Electronic Signature Verification Key Certificate and provision of the Certificate of Acceptance and Transfer of the Electronic Signature Verification Key signed by the Client to the Bank.

- when using SES - after the Mobile Signature is issued in the Mobile App;

- when using QES FTS - after the Bank registers CK QES FTS of the Client (in accordance with Section 4 of the Regulations) in RBS System.

Upon expiration of the Client's Authorized Representative's authority, the Bank will block such Client's Authorized Representative's access to the Remote Banking System.

3.4. The Client has the right to set restrictions on the parameters of transactions that can be carried out by the Client using RBS System in the Application, which form is determined by Appendix No. 6 to the Regulations and is available at <https://131.ru/contracts> and in the Bank's office. The acceptance of the Application by the Bank is carried out using RBS System.

3.5. A One-Time Password is automatically generated by RBS System, including for the purpose of additional authentication of the Client / Authorized Representative of the Client when granting access to RBS System and/or additional confirmation of the Simple Electronic Document. The Authorized Representative of the Client should enter the received One-Time Password to complete the authentication procedure in RBS System and/or additional confirmation of the Simple Electronic Document.

3.6. Порядок смены Абонентского номера

3.6.1. Для изменения Абонентского номера Уполномоченного Представителя Клиента, используемого для получения Разового пароля Уполномоченный Представитель Клиента должен обратиться в Банк и предоставить Заявление на изменение Абонентского номера с предоставлением документов, удостоверяющих личность. Если Абонентский номер меняет Уполномоченный Представитель Клиента, уполномоченный подписывать договоры/заявления, он может подписать только Заявление на изменение Абонентского номера (Приложение №3 к настоящему Регламенту), указав в нем, что подтверждает принадлежность ему Абонентского номера.

3.6.2. Для дистанционной смены Абонентского номера Клиент/Уполномоченный Представитель Клиента направляет в Системе ДБО Заявление о смене Абонентского номера, выбрав необходимый шаблон документа. Заявление должно быть подписано ЭП обратившегося Уполномоченного Представителя Клиента. Дистанционная смена Абонентского номера возможна при наличии полномочий Уполномоченного Представителя Клиента подписывать и подать в Банк документы, заявления, сообщения, необходимые для регистрации, получения доступа, изменения условий использования Системы ДБО. Дистанционная смена Абонентского номера невозможна в случае Компрометации Электронной подписи или подозрений на Компрометацию Электронной подписи.

3.6.3. Смена Абонентского номера Клиента/Уполномоченного Представителя Клиента осуществляется Банком 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.

3.6. Procedure for Changing the Subscriber Number

3.6.1. To change the Subscriber Number of the Authorized Representative of the Client used to receive the One-Time Password, such Authorized Representative of the Client should contact the Bank and provide an Application to change the Subscriber Number providing identity documents. If the Subscriber Number is being changed by the Authorized Representative of the Client authorized to sign agreements/applications, he/she may only sign the Application to change the Subscriber Number (Appendix No. 3 to the Regulations), indicating that they confirm the ownership of the Subscriber Number.

3.6.2. For remote change of the Subscriber Number, the Client / Authorized Representative of the Client sends an Application to change the Subscriber Number through RBS System by selecting the appropriate document template. The Application should be signed by ES of the Authorized Representative of the Client submitting the request. 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, and notifications necessary for registration, access, and changes to the terms of use of RBS System. Remote change of the Subscriber Number is not possible in case of Compromise or suspicion of Compromise of the Electronic Signature.

3.6.3. The change of the Subscriber Number of the Client / Authorized Representative of the Client is carried out only after the successful 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.

- 3.6.4. При наличии технической возможности Банка и Клиента допускается направление Заявления на изменение Абонентского номера, Заявления об открытии Счета, Заявления о закрытии Счета, Заявления о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена, Заявления о внесении изменений в условия Договора, Заявление о расторжении Договора через Оператора ЭДО, согласованного с Банком. В таком случае, Заявление на изменение Абонентского номера должно быть подписано КЭП Уполномоченного Представителя Клиента, указанного в таком заявлении. Заявление об открытии Счета, Заявление о закрытии Счета, Заявление о внесении изменений в условия Договора, Заявление о расторжении Договора должно быть подписано КЭП Уполномоченного Представителя Клиента 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/Уполномоченным Представителем Клиента через Оператора ЭДО Заявления на изменение Абонентского номера Ответственным работником проводится идентификация и аутентификация Клиента/ Уполномоченного Представителя Клиента с использованием документов, удостоверяющих личность (оригиналы или нотариально заверенные копии), и документов, подтверждающих полномочия указанных лиц на использование аналогов собственноручной подписи (Электронной подписи) от имени Клиента (оригиналы или заверенные в установленном Банком порядке копии с предоставлением оригиналов для сверки, если ранее данные документы в Банк не представлялись).
- 3.6.4. If there is technical capability of the Bank and the Client, it is allowed to send the Application to change the Subscriber Number, the Application to open an Account, the Application to close an Account, the Application to amend the terms of the Agreement on the Implementation of Information Interaction Using Information Exchange Systems, and the Application to terminate the Agreement through the EDI Operator agreed with the Bank. In this case, the Application to change the Subscriber Number should be signed with QES of the Authorized Representative of the Client specified in this application. The Application to open an Account, the Application to close an Account, the Application to amend the terms of the Agreement, and the Application to terminate the Agreement should be signed with QES of the Authorized Representative of the Client who has the authority to sign and submit to the Bank documents, applications, and notifications necessary for registration, access, and changes to the terms of use of RBS System. In the event that the Client/Authorized Representative of the Client submits an Application for a change of the Subscriber Number through the EDI Operator, the Responsible Employee shall identify and authenticate the Client/Authorized Representative of the Client using identity documents (originals or notarized copies) and documents confirming the authority of the said persons to use analogues of a handwritten signature (Electronic Signature) on behalf of the Client (originals or copies certified in the manner established by the Bank with the provision of originals for verification, if these documents have not previously been submitted to the Bank).
- 3.7. Для изменения Кодовой информации Клиент/Уполномоченный Представитель Клиента должен лично обратиться в Банк с заявлением в свободной форме с предоставлением удостоверяющих личность
- 3.7. To change the Code information, the Client/Authorized Representative of the Client should personally contact the Bank with an application in free form, providing identification documents.

4. ПОРЯДОК ВЫПУСКА СЕРТИФИКАТОВ ПРОВЕРКИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ/РЕГИСТРАЦИИ СЕРТИФИКАТОВ КЭП ФНС

4.1 Для получения Сертификата ключа проверки электронной подписи для работы в Системе ДБО и осуществления обмена Электронными документами с использованием УНЭП, Уполномоченный Представитель Клиента, данные о котором указаны в Заявлении о заключении договора комплексного банковского обслуживания и (или) Заявлении о внесении изменений в условия Договора, Заявлении о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена, Карточке с образцами подписей (при её оформлении в соответствии с Правилами), прошедший Идентификацию у Ответственного работника Банка, должен лично:

- создать (посредством применения ссылки, поступившей из Банка на адрес электронной почты, указанный Клиентом/Уполномоченным Представителем Клиента в Заявлении о заключении договора комплексного банковского обслуживания) Запрос на выпуск Сертификата ключа проверки электронной подписи;
- установить Сертификат ключа проверки электронной подписи в Системе ДБО (ссылка на Сертификат ключа проверки электронной подписи поступит на электронный адрес, указанный Клиентом/Уполномоченным Представителем Клиента в Заявлении о заключении договора комплексного банковского обслуживания), после чего распечатать автоматически сформированный Акт приема-передачи Сертификата ключа проверки электронной подписи;
- предоставить в Банк Акт приема-передачи Сертификата ключа проверки электронной подписи на бумажном носителе, заверенный собственноручной подписью Уполномоченного Представителя Клиента в течение 2 (Двух) рабочих дней, либо предоставить уникальный идентификатор, который присваивается почтовым отправлениям, выдаваемый транспортной компанией, осуществляющей отправку оригиналов документов, либо направить документ посредством Оператора ЭДО.

4. PROCEDURE FOR ISSUING ELECTRONIC SIGNATURE VERIFICATION KEY CERTIFICATES / QES FTS CERTIFICATES REGISTRATION

4.1. To obtain an Electronic Signature Verification Key Certificate for working in RBS System and exchanging Electronic Documents using EUES, each Authorized Representative of the Client, whose details are specified in the Application to enter into a Comprehensive Banking Services Agreement and/or the Application to amend the terms of the Agreement and the Application to amend an Agreement on the Implementation of Information Interaction Using Information Exchange Systems, the Specimen Signature Card (if issued in accordance with the Rules), and who has undergone identification by the Responsible Employee of the Bank, should personally:

- Create a Request for the Issuance of an Electronic Signature Verification Key Certificate (using the link sent from the Bank to the email address specified by the Client/Authorized Representative in the Application to enter into an Comprehensive Banking Services Agreement);
- Install the Electronic Signature Verification Key Certificate in RBS System (a link to the Electronic Signature Verification Key Certificate will be sent to the email address specified by the Client/Authorized Representative in the Application to enter into an Comprehensive Banking Services Agreement), and then print the automatically generated Certificate of Acceptance and Transfer of Electronic Signature Verification Key Certificate;
- Provide the Bank with the Certificate of Acceptance and Transfer of the Electronic Signature Verification Key on paper, certified by the personal signature of the Authorized Representative of the Client within 2 (Two) business days, or provide a unique identifier assigned to postal items issued by the transport company sending the original documents, or send the document via the EDI Operator.

The instructions for connecting to RBS System and generating EUES Keys are available at <https://corpdocs.131.ru//> and in the Bank's office. The Electronic Signature Verification Key Certificate should contain the following mandatory information: the full name of the Authorized Representative of the

Инструкция по подключению к Системе ДБО и генерации ключей УНЭП размещена на ресурсе <https://https://corpdocs.131.ru/> и в офисе Банка. Сертификат ключа проверки электронной подписи в обязательном порядке должен содержать: полные ФИО Уполномоченного Представителя Клиента (владельца Сертификата ключа проверки электронной подписи), наименование Клиента, адрес местонахождения, уникальный номер Сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата, уникальный ключ проверки электронной подписи, наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи, наименование Удостоверяющего центра. Не допускается внесение каких-либо изменений в Сертификат ключа проверки электронной подписи, сформированный с использованием средств Системы ДБО.

4.2 С целью регистрации Клиентом Сертификата КЭП ФНС в Системе ДБО Банк направляет Уполномоченному Представителю Клиента на электронный адрес, указанный в Заявлении о заключении договора комплексного банковского обслуживания, ссылку для прохождения удаленной регистрации, после чего Уполномоченному Представителю Клиента необходимо совершить регистрацию Сертификата КЭП ФНС (при наличии нескольких Сертификатов КЭП ФНС Клиент/Уполномоченный Представитель Клиента вправе выбрать какой из Сертификатов КЭП ФНС будет зарегистрирован). Реквизиты зарегистрированного Сертификата КЭП ФНС автоматически передаются в Банк Оператором, Клиенту/Уполномоченному Представителю Клиента становится доступным подписание ЭД с помощью КЭП ФНС в Системе ДБО.

4.3 Сертификат ключа проверки электронной подписи/Сертификата КЭП ФНС подлежит отзыву Банком в случае:

- компрометации Электронной подписи владельца Сертификата ключа проверки электронной подписи, соответствующего данному сертификату;
- получения владельцем нового Сертификата ключа проверки электронной подписи.

Client (holder of the Electronic Signature Verification Key Certificate), the name of the Client, the address of the location, the unique number of the Electronic Signature Verification Key Certificate, the start and end dates of the validity of such certificate, the unique Electronic Signature Verification Key, the name of the electronic signature tool used and/or the standards to which the electronic signature key and the electronic signature verification key comply, and the name of the Certification Authority. No changes are allowed to the Electronic Signature Verification Key Certificate generated using the tools of RBS System.

4.2. To register the Client's QES FTS Certificate in RBS System, the Bank sends a link to the Client's Authorized Representative via the email address specified in the Application to enter into a Comprehensive Banking Services Agreement for Remote Registration, link for remote registration. The Client's Authorized Representative should then complete registration of QES FTS Certificate (if there are several QES FTS Certificates of the Client/Authorized Representative has the right to choose which QES FTS Certificate to register). The details of the registered QES FTS Certificate are automatically transmitted to the Bank by the Operator, and the Client/Authorized Representative becomes able to sign ED using QES FTS in RBS System.

4.3. The Electronic Signature Verification Key Certificate / QES FTS Certificate is subject to revocation by the Bank in the following cases:

- Compromise of the Electronic Signature of the holder of the Electronic Signature Verification Key Certificate corresponding to this certificate;
- Receipt of a new Electronic Signature Verification Key Certificate by the holder.

5. ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ/СЕРТИФИКАТА КЭП ФНС

- 5.1. Срок действия Сертификата ключа проверки электронной подписи составляет один календарный год с даты начала его действия. Сертификат ключа проверки электронной подписи действует в пределах срока должностных полномочий Владельца Сертификата ключа проверки электронной подписи, а в случае их прекращения (без предоставления документов о продлении) автоматически отключается.
- 5.2. Срок действия Сертификата КЭП ФНС составляет 15 (Пятнадцать) месяцев с даты начала его действия. В случае прекращения действия должностных полномочий Владельца Сертификат КЭП ФНС, Сертификат КЭП ФНС прекращает свое действие с момента внесения соответствующей записи в реестр УЦ ФНС.
- 5.3. При каждом входе в Систему ДБО за 30 (Тридцать) дней до окончания срока действия Сертификата ключа проверки Электронной подписи/Сертификата КЭП ФНС Система ДБО сообщает о скором его окончании.
- 5.4. До истечения срока действия Сертификатов ключей проверки Электронной подписи Клиент/Уполномоченный Представитель Клиента имеет возможность провести плановую процедуру обновления Сертификата ключа проверки электронной подписи (процедура осуществляется аналогично предусмотренной разделом 4 настоящего Регламента).
- 5.5. Регистрация Сертификата КЭП ФНС осуществляется после его обновления (действия выполняются аналогично действиям, содержащимся в п. 3.8. настоящего Регламента) после чего Клиенту/Уполномоченному Представителю Клиента необходимо осуществить регистрацию Сертификата КЭП ФНС (действия выполняются аналогично действиям, содержащимся в разделе 4 настоящего Регламента).

6. ПОРЯДОК БЛОКИРОВКИ И ВОССТАНОВЛЕНИЯ ДОСТУПА К

5. PROCEDURE FOR THE SCHEDULED REPLACEMENT OF THE ELECTRONIC SIGNATURE VERIFICATION KEY CERTIFICATE / QES FTS CERTIFICATE

- 5.1. The validity period of the Electronic Signature Verification Key Certificate is one calendar year from the date of its validity. The Electronic Signature Verification Key Certificate is valid within the term of office of the Owner of the Electronic Signature Verification Key Certificate, and in case of their termination (without providing renewal documents) it is automatically disabled.
- 5.2. The validity period of QES FTS Certificate is 15 (Fifteen) months from the date of its validity. In case of termination of the official powers of the Owner of QES FTS Certificate, QES FTS Certificate shall cease to be valid from the moment the corresponding entry is made in the register of the CA FTS.
- 5.3. Upon each login to RBS System, 30 (Thirty) days before the expiration of the Electronic Signature Verification Key Certificate / QES FTS Certificate, RBS System notifies the user of its impending expiration.
- 5.4. Before the expiration of the Electronic Signature Verification Key Certificates, the Client / Authorized Representative of the Client has the opportunity to carry out a scheduled procedure for updating the Electronic Signature Verification Key Certificate (the procedure is carried out in the same way as that provided for in Section 4 of the Regulations).
- 5.5. Registration of QES FTS Certificate is carried out after its renewal (actions are performed similarly to the actions contained in Clause 3.8 of the Regulations) after which the Client/Authorized Representative of the Client should register QES FTS Certificate (actions are performed similarly to the actions contained in Section 4 of the Regulations).

6. PROCEDURE FOR BLOCKING

СИСТЕМЕ ДБО

6.1. Основанием для блокировки доступа Клиента и (или) его Уполномоченного Представителя к Системе ДБО являются:

- 6.1.1.** Получение Банком от Уполномоченного Представителя Клиента Заявления о внесении изменений в условия Договора (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;
- 6.1.2.** Компрометация Электронной подписи и/или использование Электронной подписи без согласия Уполномоченного Представителя Клиента;
- 6.1.3.** Замена Карточки с образцами подписей и оттиска печати и (или) Соглашения о сочетании электронных подписей, при их оформлении в соответствии с Правилами;
- 6.1.4.** Прекращение или изменение полномочий или данных Уполномоченного Представителя Клиента;
- 6.1.5.** Смена Абонентского номера Уполномоченного Представителя Клиента;
- 6.1.6.** Утраты Аутентификационных данных;
- 6.1.7.** Непредставление или представление недостоверных сведений и документов, запрашиваемых Банком, в том числе в целях выполнения требований законодательства Российской Федерации и нормативных актов Банка России;
- 6.1.8.** Выявление Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, установленным Банком России или подозрений на их совершение;
- 6.1.9.** Направление Клиентом Заявления о внесении изменений в условия Договора, Заявления о внесении изменений в Соглашение об осуществлении информационного взаимодействия с

AND RESTORING ACCESS TO RBS SYSTEM

6.1 The grounds for blocking the Client's and/or his/her Authorized Representative's access to RBS System are:

- 6.1.1.** Receipt by the Bank of an Application to amend the terms of the Agreement from the Authorized Representative of the Client (containing information about the change of the Authorized Representative of the Client / change of his/her data / termination of authority or other information causing the Bank to doubt the possibility of access and/or use of RBS System by the Authorized Representative of the Client), a request to suspend access to RBS System, indicating the reasons for such suspension;
- 6.1.2.** Compromise of the Electronic Signature and/or use of the Electronic Signature without the consent of the Authorized Representative of the Client;
- 6.1.3.** Replacement of the Specimen Signature Card and/or the Agreement on the Combination of Electronic Signatures, if issued in accordance with the Rules;
- 6.1.4.** Termination or change of the authority or data of the Authorized Representative of the Client;
- 6.1.5.** Change of the Subscriber Number of the Authorized Representative of the Client;
- 6.1.6.** Loss of Authentication Data;
- 6.1.7.** Failure to provide or provision of inaccurate 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;
- 6.1.8.** Identification by the Bank of a transaction corresponding to the signs of transferring funds without the voluntary consent of the Client, as established by the Central Bank of Russia, or suspicions of such actions;
- 6.1.9.** Submission by the Client of an Application to amend the terms of the Agreement, Applications to amend the Agreement on the Implementation of Information Interaction Using Information Exchange Systems within the framework of which

использованием Систем информационного обмена, в рамках которого происходит приостановление предоставления доступа к Системе ДБО.

6.2. При наступлении событий, указанных в пп. 6.1.3, 6.1.7, 6.1.8 доступ в Систему ДБО блокируется всем Уполномоченным Представителям Клиента.

6.3. Клиент вправе осуществить блокировку доступа к Системе ДБО, в случаях, не связанных с компрометацией, или подозрении на компрометацию Электронной подписи.

6.3.1. Порядок блокировки доступа к Системе ДБО дистанционным способом:

Для дистанционной блокировки доступа к Системе ДБО Уполномоченному Представителю Клиента необходимо обратиться в Банк с соответствующим запросом по следующим контактными 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 Ответственный работник Банка связывается с Уполномоченным Представителем Клиента с использованием контактных данных такого лица, указанных Уполномоченным Представителем Клиента в Заявлении о заключении договора комплексного банковского обслуживания, Заявлении о внесении изменений в Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена, при этом, Уполномоченный Представитель Клиента должен сообщить Ответственному работнику Банка сведения, необходимые для аутентификации Уполномоченного Представителя Клиента.

6.3.2. Порядок блокировки доступа к Системе ДБО при личном обращении Уполномоченного Представителя Клиента в Банк:

access to RBS System is suspended.

6.2. Upon the occurrence of the events specified in clauses 6.1.3, 6.1.7, and 6.1.8, access to RBS System is blocked for all Authorized Representatives of the Client.

6.3. The Client has the right to block access to the RBS System in cases not related to compromise or suspicion of compromise of the Electronic Signature.

6.3.1. Procedure for blocking access to RBS System remotely:

To block access to RBS System remotely, the Authorized Representative of the Client should contact the Bank with a corresponding request at the following contact details: `dbo@131.ru` or using RBS System, indicating the data of the Authorized Representative of the Client allowing their identification. To process the request for remote blocking, the authorized employee of the Bank contacts the Authorized Representative of the Client using the contact details of such person specified by the Authorized Representative of the Client in the Application for the Product and the Application, and the Authorized Representative of the Client should provide the authorized employee of the Bank with the information necessary for authentication.

6.3.2. Procedure for blocking access to RBS System upon personal application of the Authorized Representative of the Client to the Bank:

6.3.2.1. 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.

6.3.2.2. Подача запроса на блокировку доступа к Системе ДБО Уполномоченного Представителя Клиента возможна только в течение Операционного времени Банка.

6.4. Блокировка доступа осуществляется незамедлительно после получения соответствующего запроса и аутентификации Уполномоченного Представителя Клиента Банком. 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.

6.5. Порядок восстановления доступа к Системе ДБО:
В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п.6.1.2–6.1.6, 6.1.9 разблокировка возможна после получения Банком письменного обращения (Заявления о разблокировке 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>, а также в офисе Банка. Одновременно с обращением Уполномоченный Представитель Клиента должен предоставить документы, удостоверяющие его личность и подтверждающие его полномочия и:

6.3.2.1. The Authorized Representative of the Client should apply directly to the Bank's office at its legal address with a corresponding written application to block access to RBS System, signed by such person. Simultaneously with the request, the Authorized Representative of the Client should provide identity documents and documents confirming his/her authority.

6.3.2.2. Submission of a request to block access to RBS System by the Authorized Representative of the Client is possible only during the Bank's operating hours.

6.4. Access is blocked immediately after receiving the corresponding request and authenticating the Authorized Representative of the Client by the Bank. If the request is received by the Bank outside operating hours, such a request will be processed, and access to RBS System will be blocked during the operating hours of the nearest working day following the date of receipt of such request by the Bank.

6.5. Procedure for restoring access to RBS System:
If the grounds for blocking access to RBS System were the circumstances specified in clauses 6.1.2–6.1.6, 6.1.9, unblocking is possible after the Bank receives a written request (Application to unblock access to RBS System) from the Authorized Representative of the Client upon personal visit to the Bank's office. The form of such an application is determined by the Bank and is available at <https://131.ru/contracts> and in the Bank's office. Simultaneously with the request, the Authorized Representative of the Client should provide identity documents and documents confirming his/her authority and:

- a) При использовании УНЭП/КЭП ФНС: проведенной процедуры внеплановой смены Сертификата ключа проверки Электронной подписи/Сертификата КЭП ФНС в соответствии с разделом 8 настоящего Регламента;
- b) При смене Абонентского номера Уполномоченного Представителя Клиента. В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п. 6.1.6 Регламента, разблокировка возможна в соответствии с учетом проведения процедуры Идентификации Уполномоченного Представителя Клиента. Дистанционная разблокировка в учетом проведенной процедуры Идентификации Уполномоченного Представителя Клиента возможна при отсутствии у Банка оснований полагать, что Средства подтверждения Электронного документа стали известны неуполномоченным третьим лицам.

6.6. В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п.6.1.8 Регламента, разблокировка возможна после получения Банком от Клиента подтверждения распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, установленным Банком России, при отсутствии иных установленных законодательством Российской Федерации оснований.

6.7. В случае, если основанием для блокировки доступа к Системе ДБО послужили обстоятельства, указанные в п.6.1.7 Регламента, доступ к Системе ДБО возобновляется после представления сведений и документов, запрашиваемых Банком. Документы предоставляются Уполномоченным Представителем Клиента Ответственному работнику в офисе Банка по его юридическому адресу в течение Операционного времени Банка.

- a) When using an EUES / QES FTS: of the unscheduled replacement procedure done for the Electronic Signature Verification Key Certificate / QES FTS Certificate in accordance with Section 8 of the Regulations;
- b) When the Subscriber Number of the Client's Authorized Representative changes. If the circumstances specified in Clause 6.1.6 of the Regulations served as the basis for blocking access to RBS System, unblocking is possible subject to the completion of the Identification Procedure of the Client's Authorized Representative. Remote unblocking, subject to the completed Identification Procedure of the Client's Authorized Representative, is possible if the Bank has no grounds to believe that the Electronic Document Verification Facilities have become known to unauthorized third parties.

6.6. If the grounds for blocking access to RBS System were the circumstances specified in clause 6.1.8 of the Regulations, unblocking is possible after the Bank receives confirmation from the Client of the order to perform a transaction corresponding to the signs of transferring funds without the voluntary consent of the Client, as established by the Central Bank of Russia, in the absence of other grounds established by the legislation of the Russian Federation.

6.7. If the grounds for blocking access to RBS System were the circumstances specified in Clause 7.1.7 of the Regulations, access to RBS System is restored after the provision of the information and documents requested by the Bank. The documents are submitted by the Authorized Representative of the Client to the Responsible Employee at the Bank's office at its legal address during the Bank's operating hours.

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

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

7.2. Банк уведомляет Клиента о наступлении указанных в п. 7.1 Регламента обстоятельствах любым доступным Банку способом, используя имеющиеся в распоряжении Банка контактные данные Клиента, ранее предоставленные Клиентом.

7.3. Клиент уведомляет Банк о наступлении указанных в п. 7.1 Регламента обстоятельствах любым из нижеперечисленных способов:

- Письменное Уведомление о компрометации на бумажном носителе (передается в офисе Банка);
- Сканированная копия письменного Уведомления о компрометации, переданная 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, либо предоставить уникальный идентификатор, который присваивается почтовым отправлениям, выдаваемый транспортной компанией, осуществляющей отправки оригиналов документов, либо направить экземпляры документов посредством Оператора ЭДО.
- Форма Уведомления о компрометации определяется Банком и является Приложением №4 к Регламенту.

7.4. С момента получения Банком уведомления Клиента или выявления Банком обстоятельств, указанных в п. 7.1 Регламента, доступ Клиента (его

7. PROCEDURE FOR ACTIONS IN CASE OF COMPROMISE OR SUSPICION OF COMPROMISE OF THE ELECTRONIC SIGNATURE

7.1 If one of the Parties identifies a compromise of the Electronic Signature or signs (suspicions) thereof, the identifying Party notifies the other Party.

7.2. The Bank notifies the Client of the circumstances specified in clause 7.1 of the Regulations by any means available to the Bank, using the contact details of the Client previously provided by the Client.

7.3. The Client notifies the Bank of the circumstances specified in Clause 7.1 of these Regulations by any of the following methods:

- Written Notice of Compromise on paper (submitted at the Bank's office);
- Scanned copy of the written Notice of Compromise sent to the Bank's email address: dbo@131.ru. The Client is obliged to submit the original of such Notice of Compromise on paper to the Bank within 2 (two) working days, or provide a unique identifier assigned to the shipment by the transport company delivering the original documents, or send the documents via EDI Operator.
- The form of the Notice of Compromise is determined by the Bank and is Appendix No. 4 to the Regulations.

7.4. From the moment the Bank receives the Client's notification or identifies the circumstances specified in Clause 7.1 of the Regulations, the Client's (his/her Authorized

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 блокировке доступа к Системе ДБО направлены на обеспечение сохранности средств на Счете, защиту интересов Клиента и недопущению мошеннических операций и практик.

7.5. С момента направления Клиентом Банку или получения Клиентом от Банка уведомления о наступлении указанных в п. 7.1 Регламента обстоятельствах, Клиент/Уполномоченный Представитель Клиента не вправе использовать скомпрометированную Электронную подпись (ее ключ и (или) средства)/Аутентификационные данные/Абонентский номер. В случае любого использования Клиентом/Уполномоченным Представителем Клиента такой Электронной подписи/Аутентификационных данных/Абонентского номера после наступления указанных в п. 7.1 Регламента обстоятельств, Клиент/Уполномоченный Представитель Клиента самостоятельно несет риск наступления неблагоприятных последствий для него, в том числе правовых и финансовых.

7.6. В случае компрометации ключа КЭП ФНС блокировка Квалифицированного сертификата находится в компетенции УЦ ФНС. Для разблокировки Клиенту следует обратиться в УЦ ФНС.

7.7. Разблокировка доступа к Системе ДБО осуществляется в соответствии с п. 6.5 Регламента при получении Банком Заявления о разблокировке доступа в Системе ДБО на бумажном носителе.

8. ПОРЯДОК ПРОВЕДЕНИЯ ВНЕПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ

Representatives') access to RBS System is blocked until such access is unblocked. The Client is notified and agrees that the Bank is not responsible, including financially, for any fact of blocking the Client's and/or his/her Authorized Representatives' access to RBS System, as the Bank's actions to block access to RBS System are aimed at ensuring the safety of funds in the Account, protecting the Client's interests, and preventing fraudulent transactions and practices.

7.5. From the moment the Client sends a notification to the Bank or receives a notification from the Bank about the occurrence of the circumstances specified in clause 7.1 of the Regulations, the Client is not entitled to use the compromised Electronic Signature (its key and/or tools)/Authentication Data/Subscriber Number. In case of any use by the Client of such Electronic Signature/Authentication Data/Subscriber Number after the occurrence of the circumstances specified in clause 7.1 of the Regulations, the Client / Authorized Representative of the Client independently bears the risk of adverse consequences, including legal and financial ones.

7.6. In case of compromise of QES FTS key, CA FTS is responsible for blocking the Qualified Certificate. To unblock it, the Client should contact CA FTS.

7.7. Access to RBS System is unblocked in accordance with Clause 6.5 of the Regulations upon receipt by the Bank of an Application for unblocking access to RBS System on paper.

8. PROCEDURE FOR UNSCHEDULED REPLACEMENT OF THE ELECTRONIC SIGNATURE VERIFICATION KEY

ПОДПИСИ/КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЭП ФНС

CERTIFICATE / QES FTS QUALIFIED CERTIFICATE

- 8.1.** Указанный раздел применяется в случае использования Клиентом (его Уполномоченными Представителями) УНЭП/КЭП ФНС. 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 Клиента/Уполномоченного Представителя Клиента;
 - выхода из строя ФКН.
- 8.2.** После получения Банком Уведомления о компрометации Банк отзывает (аннулирует) Сертификат скомпрометированного ключа проверки электронной подписи.
- 8.3.** В случае возникновения одного из событий, отраженных в п. 8.1. Клиент/Уполномоченный Представитель Клиента инициирует процедуру внеплановой смены Квалифицированного сертификата КЭП ФНС путем обращения в УЦ ФНС.
- 8.4.** Для активации нового ключа Электронной подписи и соответствующего ему Сертификата ключа проверки Электронной подписи Клиент/Уполномоченный Представитель Клиента лично обращается в офис Банка с запросом 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.
- 8.5.** Для активации Ключа КЭП ФНС и Сертификата КЭП ФНС действия выполняются аналогично п. 3.8. и разделу 4 настоящего Регламента.
- 8.1** This section applies if the Client (his/her Authorized Representatives) uses EUES / QES FTS. The unscheduled replacement of the Electronic Signature Keys / the Authorized Representative of the Client and the corresponding Electronic Signature Verification Key Certificates is performed in the following cases:
- Established fact of Compromise of the Electronic Signature or suspicion thereof;
 - Change of registration data of the Client / Authorized Representative of the Client;
 - Malfunction of FKC.
- 8.2.** After receiving the Notice of Compromise, the Bank revokes (cancels) the compromised Electronic Signature Verification Key Certificate.
- 8.3.** In case of one of the events specified in Clause 8.1, the Client/Authorized Representative of the Client initiates the procedure for an unscheduled change of the QES FTS Qualified Certificate by contacting CA FTS.
- 8.4.** To activate a new Electronic Signature Key and the corresponding Electronic Signature Verification Key Certificate, the Client / Authorized Representative of the Client personally contacts the Bank's office with an application for the issuance of an Electronic Signature Verification Key Certificate in free form and in the manner specified in Section 4 of the Regulations, providing identity documents and documents confirming his/her authority.
- 8.5.** To activate QES FTS Key and QES FTS Certificate, the actions are performed similarly to Clause 3.8 and Section 4 of the Regulations.

9. ПОРЯДОК ПРОВЕРКИ ПОДЛИННОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ. ПОРЯДОК РАССМОТРЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

- 9.1.** 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 процедура проверки авторства и (или) целостности Электронного документа, подписанного Электронной подписью Уполномоченного Представителя Клиента.
- 9.2.** Стороны признают информацию, содержащуюся в программно-аппаратных средствах и системных журналах Банка, достаточной для проверки подлинности КЭП ФНС/УНЭП, ПЭП (в том числе Мобильной подписи) в Электронном документе/Простом ЭД.
- 9.3.** При подтверждении подлинности ПЭП в Простом ЭД осуществляется установление факта использования Клиентом корректного Средства простой ЭП программно-техническими средствами Оператора согласно Правилам КИС "Besafe".
- 9.4.** Подтверждение подлинности КЭП ФНС/УНЭП в Электронных документах осуществляется путем проверки соответствующим средством Электронной подписи с использованием Квалифицированного сертификата КЭП ФНС/Сертификата ключа проверки электронной подписи принадлежности такой Электронной подписи в Электронном документе Клиента/Уполномоченному Представителю Клиента (владельцу соответствующего сертификата) и отсутствия искажений в подписанном данной Электронной подписью Электронном документе, в соответствии с процедурой, приведенной в п.10.10 Регламента.

9. PROCEDURE FOR VERIFYING THE AUTHENTICITY OF AN ELECTRONIC SIGNATURE. PROCEDURE FOR RESOLVING DISPUTES

- 9.1** The procedure for verifying the authenticity of the Electronic Signature is initiated by the Bank or the Client. The procedure for verifying the authenticity of the Electronic Signature, when exchanging Electronic Documents between the Bank and the Client using RBS System, signed with an Electronic Signature, refers to the Bank or the Client having doubts regarding the authorship and/or integrity of the Electronic Document signed with the Electronic Signature of the Authorized Representative of the Client.
- 9.2.** The Parties recognize that the information contained in the Bank's hardware and software systems and system logs is sufficient to verify the authenticity of QES FTS / EUES, SES (including Mobile Signature) in the Electronic Document / Simple ED.
- 9.3.** When confirming SES authenticity in the Simple ED, the fact of the Client's use of the correct Simple ED Tool is established by the Operator's software and hardware in accordance with Besafe CIS Rules.
- 9.4.** Confirmation of the authenticity of QES FTS / EUES in Electronic Documents is carried out by verifying the corresponding Electronic Signature facility using QES FTS Qualified Certificate / Electronic Signature Verification Key Certificate to confirm that such Electronic Signature in the Electronic Document belongs to the Client / Authorized Representative of the Client (the Certificate Holder) and that there are no distortions in the Electronic Document signed with this Electronic Signature, in accordance with the procedure set out in Clause 10.10 of the Regulations.

9.5. Процедура проверки подлинности Электронной подписи при обмене Электронными документами Клиентом и Банком с использованием Системы ДБО, в случае применения Клиентом КЭП ФНС/УНЭП основывается на математических свойствах алгоритма Электронной подписи, реализованного в соответствии с актуальным стандартом Российской Федерации ГОСТ Р 34.10-2012, гарантирующего невозможность подделки значения КЭП ФНС/УНЭП 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.

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 КЭП ФНС/УНЭП, Квалифицированного сертификата КЭП ФНС/Сертификата ключа проверки электронной подписи Уполномоченного Представителя Клиента, использованный при создании КЭП ФНС/УНЭП, историю настроек Системы ДБО для использования КЭП ФНС/УНЭП в системных журналах Банка, а также данные Средств подтверждения Электронных документов, использованные при создании КЭП ФНС/УНЭП в оспариваемом Электронном документе. Банк обеспечивает защиту данных от возможных искажений в процессе хранения.

9.6. В случае, если оспариваемый Электронный документ/Простой ЭД является частью пакета Простых ЭД/Электронных

9.5. The procedure for verifying the authenticity of the Electronic Signature when exchanging Electronic Documents between the Client and the Bank using RBS System, in the case of the Client using a QES FTS / EUES, is based on the mathematical properties of the Electronic Signature algorithm implemented in accordance with the current Russian standard GOST R 34.10-2012, which guarantees the impossibility of forging the value of QES FTS / EUES by any person who does not possess the key of such Electronic Signature. The outcome of resolving a dispute is either proving the authenticity, integrity, and authorship of the disputed Electronic Document to the Client (his/her Authorized Representative) or establishing the fact that the Bank received a distorted Electronic Document.

In the event of disputes, the Bank ensures the storage of Electronic Documents in a special database for the periods established by the legislation of the Russian Federation. Each storage unit includes the data of the Electronic Document, the Electronic Signature lines with QES FTS / EUES parameters, QES FTS Qualified Certificate / Electronic Signature Verification Key Certificate of the Authorized Representative of the Client used to create QES FTS / EUES, the history of RBS System settings for using QES FTS / EUES in the Bank's system logs, as well as the Electronic Document Confirmation Tools used to create QES FTS / EUES in the disputed Electronic Document. The Bank ensures the protection of data from possible distortions during storage.

9.6. If the disputed Electronic Document / Simple ED is part of a package of Simple EDs / Electronic Documents, the Electronic

документов, то процедура проверки подлинности Электронной подписи осуществляется под пакетом Электронных документов, в состав, которого входит оспариваемый Электронный документ.

9.7. Рассмотрение конфликтных ситуаций осуществляется в порядке, предусмотренном Правилами КИС «Besafe».

9.8. Ответственность Сторон при оспаривании Электронных документов, подписанных Электронной подписью, обмен которыми осуществляется с использованием Системы ДБО.

9.8.1. Банк не несет ответственности перед Клиентом в случаях, указанных в Правилах (включая приложения к ним), а также при установлении Технической комиссией совокупности следующих фактов при проверке КЭП ФНС/УНЭП под оспариваемым Электронным документом:

- ключ проверки Электронной подписи в оспариваемом Электронном документе принадлежит Уполномоченному Представителю Клиента - Владелец сертификата ключа проверки электронной подписи/Владельцу квалифицированного сертификата КЭП ФНС;
- Сертификат ключа проверки электронной подписи/Квалифицированного сертификата КЭП ФНС Уполномоченного Представителя Клиента — владельца соответствующего сертификата 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

Signature verification procedure is carried out for the package of Electronic Documents, which includes the disputed Electronic Document.

9.7. Conflict situations are resolved in accordance with the procedure established by Besafe CIS Rules.

9.8. Liability of the Parties in case of disputes regarding Electronic Documents signed with an Electronic Signature exchanged using RBS System.

9.8.1. The Bank is not liable to the Client in the cases specified in the Rules (including their appendices), as well as when the Conciliation Commission establishes the following facts during the verification of QES FTS / EUES under the disputed Electronic Document:

- The Electronic Signature Verification Key in the disputed Electronic Document belongs to the Authorized Representative of the Client—the Holder of the Electronic Signature Verification Key Certificate / Holder of QES FTS qualified certificate;
- The Electronic Signature Verification Key Certificate / QES FTS Qualified Certificate of the Authorized Representative of the Client—the holder of the corresponding Certificate was valid at the time the Bank received the disputed Electronic Document;
- The Bank did not receive a Notice of Compromise of the Electronic Signature Key and/or an application to block access to RBS System by the Authorized Representative of the Client using the Electronic Document Confirmation Facility with which the disputed Electronic Document was signed, or the moment the Bank received the Notice of Compromise of the Electronic Signature Key and/or the application to block access was later than the moment the Bank received the disputed Electronic Document.

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.

9.8.2. Ответственность Банка наступает исключительно при наличии доказанной вины последнего и наличии прямой причинно-следственной связи между наступившими событиями, доказанной виной Банка и негативными для Клиента последствиями (ущербом). В любом случае, ни при каких обстоятельствах, Банк не возмещает Клиенту упущенную выгоду.

9.8.3. Клиент/Уполномоченный Представитель Клиента несут ответственность перед Банком во всех и любых случаях невыполнения и/или ненадлежащего выполнения Правил (включая приложения к ним), Регламента, Правил КИС “Besafe”, Правил УЦ, 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, связанных с таким нарушением/ненадлежащим исполнением.

9.8.2. The Bank’s liability arises exclusively in the presence of proven fault on its part and a direct causal connection between the events that occurred, the proven fault of the Bank, and the negative consequences (damage) for the Client. In any case, under no circumstances does the Bank compensate the Client for lost profits.

9.8.3. The Client/Authorized Representative of the Client is liable to the Bank in all and any cases of non-fulfillment and/or improper fulfillment of the Rules (including their appendices), the Regulations, Besafe CIS Rules, CA Rules, provisions of the legislation of the Russian Federation, and the requirements of the Bank, and bears the risk of any legal and/or financial consequences, including adverse consequences for the Client, the Bank, and other persons related to such violation/improper performance.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

10.2. Правоотношения Сторон, урегулированные Регламентом, а также любые иные правоотношения Сторон, связанные с выполнением Регламента, подлежат регулированию и толкованию в

10. FINAL PROVISIONS

10.1 The Regulations are drawn up in Russian and English. In case of any discrepancies, the Russian text of the Regulations shall prevail.

10.2. The legal relations of the Parties governed by the Regulations, as well as any other legal relations of the Parties related to the implementation of the Regulations, shall be regulated and interpreted in accordance with the legislation of the Russian Federation.

соответствии с законодательством Российской Федерации.

- 10.3.** В случае, если любая из Сторон откажется от исполнения решения Технической комиссии, все споры и разногласия подлежат разрешению в соответствии с настоящим пунктом. Все споры, возникающие между Клиентом и Банком в рамках выполнения Регламента или в связи с ним, подлежат разрешению 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 – 15 (пятнадцать) рабочих дней с даты ее получения Банком.
- 10.4.** В случае изменения положений законодательства Российской Федерации, при которых положения Регламента входят в противоречие с положениями законодательства Российской Федерации, к таким правоотношениям Сторон подлежат применению положения законодательства Российской Федерации.
- 10.5.** В случае признания какого-либо условия Регламента недействительным, это не влечет недействительности Регламента в целом и/или любых иных положений Регламента. Взамен недействительного положения к правоотношениям Сторон подлежат применению нормы законодательства Российской Федерации.
- 10.6.** Банк вправе в одностороннем, внесудебном порядке вносить изменения в Регламент и/или приложения к нему. Изменения в Регламент вступают в силу и
- 10.3.** If either Party refuses to comply with the decision of the Conciliation Commission, all disputes and disagreements shall be resolved in accordance with this clause. All disputes arising between the Client and the Bank in connection with or related to the implementation of these Regulations shall be resolved in accordance with the legislation of the Russian Federation through negotiations, and if such resolution is impossible, in the Arbitration Court of the Republic of Tatarstan. The Client has the right to submit a written claim to the Bank, signed by the Authorized Representative of the Client and sealed by the latter (if applicable), by contacting the Bank's office at its legal address. The pre-trial written procedure for resolving disputes with the Bank, within the framework of these Regulations, is mandatory. The response time to a pre-trial claim is 15 (Fifteen) working days from the date of its receipt by the Bank.
- 10.4.** In case of changes in the provisions of the legislation of the Russian Federation, under which the provisions of these Regulations conflict with the provisions of the legislation of the Russian Federation, the provisions of the legislation of the Russian Federation shall apply to such legal relations of the Parties.
- 10.5.** If any provision of these Regulations is declared invalid, this shall not invalidate the Regulations as a whole and/or any other provisions of these Regulations. In place of the invalid provision, the norms of the legislation of the Russian Federation shall apply to the legal relations of the Parties.
- 10.6.** The Bank has the right to unilaterally and out of court amend these Regulations and/or its appendices. Amendments to these

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 Банком 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 Регламентом, а также изменениями в нем. Не ознакомление или несвоевременное ознакомление Клиента и/или его Уполномоченных Представителей с изменениями, внесенными в Регламент, не является основанием для их неприменения к правоотношениям Сторон. В случае несогласия Клиента с изменениями в Регламент, последний вправе расторгнуть Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена в рамках использования Системы ДБО, 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 Регламенту. В случае неполучения Банком, до вступления в силу изменений в Регламент письменного уведомления Клиента, изменения считаются безоговорочно принятыми Клиентом, заключение дополнительных соглашений Сторонами не требуется.

10.7. ЗАО «Центр Цифровых Сертификатов» (ИНН 5407187087) вправе в одностороннем внесудебном порядке вносить изменения в Правила КИС «BeSafe» и Правила УЦ. Текст изменений доводится до сведения Клиентов посредством уведомления в срок, указанный в Правилах КИС «BeSafe/» Правилах УЦ, до даты

Regulations shall enter into force and apply to the legal relations of the Parties after 10 (Ten) calendar days from the date of publication of such amendments or the new version of the Regulations at: <https://131.ru/contracts> or notification of the Client of such amendments by any other means available to the Bank. Before each interaction with the Bank using RBS System, including sending any Electronic Document to the Bank, as well as at least once every 10 (Ten) calendar days, the Client and its Authorized Representatives are obliged to familiarize themselves with these Regulations and any amendments thereto. Failure to familiarize or untimely familiarization of the Client and/or his/her Authorized Representatives with amendments to these Regulations is not grounds for their non-application to the legal relations of the Parties. In case of the Client's disagreement with amendments to the Regulations, the Client has the right to terminate the Agreement on Information Interaction Using Information Exchange Systems within the framework of using RBS System, in the manner and under the conditions specified in the Rules, unless otherwise provided in a separate agreement between the Parties, by notifying the Bank in writing no later than the date such amendments enter into force, in accordance with these Regulations. If the Bank does not receive written notification from the Client before the amendments to these Regulations enter into force, the amendments are considered unconditionally accepted by the Client, and no additional agreements between the Parties are required.

10.7. Digital Certificate Center CJSC (INN (Taxpayer Identification Number) 5407187087) has the right to unilaterally and extrajudicially amend BeSafe CIS Rules and CA Rules. The text of the amendments will be communicated to Clients by notification within the time period specified in BeSafe CIS Rules/CA Rules, prior to the effective date of such amendments. Notification will be made by posting the relevant information on the websites www.besafe.ru and www.authority.ru.

вступления в силу таких изменений. Уведомление осуществляется путем размещения соответствующей информации на сайте www.besafe.ru и www.authority.ru.

11. СПИСОК ПРИЛОЖЕНИЙ

- 11.1. Приложение №1** Акт приема-передачи ФКН Системы ДБО Faktura.ru
- 11.2. Приложение №2** Заявление о разблокировке доступа в системе ДБО Faktura.ru /смене Абонентского номера
- 11.3. Приложение №3** Уведомление о компрометации ключа Электронной подписи (прекращении действия средства подтверждения и (или) об утрате средства подтверждения, и (или) об использовании Системы ДБО Faktura.ru без согласия Клиента)
- 11.4. Приложение №4** Инструкция по обеспечению информационной безопасности при работе в Системе ДБО Faktura.ru
- 11.5. Приложение №5** Требования к программно-техническим средствам для проведения расчетных операций в электронной форме в Системе ДБО Faktura.ru
- 11.6. Приложение №6** Заявление на установление ограничений по параметрам операций с использованием Системы дистанционного банковского обслуживания Faktura.ru АО «Банк 131»

11. LIST OF APPENDICES

- 11.1. Appendix No. 1:** Act of Acceptance and Transfer of FKC of Faktura.ru RBS System.
- 11.2. Appendix No. 2:** Application for Unblocking Access to Faktura.ru RBS System / Changing the Subscriber Number.
- 11.3. Appendix No. 3:** Notice of Compromise of the Electronic Signature Key (Termination of the Confirmation Tool and/or Loss of the Confirmation Tool, and/or Use of Faktura.ru RBS System Without the Client's Consent).
- 11.4. Appendix No. 4:** Information Security Guidelines for Working in Faktura.ru RBS System.
- 11.5. Appendix No. 5:** Requirements for Software and Hardware for Conducting Settlement Operations in Electronic Form in Faktura.ru RBS System.
- 11.6. Appendix No. 6:** Application for Setting Restrictions on Transaction Parameters Using Faktura.ru Remote Banking Service System of Bank 131 JSC.

Приложение №1 к Регламенту дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru

АКТ № _____
приема-передачи ФКН Системы ДБО
Faktura.ru
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, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru (далее – «Регламент») (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 Faktura.ru в соответствии с Правилами комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131», Условиями осуществления информационного взаимодействия с использованием Системы информационного обмена и Регламентом:

Appendix No. 1 to the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System

Acceptance and Delivery Certificate No.
of FKM of Faktura.ru RBS System

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, represented by _____, represented by _____, acting under _____, on the other part, referred together herein as Parties and individually as a Party, within the framework of the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System (hereinafter - the Regulations) (Statement of Accession No. _____ dated _____ 20__), have drawn up this Certificate as follows:

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:

п/а / п/п	Full name (of Client`s Authorized person) / ФИО (Уполномоченного лица клиента)	FKM / ФКН
1.		Rutoken ES 3.0 electronic key No. ____ / электронный ключ РутOKEN «РутOKEN ЭЦП 3.0» № _____

Передал
АО «Банк 131»
420111, Российская Федерация, Республика

Transferred
Bank 131 JSC
420011, Russian Federation, Republic of Tatarstan, Kazan,

Татарстан,
город Казань, улица Карла Маркса, здание 28
ИНН/ОГРН 1655505780/1241600056390

Karl Marx St., 28 INN (Taxpayer Identification Number)
1655505780
OGRN (Primary State Registration Number) 1241600056390

от Банка: _____
(должность)

from the Bank: _____
(position)

(подпись) (расшифровка подписи)

(signature) (printed name)

Принял
Наименование
Адрес
ИНН/ОГРН

Accepted
Name
Address
INN (Taxpayer Identification Number)
OGRN (Primary State Registration Number)

от Клиента: _____
(должность) М.П.

from the Client: _____
(position) L.S.

(подпись) (расшифровка подписи)

(signature) (printed name)

Приложение №2 к Регламенту дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru

Заявление

о разблокировке доступа в системе ДБО Faktura.ru /смене Абонентского номера

г. Казань

«__» _____ 20__ г.

Appendix No. 2 to the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System

Application

on unlocking Faktura.ru RBS system access / subscriber number 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	
OGRN (Primary State Registration Number) / ОГРН	
E-mail address/Адрес электронной почты ¹	
Subscriber Number/ Абонентский номер ²	

В соответствии с Регламентом дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru (далее - Система ДБО) прошу:

In accordance with the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System (hereinafter referred to as RBS System), I hereby request to:

- ☐ - unblock access to RBS System using previously provided access data (I agree with the terms and ground for the blocking, have 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);
- ☐ - establish a new Subscriber number for access to RBS System, for passing the procedure of authentication and signing of Electronic documents when using it, for the specified Authorized persons: / установить новый Абонентский номер для доступа в Систему ДБО, прохождения процедуры аутентификации и подписания 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: + (____)_____.

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

I hereby confirm that the Subscriber number specified in this application belongs exclusively and only to me, other persons have no access to it.

_____/_____/«__» _____ 20__ г /
(Signature/Подпись) (Full name/ФИО) (Date/Дата)

L.S. / М.П.

To be filled in by the Bank / Заполняется Банком

The Client's Authorized Persons have been identified, and their credentials and documents have been verified / Идентификация

¹ Please indicate e-mail address of the authorized person. Required field. / Укажите адрес электронной почты уполномоченного лица. Обязательное поле

² Please indicate the subscriber number of the authorized person. Required field. / Укажите абонентский номер уполномоченного лица. Обязательное поле.

Уполномоченных лиц Клиента проведена, полномочия и документы проверены

The application was registered with Bank / Заявление зарегистрировано в Банке «___» _____ 20___ г.:

_____/_____/_____ «___» _____ 20___ г

(position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)

Bank employee who checked ES / Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____ 20___ г

(position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)

Marked as executed / Отметка об исполнении:

Responsible Bank Employee / Ответственный работник Банка:

_____/_____/_____ «___» _____ 20___ г

(position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)

Приложение №3 к Регламенту дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru

Appendix No. 3 to the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System

УВЕДОМЛЕНИЕ

о компрометации ключа Электронной подписи (прекращении действия средства подтверждения и (или) об утрате средства подтверждения, и (или) об использовании Системы ДБО Faktura.ru 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 Faktura.ru RBS System without the consent of the Client)

г. Казань

Kazan

«__» _____ 20__ г.

_____ 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	
OGRN (Primary State Registration Number) / ОГРН	

в соответствии с Регламентом дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru (далее - Регламент), настоящим уведомляю АО «Банк 131» о Компрометации Электронной подписи в связи с

In accordance with the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System (hereinafter referred to as the Regulations) I hereby notify 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 с «__» _____ 20__ г.

заблокировать указанные ниже Средства подтверждения, использовавшиеся в рамках Регламента согласно заявлению о присоединении № _____ от «__» _____ 20__ г., и остановить обработку Электронных документов, подписанных/подтвержденных указанными средствами:

I request to block the Means of Confirmation noted below that were used within the frame of the Regulations on Remote Banking Service according to Statement of accession No. _____ dated _____ 20__ since _____ 20__ and stop the Electronic Documents processing that were signed/confirmed by the mentioned means:

☐ Сертификаты ключей Электронной подписи:

☐ Certificate of the electronic signature verification key:

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

☐ Cloud signature: / Облачная подпись:

№	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		

_____/_____/«__»____20__г /
(Signature/Подпись) (Full name/ФИО) (Date/Дата)

L.S. / М.П.

To be filled in by the Bank / Заполняется Банком

The Client's Authorized Persons have been identified, and their credentials and documents have been verified, the application was registered with Bank / Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены, Заявление зарегистрировано в Банке «__»____20__г.:

_____/_____/____«__»____20__г
(position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)

Bank employee who checked ES / Работник Банка, проверивший ЭП:

_____/_____/____«__»____20__г
(position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)

Marked as executed / Отметка об исполнении:

Responsible Bank Employee / Ответственный работник Банка:

_____/_____/____«__»____20__г
(position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)

Приложение №4 к Регламенту дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru

Инструкция по обеспечению информационной безопасности при работе в Системе ДБО Faktura.ru

В целях обеспечения информационной безопасности при работе в Системе ДБО Faktura.ru (далее – Система ДБО) АО «Банк 131», **Клиент обязан:**

1. При осуществлении доступа к Системе ДБО, удостовериться в правильности указанного адреса в адресной строке браузера (<https://bank.131.ru/>) и наличии значка защищенного соединения (замок), исключая выход на сайты, внешне маскирующиеся под Систему ДБО .
2. При использовании Мобильной подписи и/или иного вида Электронной подписи внимательно проверять информацию об Операции, полученную в СМС-сообщении или в PUSH-сообщении.
3. Своевременно устанавливать доступные обновления операционной системы и приложений.
4. Не подвергать используемое устройство операциям повышения привилегий / взлома операционной системы устройства (jail-break, rooting).
5. Использовать антивирус для устройств, своевременно устанавливать на него обновления вирусных баз.
6. Никогда не передавать свое устройство и/или sim-карту третьим лицам.
7. Ключи Усиленной неквалифицированной Электронной подписи и КЭП ФНС хранить только на ФКН в недоступном для посторонних и неуполномоченных лиц месте (запирающийся персональный сейф, металлический шкаф).
8. Не снимать копии с ФКН, не передавать ФКН лицам, к ним не допущенным, не записывать на ФКН постороннюю информацию.
9. Не использовать в качестве Пароля:
 - последовательность символов, состоящих из одних цифр (в том числе даты, номера телефонов, номера автомобилей и т.п.);
 - последовательность повторяющихся букв или цифр;
 - идущие подряд в раскладке клавиатуры или в алфавите символы;
 - имена и фамилии;
 - ИНН или другие реквизиты Клиента/Уполномоченного Представителя Клиента.

Appendix No. 4 to the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System

Information security guidelines for working in Faktura.ru RBS System

To ensure information security when working in Faktura.ru RBS System (hereinafter referred to as the "RBS System") of Bank 131 JSC, **the Client is obliged to:**

1. When accessing RBS System, ensure that the address in the browser's address bar is correct (<https://bank.131.ru/>) and that the secure connection icon (lock) is present, avoiding websites that mimic RBS System.
2. When using a Mobile Signature and/or any other type of Electronic Signature, carefully verify the transaction information received in an SMS or PUSH notification.
3. Promptly install available updates for the operating system and applications.
4. Avoid performing operations to gain elevated privileges / hacking the device's operating system (jailbreak, rooting).
5. Use antivirus software for devices and promptly update its virus databases.
6. Never transfer your device and/or SIM card to third parties.
7. Store Enhanced Unqualified Electronic Signature Keys and QES FTS Keys only on FKC in a place inaccessible to unauthorized persons (e.g., a personal safe or metal cabinet).
8. Do not make copies of the FKC, do not transfer the FKC to unauthorized persons, and do not record unrelated information on the FKC.
9. Do not use the following as a Static Password:
 - A sequence of digits only (including dates, phone numbers, car numbers, etc.);
 - A sequence of repeating letters or numbers;
 - Consecutive characters on the keyboard or in the alphabet;
 - Names and surnames;
 - Taxpayer Identification Number (INN) or other details of the Client/Authorized Representative of the Client.

При использовании Мобильной подписи (ОС Android 11.0+):

- Для выпуска и использования Мобильной подписи на устройстве должны быть активированы биометрические данные (TouchID/FaceID) или код разблокировки устройства.
- После успешной авторизации через биометрические данные/код разблокировки Клиент может подписывать электронные документы без повторного ввода биометрических данных в течение 1 (Одного) часа. По истечении указанного срока потребуется повторное подтверждение.
- Время на подтверждение каждой операции ограничено 5 (Пятью) минутами.
- Для обеспечения целостности и безопасности электронного сообщения при использовании Мобильной подписи применяется Имитовставка в соответствии с требованиями Положения Банка России от 30.01.2025 № 851-П.
- Мобильная подпись поддерживает групповое подписание платёжных поручений в Мобильном приложении.

При выявлении признаков Компрометации ЭП или вредоносного программного обеспечения немедленно уведомить Банк по телефону 8 (800) 100-13-10 (обращения принимаются в круглосуточном режиме) и направить Уведомление по форме Приложения №4. Не восстанавливать работоспособность поврежденного персонального компьютера до проведения экспертизы.

Требования к Паролю:

- Длина пароля должна быть не менее 8 символов.
- В числе символов пароля должны присутствовать строчные и прописные буквы, цифры и специальные символы (!, ", #, \$, %, &, ', (,), *, +, -, ., /, @, :, ;, <, =, >, ?, [, \,], ^, _ ` , {, }, ~);
- Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, а также выбирать пароли, которые уже использовались ранее;
- Личный пароль Клиент не имеет права сообщать никому;
- При смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 4 символа;
- Срок действия пароля пользователя не более 1 года (365 дней).
- Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).
- После 5-и неудачных попыток ввода пароля, учетная запись Клиента блокируется до выяснения причин ввода неправильного пароля.

When using Mobile Signature (Android OS 11.0+):

- To issue and use Mobile Signature, biometric data (TouchID/FaceID) or a device unlock code should be activated on the device.
- After successful authorization via biometric data/unlock code, the Client can sign electronic documents without re-entering biometric data for 1 (one) hour. After this period, re-confirmation will be required.
- The confirmation time for each transaction is limited to 5 (five) minutes.
- To ensure the integrity and security of the electronic message when using Mobile Signature, Message Authentication Code is used in accordance with the requirements of Bank of Russia Regulation No. 851-П dated 30/01/2025.
- Mobile Signature supports group signing of payment orders in the Mobile App.

If signs of ES Compromise or malware are detected, immediately notify the Bank by telephone at 8 (800) 100-13-10 (requests are accepted 24/7) and send Notification in the form of Appendix No. 4. Do not restore the functionality of the damaged personal computer until an examination has been carried out.

Requirements for Static Passwords:

- The password length should be at least 8 characters.
- The password should include lowercase and uppercase letters, numbers, and special characters (!, ", #, \$, %, &, ', (,), *, +, -, ., /, @, :, ;, <, =, >, ?, [, \,], ^, _ ` , {, }, ~);
- It is prohibited to use an "empty" password, the system login name, or previously used passwords;
- The Client should not disclose his/her personal password to anyone;
- When changing the password, the new combination of characters should differ from the previous one by at least 4 characters;
- The password validity period should not exceed 1 year (365 days);
- The password should not include easily guessable combinations of characters (names, surnames, workstation names, etc.) or common abbreviations (e.g., PC, LAN, USER, etc.);

- Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в доступных третьим лицам местах, передавать неуполномоченным лицам.

Необходимо:

- Установить на персональном компьютере (ноутбуке) парольную защиту на вход в Операционную систему.
- Хранить пароль доступа к ключу КЭП ФНС/УНЭП отдельно от ФКН.
- 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.
- 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.
- Не копировать содержимое ФКН, содержащего ключ ЭП, и не передавать его никому даже на короткое время.
- Закончив работу в Системе ДБО или прервав её (даже на несколько минут), извлечь ФКН, содержащий ключ КЭП ФНС/УНЭП, и убрать его в недоступное другим лицам место.
- Применять на рабочем месте лицензионные средства защиты от вредоносного кода с возможностью автоматического обновления баз данных сигнатур вредоносного кода.
- Если в качестве компьютера для работы в Системе ДБО используется переносной компьютер (ноутбук), исключить его подключение к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.)
- Осуществлять постоянный контроль отправляемых платежных (расчетных) документов при работе с Системой ДБО, а также за состоянием расчетных (банковских) счетов, операциям по ним и остаткам.
- 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 (800) 100 13 10 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 Электронной подписи, в том числе, относятся:

- утрата ФКН, с последующим обнаружением или без такового;
- нарушение правил хранения, использования и уничтожения (в том числе после окончания срока действия) ключа КЭП ФНС/УНЭП;
- утеря, передача и/или предоставлением доступа

- After 5 unsuccessful password attempts, the Client's account will be blocked until the reasons for the incorrect password entry are clarified;
- It is strictly prohibited to write passwords on paper or in text files at the workplace, leave them in places accessible to third parties, or disclose them to unauthorized persons.

Required:

- Set password protection for the operating system on the personal computer (laptop).
- Store the password for accessing QES FTS / EUES key separately from the FKC.
- Connect the FKC containing ES Key only when using RBS System and signing Electronic Documents. Do not leave the FKC containing ES Key permanently connected to the computer.
- Do not use the FKC containing ES Key for any other purposes, particularly do not store arbitrary information unrelated to working with RBS System on it.
- Do not copy the contents of the FKC containing ES Key or transfer it to anyone, even temporarily.
- After finishing work in RBS System or interrupting it (even for a few minutes), remove the FKC containing QES FTS / EUES key and store it in a place inaccessible to others.
- Use licensed anti-malware software with automatic updates for malware signature databases at the workplace.
- If a portable computer (laptop) is used for working in RBS System, avoid connecting it to public networks in places with free Internet access (office centers, cafes, etc.).
- Continuously monitor payment (settlement) documents sent when working with RBS System, as well as the status of settlement (bank) accounts, transactions, and balances.
- In case of detecting signs of compromise of the Electronic Signature or malware on the computer used for working in RBS System, immediately notify the Bank by phone: 8 (800) 100 13 10 from 9:00 AM to 6:00 PM (on business days), or personally visit the Bank to block the compromised ES Keys and replace them.

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 Разового 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 Разового пароля/Пароля, функционального ключевого носителя, аппаратного средства и/или SIM-карты с Абонентским номером;
- несанкционированный доступ к адресу электронной почты, указанному в Заявлении;
- прекращение полномочий или увольнение Уполномоченных лиц, имеющих доступ к Средству подтверждения;
- случаи, когда нельзя достоверно установить, что произошло с ФКН (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).

При обнаружении несанкционированных доступов в Систему ДБО, платежных и иных операций в Системе ДБО, Компрометации или подозрении на Компрометацию Электронной подписи немедленно уведомить Банк и направить «Уведомление о компрометации» в порядке, установленном Регламентом дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО, а также обратиться с соответствующим заявлением в правоохранительные органы.

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.

Требования:

- Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы по Системе ДБО, заблокировать 3389 (RDP Remote desktop).

Events related to the Compromise of the Electronic Signature include:

- Loss of the FKC, with or without subsequent discovery;
- Violation of the rules for storage, use, and destruction (including after expiration) of QES FTS / EUES key;
- Loss, transfer, and/or provision of access to unauthorized third parties to hardware (including mobile phones or other devices) and/or SIM cards with a Subscriber number, including those used for sending One-Time Passwords;
- Suspicions that the Electronic Document Confirmation Tools have become known to unauthorized third parties;
- Suspicions of information leakage or distortion;
- Unauthorized copying or suspicion of copying One-Time Password / Password, Functional Key Carriers, hardware, and/or SIM cards with a Subscriber number;
- Unauthorized access to the email address specified in the Application;
- Termination of authority or dismissal of Authorized Persons with access to the Confirmation Tools;
- Cases where it is impossible to reliably determine what happened to the FKC (including cases where the carrier has malfunctioned, and it cannot be conclusively disproven that this occurred as a result of unauthorized actions by third parties, or other types of disclosure of key information).

If unauthorized access to RBS System, payment, or other operations in RBS System, Compromise or suspicion of Compromise of the Electronic Signature is detected, immediately notify the Bank and send a "Notice of Compromise" in the manner established by the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC using RBS System, and submit a corresponding statement to law enforcement agencies.

It is prohibited to restore the functionality of a damaged computer before conducting a technical examination. Work with RBS System is permitted only after reinstalling the operating system with formatting of the hard drives and replacing all of the Client's ES keys.

Requirements:

- Disable remote and terminal connections to

- Включить в операционной системе журнал безопасности Windows.
- Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д. (далее по тексту – ПО).
- Обеспечить возможность своевременного обновления системного и прикладного ПО.
- Доступ в помещение, где размещен компьютер с Системой ДБО, предоставлять только Уполномоченным лицам.
- 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.
- Исключить доступ к компьютерам, используемым для работы в Системе ДБО, посторонних лиц и персонала, неуполномоченных на работу в Системе ДБО и/или обслуживание компьютеров.
- При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.
- Запрещено передавать логины и пароли третьим лицам в том числе иным Уполномоченным Представителям Клиента.

АО «Банк 131» не осуществляет рассылку электронных писем с просьбой прислать ключи Электронных подписей и/или пароль к Системе ДБО и никогда не запрашивает у Клиента эту информацию.

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 Клиент не должен сообщать данную информацию и должен немедленно сообщить об этом в Банк.

- computers used for working with RBS System, block port 3389 (RDP Remote Desktop).
- Enable the Windows security log in the operating system.
- Use only licensed software: operating systems, anti-malware tools, office suites, etc. (hereinafter referred to as "Software").
- Ensure the ability to promptly update system and application software.
- Grant access to the room where the computer with RBS System is located only to Authorized Persons.
- It is recommended to isolate the computer used for preparing and sending Electronic Documents to the Bank in a separate network segment, excluding it from the Client's general local network.
- Prohibit access to computers used for working in RBS System by unauthorized persons and personnel not authorized to work in RBS System or service the computers.
- When servicing the computer by IT staff, ensure control over their actions.
- It is prohibited to transfer logins and passwords to third parties, including other Authorized Representatives of the Client.

Bank 131 JSC does not send emails requesting the submission of Electronic Signature keys and/or passwords for RBS System and never requests this information from the Client.

The Bank does not make phone calls, send emails, SMS messages, or use other methods to request confidential information (passwords, code words, etc.). If such a request is received, under no circumstances should the Client disclose this information and should immediately report it to the Bank.

Приложение №5 к Регламенту дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО БИФИТ

Требования к программно-техническим средствам для проведения расчетных операций в электронной форме с использованием Системы ДБО Faktura.ru (далее – Система ДБО)

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

1.1. При использовании КЭП ФНС/УНЭП:

- Персональный компьютер с портом USB и предустановленной операционной системой (ОС) Windows 7 и выше, MacOS³

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

- доступ в сеть Интернет;

- принтер.

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

При эксплуатации Системы ДБО запрещается:

- Установка программного обеспечения сторонних фирм, а также сознательное внесение изменений в файлы программного и информационного обеспечения Системы ДБО ;

- Доступ к Системе ДБО неуполномоченных лиц;

При эксплуатации Системы ДБО Клиент обязан:

- Использовать систему ДБО только на исправном и проверенном на отсутствие компьютерных вирусов персональном

Appendix No. 5 to the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using BIFIT RBS System

Requirements for Software and Hardware for Conducting Settlement Operations in Electronic Form Using Faktura.ru RBS System (hereinafter referred to as the "RBS System")

1. Requirements for Software and Hardware (purchased by the Client at their own expense from third parties):

1.1. When using QES FTS / EUES:

- A personal computer with a USB port and a pre-installed operating system (OS) Windows 7 and above, MacOS⁵;

- An up-to-date version of an internet browser: Chrome 47 and above / Firefox 44.0 and above / Internet Explorer 10 and above / Opera 36 and above / Safari 9 and above;

- Internet access;

- Printer.

2. To use RBS System with EUES, a dedicated computer with a pre-installed Microsoft Windows operating system is required. If, at the Client's request, RBS System is installed on a computer with pre-installed third-party operating systems, the Bank is not responsible for the functionality of RBS System.

Prohibited Actions When Using RBS System:

- Installation of third-party software, as well as intentional modification of the software and information files of RBS System;
- Access to RBS System by unauthorized persons.

Obligations of the Client When Using RBS System:

- Use RBS System only on a functional and virus-free personal computer (laptop);
- Prevent the computer with the installed RBS System from being infected with computer viruses or other malicious programs;
- Use only legal and licensed software;

³ Инструкция по работе с MacOS размещена на официальном сайте Банка.

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.

- Ensure the technical functionality of the equipment included in RBS System workstation;
- Use antivirus protection tools and ensure regular updates of antivirus databases.

The need for backup of RBS System user workstation is determined by the Client and, if necessary, is carried out by the Client independently.

Приложение №6 к Регламенту дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО Faktura.ru

Appendix No. 6 to the Regulations on Remote Banking Services for Legal Entities, Individual Entrepreneurs, and Individuals engaged in private practice at Bank 131 JSC in the manner established by the legislation of the Russian Federation using Faktura.ru RBS System

Заявление № _____
на установление ограничений по параметрам операций с использованием Системы дистанционного банковского обслуживания Faktura.ru АО «Банк 131» (далее – Система ДБО)

Application No. _____
for the establishment of restrictions on the parameters of operations using Faktura.ru Remote Banking Service System of Bank 131 JSC (hereinafter referred to as RBS System)

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	
OGRN (Primary State Registration Number) / ОГРН	

В соответствии с условиями Соглашения об осуществлении информационного взаимодействия с использованием Систем информационного обмена – Системы ДБО Faktura.ru прошу установить ограничения по параметрам Операций по Счету(-ам) №:

In accordance with the terms of the Agreement on the Implementation of Information Interaction Using the Information Exchange Systems – Faktura.ru RBS System, I request that restrictions be established on the parameters of Transactions for Account(s) No.:

☐	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			
	Account No. Номер счета	Signature Type (EUES / QES FTS/ Mobile Signature)/ Тип подписи (УНЭП/КЭП ФНС/Мобильная подпись)	Period (1 operation/1 day/1 week/1 month) /Период (1 операция/1 день/1 неделя/1 месяц)	Maximum amount of money transfer in the Account currency / Максимальная сумма перевода денежных средств в валюте Счета
☐	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)		1. Recipient's Name / Наименование получателя _____ Account Number / Номер счета _____ BIC / БИК _____ INN (Taxpayer Identification Number) (if any) / ИНН (если есть) _____ 2. ...	
☐	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)	
☐	countries where the Client can make money transfers (the geographical location is determined by the IP address ⁴ 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 ⁴ 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 Faktura.ru ☐ 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

_____/_____/«__»____20__г /
 (Signature/Подпись) (Full name/ФИО) (Date/Дата)

L.S. / М.П.

To be filled in by the Bank / Заполняется Банком

The application was accepted at ____ hours ____ minutes on _____, 20__. / Заявление принял ____ часов ____ минут «__» _____20__г.

Bank employee who accepted the application: / Работник Банка, принявший заявление:

_____/_____/«__»____20__г
 (position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)
 (printed name/расшифровка подписи.)

Bank employee who checked ES / Работник Банка, проверивший ЭП:

_____/_____/«__»____20__г
 (position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)
 (printed name/расшифровка подписи.)

The restrictions were established on _____, 20__ (the date the restrictions were established is indicated). / Ограничения установлены «__» _____20__г. (проставляется дата установки ограничений).

Responsible Bank Employee / Ответственный работник Банка:

_____/_____/«__»____20__г
 (position/должность) (signature/подпись) (printed name/расшифровка подписи) (date/дата)

⁴ When using VPN services or anonymizers, the final IP address of the device from which access to the RBS is made will be determined. This may result in the unavailability of RBS System. / 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.