

**СОГЛАШЕНИЕ
ОБ ОБЩИХ ПРАВИЛАХ И УСЛОВИЯХ
ПРЕДОСТАВЛЕНИЯ БАНКОВСКИХ УСЛУГ
С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ БАНК-
КЛИЕНТ «ELBRUS Internet»**

**1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ,
ПРИМЕНЯЕМЫЕ В СОГЛАШЕНИИ**

Если не указано иное, термины и определения, используемые в настоящем Соглашении, имеют следующие значения:

Аппаратные средства и программное обеспечение – программно-технические средства, необходимые для пользования Услугами посредством Системы и обеспечивающие обработку и/или передачу данных.

Банк – АО «Райффайзенбанк», включая его филиалы.

Доверенность на действия в Системе – доверенность, автоматически выдаваемая Клиентом каждому из Подписантов, данные о которых предоставлены/или будут представлены в будущем Клиентом Банку, на подключение с использованием функционала Системы новых услуг/изменение их перечня/отключение услуг, заключение от имени Клиента соглашений с Банком посредством Системы (в том числе, акцепт оферты Банка), получение информации, представляющей собой банковскую тайну, совершение иных юридически значимых действий и получение (а также предоставление) любой информации от Банка (Банку), включенная в текст настоящего Соглашения и действующая со дня представления Клиентом Банку информации о Подписанте и по день, являющийся последним днем осуществления Подписантом действий в Системе.

Документы ВК – документы, направляемые Сторонами друг другу посредством Системы во исполнение обязанности Банка по выполнению функций агента валютного контроля в отношении операций Клиента, к которым относятся: паспорт сделки, заявление о переоформлении паспорта сделки, справка о валютных операциях, справка о подтверждающих документах, заявление о закрытии паспорта сделки, письма Клиента, адресованные отделу валютного контроля Банка, с вложениями и без, в том числе, письмо в Банк с вложением цифровых копий документов, ведомости банковского контроля, других документов, запросы и уведомления Банка, сформированные Банком ведомости банковского контроля, а также другие документы, обмен которыми предусмотрен нормативными актами в области валютного контроля. Список Документов ВК определяется Банком и может изменяться Банком. В целях проверки полномочий Подписантов и направления на обработку Документов ВК в то структурное подразделение Банка, которое проводит валютный

**AGREEMENT ON GENERAL RULES AND
CONDITIONS OF PROVIDING BANKING
SERVICES WITH THE USE OF THE «ELBRUS
Internet» BANK-CLIENT SYSTEM**

**1. TERMS AND DEFINITIONS USED IN THE
AGREEMENT**

Unless otherwise stated, terms and definitions used in this Agreement have the following meaning:

Hardware and Software - software and hardware facilities that are necessary for use of Services with the help of the System and provide for processing and/or transfer of data.

Bank – AO Raiffeisenbank including its branches.

Proxy Notice relating to Actions in the System - a proxy that is automatically issued by the Client to each Signatory, information on which is or will be presented in future by the Client to the Bank, for enabling new services/changing their list/disabling the services through the functionality of the System, conclusion of agreements on behalf of the Client with the Bank with the help of the System (including Bank offer acceptance), receipt of information which is the bank privacy, performance of other legally significant actions and obtaining (as well as providing) any information from the Bank (to the Bank), included into the text of this Agreements and valid from the day when the Client provides the Bank with information on the Signatory and until the day, which is the last day for performance of actions in the System by the Signatory.

CC Documents - documents sent by the Parties to each other with the help of the System in fulfilment of the Bank's duty on performing the functions of the currency control agent regarding the Client's operations, which include: transaction certificate, application for renewal of the transaction certificate, certificate on currency operations, certificate on supporting documents, application for closing the transaction certificate, letters of the Client, addressed to the department of the currency control of the Bank with and without attachments, including the letter to the Bank with the attachment of digital copies of documents, bank control records, other documents, requests and notices of the Bank, bank control records, formed by the Bank as well as other documents, the exchange of which is provided for by regulations in currency control. The list of the CC Documents is determined by the Bank and can be amended by it. In order to check the authorities of Signatories and to send the CC Documents for processing into the Bank's subdivision responsible for the currency control, when forming the CC Documents the Client chooses the Account to which the formed

контроль, Клиент выбирает при формировании Документов ВК Счет, к которому относится формируемый документ. Если Документ ВК формируется в отношении операций, не предполагающих расчетов, выбирается любой номер банковского счета из открытых Клиенту в соответствующем филиале/головном офисе Банка.

Заявление на заключение соглашения – Заявление на заключение Соглашения об общих правилах и условиях предоставления банковских услуг с использованием Системы Банк-Клиент «ELBRUS Internet» и подключение к Системе Банк-Клиент «ELBRUS Internet» в АО «Райффайзенбанк», размещенное на сайте Банка в сети Интернет по адресу <http://www.raiffeisen.ru>.

Закрытый ключ усиленной электронной подписи – уникальная последовательность символов, известная только владельцу Сертификата ключа подписи (Пользователю, кроме Оператора) и предназначенная для генерации усиленной электронной подписи в Электронном документе.

Имя пользователя – уникальная последовательность символов для регистрации Пользователя в Системе.

Карточка с образцами подписей и оттиска печати (далее – **КОП**) – карточка с образцами подписей и оттиска печати Клиента, представляемая в Банк и отражающая информацию об уполномоченных представителях Клиента (Подписантах), наделенных правом подписи, и оформляемая в соответствии с нормами Инструкции Банка России от 30.05.2014 №153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов.

Клиент – юридическое лицо или индивидуальный предприниматель.

Ключи – совокупность Открытого и Закрытого ключей усиленной электронной подписи, принадлежащих Подписанту, Подписанту ВК, Ревизору, Контролеру.

Контролер - Пользователь, наделенный Клиентом на основании доверенности (Приложение № 5 к Соглашению) правом просматривать информацию по Счетам Клиента, создавать Электронные документы с использованием Системы, выполнять с использованием Системы иные действия в отношении Электронных документов и подписывать Электронной подписью Электронные документы и Документы ВК, не заменяя при этом лиц, указанных в КОП, и/или в доверенности по форме Приложения № 5 к настоящему Соглашению.

Компрометация Регистрационных данных и/или Ключей – утрата доверия к Регистрационным данным и/или Закрытому ключу, обеспечивающим безопасность информации в Системе.

Мобильное приложение «ELBRUS Mobile» (далее – «ELBRUS Mobile» или Мобильное приложение)

document belongs. If the CC Document is formed regarding operations that do not presume calculations, then any number of the bank account is chosen from those opened to the Client in a corresponding affiliate/head office of the Bank.

Application for concluding the Agreement – the Application for concluding the Agreement on general rules and conditions of providing banking services with the use of the «ELBRUS Internet» Bank-Client System and connection to the «ELBRUS Internet» Bank-Client System in AO «Raiffeisenbank» published on the Bank's website on the Internet <http://www.raiffeisen.ru>.

Privacy Key of the Enhanced Digital Signature - a unique sequence of symbols known only to the owner of the Signature Key Certificate (for a User, except a Controller) and designed for the generation of the enhanced digital signature in any E-Document.

User Name - a unique sequence of symbols for the registration of a User in the System

Sample Signatures and Seal Card (hereinafter referred to as **SSC**) - a card with sample signatures and seal of the Client, presented to the Bank and reflecting information on authorized representatives of the Client (Signatories), authorized with signing powers and registered according to provisions of Instruction of the Bank of Russia of May 30, 2014 No. 153-И «On opening and closing bank accounts, deposit accounts (deposits) and term deposit accounts».

Client – legal entity or individual entrepreneur.

Keys - collection of the Public and Privacy key of the enhanced digital signature owned by a Signatory, a CC Signatory, an Auditor, a Controller.

Controller - a User on the basis of the proxy notice (Annex no. 5 to the Agreement) authorized by the Client to review information on the Client's Accounts, to create E-Documents with the use of the System, to perform other actions regarding E-Documents with the use of the System and to use the Digital Signature to sign E-Documents and CC Documents, at the same time not replacing persons indicated in the SSC and/or in the proxy notice in the form of Annex no. 5 to this Agreement.

Compromise of Registration Data and/or Keys - loss of confidence in Registration data and/or Privacy key providing for information safety in the System.

Mobile Application «ELBRUS Mobile» (hereinafter referred to as «ELBRUS Mobile» or Mobile

– приложение для Мобильных устройств Клиентов, являющееся одним из каналов дистанционного банковского обслуживания, предназначенное для передачи в Банк Электронных документов и/или других электронных данных.

Мобильное устройство – переносное техническое устройство Клиента в виде смартфона или электронного планшета на базе операционных систем iOS и Android.

Одноразовый код - уникальная последовательность символов, предназначенная для подтверждения операций в «ELBRUS Mobile» или «ELBRUS Internet», направленная Банком Подписанту в виде SMS-сообщения на номер мобильного телефона, зарегистрированный в Банке для целей получения Подписантом Одноразового кода («SMS-OTP»).

Оператор – Пользователь, наделенный Клиентом правом просматривать информацию по Счетам Клиента на основании доверенности (Приложение № 5 к Соглашению), создавать Электронные документы, выполнять с использованием Системы иные действия в отношении Электронных документов, за исключением права подписания Электронных документов ЭП.

Открытый ключ усиленной электронной подписи – уникальная последовательность символов, соответствующая Закрытому ключу усиленной электронной подписи, доступная Банку и Пользователю (кроме Оператора), и предназначенная для подтверждения подлинности усиленной электронной подписи в Электронном документе.

Пароль – уникальная последовательность символов, связанная в Системе с соответствующим Именем Пользователя.

ПИН-конверт - запечатанный конверт с Регистрационными данными.

Подписант - Пользователь, уполномоченный Клиентом давать Банку распоряжения о совершении операций по Счетам Клиента с использованием Системы и наделенный правом подписания Электронных документов ЭП. Права формирования ЭП Подписанта соответствуют полномочиям, которыми он наделен Клиентом, что подтверждается данными, отраженными в имеющейся в Банке и принятой Банком в работу КОП, и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению. Каждый Подписант, указанный в КОП, или Информационной карточке и имеющий доверенность, составленную Клиентом по форме Приложения № 5, автоматически получает от Клиента Доверенность на действия в Системе.

Подписант документов ВК (Подписант ВК) - Пользователь, уполномоченный Клиентом принимать от Банка, составлять и направлять в Банк Документы ВК с использованием Системы и

Application) - an application for Mobile Devices of Clients acting as one of the channels for remote banking servicing designed for transferring of E-Documents and/or other electronic data to the Bank.

Mobile Device - a Client portable technical device such as smartphone or electronic tablet on the basis of iOS and Android software

One-Time Code - a unique sequence of symbols designed to confirm actions in «ELBRUS Mobile» or «ELBRUS Internet» sent by the Bank to the Signatory in the form of an SMS to the mobile number, registered in the Bank in order for the Signatory to get the One-Time Code («SMS-OTP»).

Operator - a User authorized by the Client to review information on the Client's Accounts on the basis of the proxy notice (Annex no. 5 to the Agreement), to create E-Documents and to perform other actions regarding E-Documents with the use of the System except for signing E-Documents with his digital signature.

Public Key of the Enhanced Digital Signature - a unique sequence of symbols corresponding to the Privacy Key of the Enhanced Digital Signature available to the Bank and the User (except the Controller) and designed to confirm the authenticity of the enhanced digital signature in a E-Document.

Password - a unique sequence of symbols, associated in the System with a corresponding User Name.

PIN-envelope - a sealed envelope with Registration Data.

Signatory - a User authorized by the Client to provide the Bank with orders to perform actions on the Client's Accounts with the use of the System and provided with powers to sign E-Documents with Digital Signature. The rights to create the Signatory's Digital Signatures correspond to powers received from the Client, as evidenced by data, reflected in the SSC owned and accepted by the Bank and/or by the proxy notice in Annex no. 5 to this Agreement accepted by the Bank. Every Signatory indicated in the SSC or Information Card and having the proxy notice drawn up by the Client in the form of Annex no. 5 automatically receives from the Client the Proxy notice relating to actions in the System.

Signatory of CC Documents (CC Signatory) - a User authorized by the Client to receive from the Bank, to draw up and send to the Bank the CC Documents with the use of the System and provided with powers to sign

наделенный правом подписания Электронных документов, являющихся Документами ВК, ЭП (право доступа «Подпись для ВК») на основании доверенности (Приложение № 5 к настоящему Соглашению).

Пользователь – физическое лицо, надлежащим образом наделенное Клиентом правом доступа в Систему в роли Подписанта, Подписанта ВК, Оператора, Контролера или Ревизора.

Простая электронная подпись (далее – ПЭП) – значение Хэш-функции, вычисленное по всем реквизитам Электронного документа (номер лицевого счета, номер телефона, номер обязательства и т.д.), паролю, введенному Клиентом при входе в Систему, и Одноразовому коду, подтверждающему реквизиты получателя средств и/или реквизиты плательщика, а также факт формирования Простой электронной подписи определенным Пользователем.

Рабочий день – любой день, в который Банк проводит операции на территории Российской Федерации, кроме субботы, воскресенья и официальных выходных дней, а также дней, когда в соответствии с законодательством Российской Федерации кредитные организации не работают.

Ревизор - Пользователь, наделенный Клиентом на основании доверенности (Приложение № 5 к Соглашению) правом просматривать информацию по Счетам Клиента, создавать Электронные документы (Рублевое платежное поручение, Заявление на перевод средств в иностранной валюте, Заявка на покупку валютных средств, Заявка на продажу валютных средств, Заявка на конвертацию, Распоряжение о распределении средств с транзитного счета, Заявка на размещение депозита) с использованием Системы, создавать и подписывать Усиленную электронную подписью Шаблоны Электронных документов, выполнять с использованием Системы иные действия в отношении Электронных документов. Если Шаблон создан и подписан Ревизором, то у Пользователей не будет возможности создать ЭД не по Шаблону.

Регистрационные данные – уникальное сочетание Имени пользователя и Пароля, зарегистрированные в Системе на имя конкретного Пользователя, которые однозначно идентифицируют данного Пользователя в Системе (в том числе, позволяют однозначно определить, что конкретное действие в Системе совершено определенным Пользователем) и обеспечивают доступ этого Пользователя в Систему с четко установленными правами доступа.

Сертификат ключа подписи – документ в электронном виде, который включает в себя Открытый ключ и выдается Пользователю для подтверждения подлинности усиленной электронной подписи и идентификации владельца Сертификата ключа подписи.

E-Documents being the CC Documents with the Digital Signature (access right «Signature for CC») on the basis of the proxy notice (Annex no. 5 to this Agreement).

User - an individual duly authorized by the Client to access the System as a Signatory, a CC Signatory, an Operator, a Controller and an Auditor.

Simple Digital Signature (hereinafter referred to as the **SDS**) - a hash value calculated according to all details of an E-Document (personal account number, telephone number, commitment number etc.), password, entered by the Client when signing in to the System and One-Time Code which confirms the details of the funds recipient as well as the fact of forming a Simple digital signature by a specific User.

Working Day - any day when the Bank conducts operations on the territory of the Russian Federation except for Saturdays, Sundays and official holidays as well as days when credit institutions are out of work according to the legislation of the Russian Federation.

Auditor – a user authorized by the Client on the basis of the proxy notice (Annex no. 5 to this Agreement) to review information on the Client's Accounts, to create E-Documents (Ruble bank transfer, Foreign Currency Payment Order, Request for Foreign Currency Purchasing, Request for Foreign Currency Selling, Currency Exchange Request, Order for Allocation of Transit Account Funds, Deposit Application) with the use of the System, to create and sign templates of Documents by enhanced electronic signature, to perform other actions regarding E-Documents with the use of the System. If a template was created and signed by the Auditor, Users will not have an ability to create E-Documents not from a template.

Registration Data - a unique combination of a User Name and a Password, registered in the System in the name of a particular User, which uniquely identifies this User in the System (including the option to identify that a particular action in the System was performed by a particular User) and provides for this User's access to the System with clearly defined access rights.

Signature Key Certificate - an electronic document, which comprises a Public Key and is provided to the User in order to confirm the authenticity of the enhanced digital signature and identification of the owner of the Signature Key Certificate.

Система Банк-Клиент «Electronic Banking Raiffeisenbank Unified System Internet» (далее - **Система Банк-Клиент «ELBRUS Internet»** или **«Система»**) – система дистанционного банковского обслуживания, предназначенная для обработки и передачи Электронных документов и/или других электронных данных, используемая для предоставления и пользования Услугами через сеть Интернет.

Скан-копии документов – отсканированные цифровые копии (образы) документов, обосновывающих проведение валютных операций, в том числе копии подтверждающих документов в рамках действующих паспортов сделок, прикрепленные к подписанным ЭП Электронным документам, с вложенным файлом произвольного формата или Документам ВК, направляемым с использованием специальной формы, предусмотренной в Системе.

Средства доступа – Регистрационные данные и Устройство USB-token.

Средство криптографической защиты информации (далее – **СКЗИ**) - программное средство, реализующее криптографические алгоритмы преобразования данных и предназначенное для защиты информации от несанкционированного доступа при ее обработке, передаче по каналам связи и хранении.

Счет Клиента или Счет – банковский или иной счет(-а) Клиента в валюте РФ и/или в иностранной валюте, открытый(-ые) в Банке на имя Клиента на основании заключенных договоров, операции по которому(-ым) могут производиться с использованием Системы.

Тарифы - тарифы на открытие и ведение Счетов Клиента согласно договорам, в рамках которых открыты Счета Клиента.

Уровень доступа – уровень прав доступа Пользователя к Электронным документам, установленный Клиентом.

Усиленная электронная подпись (далее – **УЭП**) – электронная подпись, полученная в результате криптографического преобразования информации, позволяющая определить лицо, подписавшее Электронный документ, а также обеспечивающая возможность контроля целостности и подтверждения подлинности Электронных документов, исходящих от каждой из Сторон.

Услуги – услуги, оказываемые Банком по настоящему Соглашению.

Устройство USB-token - устройство для записи и защищенного хранения Открытого и Закрытого ключа УЭП.

Хэш-функция – однонаправленное отображение (сверка) содержимого файла или блока данных произвольного размера в блок данных фиксированного размера, обладающее заданными

Bank-Client System «Electronic Banking Raiffeisenbank Unified System Internet» (hereinafter referred to as the **«ELBRUS Internet» Bank-Client System or the «System»**) - a system of the remote banking servicing designed for processing and transferring of E-Documents and/or other electronic data, and used for providing with and using Services via Internet.

Scanned Copies of Documents - scanned digital copies (images) of documents that prove the execution of currency operations, including copies of supporting documents within the limits of valid transaction certificates, attached to E-Documents signed with the digital signature with the attached free-format file or CC Documents, sent with the use of a special form, provided for in the System.

Access Means - Registration Data and USB-token Device.

Cryptographic Information Protection Facility (hereinafter referred to as the **CIPF**) - a software tool, which realizes the cryptographic algorithms of converting data and designed for information protection from unauthorized access during the process of its processing, transmitting via communication links and storing.

Client's Account or Account - a Client bank or another account(s) in the RF currency and/or foreign currency opened with the Bank in the name of the Client on the basis of executed agreements, the operations on which can be performed with the use of the System.

Tariffs – tariffs for opening and maintaining Client's Accounts according to agreements within Accounts are opened.

Access level – an access level of User's rights to E-Documents defined by the Client.

Enhanced Digital Signature (hereinafter referred to as the **EDS**) - a digital signature resulting from the cryptographic conversion of information, which allows to identify a person who signed the E-Document and provides the ability to control the integrity and to confirm the authenticity of E-Documents issued by each Party.

Services - services provided by the Bank under this Agreement.

USB-token Device - a device for record and protected storage of the Public and Privacy EDS key.

Hash-function - a unidirectional mapping (verification) of content of a file or a data set of an arbitrary size to the data set of a fixed size with a predetermined

математическими свойствами; используется при формировании УЭП и ПЭП.

Шаблон – форма ЭД с уже заполненными или частично заполненными полями, которую можно использовать при создании ЭД.

Электронный документ (ЭД) – электронный образ документа (платежного или иного), информация в котором представлена в электронно-цифровой форме, подписанный ЭП конкретного Пользователя, либо Банком.

Электронная подпись (далее – ЭП) – термин в настоящем Соглашении применяется в соответствии с Федеральным законом от 06.04.2011 «Об электронной подписи». В целях настоящего Соглашения в качестве Электронной подписи используется Простая электронная подпись и/или Усиленная электронная подпись.

IMSI (International Mobile Subscriber Identity) – международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи GSM, UMTS или CDMA. Информация об IMSI фиксируется в Банке автоматически на основании информации, предоставляемой оператором мобильной связи, по номеру мобильного телефона, предоставляемого в Банк при подключении услуги «SMS-OTP».

«SMS для Бизнеса» – услуга Банка по предоставлению информации об операциях в Системе, результатах обработки ЭД и событий в Системе в виде коротких SMS или E-mail сообщений на зарегистрированный номер телефона сотовой связи или на зарегистрированный адрес электронной почты Подписанта.

«SMS-OTP» (SMS One-time password) – услуга, предоставляемая Банком посредством отправки SMS-сообщений на зарегистрированный номер телефона Пользователя, содержащих Одноразовый код, предназначенный для подтверждения операций в «ELBRUS Mobile» или «ELBRUS Internet», подключаемая в порядке, указанном в пунктах 3.14 и 3.15 настоящего Соглашения.

2. ПРЕДМЕТ СОГЛАШЕНИЯ

2.1. Настоящее Соглашение определяет порядок предоставления Банком Клиенту Услуг с использованием Системы, а также порядок оплаты Клиентом предоставленных Банком Услуг.

Перечень Услуг, предоставляемых Клиенту в Системе (далее – «Перечень Услуг»), установлен в Приложении № 1 к настоящему Соглашению и может быть в любое время изменен Банком в одностороннем порядке с предварительным уведомлением Клиента за 10 (Десять) календарных дней до даты вступления в силу соответствующих изменений любым из способов (по усмотрению

mathematical properties; is used for the process of forming the EDS and the SDS.

Template – a form of E-Document with completed or partially completed fields which can be used when E-Documents are created.

E-Document - an electronic image of a document (payment or any other), the information in which is represented in an electronic-digital form, signed with a Digital Signature of a specific User or by the Bank.

Digital Signature (hereinafter referred to as the **DS**) - the term in this Agreement is used according to Federal Law of 06.04.2011 «On digital signature». For the purpose of this Agreement, the term Simple Digital Signature and/or Enhanced Digital Signature is used for the Digital Signature.

IMSI (International Mobile Subscriber Identity) – an international mobile agent identifier (an individual customer number), associated with each user of mobile connection GMC, UMTS or CDMA. Information on IMSI is automatically fixed in the Bank on the basis of information, provided by the mobile connection operator, to the mobile number, presented to the Bank when enabling the «SMS-OTP» service.

«SMS for Business» - a Bank service on providing information on operations in the System, results of E-Document processing and events in the System in the form of short SMS or E-mail messages to the registered telephone number or registered e-mail address of the Signatory.

«SMS-OTP» (SMS One-time password) - a service provided by the Bank by sending SMS to the registered telephone number of the User, containing a One-Time code, designated for confirmation of operations in «ELBRUS Mobile» or «ELBRUS Internet», connected subject to paragraphs 3.14 and 3.15 of this Agreement.

2. SUBJECT OF THE AGREEMENT

2.1. This Agreement determines the order of providing Services by the Bank to the Client with the use of the System as well as the payment order for Services, provided by the Bank.

List of Services, provided to the Client in the System (hereinafter referred to as the «List of Services») is stipulated in Annex no. 1 to this Agreement and is subject to being unilaterally amended by the Bank in any time with 10 (ten) calendar days prior notice to the Client before the effective date of corresponding amendments by any of the following methods (at the discretion of the Bank): by a written notification (in Bank's form), by

Банка): письменным уведомлением (по форме Банка), путем публикации на сайте Системы в сети Интернет <http://elbrus.raiffeisen.ru>, опубликованием информации в Системе (раздел «Письма из Банка»), публикацией на сайте Банка в сети Интернет <http://www.raiffeisen.ru>.

2.2. Услуги по настоящему Соглашению оказываются Банком в соответствии с законодательством Российской Федерации, нормативными актами Банка России и настоящим Соглашением и подлежат оплате Клиентом в порядке, предусмотренном Соглашением.

3. ПОРЯДОК ЗАКЛЮЧЕНИЯ СОГЛАШЕНИЯ И ПРЕДОСТАВЛЕНИЯ УСЛУГ

3.1. Текст Соглашения публикуется на сайте Банка в сети Интернет по адресу: <http://www.raiffeisen.ru>. По запросу Клиента текст Соглашения может быть передан Клиенту на бумажном носителе, выслан в электронной форме по адресу электронной почты, указанному в запросе.

3.2. Заключение Соглашения между Банком и Клиентом осуществляется путем присоединения Клиента к изложенным в Соглашении условиям в целом (акцепта условий) в соответствии со статьей 428 Гражданского кодекса Российской Федерации, и производится путем подачи Клиентом (его уполномоченным представителем) в Банк Заявления на заключение соглашения (в двух экземплярах) с одновременным предоставлением в Банк всех сведений и документов, необходимых в соответствии с действующим законодательством Российской Федерации, установленными в соответствии с ним банковскими правилами, текстом Соглашения, для заключения Соглашения. Соглашение считается заключенным между Банком и Клиентом, и вступает в силу с момента учинения Банком на тексте Заявления на заключение соглашения экземпляра Клиента отметки о принятии Банком Заявления на заключение соглашения.

3.3. Банк вправе отказать лицу, обратившемуся для заключения Соглашения, в заключении Соглашения.

3.4. Доступ Клиента в Систему предоставляется через прикладное программное обеспечение для просмотра web-страниц – браузер, а в случае использования Клиентом «ELBRUS Mobile» через мобильное приложение.

3.5. Для организации доступа в Систему и оказания Услуг Банк предоставляет Клиенту Регистрационные данные для регистрации Пользователей в Системе.

3.6. Банк и Клиент договорились о том, заключая настоящее Соглашение, Клиент в течение всего срока действия настоящего Соглашения автоматически в настоящем и будущем (без выдачи дополнительной доверенности) представляет право

publishing on the System's website on the Internet <http://elbrus.raiffeisen.ru>, by publishing the information in the System (Bank's Letters Section) or by publishing on the Bank's website on the Internet <http://www.raiffeisen.ru>.

2.2. Services under this Agreement are provided by the Bank in accordance with the legislation of the Russian Federation, regulations of the Bank of Russia and this Agreement and are due for payment by the Client in the order, provided for by the Agreement.

3. ORDER OF CONCLUDING THE AGREEMENT AND PROVIDING THE SERVICES

3.1. The text of the Agreement is published on the Bank's website on the Internet <http://www.raiffeisen.ru>. Under the Client's request the text of the Agreement may be transferred in a hard copy to the Client, sent in an electronic form by e-mail specified in a request.

3.2. Conclusion of the Agreement between the Bank and the Client is provided by joining of the Client to terms set in the Agreement in general (acceptance of terms) under the article 428 of the Civil Code of the Russian Federation and submission of the Application for conclusion of the Agreement (in two copies) by the Client (authorized representative) with the simultaneous provision of all necessary information and documents to the Bank according to the applicable legislation of the Russian Federation, bank rules and text of the Agreement set in accordance with legislation.

The Agreement is considered as concluded between the Bank and the Client and enters into force from the moment of signing the Client's copy of the Application for conclusion of the Agreement by the Bank.

3.3. The Bank has the right to refuse person applied for conclusion of the Agreement.

3.4. The Client's access to the System is provided with the help of the application software for viewing the webpages - a browser, and with the help of the mobile application in case the Client uses «ELBRUS Mobile».

3.5. In order to organize the access to the System and to provide Services, the Bank provides the Client with registration data for registration of Users in the System.

3.6. Both the Bank and the Client agreed that by concluding this Agreement the Client during the whole term of this Agreement now and in future (without any additional proxy notice) automatically provides the right to sign E-Documents with the Digital Signature to any

подписания Электронных документов ЭП любому Подписанту, указанному в КОП или указанным в Информационной карточке при условии указания их в КОП, а также тому Подписанту, в отношении которого Клиент выдал доверенность по форме Приложения № 5 к настоящему Соглашению, которую Банк принял в работу.

Клиент может выбрать для каждого из своих Подписантов один из следующих вариантов подписания ЭД:

3.6.1. С использованием ПЭП после самостоятельного подключения в Системе конкретному Пользователю услуги «SMS-ОТП». В целях обеспечения безопасности, при использовании «SMS-ОТП», Банком установлены ограничения на лимиты¹ совершаемых операций для заверенных² и незаверенных³ контрагентов.

3.6.2. С использованием УЭП после предоставления Банком персонального Устройства USB-token вместе с Регистрационными данными. Средства доступа передаются Банком Пользователю(-ям) или уполномоченному представителю Пользователя(-ей) в течение 3 (Трех) Рабочих дней с даты вступления в силу настоящего Соглашения.

Для обеспечения защиты ЭП каждый Подписант с правом подписи, относящейся к I группе подписей или единственной подписи, обязан использовать для хранения Закрытого ключа усиленной электронной подписи персональное Устройство USB-token, предоставленное Банком вместе с Регистрационными данными. Средства доступа передаются Банком Пользователю(-ям) или уполномоченному представителю Пользователя(-ей) в течение 10 (Десяти) Рабочих дней с даты вступления в силу настоящего Соглашения.

Уполномоченному представителю Пользователя(-ей) при получении Средств доступа необходимо предоставить в Банк доверенность на получение Средств доступа по форме Приложения № 7 к настоящему Соглашению.

Пользователю (ям) при получении Средств доступа в дату отличную от даты подачи Заявления на заключение соглашения необходимо предоставить в Банк Заявление на выдачу Устройства USB-token/ Регистрационных данных (ПИН-конвертов) по форме Приложения № 6 к настоящему Соглашению. Предоставление Устройств USB-token новым

Signatory, indicated in the SSC or indicated in the Information Card subject to their indication in the SSC, as well as to that Signatory, in relation to which the Client issued the proxy notice in the form of Annex no. 5 to this Agreement, accepted by the Bank into operation.

The Client can choose one of the following options of signing the E-Document for each of its Signatories:

3.6.1. With the use of the SDS upon an independent connection of an «SMS-OTP» service to a particular User in the System. For safety when using the «SMS-OTP» the Bank sets restrictions to the limits¹ of performed operations for the certified² and uncertified³ counterparties.

3.6.2. With the use of the EDS upon being provided by the Bank with a personal USB-token Device together with Registration Data. The access means are provided by the Bank to the User(s) or authorized representative of the User(s) within 3 (Three) Working Days after this Agreement enters into force.

In order to ensure the DS protection, every Signatory with signatory rights relating to Group I of signatures or a single signature, is obliged to use his personal USB-token Device, provided by the Bank together with Registration Data, for storage of the Privacy Key of the Enhanced Digital Signature. The access means are provided by the Bank to the User(s) or authorized representative of the User(s) within 10 (Ten) Working Days after this Agreement enters into force.

Upon receipt of the Access Means, the Authorized representative of the User(s) is obliged to provide the Bank with the proxy notice relating to obtaining the Access Means in the form of Annex no. 7 to this Agreement.

In case of obtaining the Access Means on a date other than the date of filing the Application for concluding the agreement, the User(s) shall provide the Bank with an Application for obtaining the USB-token/Registration Data (PIN-envelopes) in the form of Annex no. 6 to this Agreement.

Providing new Signatories with USB-token Devices and

¹ Допустимый Лимит на совершение операций при использовании «SMS-ОТП» составляет в сумме не более 1 млн. руб. в сутки для незаверенных контрагентов, и 3 млн. руб. в сутки для заверенных контрагентов, либо равной рублевому эквиваленту иностранной валюты, по курсу, установленному ЦБ РФ на последний рабочий день квартала, предшествующего кварталу, в котором осуществляется операция. Например, для расчета лимита на операции 16.05.2017 используется курс, установленный ЦБ на 31.03.2017.

The permissible Limit transactions with the use of the «SMS-OTP» makes not more than 1 million rubles a day for uncertified counterparties and 3 million rubles a day for certified counterparties, or is equal to a ruble equivalent of a foreign currency according to the exchange rate stipulated by the Central Bank of the Russian Federation on the final business day of the quarter prior to the quarter in which transaction is done. For example, for calculation of the limit transaction on 16.05.2016 is used the exchange rate stipulated by the Central Bank of the Russian Federation on March 31, 2017.

² Контрагент, занесенный в справочник Системы и подписанный Ключом.
A counterparty, registered in the System guide and signed with the Key.

³ Контрагент, вносимый Клиентом вручную или выбираемый из справочника Системы, не подписанный Ключом.
A counterparty, registered by the Client manually or chosen from the System guide, not signed with the Key.

Подписантам, выдача новых Регистрационных данных производится на основании Заявления Клиента на выдачу Устройства USB-token/ Регистрационных данных (ПИН-конвертов) по форме Приложения № 6 к настоящему Соглашению.

Банк и Клиент договорились о том, что Клиент в течение всего срока действия настоящего Соглашения автоматически (без выдачи дополнительной доверенности) представляет право любому Подписанту, использующему УЭП, самостоятельно подключить в Системе «ELBRUS Internet» услуги «ELBRUS Mobile» и/или «SMS-OTP» и/или «SMS для Бизнеса» Клиенту.

3.7. Защита Электронных документов в Системе обеспечивается с помощью СКЗИ, предоставляемых Банком в составе Системы. Перечень СКЗИ, поддерживаемых Системой, указан в Порядке подключения и обслуживания в Системе Банк-Клиент «ELBRUS Internet», приведенном в Приложении № 2 (далее – «Порядок подключения») к настоящему Соглашению. Порядок подключения может быть изменен Банком в одностороннем порядке с предварительным уведомлением Клиента за 10 (Десять) календарных дней до даты вступления в силу новой редакции любым из доступных способов, указанным в пункте 2.1. настоящего Соглашения, по усмотрению Банка.

3.8. Проверка IMSI совершается в момент инициации процесса подписания ЭД в Мобильном приложении или в Системе. Если ЭД не проходит проверку в связи с тем, что IMSI не зарегистрирован в Мобильном приложении или в Системе, то ЭД в обработку Банком не принимается.

3.9. Аппаратные средства и программное обеспечение, имеющиеся у Клиента и/или приобретаемые им для целей реализации положений настоящего Соглашения, должны соответствовать требованиям Банка, приведенным в Разделах 2 и 3 Порядка подключения.

3.10. Возможность пользования Системой и «ELBRUS Mobile» предоставляется Пользователю после регистрации Пользователя в Системе в соответствии с Порядком подключения.

3.11. Перечень Подписантов, а также объем прав Подписантов применительно к их работе в Системе, устанавливаются в соответствии с предоставленной в Банк Клиентом и принятой Банком в работу КОП, и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению, а также Доверенностью на действия в Системе и настоящим Соглашением.

В случае если Клиенту необходимо ограничить права доступа к Системе (осуществление функций Подписантов) лицам, образцы подписей которых имеются в предоставленной в Банк Клиентом КОП, Клиент должен предоставить в Банк Информационную карточку клиента по форме

new Registration Data is performed on the basis of the Client's Application for obtaining the USB-token Device/Registration Data (PIN-envelopes) in the form of Annex 6 to this Agreement.

Both the Bank and the Client agreed that during the whole term of this Agreement the Client automatically (without any additional proxy notice) provides any Signatory using the EDS with the right to enable for the Client services «ELBRUS Mobile» and/or «SMS-OTP» and/or «SMS for Business» in the «ELBRUS Internet» System.

3.7. The protection of E-Documents in the System is ensured with the help of CIPF, provided by the Bank within the System. The list of CIPF supported by the System is provided in the Procedure of connection and servicing in the «ELBRUS Internet» Bank-Client System given in Annex no. 2 (hereinafter referred to as the «Connection Procedure») to this Agreement. The Connection Procedure is subject to unilateral amendment by the Bank with 10 (ten) calendar days prior notice to the Client before the effective date of a new revision by any of available means stipulated in para 2.1 of this Agreement at the discretion of the Bank.

3.8. IMSI check is performed at the moment of initiating the process of signing the E-Document in the Mobile Application or in the System. If the E-Document fails the check because the IMSI is not registered in the Mobile Application or in the System, the E-Document is not accepted for operation by the Bank.

3.9. Hardware and software owned and/or acquired by the Bank for purposes of implementing the provisions of this Agreement are to correspond to the requirements of the Bank presented in Sections 2 and 3 of the Connection Procedure.

3.10. The User is provided with the possibility to use the System and «ELBRUS Mobile» upon his registration in the System according to the Connection Procedure.

3.11. The list of Signatories as well as the scope of their rights regarding their work in the System are stipulated according to the SSC presented to the Bank by the Client and accepted by the Bank for operation and/or according to the proxy notice in the form of Annex no. 5 to this Agreement accepted by the Bank for operation as well as according to the Proxy notice relating to operations in the System and this Agreement.

In case where the Client needs to limit the access rights to the System (exercise of Signatories' rights) to persons, the signature samples of whom are in the SSC provided by the Client to the Bank, the Client is to provide the Bank with the Information Card of the Client in the form of Annex no. 4 to this Agreement which is duly signed

Приложения № 4 к настоящему Соглашению, которая должным образом заверяется подписями уполномоченных лиц Клиента и скрепляется оттиском его печати.

Права доступа Операторов, Подписантов ВК, Контролеров и Ревизоров устанавливаются в соответствии с предоставленной в Банк Клиентом и принятой Банком в работу доверенностью и настоящим Соглашением.

3.12. Клиент имеет возможность подключить или, соответственно, отключить Услугу «SMS для Бизнеса», «ELBRUS Mobile» и/или «SMS-ОТР» в разделе «Дополнительные услуги» в Системе. Услуга подключается/отключается Банком в течение 1 (Одного) Рабочего дня.

3.13. Клиент имеет возможность предоставить доступ в Систему уполномоченным лицам с правами доступа Оператора, Подписанта ВК, Контролера, Ревизора на основании Заявления на подключение/отключение Пользователей от Системы Банк-Клиент «ELBRUS Internet» в АО «Райффайзенбанк» по форме Приложения № 6 к настоящему Соглашению и доверенности по форме Приложения № 5 к Соглашению для подключения Операторов, Контролеров, Ревизоров и Подписантов ВК.

Одно и то же лицо не может одновременно иметь более одного Уровня доступа в Системе.

3.14. Для отключения Пользователей с правами доступа Оператора, Подписанта ВК, Контролера и Ревизора от доступа в Систему, Клиент направляет в Банк Заявление на подключение/отключение Пользователей от Системы Банк-Клиент «ELBRUS Internet» по форме Приложения № 6 к Соглашению. Банк в течение 2 (Двух) Рабочих дней после его получения отключает от доступа в Систему Пользователей, в нем указанных. Услуги, подключенные в Системе Банк-Клиент «ELBRUS Internet» такому Пользователю будут отключены Банком по умолчанию.

3.15. В процессе регистрации в Системе Подписантов, Подписантов ВК, Контролера и Ревизора для каждого из перечисленных Пользователей:

3.15.1. в случае дальнейшего подтверждения операций УЭП (или подтверждение шаблонов Электронных документов) с использованием персонального устройства USB-token, генерируются Ключи. Порядок регистрации и активации Ключей указан в Порядке подключения.

3.15.2. в случае дальнейшего подтверждения операций ПЭП, Клиент осуществляет подключение услуги «SMS-ОТР» самостоятельно, на принадлежащий ему номер мобильного телефона, в разделе «Дополнительные услуги» в Системе с использованием УЭП с учетом указанного сторонами в п. 3.6.2 настоящего Соглашения.

3.15.3. передача Регистрационных данных, Ключей,

by authorized persons of the Client and shall be under its seal.

Access rights of Operators, CC Signatories, Controllers and Auditors are determined according to the proxy notice provided by the Client to the Bank and accepted by the latter for operation and this Agreement.

3.12. The Client enables or disables the «SMS for Business» Service, «ELBRUS Mobile» and/or «SMS-OTP» by itself in the «Additional Services» Section in the System. The service is enabled/disabled by the Bank within 1 (One) Working Day.

3.13. The Client is able to provide the access to the System to authorized persons with the access rights of the Operator, CC Signatory, Controller, Auditor on the basis of the Application for connection/disconnection of Users from the «ELBRUS Internet» Bank-Client System in AO Raiffeisenbank in the form of Annex no. 6 to this Agreement and the proxy notice in the form of Annex no. 5 to this Agreement for connection of Operators, Controllers, Auditors and CC Signatories.

The same person cannot have more than one Access level to the System.

3.14. In order to disconnect Users with the access rights of the Operator, CC Signatory, Controller and Auditor from the access to the System, the Client shall provide the Bank with the Application for connection/disconnection of Users from the «ELBRUS Internet» Bank-Client System in the form of Annex no. 6 to this Agreement. Within 2 (Two) working days upon receipt of such Application the Bank disconnects Users indicated therein from the access to the System. Services connected to the «ELBRUS Internet» Bank-Client System for such User will be disconnected by the Bank by default.

3.15. During the process of registration of Signatories, CC Signatories, Controller and Auditor for each of the listed Users in the System:

3.15.1 in case of further confirmation of operations with the EDS with the use of a personal USB-token Device the Keys are generated. The procedure of registration and activation of Keys is provided in the Connection Procedure.

3.15.2 in case of further confirmation with the SDS (or confirmation E-Documents' templates), the Client links the «SMS-OTP» service by itself, to its mobile number, in the «Additional Services» Section in the System with the use of the EDS taking into account of what was indicated by the parties in para. 3.6.2 of this Agreement.

3.15.3. transfer of Registration Data, Keys, USB-token

Устройств USB-token, Одноразовых кодов между Пользователями, а также неуполномоченным лицам и любым третьим лицам, запрещена.

3.16. Клиент имеет возможность:

3.16.1. Самостоятельно подключить, изменить параметры или отключить Услугу «SMS для Бизнеса» в разделе «Дополнительные услуги» в Системе с использованием УЭП, направив заявление в электронном виде. Услуга подключается/отключается Банком в течение 1 (Одного) Рабочего дня.

3.16.2. Самостоятельно подключить, или отключить «ELBRUS Mobile» в разделе «Дополнительные услуги» в Системе с использованием УЭП, направив заявление в электронном виде. Услуга подключается/отключается Банком в течение 1 (Одного) Рабочего дня.

3.16.3. Самостоятельно подключить или отключить «SMS-OTP» для получения Одноразового кода в виде SMS-сообщения, в разделе «Дополнительные услуги» в Системе, подписав заявление в электронном виде в Системе с использованием УЭП. Услуга «SMS-OTP» подключается/отключается Банком в течение 1 (Одного) Рабочего дня. В целях предоставления услуги «SMS-OTP» в случае, когда Оператором сотовой связи Пользователя является ПАО МегаФон, Пользователь предоставляет в Банк «Согласие Пользователя на передачу его идентификаторов в АО «Райфаайзенбанк» при подключении услуги «SMS-OTP» по форме Приложения № 8 к Соглашению в течение 10 (Десяти) Рабочих дней после подключения Услуги в Системе.

3.17. Электронные документы, передаваемые через Систему, содержащие распоряжения Клиента о совершении операций по Счетам, Документы ВК составляются и оформляются в соответствии с законодательством Российской Федерации, нормативными актами Банка России и являются основанием для совершения Банком операций по Счетам, выполнения Банком функций агента валютного контроля. Электронные документы, передаваемые через Систему, исполняются Банком либо принимаются Клиентом без их последующего представления Клиентом либо Банком на бумажном носителе.

3.18. Сроки исполнения Электронных документов, содержащих распоряжения Клиента о совершении операций по Счетам и Документов ВК, переданных по Системе, регламентируются Сроками предоставления расчетных документов и документов валютного контроля для исполнения текущим банковским днем, размещенными на сайте Банка в сети Интернет по адресу <http://www.raiffeisen.ru>, Тарифами, Перечнем Услуг и нормами действующего законодательства Российской Федерации.

Devices, One-Time Codes between Users and to unauthorized persons and other third parties is prohibited.

3.16. The Client is able:

3.16.1 To enable, change parameters or disable the «SMS for Business» Service by itself in the «Additional Services» Section in the System with the use of the EDS by sending the application in the electronic form. The service is enabled/disabled by the Bank within 1 (One) Working Day.

3.16.2. To enable or disable «ELBRUS Mobile» by itself in the «Additional Services» Section in the System with the use of the EDS by sending the application in the electronic form. The service is enabled/disabled by the Bank within 1 (One) Working Day.

3.16.3. To enable or disable «SMS-OTP» by itself in order to get a One-Time Code in the form of the SMS, in the «Additional Services» Section in the System by signing the application in the electronic form in the System with the use of the EDS. The «SMS-OTP» service is enabled/disabled by the Bank within 1 (One) Working Day. In order to provide the «SMS-OTP» service in case where the User's cellular mobile operator is the PJSC MegaFon, the User shall provide the Bank with the «User's Agreement to transfer his identifiers to AO Raiffeisenbank when enabling the «SMS-OTP» Service» in the form of Annex 8 to this Agreement within 10 (Ten) Working Days upon enabling the Service in the System.

3.17. E-Documents transferred through the System and containing orders of the Client on performing operations on Accounts, CC Documents are prepared and issued according to the legislation of the Russian Federation, regulations of the Bank of Russia and are the basis for the Bank to perform operations on Accounts and perform functions of the currency control agent. E-Documents transferred through the System are either executed by the Bank or accepted by the Client without their further provision by the Client or by the Bank in a hard copy.

3.18. The terms for execution of E-Documents containing the Client's orders on performing operations on Accounts and CC Documents, transferred through the System are regulated in the Timing of payment and currency control documents for execution on the same banking day published on the Bank's website on the Internet at <http://www.raiffeisen.ru>, by Tariffs, List of Services and regulations of the applicable legislation of the Russian Federation.

3.19. Электронные документы, подписанные ЭП, признаются имеющими равную юридическую силу с документами, оформленными на бумажном носителе, подписанными собственноручными подписями уполномоченных лиц Клиента и заверенными оттиском печати Клиента, составленными в соответствии с законодательством Российской Федерации, а также нормативными актами Банка России.

Банк не несет ответственность за правильность составления и оформления Клиентом Электронных документов, а также за содержание и правильность заполнения Клиентом форм Электронных документов, предусмотренных Системой.

Стороны признают, что Скан-копии документов для целей валютного контроля, переданных Клиентом в Банк через Систему, равны по юридической силе копиям документов на бумажном носителе, заверенных уполномоченными лицами и печатью Клиента.

Реквизиты Клиента (в том числе, платежные реквизиты), необходимые к включению в текст Электронных документов, составляемых в Системе, загружаются в Систему автоматически из информационных систем Банка, содержащих указанные реквизиты, которые были сохранены на основе данных документов, представленных Клиентом в Банк для формирования юридического дела. В случае внесения изменений в реквизиты Клиента, Клиент несет ответственность за своевременное представление в Банк соответствующих документов, необходимых для отражения таких изменений.

3.20. Клиент соглашается с получением Услуг через сеть Интернет, осознавая, что сеть Интернет не является безопасным каналом связи, и соглашается нести все риски, связанные с подключением его вычислительных средств и Мобильных устройств к сети Интернет, возможным нарушением конфиденциальности и целостности информации при работе через сеть Интернет. Стороны также признают, что выход из строя Мобильных устройств Клиента в результате вмешательства третьих лиц через сеть Интернет рассматривается как выход из строя по вине Клиента.

Клиент самостоятельно и за свой счет обеспечивает подключение Мобильных устройств к сети Интернет, доступ к сети Интернет, а также обеспечивает их защиту от несанкционированного доступа и вредоносного программного обеспечения.

3.21. Электронные документы, успешно прошедшие контроль достоверности ЭП, хранятся в базе данных Системы в Банке в течение срока, устанавливаемого законодательством Российской Федерации и актами Банка России.

Стороны признают ЭП документа достоверным в случае, если он успешно прошел проверку на

3.19. E-Documents signed with the DS are considered to be of the same legal force with the documents executed in hard copy signed by a manual signature of the Client's authorized persons with the affixed Client's seal, executed in accordance with the legislation of the Russian Federation and regulations of the Bank of Russia.

The Bank bears no responsibility for the correct preparation and execution of E-Documents by the Client as well as for the content and correct Client's filling in of forms of E-Documents, provided for by the System.

The Parties acknowledge that for the purposes of the currency control the Scanned copies of documents, transferred by the Client to the Bank through the System are equal in their legal force to the documents executed in hard copy and signed by the Client's authorized persons with its seal affixed.

Client's details (including payment details), required to be added to the text of E-Documents, prepared in the System, are uploaded to the System automatically from the information systems of the Bank that contain such details, which were saved on the basis of these documents, provided by the Client to the Bank for the formation of its legal file. In case of any changes made into the Client's details, the latter bears responsibility for the timely provision of corresponding documents to the Bank necessary for the reflection of such changes.

3.20. The Client agrees to receive Services through Internet and acknowledges that Internet is not a safe information channel and undertakes all the risks associated with connection of its computing instruments and Mobile Devices to Internet, possible violation of confidentiality and integrity of information when working through the Internet. The Parties also acknowledge that the failure of the Client's Mobile Devices as a result of third parties intervention through the Internet is considered to be the failure due to the Client's fault.

The Client at its own expense connects its Mobile Devices to the Internet, provides for the access to the Internet and ensures their protection against unauthorized access and malicious software.

3.21. E-Documents that have successfully passed the DS authenticity control are stored in the System's database in the Bank during the term, stipulated by the legislation of the Russian Federation and regulations of the Bank of Russia.

The Parties acknowledge the authenticity of the document's DS in case it has successfully passed the

сервере Банка.

В случае сомнения Клиента или Банка в достоверности результатов такой проверки, ЭП проверяется согласительной комиссией в соответствии с Порядком разрешения разногласий при обмене (в связи с обменом) электронными документами, заверенными электронной подписью (Приложение № 3 к Соглашению). Бремя доказывания достоверности ЭП лежит на Стороне, подписавшей Электронный документ.

3.22. Руководство по использованию Системы размещено на сайте Системы в сети Интернет <http://elbrus.raiffeisen.ru> и может быть изменено Банком в одностороннем порядке, с предварительным уведомлением Клиента за 10 (Десять) календарных дней до даты вступления в силу соответствующих изменений путем публикации на сайте Системы <http://elbrus.raiffeisen.ru> и на сайте Банка в сети Интернет <http://www.raiffeisen.ru>.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Клиент обязан:

4.1.1. использовать функционал Системы исключительно в рамках реализации своих прав и обязанностей, проистекающих из положений настоящего Соглашения, передавать в Банк с использованием Системы только документы, передача которых предусмотрена настоящим Соглашением, и не допускать применение Системы как средства коммуникации с третьими лицами;

4.1.2. в случае внесения изменений в действующую КОП Клиента, имеющуюся в Банке:

а) одновременно с новой КОП и пакетом документов, ее сопровождающим, необходимо представить в Банк:

- Заявление на выдачу Устройства USB-token / Регистрационных данных (ПИН-конвертов) по форме Приложения № 6 к Соглашению;

- при необходимости ограничить права Подписантов в Системе, обновленную Информационную карточку клиента по форме Приложения № 4, заверенную подписями уполномоченных лиц Клиента и скрепленную оттиском печати Клиента.

Банк отключает действующих Подписантов, отсутствующих в новой КОП, после принятия новой КОП Банком. Если до принятия Банком новой КОП Клиенту необходимо отключить Подписантов согласно действующей на данный момент КОП, Клиент предоставляет в Банк Заявление на подключение/ отключение Пользователей от Системы Банк-Клиент «ELBRUS Internet» по форме Приложения № 6 к Соглашению.

б) осуществить в Системе действия в соответствии с Порядком подключения по подключению

check on the Bank's server.

In case of either Client's or Bank's doubt in the validity of such check results, the DS is checked by the conciliation commission in accordance with the Procedure for the settlement of discrepancies during the process of exchanging (in connection with the exchange) the e-documents, signed with the digital signature (Annex no. 3 to the Agreement) The burden of proving the DS validity lies on the Party that signed the E-Document.

3.22. The guide for using the System can be found on the System's website on the Internet at <http://elbrus.raiffeisen.ru> and is subject to unilateral amendment by the Bank with 10 (ten) calendar days prior notice to the Client before the effective date of corresponding amendments by publishing on the System's website <http://elbrus.raiffeisen.ru> and on the Bank's website on the Internet <http://www.raiffeisen.ru>.

4. RIGHTS AND RESPONSIBILITIES OF THE PARTIES

4.1. The Client is obliged:

4.1.1. to use the functionality of the System only within the limits of exercising its rights and obligations resulting from provisions of this Agreement, to use the System to provide the Bank only with those documents, the provision of which is provided for by this Agreement and to avoid using the System as a communication method with third parties;

4.1.2. in case of introducing amendments to the existing SSC of the Client, stored in the Bank:

a) it is required to provide the Bank with the following documents along with a new SSC and supporting documents package:

- Application for obtaining the USB-token Device / Registration data (PIN-envelopes) in the form of Annex no. 6 to the Agreement;

- if necessary, to restrict the rights of the Signatories in the System, renewed Information Card of the Client in the form of Annex no. 4 signed by the Client's authorized persons with its seal affixed.

The Bank disconnects the existing Signatories that are absent in this new SSC as soon as the Bank accepts the new SSC. If the Client has to disconnect the Signatories according to the currently existing SSC prior to acceptance of a new one by the Bank, the Client provides the Bank with an Application for connecting/disconnecting the Users from the «ELBRUS Internet» Bank-Client System in the form of Annex no. 6 to the Agreement

b) to perform actions in the System in accordance with the Procedure for connection of Signatories according to

Подписантов в соответствии с новой КОП;

4.1.3. в случае если перечень Подписантов, а также объем прав Подписантов применительно к их работе в Системе, устанавливаются в соответствии с предоставленной в Банк доверенностью по форме Приложения № 5 к настоящему Соглашению:

4.1.3.1. одновременно с доверенностью по форме Приложения № 5 к настоящему Соглашению, необходимо представить в Банк:

а) Заявление на выдачу Устройства USB-token / Регистрационных данных (ПИН-конвертов) по форме Приложения № 6 к Соглашению;

б) осуществить в Системе действия в соответствии с Порядком подключения по подключению Подписантов на основании доверенности по форме Приложения № 5 к настоящему Соглашению;

4.1.3.2. в случае отзыва доверенности по форме Приложения № 5 к настоящему Соглашению на Подписантов, имеющейся в Банке:

а) ограничить права Подписантов в Системе путем предоставления в Банк Заявления на подключение/отключение Пользователей от Системы Банк-Клиент «ELBRUS Internet» по форме Приложения № 6 к Соглашению;

б) осуществить в Системе действия (в соответствии с порядком, предусмотренным в Порядке подключения) по изменению списка Подписантов и их полномочий;

4.1.4. в случае изменения списка уполномоченных лиц Пользователей с правами доступа Оператор, Подписант ВК, Контролер или Ревизор:

а) предоставить в Банк Заявление на подключение/отключение Пользователей от Системы Банк-Клиент «ELBRUS Internet» в АО «Райффайзенбанк» по форме Банка (Приложение № 6 к Соглашению);

б) осуществить в Системе действия в соответствии с Порядком подключения по подключению Пользователей;

4.1.5. в случае отзыва доверенности на подписание Документов ВК Клиента, имеющейся в Банке:

а) ограничить права Подписантов ВК в Системе путем предоставления в Банк Заявления на подключение/отключение Пользователей от Системы Банк-Клиент «ELBRUS Internet» по форме Приложения № 6 к Соглашению;

б) осуществить в Системе действия в соответствии с Порядком подключения по изменению списка Подписантов документов ВК и их полномочий;

4.1.6. контролировать срок действия полномочий Операторов, Подписантов ВК, Контролеров и всех Пользователей;

4.1.7. обеспечивать конфиденциальность Регистрационных данных и Ключей;

4.1.8. выполнять требования Порядка подключения и Руководства по использованию Системы по установке СКЗИ и организовать внутренний режим

the new SSC;

4.1.3. if the list of Signatories as well as the scope of their rights regarding their work in the System are stipulated according to the proxy notice, provided to the bank in the form of Annex no. 5 to this Agreement:

4.1.3.1. the following documents are to be provided to the Bank along with the proxy notice in the form of Annex no. 5 to this Agreement:

a) Application for obtaining the USB-token Device / Registration data (PIN-envelopes) in the form of Annex no. 6 to the Agreement;

b) to perform actions in the System in accordance with the Procedure for connection of Signatories according to the proxy notice in the form of Annex no. 5 to this Agreement.

4.1.3.2. in case of a revocation of the proxy notice in the form of Annex 5 to this Agreement for Signatories, stored in the Bank:

a) to restrict the rights of Signatories in the System by providing the Bank with the Application for connection/disconnection of Signatories from the «ELBRUS Internet» Bank-Client System in the form of Annex no. 6 to the Agreement;

b) to perform actions in the System (according to the procedure, provided for in the Connection procedure) on amending the list of Signatories and their powers;

4.1.4. in case of introducing amendments to the list of authorized persons of the Users with the access rights of the Operator, CC Signatory, Controller or Auditor:

a) to provide the Bank with the Application for connection/disconnection of Users from the «ELBRUS Internet» Bank-Client System to AO Raiffeisenbank in the Bank's form (Annex no. 6 to the Agreement);

b) to perform actions in the System in accordance with the Procedure for connection of Users;

4.1.5. in case of revocation of the proxy notice in relation to signing the CC Documents of the Client, stored in the Bank:

a) to restrict the rights of CC Signatories in the System by providing the Bank with the Application for connection/disconnection of Signatories from the «ELBRUS Internet» Bank-Client System in the form of Annex no. 6 to the Agreement;

b) to perform actions in the System on introducing amendments to the list of Signatories of CC Documents and their powers according to the Connection Procedure

4.1.6. to perform control over the term of Operators, CC Signatories, Controllers and all Users;

4.1.7. to ensure the confidentiality of Registration data and Keys;

4.1.8. to meet the requirements of the Connection procedure and Guide for using the System on installing the CIPF and to provide for the internal mode of

функционирования рабочих мест при работе с Системой таким образом, чтобы исключить возможность использования неуполномоченными лицами СКЗИ, Регистрационных данных Пользователей, а также Ключей;

4.1.9. в случае обнаружения в Системе несанкционированных Клиентом операций и/или возникновения у него подозрений в Компрометации Регистрационных данных и/или Ключей Пользователей:

а) немедленно сообщить о данном факте и всех известных ему обстоятельствах в Банк любым доступным способом (по телефону, сообщением в Системе или письменно) и неукоснительно следовать указаниям, полученным от Банка;

б) предоставить в Банк Заявление на выдачу Устройства USB-token/ Регистрационных данных (ПИН-конвертов) по форме Приложения № 6 к настоящему Соглашению для получения новых Средств доступа;

4.1.10. обеспечить хранение Закрытых ключей усиленной электронной подписи Подписантами, на Устройствах USB-token, предоставленных Банком;

4.1.11. обеспечить конфиденциальность Одноразовых кодов;

4.1.12. своевременно оплачивать Услуги, оказываемые Банком по настоящему Соглашению, согласно Тарифам;

4.1.13. использовать предоставленное Банком Программное обеспечение только для целей, определенных Соглашением, самостоятельно не изменять и не модифицировать программное обеспечение Системы.

4.1.14. для обеспечения безопасности не использовать одно и то же Мобильное устройство для работы в Системе «ELBRUS Internet»/ «ELBRUS Mobile» и приема/передачи SMS-сообщений с Одноразовым кодом.

4.1.15. обеспечить сохранность Мобильных устройств с установленным Мобильным приложением, а также Мобильных устройств, номера которых зарегистрированы в Банке для целей получения Пользователем Одноразового кода («SMS-OTP»). В случае утери Мобильного устройства с установленным Мобильным приложением, равно как и Мобильного устройства, номер которого зарегистрирован в Банке для целей получения Пользователем Одноразового кода («SMS-OTP»), незамедлительно отключить «SMS-OTP» в Системе или проинформировать Банк.

4.1.16. информировать Подписантов Клиента о недопущении ситуаций переполнения памяти Мобильных устройств, что может стать препятствием для приема SMS-сообщений с Одноразовым кодом.

4.1.17. информировать Банк, в случае замены/утери зарегистрированной SIM-карты Подписанта, путем

workplaces operation when working with the System so that to exclude the possibility for unauthorized persons to use the CIPF, Registration data of Users and the Keys;

4.1.9. in case where the Client finds any unauthorized operations in the System and/or if it suspects Compromising the Registration data and/or Keys of Users:

a) it shall immediately notify the Bank of this fact and all circumstances known to it by any means available (by phone, via message in the System or in writing) and keep strictly to instructions, received from the Bank;

b) to provide the Bank with the Application for obtaining the USB-token Device, Registration data (PIN-envelopes) in the form of Annex no. 6 to this Agreement to get new Access Means;

4.1.10. to ensure the storage of the Privacy keys of the enhanced digital signature by the Signatories on the USB-token devices provided by the Bank;

4.1.11. to ensure the confidentiality of One-Time Codes;

4.1.12. to timely pay for the Services provided by the Bank under this Agreement according to Tariffs;

4.1.13. to use the Software provided by the Bank only for purposes provided for in this Agreement and not to amend or modify the Software of the System by itself.

4.1.14. for safety purposes not to use the same Mobile Device for work in the «ELBRUS Internet»/«ELBRUS Mobile» System and for receipt/sending of SMS with the One-Time Code.

4.1.15. to ensure the safety of Mobile Devices with the installed Mobile Application as well as Mobile Devices which numbers are registered in the Bank for the purpose of obtaining the One-Time Code («SMS-OTP») by the User. In case of loss of the Mobile Device with the installed Mobile Application as well as of the Mobile Device which number is registered in the Bank for the purpose of obtaining the One-Time Code («SMS-OTP») by the User, the User shall immediately disable the «SMS-OTP» function in the System and to inform the Bank thereabout.

4.1.16. to inform the Client's Signatories on non-admission of a situation with the memory overflow on Mobile Devices which can block the receipt of SMS with the One-Time Code.

4.1.17. to notify the Bank in case of change/loss of the registered SIM-card of the Signatory by sending an E-

направления ЭД «Письмо в Банк» подписанного УЭП, с информацией о необходимости обновления IMSI для номера телефона <указывается номер телефона>, принадлежащего уполномоченному лицу <указывается ФИО уполномоченного лица> для продолжения использования «SMS-ОТР».

4.1.18. Клиент настоящим даёт Банку поручение и согласие на передачу любой информации, которая получена Банком в ходе отношений с Клиентом и будет направлена Банком Клиенту в его интересах, на любой адрес электронной почты, предоставленный Клиентом (или Подписантом) в Банк в качестве контактного адреса электронной почты, и на любой номер мобильного телефона, предоставленный Клиентом (или Подписантом) в качестве контактного номера мобильного телефона. При этом, Клиент подтверждает, что ознакомлен с тем, что электронная почта и мобильная связь не являются каналами связи, обеспечивающими максимальную степень защиты передаваемой по ним информации, и отказывается от любых претензий (в том числе, материальных) к Банку в связи с тем, что в результате использования электронной почты или мобильной связи информация, передаваемая с их помощью, может потенциально стать доступной третьим лицам, что может повлечь за собой негативные обстоятельства для Клиента.

Для обновления или дополнения контактных адресов электронной почты и контактных номеров мобильных телефонов уполномоченных лиц Клиента, Клиент направляет в Банк заявление по системе «Банк–Клиент» в виде документа свободного формата подписанного УЭП или на бумажном носителе.

4.2. Клиент имеет право:

4.2.1. получать от Банка консультации по вопросам использования Системы в рамках реализации им прав и обязанностей, проистекающих из положений настоящего Соглашения;

4.2.2. в любое время инициировать внеплановую замену Ключей, предоставив в Банк заявление по форме Приложения № 6 настоящего Соглашения;

4.2.3. отключать Услугу «SMS для Бизнеса» без расторжения настоящего Соглашения в порядке, установленном в пунктах 3.12.1. настоящего Соглашения;

4.2.4. создавать и отправлять в Банк Электронные документы в соответствии с Перечнем услуг, получать информацию об исполнении Электронных документов, переданных в Банк; отзывать Электронные документы до момента их полного исполнения Банком;

4.2.5. расторгнуть настоящее Соглашение в порядке, предусмотренном разделом 8 Соглашения при условии погашения задолженности по оплате Услуг Банка по настоящему Соглашению (в случае наличия такой задолженности).

Document «Letter to the Bank» signed with the EDS with information on the necessity to renew the IMSI for the telephone number <telephone number is indicated here> which belongs to the authorized person <the name of the authorized person is indicated here> to continue using the «SMS-ОТР» function.

4.1.18. The Client hereby instructs the Bank and gives its consent to transmit any information, which is obtained through the Bank's relationships with the Client and will be sent by the Bank to the Client in its interests to any email address provided by the Client (or by the Signatory) to the Bank as a contact email, and to any mobile number provided by the Client (or by the Signatory) as a contact mobile number. Whereby, the Client shall confirm that it knows that email and mobile services are not communication channels that provide the maximum degree of protection of the information transmitted via them and disclaim any and all claims (including material) to the Bank due to the fact that using email or mobile communication, the information transmitted via them could potentially be made available to third parties which may result in adverse circumstances for the Client.

For updates or additions to the contact e-mails and contact mobile numbers of the Authorized persons of the Client, the Client shall provide the Bank with the application via the Bank-Client System in the form of the free-format document signed with the EDS or executed in hard copy.

4.2. The Client has a right:

4.2.1. to receive consultations from the Bank on using the System within the limits of exercising its rights and obligations, resulting from the provisions of this Agreement;

4.2.2. at any time to initiate the non-scheduled replacement of Keys by providing the Bank with the application in form of Annex no. 6 to this Agreement;

4.2.3. to disable the «SMS for Business» Service not terminating this Agreement in the order, stipulated in paras 3.12.1. of this Agreement;

4.2.4. to create and send to the Bank E-Documents according to the List of Services, to receive information on the execution of E-Documents, sent to the Bank; to revoke E-Documents prior to their full execution by the Bank;

4.2.5. to terminate this Agreement in the order provided for in Section 8 of the Agreement subject to redemption of any debt on payment for the Bank Services under this Agreement (if any).

4.2.6. представлять Подписантам права на осуществление в Системе действия от имени Клиента согласно Доверенности на действия в Системе.

4.3. Банк обязан:

4.3.1. выдать Клиенту Средства доступа для Пользователей в течение 10 (Десяти) Рабочих дней с даты вступления в силу настоящего Соглашения, при одновременном выполнении Клиентом со своей стороны всех необходимых действий, указанных по тексту настоящего Соглашения и его приложений;

4.3.2. консультировать Клиента по вопросам использования Клиентом Системы в рамках реализации им прав и обязанностей, проистекающих из положений настоящего Соглашения;

4.3.3. выполнять распоряжения Клиента о совершении операций по Счетам и обеспечить Клиенту доступ к информации по Счетам при условии, что такой доступ осуществляется посредством использования действительных Регистрационных данных и Ключей и/или Одноразовых кодов;

4.3.4. приостановить обслуживание Клиента в Системе в случае получения от Клиента сведений о несанкционированных Клиентом операциях, Компрометации Регистрационных данных и/или Ключей. Приостановление обслуживания осуществляется на основании сообщения Клиента в соответствии с п. 4.1.9. настоящего Соглашения, для подтверждения которого Клиент должен направить в Банк письменное заявление, заверенное подписью уполномоченного лица Клиента и оттиском печати Клиента, в течение 1 (Одного) Рабочего дня с момента оповещения Банка;

4.3.5. принять все меры для уведомления Клиента о блокировке доступа Пользователей в Систему в течение 1 (Одного) часа с момента блокировки любыми доступными способами: сообщением в Системе (если это технически возможно) (раздел «Письма из Банка») или по контактными телефонам и/или адресам электронной почты Клиента, данные о которых имеются в юридическом деле Клиента в Банке;

4.3.6. не менее чем за 5 (Пять) календарных дней извещать Клиента о дате проведения плановых работ по поддержанию работоспособности Системы, которые могут прервать доступ Клиента к пользованию Системой в период приема Банком передаваемых по Системе Электронных документов, путем публикации на сайте Системы в сети Интернет <http://elbrus.raiffeisen.ru> и/или опубликованием информации в Системе (раздел «Письма из Банка»);

4.3.7. при выходе из строя программного обеспечения Банка, обеспечивающего функционирование Системы, а также в иных случаях невозможности предоставления Клиенту Услуг по

4.2.6. to provide the Signatories with the rights to perform actions in the System on behalf of the Client according to the Proxy notice in relation to actions in the System.

4.3. The Bank is obliged:

4.3.1. to provide the Client with the Access Means for Users within 10 (Ten) Working Days from the date when this Agreement enters into force subject to the simultaneous performance by the Client of all necessary actions, indicated in the text of this Agreement and annexes hereto;

4.3.2. to consult the Client on using the System by the Client within the limits of exercising its rights and obligations, resulting from the provisions of this Agreement;

4.3.3. to execute orders of the Client on performing operations on Accounts and to provide the Client with the access to information on Accounts provided that such access is performed by using the valid Registration Data and Keys and/or One-Time Codes;

4.3.4. to suspend the servicing of the Client in the System in case of getting information from the Client on unauthorized operations, Compromising of Registration data and/or the Keys. The suspension of services provision is performed on the basis of the Client's notification according to para. 4.1.9. of this Agreement for the conformation of which the Client shall provide the Bank with a written application under signature of the Client's authorized person and its seal affixed during 1 (One) Working day from the moment of notifying the Bank;

4.3.5. to take all due measures to notify the Client on blocking the access of Users to the System within 1 (One) hour from the moment of blocking by any means available: by the message in the System (if technically possible) («Bank Letters» Section) or on contact telephone numbers and/or e-mail addresses of the Client the information on which is in the legal file of the Client in the Bank;

4.3.6. to notify the Client on the date of performing scheduled works on maintaining the System at least 5 (Five) calendar days prior to such works that can abort the Client's access to the System during the process of transferring the E-Documents to the Bank via the System by publishing on the System's website on the Internet <http://elbrus.raiffeisen.ru> and/or publishing information in the System («Bank Letters» Section);

4.3.7. in case of failure of the Bank's software ensuring the functioning of the System as well as in other cases of impossibility to provide the Client with Services under this Agreement, to immediately notify the Client

настоящему Соглашению, немедленно извещать Клиента любым доступным способом - сообщением в Системе (если это технически возможно) (раздел «Письма из Банка») или по контактными телефонам и/или адресам электронной почты Клиента, данные о которых имеются в юридическом деле Клиента в Банке.

4.3.8. оказывать Клиенту услуги согласно распоряжениям его Подписантов в Системе, действующих согласно Доверенности на действия в Системе и на основании прочих пунктов настоящего Соглашения.

4.4. Банк имеет право:

4.4.1. блокировать доступ Пользователей к функционалу Системы без предварительного уведомления Клиента, если, по мнению Банка, такая мера необходима для обеспечения безопасности Системы и/или обеспечения и защиты интересов Клиента, либо в случае получения Банком информации, вынуждающей Банк поступить подобным образом;

4.4.2. отказать Клиенту в приеме и обработке ЭД, содержащего распоряжение Клиента о совершении операций по Счетам, подписанное ЭП, или оставить его без исполнения, в случаях:

а) обнаружения ошибок, допущенных Клиентом при его оформлении,

б) если, по мнению Банка, есть признаки несанкционированного доступа и/или Компрометации Регистрационных данных и/или Ключей Пользователей,

в) непредставления Клиентом необходимых документов, подтверждающих основание совершения операции по Счету, если это предусмотрено действующим законодательством Российской Федерации;

г) несоответствия IMSI информации, предоставленной оператором мобильной связи по номеру мобильного телефона Пользователя, предоставленного Пользователем/Клиентом при подключении услуги «SMS-ОТР»;

д) превышения лимитов, указанных в п. 3.6.1. настоящего Соглашения, при совершении операций с использованием «SMS-ОТР».

4.4.3. не принимать документ для целей валютного контроля в виде произвольного документа в виде текстового сообщения или произвольного документа с вложенным файлом (в том числе, содержащего Скан-копии документов), если данный документ должен быть в Системе оформлен с использованием электронной формы и/или особые требования к его оформлению предъявляются законодательством Российской Федерации;

4.4.4. отказать в приеме присланных в электронном виде по Системе Скан-копий документов, обосновывающих проведение валютных операций, если качество отсканированных копий (образов) не

thereabout with all means available - by the message in the System (if technically possible) («Bank Letters» Section) or on contact telephone numbers and/or e-mail addresses of the Client the information on which is in the legal file of the Client in the Bank;

4.3.8. to provide the Client with services according to orders of its Signatories in the System acting according to the Proxy Notice in relation to actions in the System and on the basis of other paragraphs of this Agreement.

4.4. The Bank has a right:

4.4.1. to block the access of Users to the System without prior notification of the Client if the Bank considers such a measure to be necessary to ensure the safety of the System and/or ensuring and protecting the Client's interests or in case the Bank received information forcing the Bank to do the same;

4.4.2. to refuse to accept and process the E-Document from the Client containing the Client's order on performing operations on Accounts, signed with the DS, or to leave it unexecuted in the following cases:

a) if there are mistakes made by the Client when preparing the E-Document,

b) if in the opinion of the Bank there are signs of unauthorized access and/or Compromise of the Registration Data and/or the Keys of Users,

c) if the Client failed to provide necessary documents that prove the reason of performing actions on the Account if it is provided for by the applicable legislation of the Russian Federation;

d) if there is any discrepancy in the IMSI information, provided by the mobile phone service provider to the mobile number of the User, provided by the User/Client when enabling the «SMS-ОТР» service;

e) in case of exceeding the limits, provided for in para 3.6.1 of this Agreement when performing operations with the use of the «SMS-ОТР» service.

4.4.3. for purposes of the currency control not to accept a document in the form of a free document, in the form of a text message or a free document with the attached file (including those with the attached Scanned Copies of Documents) if this document is subject to registration in the System with the use of an electronic form and/or if special requirements to its execution are provided for in the legislation of the Russian Federation;

4.4.4. to refuse the acceptance of Scanned Copies of Documents sent electronically via the System that prove the performance of currency operations if the quality of the scanned copies (images) is not good enough for the

позволяет Банку прочитать и/или однозначно понять содержащуюся в документе информацию;

4.4.5. если нормативные акты в области валютного контроля предусматривают обязанность Клиента одновременно предоставить в Банк комплект документов (в том числе, документы для целей валютного контроля в виде электронных форм, электронные документы в виде произвольного сообщения (содержащие информацию, необходимую Банку для осуществления валютного контроля, в частности, для подписания документов валютного контроля), Скан-копии документов, обосновывающих проведение валютных операций, прикрепленные к подписанному ЭП электронному сообщению (письму) или документу для целей валютного контроля), принимать такие документы только при условии, что все входящие в комплект документы представлены по Системе в течение 1 (Одного) Рабочего дня;

4.4.6. отказать в приеме документов для целей валютного контроля по Системе в виде Скан-копий документов, если нормативные акты в области валютного законодательства Российской Федерации и/или нормативные акты Банка России предусматривают обязанность Клиента предоставить документы в Банк в оригинале;

4.4.7. отказать в приеме документов Клиента для целей валютного контроля в виде электронных форм, произвольных сообщений, в том числе, с прикрепленными Скан-копиями документов, в случае неверного указания Клиентом номера Счета(-ов), к операциям по которому(-ым) относятся передаваемые документы;

4.4.8. отказать Клиенту в отзыве ранее переданного в Банк Электронного документа, если на момент поступления требования Клиента об отзыве Электронного документа, Банком были совершены действия по исполнению указанного Электронного документа, делающие его отзыв невозможным в соответствии с положениями действующего законодательства Российской Федерации и/или положениями нормативных актов Банка России;

4.4.9. отказать Клиенту в приеме от него распоряжений на проведение операций по Счету, подписанных ЭП Клиента, после предварительного предупреждения Клиента об этом любым доступным Банку способом взаимодействия с Клиентом, в случаях выявления признаков подозрительных операций в целях законодательства РФ в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма/непредставления Клиентом информации (документированных сведений), необходимой для исполнения Банком требований законодательства РФ в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. В этом

Bank to read and/or definitely understand information, contained in the document;

4.4.5. if regulations in the field of the currency control provide for the obligation of the Client to simultaneously provide the Bank with the documents package (incl. documents for the currency control purposes in the form of electronic forms, electronic documents in the form of a free notification (containing information required by the Bank for the purposes of current control, in particular for signing of currency control documents), Scanned Copies of Documents, proving the performance of currency operations attached to the electronic message (letter) or document, signed with the DS, for purposes of the currency control) to accept such documents only provided that all documents in the package are presented via the System within 1 (One) Working Day;

4.4.6. to refuse to accept documents for the purposes of the currency control via the System in the form of the Scanned Copies of Documents if regulations in the area of the currency legislation of the Russian Federation and/or regulations of the Bank of Russia provide for the Client's obligation to provide the Bank with the original documents;

4.4.7. to refuse to accept documents for the purposes of the currency control by way of electronic forms, free notifications incl. those with the attached Scanned Copies of Documents if the Client has indicated a wrong number of the Account(s) to the operations on which the transmitter documents relate;

4.4.8. to refuse to revoke a E-Document previously transmitted by the Client to the Bank if as of the moment of receiving the Client's requirement to revoke the E-Document, the Bank has already performed actions for the execution of such E-Document, which makes its revocation impossible in accordance with provisions of the applicable legislation of the Russian Federation and/or provisions of regulations of the Bank of Russia;

4.4.9. to refuse to accept the Client's orders for performing operations on the Account, signed with the Client's DS upon prior notification of the Client thereon by any means of interaction with the Client, available to the Bank, in cases of revealing any signs of suspicious operations for the purposes of the legislation of the Russian Federation in the field of counteraction to legitimization (laundering) of proceeds of crime and financing the terrorism/non-provision by the Client of information (documented information) required by the Bank to satisfy the requirements of the legislation of the Russian Federation in the field of counteraction to legitimization (laundering) of proceeds of crime and financing the terrorism. In this case the Client is obliged at the request of the Bank to provide duly executed

случае Клиент обязуется по требованию Банка предоставлять надлежащим образом оформленные расчетные документы на бумажном носителе;

4.4.10. модифицировать программное обеспечение Банка, обеспечивающее функционирование Системы, уведомив об этом Клиента за 10 (Десять) календарных дней до введения таких изменений в действие путем публикации на сайте Системы в сети Интернет <http://elbrus.raiffeisen.ru> и/или опубликованием информации в Системе (раздел «Письма из Банка»);

4.4.11. списывать со Счета(-ов) Клиента суммы денежных средств в счет оплаты Услуг Банка, причитающихся Банку по настоящему Соглашению. Настоящим Клиент предоставляет Банку согласие (акцепт) на списание со Счетов Клиента в валюте РФ или иностранной валюте, открытых в Банке, сумм денежных средств в счет оплаты услуг Банка, причитающихся Банку по настоящему Соглашению. Стороны признают указанное в настоящем пункте Соглашения дополнением ко всем договорам, заключенным между Клиентом и Банком, на основании которых Клиенту в Банке открыты Счета;

4.4.12. приостановить оказание Услуг Клиенту в Системе в одностороннем порядке в случае:

- образования задолженности Клиента по оплате Услуг, оказываемых по настоящему Соглашению, в течение 3 (Трех) календарных месяцев подряд, за исключением Услуги «SMS для Бизнеса», приостановление которой осуществляется в случае образования задолженности Клиента за 1 (Один) календарный месяц. Возобновление оказания Услуг Клиенту осуществляется только после погашения Клиентом задолженности и на основании поступившего в Банк письменного заявления Клиента, заверенного подписью уполномоченного лица Клиента и оттиском печати Клиента (при ее наличии у Клиента);

- в случае указания Клиентом/Пользователем неверного номера телефона при подключении к Услуге «SMS для Бизнеса» или «SMS-ОТП»;

- при наличии у Банка оснований полагать, что номер телефона, ранее зарегистрированный в Банке для предоставления Услуги «SMS для Бизнеса» или «SMS-ОТП», более не принадлежит Клиенту (конкретному Пользователю).

Банк не несет ответственности за убытки, понесенные Клиентом в связи с указанием Клиентом/Пользователем неверного номера телефона при подключении к Услугам «SMS для Бизнеса», «SMS-ОТП», либо в связи с неисполнением или ненадлежащим исполнением Клиентом иной обязанности, предусмотренной настоящим Соглашением.

4.4.13. расторгнуть настоящее Соглашение в случае не погашения Клиентом задолженности по оплате

accountancy documents in hard copy;

4.4.10. to modify the Bank's software, which ensures the functioning of the System upon prior notification of the Client 10 (Ten) calendar days prior to commissioning of such modifications by publishing on the System's website on the Internet <http://elbrus.raiffeisen.ru> and/or publishing information in the System («Bank Letters» Section);

4.4.11. to write-off the amounts from the Client's Account(s) for payment for the Bank Services that become due and payable to the Bank under this Agreement. The Client hereby provides the Bank with its consent (accept) to write-off the amounts from the Client's Accounts opened with the Bank in the currency of the Russian Federation or foreign currency for payment for the Bank Services that become due and payable to the Bank under this Agreement. The Parties acknowledge the agreement, indicated in this paragraph to be the annex to all agreements, concluded between the Client and the Bank on the basis of which Accounts are opened with the Bank for the Client;

4.4.12. to unilaterally suspend the provision of Services to the Client in the System in case:

- if there is any outstanding amount on payment for Services, provided under this Agreement, within 3 (Three) consecutive calendar months except for the «SMS for Business» Service the suspension of which is performed in case of any outstanding amount for 1 (One) calendar month. The renewal in providing the Services to the Client is provided only after the debt redemption by the Client and on the basis of the written application of the Client, received by the Bank, under signature of the authorized Client's person and its seal affixed (if any);

- if the Client/User has indicated a wrong telephone number when enabling the «SMS for Business» Service or «SMS-OTP»;

- if the Bank has reasons to think that the telephone number, which was previously registered in the Bank for the provision of the «SMS for Business» Service or «SMS-OTP» no longer belongs to the Client (particular User).

The Bank bears no responsibility for damages borne by the Client in connection with the indication by the Client/User of a wrong telephone number when enabling the «SMS for Business» Service, «SMS-OTP» or in connection with the non-performance or improper performance by the Client of any other obligation, provided for by this Agreement.

4.4.13. to terminate this Agreement if the Client fails to pay for its debt for provision of Services under this

Услуг, оказываемых по настоящему Соглашению, в течение 6 (Шести) календарных месяцев, с момента возникновения задолженности по оплате Услуг, оказываемых по настоящему Соглашению. При этом такое одностороннее расторжение Соглашения Банком не может рассматриваться Клиентом как возможность не производить погашения суммы задолженности перед Банком за оказанные в рамках настоящего Соглашения Услуги.

4.4.14. не осуществлять техническую поддержку «ELBRUS Mobile», версия которого ниже предыдущего Мобильного приложения, выпущенного Банком.

4.4.15. в целях обеспечения защиты интересов Клиентов, а также для выполнения требований законодательства РФ проводить идентификацию устройства Клиента, с использованием которого осуществляется доступ в Систему и (или) ELBRUS-Mobile. Информация, полученная в процессе проведения указанной идентификации (далее - Информация), может быть использована Банком для выявления фальсифицированных электронных сообщений для защиты денежных средств Клиента от преступных действий третьих лиц. Информация может быть передана Банком специализированной организации для ее исследования и представления Банку рекомендаций относительно адекватных мер защиты интересов Клиентов, при этом, Банк гарантирует, что Информация может быть передана указанной организации только в обезличенном виде, исключая идентификацию Клиента данной организацией. Кроме того, Информация представляет собой исключительно технические сведения об устройстве Клиента, с использованием функционала которого осуществляется доступ в Систему, и не является финансовой информацией, или информацией, представляющей собой банковскую или иную охраняемую законом тайну.

5. СТОИМОСТЬ УСЛУГ И ПОРЯДОК ОПЛАТЫ

5.1. Стоимость Услуг по настоящему Соглашению и порядок оплаты определяются Тарифами.

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Стороны несут ответственность за невыполнение и/или ненадлежащее выполнение своих обязательств по настоящему Соглашению, в том числе, в соответствии с действующим законодательством Российской Федерации.

6.2. Банк не несет ответственность за убытки, понесенные Клиентом в результате:
а) того, что Клиентом Банку была предоставлена неполная, неточная и/или недостоверная информация;
б) неспособности Клиента использовать функционал

Agreement during 6 (Six) calendar months from the moment of incurring of the payment debt for providing the Services under this Agreement. At the same time, such unilateral termination of the Agreement by the Bank cannot be considered by the Client as the possibility not to redeem the Bank debt for Services, provided under this Agreement.

4.4.14. not to provide any technical support to «ELBRUS Mobile» the version of which is lower than the previous Mobile Application, issued by the Bank.

4.4.15. for safety of Clients' interests as well as under the legislation of the Russian Federation to conduct identification of Client's device via which access to the System and (or) ELBRUS-Mobile is provided. Information received from such identification (hereinafter – Information) may be used for searching fraudulent electronic messages by the Bank for safety Client's funds from criminal activities of third parties. Information may be passed to a specialized organisation by the Bank for its research and representation of recommendations to the Bank about adequate measures to protect Client's interests, at the same time the Bank guarantees that Information may be passed impersonal to mentioned organisation excluding Client's identification by this organisation. Moreover, Information represents only technical data on the Client's device via which the access to the System is provided and is not financial information or information which is the bank privacy or another legally protected privacy.

5. COST OF SERVICES AND PAYMENT ORDER

5.1. The cost of Services under this Agreement and the order of their payment are determined by the Tariffs.

6. RESPONSIBILITY OF THE PARTIES

6.1. The Parties bear responsibility for the non-performance and/or improper performance of their responsibilities under this Agreement including in correspondence to the applicable legislation of the Russian Federation.

6.2. The Bank bears no responsibility for damages incurred by the Client as the result of:
а) providing the Bank with incomplete, inaccurate and/or misleading information by the Client;
б) the Client's inability to use the functionality of the

Системы из-за сбоев/поломок Аппаратных средств и/или сбоев в работе программного обеспечения Клиента, в том числе, поставленных Клиенту третьими лицами, и/или когда информация, полученная Клиентом и/или Банком, оказалась неточной, неполной и/или несвоевременно предоставленной в результате таких поломок или сбоев;

в) отключения линий связи или энергоснабжения, а также сбоев или задержек в доступе к Услугам, предоставляемым Банком посредством Системы, вызванных обстоятельствами непреодолимой силы;

г) действий третьих лиц в Системе в отношении Счета/Счетов Клиента, а также денежных средств, размещенных на Счете/Счетах, с использованием Регистрационных данных Пользователей и Ключей Подписантов и/или Одноразовых кодов;

д) несанкционированных действий Пользователей и/или внутренних конфликтов на стороне Клиента (в частности, в случае возникновения споров о нецелевом использовании денежных средств при осуществлении операций по Счетам между Подписантами, наделенными равными правами доступа в Систему; при поступлении в Банк надлежащим образом оформленного уполномоченным представителем государственного органа сообщения (письма, решения, постановления, выписки), подтверждающего наличие у Клиента неразрешенного внутрикорпоративного спора и т.д.);

е) нарушения Клиентом правил пользования Системой, указанных в Порядке подключения;

ж) неспособности Клиента использовать Систему из-за несовместимости программного обеспечения Банка и программного обеспечения Клиента.

6.3. Банк не несет ответственности за последствия, возникшие в результате того, что Клиент не ознакомился с сообщениями, опубликованными Банком на сайте Системы в сети Интернет <http://elbrus.raiffeisen.ru>, в Системе (раздел «Письма из Банка»), на сайте Банка в сети Интернет <http://www.raiffeisen.ru>.

7. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

7.1. При возникновении споров, связанных с принятием/непринятием к исполнению Банком Электронного документа Клиента, Стороны руководствуются Порядком разрешения разногласий при обмене (в связи с обменом) электронными документами, заверенных электронной подписью (Приложение № 3 к Соглашению).

7.2. Иные споры Сторон, связанные с заключением, исполнением, изменением, прекращением настоящего Соглашения, разрешаются по обоюдному согласию в ходе переговоров, то есть, во внесудебном порядке.

7.3. Споры, по которым не достигнуто соглашение

System due to faults/failures of Hardware and/or failures in the Client's software including those, delivered to the Client by third parties and/or if the information, received by the Client and/or by the Bank appeared to be inaccurate, incomplete and/or provided late due to such failures or disruptions;

c) shutdown of connection or power supply lines as well as failures or delays in access to the Services provided by the Bank through the System, caused by force majeure circumstances;

d) actions of third persons in the System in relation to the Account/Accounts of the Client as well as funds, allocated on the Account/Accounts with the use of Registration Data of Users and Signatories' Keys and/or One-Time Codes;

e) unauthorized actions of Users and/or internal conflicts on the Client's side (in particular, in the event of a dispute about the misuse of funds when performing operations on Accounts between the Signatories, vested with the equal access rights to the System; when the Bank receives the duly executed notification of the authorized state authority representative (letter, decision, resolution, extract), which proves that the Client has an unsettled intra-corporate dispute etc.)

f) violation by the Client of the rules for using the System, indicated in the Connection Procedure;

g) inability of the Client to use the System due to incompatibility of the Bank's software with the Client's software.

6.3. The Bank bears no responsibility for consequences that appeared due to the fact that the Client failed to familiarize itself with notifications, published by the Bank on the System's Website on the Internet <http://elbrus.raiffeisen.ru>, in the System («Bank Letters» Section), on the Bank's Website in the Internet <http://www.raiffeisen.ru>.

7. DISPUTE SETTLEMENT PROCEDURE

7.1. In case of any disputes connected with acceptance/non-acceptance by the Bank of any E-Document of the Client, the Parties are guided by the Dispute Settlement Procedure for the exchange (in connection with the exchange) of e-documents, signed with the digital signature (Annex no. 3 to the Agreement).

7.2. Other disputes of the Parties connected with the conclusion, execution, amendment and termination of this Agreement are to be settled by mutual consent in the course of negotiations, i.e. extrajudicially.

7.3. All disputes on which the agreement of the Parties is

Сторон, разрешаются в Арбитражном суде г. Москвы в случае подведомственности спора арбитражным судам.

8. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

8.1. Настоящее Соглашение вступает в силу с даты его заключения и действует до конца текущего календарного года.

8.2. Любая из Сторон имеет право расторгнуть настоящее Соглашение по своему усмотрению, предварительно уведомив другую Сторону о своем намерении расторгнуть Соглашение в письменной форме.

8.3. В случае если ни одна из Сторон за 30 (Тридцать) календарных дней до истечения срока действия настоящего Соглашения не уведомила письменно другую Сторону об окончании срока его действия, настоящее Соглашение считается продленным на тех же условиях на каждый следующий календарный год.

8.4. Банк также имеет право расторгнуть настоящее Соглашение в случае невыполнения Клиентом требований к порядку пользования Системой, нарушения порядка оплаты Услуг, оказываемых Клиенту Банком по настоящему Соглашению, или в любой другой момент, если сочтет такую меру необходимой в целях обеспечения безопасности Системы, уведомив об этом Клиента любым доступным способом в порядке, указанном в п. 2.1. настоящего Соглашения.

8.5. В случае закрытия Клиентом всех Счетов, открытых в Банке, настоящее Соглашение прекращает свое действие с даты прекращения договора банковского счета, на основании которого был открыт последний из Счетов, подлежащий закрытию.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Во всем остальном, что не предусмотрено условиями настоящего Соглашения, Стороны руководствуются законодательством Российской Федерации.

Недействительность отдельных положений настоящего Соглашения не влечет за собой недействительность иных положений Соглашения и/или недействительность Соглашения в целом.

9.2. Клиент обязуется не раскрывать третьим лицам информацию, полученную от Банка и имеющую отношение к Системе и/или Банку, за исключением случаев передачи информации в обособленные подразделения/филиалы/дочерние общества Клиента.

9.3. С вступлением в силу настоящего Соглашения все предыдущие соглашения и договоры, заключенные между Сторонами, определяющие

not reached are to be settled in the Moscow City Arbitrazh Court if such a dispute is subordinate to arbitrary courts.

8. TERM OF THE AGREEMENT

8.1. This Agreement enters into force as of the date of its conclusion and is valid until the end of the current calendar year.

8.2. Either Party has a right to terminate this Agreement at its discretion upon prior written notification of the other Party on its intent to terminate the Agreement.

8.3. If 30 (Thirty) calendar days prior to the expiry of this Agreement neither Party notified the other Party in writing on its expiry, this Agreement is considered prolonged on the same terms for each subsequent calendar year.

8.4. The Bank also has a right to terminate this Agreement in case of non-fulfilment by the Client of requirements for using the System, violation of the order of payment for Services, provided to the Client by the Bank under this Agreement or at any other moment if it finds such a measure fit for the purposes of ensuring the safety of the System, notifying the Client thereabout by any available method, indicated in para. 2.1. of this Agreement.

8.5. If the Client closes all Accounts opened with the Bank, this Agreement is terminated from the date of termination of the bank account agreement, on the basis of which the last of the Accounts subject to closing was opened.

9. FINAL PROVISIONS

9.1. For all other matters, not provided for the terms of this Agreement, the Parties are guided by the legislation of the Russian Federation.

Non-validity of separate provisions of this Agreement does not invalidate other provisions of the Agreement or the Agreement in general.

9.2. The Client undertakes not to disclose to third parties information, received from the Bank or referred to the System and/or the Bank, except for cases of transmitting the information to standalone subdivisions/affiliates/subsidiaries of the Client.

9.3. From the effective date of this Agreement all precedent agreements and contract, concluded between the Parties and determining the order of providing

порядок предоставления Банком Услуг Клиенту с использованием Системы, утрачивают силу. Обязательства, возникшие в результате вышеупомянутых соглашений и договоров, остаются в силе до их полного выполнения каждой из Сторон.

9.4. Все приложения к Соглашению являются его неотъемлемыми частями.

Services by the Bank to the Client with the use of the System, become void. Responsibilities, incurred as the result of the above-mentioned agreements and contracts, remain in force until their full performance by each Party.

9.4. All Annexes to the Agreement are its integral parts.

**ПЕРЕЧЕНЬ УСЛУГ, ПРЕДОСТАВЛЯЕМЫХ
КЛИЕНТУ В СИСТЕМЕ БАНК-КЛИЕНТ**

**THE LIST OF SERVICES PROVIDED TO
THE CLIENT IN THE BANK-CLIENT
SYSTEM**

1. При помощи функционала Системы Банк осуществляет прием от Клиента следующих Электронных документов о совершении операций по Счету:

- ✓ «Рублевое платежное поручение»;
- ✓ «Запрос на отзыв Электронного документа»;
- ✓ «Заявление на перевод средств в иностранной валюте»;
- ✓ «Заявка на покупку валютных средств»;
- ✓ «Заявка на продажу валютных средств»;
- ✓ «Заявка на конвертацию»;
- ✓ «Распоряжение о распределении средств с транзитного счета»;
- ✓ «Заявка на размещение депозита»;
- ✓ «Заявление на предоставление кредита»;
- ✓ «Аккредитив в рублях РФ»;
- ✓ «Заявление на открытие внешнеторгового аккредитива»;
- ✓ «Заявление на выдачу гарантии»;
- ✓ «Подтверждение поставочной конверсионной сделки»;
- ✓ «Запрос на отзыв документов»;
- ✓ Иные электронные документы⁴.

2. Банк осуществляет прием от Клиента следующих Электронных документов:

- ✓ «Письмо в банк» с вложенным документом произвольного формата (в т.ч. с вложением Скан-копий документов для целей валютного контроля), за исключением передачи в виде вложенного документа паспорта сделки, заявления о переоформлении паспорта сделки, заявления о закрытии паспорта сделки, справки о валютных операциях, справки о подтверждающих документах⁵;

1. The Bank receives the following electronic documents on performing transactions on the Account from the Client with the help of software and hardware of the System:

- ✓ «Ruble bank transfer»;
- ✓ «E-Document Withdrawal Request»
- ✓ «Foreign Currency Payment Order»;
- ✓ «Request for Foreign Currency Purchasing»;
- ✓ «Request for Foreign Currency Selling»;
- ✓ «Currency Exchange Request»;
- ✓ «Order for Allocation of Transit Account Funds»;
- ✓ «Deposit Application»;
- ✓ «Loan Application»;
- ✓ «Letter of Credit in Russian Roubles»;
- ✓ «Application for foreign trade letter of credit»;
- ✓ «Deliverable Foreign Exchange Transaction Confirmation»;
- ✓ «Application for issue of guarantee»;
- ✓ «Documents Withdrawal Request»;
- ✓ Another electronic documents⁴.

2. Bank receives from the Client the following Electronic Documents:

- ✓ «Letter to the Bank» with an attached free format document (including the attachment of scanned copies of documents for currency control purposes), except for transfer via an attached document of the transaction certificate, application for re-registration of the transaction certificate, application for closing the transaction certificate, certificate of foreign currency

⁴ если определенный документ должен по требованию Банка в связи с нормами законодательства РФ содержать определенные сведения, чтобы быть принятым Банком, Клиент обязуется указывать соответствующие требования.
if a certain document contains some mandatory information with the bank's requirements regarding to the legislation of the Russian Federation, it will be accepted by the Bank, the Client should specify relevant requirements.

⁵ кроме случаев, когда формирование таких документов в виде электронной формы невозможно. При невозможности формирования документов в виде электронной формы допускается передача Письма в Банк с вложением Документа ВК, если при формировании такого документа использовались шаблоны, размещенные на сайте Банка или предоставленные сотрудниками подразделений Банка, ответственных за обработку Документов ВК. Перечень документов, которые могут направляться в виде вложений, приводится на сайте Банка в сети Интернет по адресу <http://www.raiffeisen.ru>.
except for cases where the generation of such documents in electronic form is impossible. In case of impossibility of the generation of the documents in electronic form it is permitted to transfer Letters to the Bank with the attached CC documents, if during the generation of such document templates from the Bank's website or provided by the Bank's units employees responsible for processing of CC documents were used. The list of documents that can be sent as attachments, is available on the Bank's website on the Internet at <http://www.raiffeisen.ru>.

- ✓ «Письмо в банк» в виде текстового сообщения.

3. Банк осуществляет передачу Клиенту следующих информационных Электронных документов:

- ✓ Информация о движении денежных средств по Счетам (с приложениями);
- ✓ «Письмо из банка» с вложенным документом произвольного формата;
- ✓ «Письмо из банка» с текстовым сообщением.

4. Банк осуществляет прием к исполнению от Клиента следующих Электронных документов для целей валютного контроля:

- ✓ «Справка о валютных операциях»;
- ✓ «Информация для валютного контроля»;
- ✓ «Справка о подтверждающих документах»;
- ✓ «Паспорт сделки по контракту» (форма 1);
- ✓ «Паспорта сделки по кредитному договору» (форма 2);
- ✓ «Заявление о закрытии паспорта сделки»;
- ✓ «Заявление о переоформлении паспорта сделки по контракту» (форма 1);
- ✓ «Заявление о переоформлении паспорта сделки по кредитному договору» (форма 2).

5. Банк осуществляет передачу Клиенту следующих Электронных документов для целей валютного контроля:

- ✓ «Ведомость банковского контроля»;
- ✓ «Справка о валютных операциях»;
- ✓ «Справка о подтверждающих документах»;
- ✓ «Паспорт сделки по контракту» (форма 1) (в том числе в формате xml);
- ✓ «Паспорт сделки по кредитному договору» (форма 2) (в том числе в формате xml).

6. Банк осуществляет прием к исполнению от Клиента следующих Электронных документов в рамках Соглашения о перечислении денежных средств на счета работников компании и предоставлении банковских карт:

- ✓ Зарплатная ведомость;
- ✓ Реестр на прикрепление к зарплатному проекту;
- ✓ Реестр на открепление от зарплатного проекта.

transactions, reference on supporting documents⁵;

- ✓ «Letter to the Bank» in the form of a text message.

3. The Bank transmits the following Informational Electronic Documents to the Client:

- ✓ Information about the movement of funds on the Accounts (with attachments);
- ✓ «Bank Letter» with an attached free-format document;
- ✓ «Bank Letter» with a text message.

4. The Bank shall accept for execution the following electronic documents for currency control purposes from the Client:

- ✓ «Certificate of currency transactions»;
- ✓ «Information for currency control»;
- ✓ «Statement of supporting documents»;
- ✓ «Transaction certificate on a contract» (Schedule 1);
- ✓ «Transaction certificates under the loan agreement» (Schedule 2);
- ✓ «Application for closing of a transaction certificate»;
- ✓ «Application for renewal of a transaction certificate on a contract» (Schedule 1);
- ✓ «Application for the reissue of a credit agreement transaction certificate» (Schedule 2).

5. Bank transmits to the Client the following Electronic Documents for currency control purposes:

- ✓ «Statement of the bank control»;
- ✓ «Statement of currency transactions»;
- ✓ «Statement of supporting documents»;
- ✓ «Transaction certificate under the contract» (Annex 1) (including the xml format);
- ✓ «Transaction certificate under the loan agreement» (Annex 2) (including the xml format).

6. The Bank shall accept for execution the following electronic documents from the Client within the Agreement on funds transfer on employee's accounts and issuing bank cards:

- ✓ Payroll;
- ✓ Register on attachment to the salary project;
- ✓ Register on detachment from the salary project.

7. «ELBRUS Mobile»:

- ✓ «Рублевое платежное поручение»;
- ✓ Просмотр информации о движении денежных средств по Счетам;
- ✓ Просмотр информации о балансе и доступном остатке денежных средств по Счетам;
- ✓ Просмотр «Писем из банка» с текстовым сообщением;
- ✓ Поиск банкоматов и отделений Банка;
- ✓ Сервис отправки реквизитов Счета контрагентам по SMS или e-mail;
- ✓ Отзыв ранее направленного в Банк платежа.

8. «SMS для Бизнеса»:

- ✓ Получение информации о движении денежных средств по Счетам;
- ✓ Получение информации о подключении/изменении/отключении Услуги «SMS для Бизнеса»;
- ✓ Сервис настройки времени для получения SMS-сообщений;
- ✓ Получение уведомлений о событиях в Системе: Осуществлен вход в Систему, Изменение Пароля Пользователя ELBRUS, Учетная запись Пользователя создана/заблокирована/разблокирована, Сертификат ключа подписи активирован/деактивирован, истечение срока действия, Изменение права подписи, Истечение срока действия подписи, Получение ДСФ от Банка;
- ✓ Получение уведомлений о статусах Электронных документов в Системе.

9. «SMS-OTP»:

- ✓ Получение уникального одноразового кода, предназначенного для подтверждения одной операции в «ELBRUS Mobile» или «ELBRUS Internet», предоставляемого Банком посредством SMS-сообщений на зарегистрированный номер Пользователя/Клиента.

7. «ELBRUS Mobile»:

- ✓ «Ruble bank transfer»;
- ✓ View of the information about the movement of funds on the Accounts;
- ✓ View of the information about the balance and the available balance of funds on the account;
- ✓ View the «Bank Letters» with a text message;
- ✓ Search for ATMs and branches of the Bank;
- ✓ The service for sending the Account details to counterparties via SMS or e-mail;
- ✓ Revocation of bank transfer/payment order sent to the Bank earlier.

8. «SMS for Business»:

- ✓ Receive information about the movement of funds on the Accounts;
- ✓ Receive information on how to enable/change/disable the «SMS for Business» Service;
- ✓ Time settings service for receiving SMS-messages;
- ✓ Receive notifications about events in the System: Logged into the System, change ELBRUS user password, user account is created/blocked/unblocked, signature key certificate is activated/deactivated, expiry, change of signature authority, expiration of signature right, receiving of FFD from the Bank;
- ✓ Receive email alerts on the statuses of Electronic Documents in the System.

9. «SMS-OTP»:

- ✓ Obtaining a unique one-time code designed to confirm a single operation in «ELBRUS Mobile» or «ELBRUS Internet» provided by the Bank through SMS-messages on the phone number of registered users/Clients.

**ПОРЯДОК ПОДКЛЮЧЕНИЯ И
ОБСЛУЖИВАНИЯ
В СИСТЕМЕ БАНК-КЛИЕНТ
«ELBRUS Internet»**

**PROCEDURE FOR CONNECTION AND
SERVICING IN THE «ELBRUS Internet»
BANK-CLIENT SYSTEM**

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1. GENERAL PROVISIONS.

1.1. Термины, используемые в тексте настоящего **Порядка подключения и обслуживания в Системе Банк-Клиент «ELBRUS Internet»** (далее - **Порядок**) с заглавной буквы, имеют то значение, какое им дано в Соглашении.

1.1. The terms used in the text of this **Procedure for connection and servicing in the «ELBRUS Internet» Bank-Client System** (hereinafter - **the Procedure**) with a capital letter, have the meaning given to them in the Agreement.

1.2. Программное обеспечение Системы загружается с сайта Системы <http://elbrus.raiffeisen.ru> на Аппаратное средство Клиента через сеть Интернет и реализовано в виде Криптоплагина, имеющего в составе компоненту, взаимодействующую с СКЗИ КриптоПро CSP производства компании ООО «КРИПТО-ПРО» <http://cryptopro.ru/>.

1.2. System Software is loaded from the System website <http://elbrus.raiffeisen.ru> on the hardware of the Client via the Internet and has the form of a crypto plugin having a component interacting with Cryptographic Information Protection Facility CryptoPro produced by «CRYPTO-PRO» LLC <http://cryptopro.ru/>.

При модификации Программного обеспечения Системы, Банк уведомляет Клиента за 10 (Десять) календарных дней до введения таких изменений в действие путем публикации на сайте Системы в сети Интернет <http://elbrus.raiffeisen.ru> и/или опубликованием информации в Системе (раздел «Письма из Банка»).

The Bank shall notify the Client on the modifications to the Software of the System within 10 (ten) days prior to the effective introduction of these modifications by publishing on the website of the System on the Internet <http://elbrus.raiffeisen.ru> and/or publication of information in the System («Bank Letters» Section).

1.3. Для хранения и работы с Закрытыми ключами усиленной электронной подписи Пользователи используют Устройства USB-token - электронный USB-ключ eToken PRO 72K Java (для Подписантов с правом подписи, относящейся к I группе подписей или единственной подписи данное условие обязательно).

1.3. To store and work with Private keys of the enhanced electronic signature, Users use a USB-token device - an electronic USB-key eToken PRO 72K Java (this condition is mandatory for Signatories that are authorized signatories belonging to the I group of signatures or the exclusive signature).

1.4. Для доступа к Системе, необходимо при установленном соединении с Интернет с помощью браузера войти на сайт Системы в сети Интернет по адресу: <http://elbrus.raiffeisen.ru>.

1.4. To access the System, it is necessary to go to the System website via a browser having a connection to the Internet: <http://elbrus.raiffeisen.ru>.

1.5. Для работы с Системой необходимо проверить соответствие Аппаратных средств и Программного обеспечения Клиента требованиям Разделов 2 и 3 настоящего Порядка.

1.5. To work with the System you need to check that the hardware and software of the client conforms to the requirements of Sections 2 and 3 of this Procedure.

1.6. Подробное описание работы в Системе представлено в Руководстве по использованию, размещенном на сайте Системы <http://elbrus.raiffeisen.ru/>.

1.6. Detailed description of the work in the System is given in the Manual posted on the website of the System <https://elbrus.raiffeisen.ru/>.

1.7. Перед работой с Системой, Клиенту необходимо ознакомиться с Общими сведениями по вопросам безопасности систем интернет-банка, размещенными на сайте Банка в сети Интернет <http://www.raiffeisen.ru/>.

1.8. При подключении Клиента к Системе, к Системе подключаются все открытые Клиенту в Банке Счета.

1.9. Система позволяет Клиенту выполнять операции, изложенные в Приложении № 1 к Соглашению.

2. ТРЕБОВАНИЯ К АППАРАТНЫМ СРЕДСТВАМ.

- IBM-совместимый компьютер с классом процессора не ниже Pentium 4 и объемом ОЗУ не менее 512 Мбайт, порт USB v1.1 (или выше), манипулятор «мышь»;
- не менее 100 Мбайт свободного дискового пространства (для подсистемы защиты и Java-приложений);
- постоянное подключение к сети Интернет, возможность работы по протоколу HTTPS (порт 443);
- устройство USB-token (выдается Банком);
- рекомендуемое для работы с Системой разрешение экрана – 1024x768 точек и выше.
- мобильный телефон, подключенный к услугам оператором сотовой связи (обязателен в случае использования услуги «SMS-OTP») с доступностью функции IMSI на стороне оператора связи.

3. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ.

- Операционная система Microsoft Windows 7/8;
- Интернет-браузеры: две последние версии браузеров Chrome, Firefox, Yandex, Opera, Safari и Internet Explorer 8.0 и выше;
- На компьютере Пользователя интернет-браузер должен поддерживать выполнение сценариев JavaScript;
- Для загрузки/установки/обновления СКЗИ необходимы права «Локальный администратор», «Опытный пользователь»;
- На компьютере должен быть установлен КриптоПлагин (доступен для загрузки при авторизации в Системе при наличии прав подписи);
- Для работы с Устройством USB-token необходимо скачать и установить драйвер устройства с сайта Банка:

1.7. Before working in the System, clients should read the General safety information of the online banking systems placed on the Bank's website on the Internet at <http://www.raiffeisen.ru/>.

1.8. When Clients connect to the System, all open client accounts in the Bank are connected to the System.

1.9. The System allows Clients to conduct operations set out in Annex no. 1 to the Agreement.

2. HARDWARE REQUIREMENTS.

- IBM-compatible PC with a processor class not lower than Pentium 4 and the capacity of RAM of 512 MB, USB v1.1 port (or higher), a mouse;
- at least 100 MB of free disk space (for the protection subsystem and Java-based applications);
- permanent connection to the Internet, ability to operate via HTTPS (port 443);
- USB-token device (given by the Bank);
- recommended screen resolution for the System - 1024x768 pixels or higher.
- mobile phone connected to the services of a mobile operator (mandatory in the case of use of «SMS-OTP» services) with available IMSI function on the side of the operator.

3. SOFTWARE REQUIREMENTS.

- Microsoft Windows 7/8 operating system;
- Internet browsers: two latest versions of Chrome, Firefox, Yandex, Opera, Safari and Internet Explorer 8.0 or higher;
- The web browser on the user's computer must support JavaScript scenarios execution;
- «Local Administrator», «Experienced User» rights are necessary to download/install/update CIPF;
- The computer must have the installed Crypto plugin (available for download when you authorize in the System in case of having signature rights);
- It is necessary to download and install the device driver with the Bank's website to work with the USB-token device:

- для 32-битной версии Windows - <http://elbrus.raiffeisen.ru/fs/pc32.msi>
- для 64-битной версии Windows - <http://elbrus.raiffeisen.ru/fs/pc64.msi>
- Наличие лицензионного регулярно обновляемого антивирусного программного обеспечения;
- Отсутствие на компьютере Пользователя ранее установленных копий ПО КриптоПро CSP версий ниже 3.6.

4. ТРЕБОВАНИЯ К СЛОЖНОСТИ ПАРОЛЯ.

- При входе в Систему осуществляется идентификация Пользователя по Имени пользователя и аутентификация по Паролю.
- В случае первого входа в Систему Пользователю необходимо сменить Пароль, выданный Банком, на новый постоянный Пароль.
- В целях безопасности постоянный Пароль для входа в Систему должен удовлетворять следующим требованиям:
 - длина Пароля должна быть не менее 8 и не более 14 символов;
 - Пароль должен одновременно включать латинские символы (A-z), цифры (0-9).
 - символы в пароле не должны быть повторяющимися (например, Qwerty111).

5. ДОСТУП В СИСТЕМУ И БЕЗОПАСНОСТЬ.

- 5.1.** Конфиденциальность передаваемой информации обеспечивается средствами протокола SSL. Целостность данных обеспечивается средствами протокола SSL и УЭП ЭД.
- 5.2.** В процессе регистрации для каждого Подписанта, Подписанта ВК, Контролера, Ревизора, имеющего право подписывать ЭД, передаваемые по Системе:
- 5.2.1.** в случае дальнейшего подтверждения операций с использованием УЭП выдается персональное устройство USB-token, создается Открытый и Закрытый ключи усиленной электронной подписи, регистрируется в Системе личный Сертификат ключа подписи и Открытый ключ усиленной электронной подписи.
- 5.2.2.** в случае дальнейшего подтверждения операций с использованием ПЭП, Клиент осуществляет подключение услуги «SMS-ОТП» согласно п. 3.14 и 3.15 к Соглашению.
- 5.3.** Подписание каждого ЭД ЭП и проверка подписи на сервере позволяет сделать

- for the 32-bit version of Windows - <http://elbrus.raiffeisen.ru/fs/pc32.msi>
- for the 64-bit version of Windows - <http://elbrus.raiffeisen.ru/fs/pc64.msi>
- Availability of licensed or a regularly updated anti-virus software;
- The absence of previously installed copies of Crypto CSP software versions below 3.6 on the user's computer.

4. REQUIREMENTS FOR PASSWORD COMPLEXITY.

- When you log on, user identification is carried out through authentication by user name and password.
- In the case of the first login a user needs to change the password given by the Bank to a new permanent password.
- For security purposes, a permanent password for entering the System must meet the following requirements:
 - The password should be at least 8 and no more than 14 characters long;
 - The password must contain both Latin characters (A-z), numbers (0-9).
 - the characters in a password should not be repeated (for example, Qwerty111).

5. ACCESS TO THE SYSTEM AND SECURITY.

- 5.1.** Privacy of transmitted information is provided by means of the SSL protocol. Data integrity is ensured by means of SSL and EDS ED.
- 5.2.** During the registration process for each Signatory, CC Signatories, Controller, Auditor that has the right to sign the ED transmitted via the System:
- 5.2.1.** in case of further confirmation of transactions with the use of EDS a personal USB-token device is given that creates public and private keys of enhanced electronic signature, a personal signature key certificate and a public key enhanced electronic signature are registered in the System.
- 5.2.2.** in case of further confirmation of operations with the use of SDS, the Client enables «SMS-ОТП» services in accordance with paras. 3.14 and 3.15 of the Agreement.
- 5.3.** Signing of each ED with a DS and signature verification on the server allows you to draw

заключение о происхождении ЭД и его не искаженности при передаче.

5.4. Срок действия Сертификата ключа подписи и Ключей Пользователя в Системе – 1 (Один) год с даты создания.

За один месяц до истечения срока действия Сертификата ключа подписи Пользователю с правами Подписант, Подписант ВК, Контролер, Ревизор формируется сообщение в Системе о необходимости продления Сертификата ключа подписи.

Для продления Сертификата ключа подписи Подписант, Подписант ВК, Контролер, Ревизор:

- создает запрос на регенерацию сертификата в разделе «Обмен криптоинформацией» подразделе «Запросы на регенерацию сертификата»;
- заполняет требуемую информацию и сохраняет изменения;
- подписывает запрос действующим Ключом Пользователя в Системе и отправляет в Банк.

Сертификат ключа подписи выпускается автоматически после направления запроса, после чего статус запроса изменится на «Обработан» и Пользователь может работать с новым Ключом.

5.5. Сертификат ключа подписи Подписанта, Подписанта ВК, Контролера, Ревизора считается действующим в момент проверки УЭП при одновременном выполнении следующих условий:

- Сертификат ключа подписи зарегистрирован в Банке;
- срок действия Сертификата ключа подписи не истек;
- действие Сертификата ключа подписи не приостановлено и не отменено.

5.6. В Системе используется двухуровневая схема подписей:

- I группа подписей;
- II группа подписей.

Клиент вправе уполномочить нескольких лиц на подписание ЭД I группой подписей или II группой подписей из числа лиц, указанных в КОП Клиента, принятой Банком в работу, и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению.

Клиент может подписывать ЭД единственной подписью:

- если в КОП и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению содержится одна собственноручная подпись лица, уполномоченного Клиентом, необходимая

conclusions about the origin of ED and its undistorted transmission.

5.4. The validity of the Signature key certificate and the User keys in the System - One (1) year from the date of creation.

One month before the expiry of the Signature key certificate a message is generated in the System for the users with the powers of a Signatory, an CC Signatory, a Controller, an Auditor notifying on the need to extend the certificate.

To extend the Signature key certificate a Signatory, CC Signatory, a Controller, an Auditor:

- creates a request to re-generate the certificate in the «Crypto information exchange» section «Request a certificate regeneration» subsection;
- fills out the required information and saves the changes;
- signs the request with the current user key in the System and sends it to the Bank.

The signature key certificate is issued automatically after the request is made, after which the status of the request will change to «Processed» and the User can work with the new key.

5.5. Signature key Certificate of a Signatory, a CC Signatory, a Controller, an Auditor is considered valid at the time of check of the EDS with the simultaneous satisfaction of the following conditions:

- The signature key certificate is registered in the Bank;
- The signature key certificate has not expired;
- the effect of the signature key certificate is not suspended or cancelled.

5.6. The System uses a two-level scheme of signatures:

- I group of signatures;
- II group of signatures;

The Client has the right to authorize more than one person to sign the ED with I group of signatures or II group of signatures from among the persons specified in the Client's Sample Signature Cards, accepted by the Bank for work and/or the proxy notice accepted by the Bank for work according to the Schedule of Annex no. 5 to this Agreement.

The Client can sign ED with the single the signature:

- if the SSCs and/or the proxy notice accepted by the Bank for work according to the Schedule of Annex no. 5 to this Agreement contain a hand-written signature of the person authorized by the Client necessary for the

для подписания документов и распоряжений о переводе средств;

- если вместе с КОП Клиент предоставил в Банк заявление, что на документах и распоряжениях о переводе средств может быть учинена только одна собственноручная подпись из образцов подписей, включенных в КОП.

5.7. В Системе используется специальный порядок подписания Документов ВК. Данные документы подписываются:

- лицами, относящимися к I группе подписей согласно КОП, и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению;
- лицами, относящимися ко II группе подписей согласно КОП, и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению;
- лицами, обладающими единственной подписью согласно КОП, и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению;
- лицами, обладающими специальной подписью (Подписант Документов ВК) (данной подписью обладают лица на основании доверенности на подписание Документов ВК, принятой Банком).

Лица, относящиеся к I и II группе подписей, а также лица, обладающие единственной подписью, могут подписывать ЭД в порядке, установленном п. 5.6., и Документы ВК – единственной подписью.

Лица, наделенные правом специальной подписи Документов ВК, могут подписывать единственной подписью только Документы ВК и не могут подписывать иные ЭД.

5.8. Система позволяет регистрировать уполномоченных лиц Клиентов с правом подписывать ЭП Электронные документы, не заменяя при этом лиц, указанных в КОП и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению - Контролеров, для которых создаются Открытые и Закрытые ключи, регистрируются в Системе личные Сертификаты ключа подписи и Открытые ключи.

5.9. В соответствии с порядком, предусмотренным Соглашением, в Системе могут быть зарегистрированы Операторы - Пользователи без права подписания ЭД. Для Операторов Открытый и Закрытый ключи не создаются.

5.10. ЭД Клиента считается подписанным

signing of documents and orders on the transfer of funds;

- if alongside with the SSC, the Client provided to the Bank an application stating that the documents and orders on the transfer of funds only a handwritten signature from the specimen signatures included in the SSC can be used.

5.7. The System uses a special procedure for signing CC documents. These documents are signed by:

- persons belonging to I Group of signatures according to the SSC and/or the proxy notice accepted by the Bank according to Annex no. 5 to this Agreement;
- persons belonging to II group of signatures according to the SSC and/or the proxy notice accepted by the Bank according to Annex no. 5 to this Agreement;
- individuals with a single signature in accordance with the SSC, and/or the proxy notice accepted by the Bank according to Annex no. 5 to this Agreement;
- persons with a special signature (Signatory of CC documents) (the person owns this signature right on the basis of the proxy notice for signing of CC documents accepted by the Bank).

Persons belonging to I and II groups of signatures, as well as persons who have a single signature, may sign EDs in the manner prescribed by paragraph 5.6, and the CC documents - with an exclusive signature.

Persons with the right to use special signature for CC documents may sign only CC documents with an exclusive signature and cannot sign any other ED.

5.8. The System allows you to register authorized persons of the Clients with the right to sign Electronic documents with a DS without replacing the persons specified in the SSC and/or the proxy notice accepted by the Bank according to Annex no. 5 to this Agreement - Controllers, for whom public and private keys are created, and personal signature key certificates and public keys registered in the System.

5.9. In accordance with the procedure provided for in the Agreement, Operators-Users not authorised to sign ED can be registered in the System. Public and private keys are not created for Operators.

5.10. ED of the Client is considered signed with a

достаточным набором ЭП, при следующих условиях:

- ЭД подписан двумя подписями (любой подписью из I группы подписей и любой подписью из II группы подписей) при наличии у Клиента нескольких уполномоченных лиц, обладающих правом подписи согласно КОП и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению.

Подписанное ЭД не отправляется в Банк без ЭП Контролера, если в Системе зарегистрировано уполномоченное лицо с правами доступа Контролер;

- ЭД подписан единственной подписью:
 - если в КОП и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению содержится одна собственноручная подпись лица, уполномоченного Клиентом, необходимая для подписания документов и распоряжений о переводе средств;
 - если вместе с КОП Клиент предоставил в Банк заявление, что на документах и распоряжениях о переводе средств может быть учинена только одна собственноручная подпись из образцов подписей, включенных в КОП.

Подписанное ЭД не отправляется в Банк без ЭП Контролера, если в Системе зарегистрировано уполномоченное лицо с правами доступа Контролер;

- ЭД, являющийся Документом ВК, подписан любой подписью I группы подписей, или любой подписью II группы подписей, или единственной подписью, или подписью любого из Подписантов ВК (уполномоченных лиц с правом специальной подписи Документов ВК может быть несколько).

6. ПОДКЛЮЧЕНИЕ К СИСТЕМЕ.

6.1. Для подключения к Системе, Клиент заключает с Банком Соглашение и определяет перечень Пользователей Системы, для чего передает в Банк:

- заполненную Информационную карточку клиента по форме Приложения № 4 к Соглашению, если не всем лицам, указанным в КОП Клиента, предоставляется право подписи ЭД в Системе;
- Список Пользователей по форме Приложения № 6 к Соглашению и

sufficient set of DS under the following conditions:

- ED is signed with two signatures (any signature of the I group of signatures and any signature of II group of signatures) if the Client has several authorized persons with a right to sign according to SSC and/or the proxy notice accepted by the Bank according to Annex no. 5 to this Agreement..

A signed ED is not sent to the Bank without the Controller's DS, if an authorized person with access rights of a Controller is registered in the System;

- ED is signed with an exclusive signature:
 - If the SSC and/or the proxy notice accepted by the Bank according to Annex no. 5 to this Agreement contains a handwritten signature of the person authorized by the Client necessary for the signing of documents and orders on the transfer of funds;
 - If the Client provided the Bank with an Application alongside with SSC which states that the documents and orders on the transfer of funds can be signed only with a handwritten signature from the sample signatures included in the SSC.

A signed ED is not sent to the Bank without the Controllerr's DS, if an authorized person with access rights of a Controller is registered in the System;

- ED that is a CC document is signed by any signature of I group signatures, or any II group signature signatures or an exclusive signature, or the signature of any of the CC signatories (there may be several authorized persons with the right of special signature for CC documents).

6. CONNECTING TO THE SYSTEM.

6.1. To connect to the System, the Client concludes with the Bank an Agreement and defines the list of users of the System for which purpose presents to the Bank:

- filled in client information card according to Annex no. 4 to the Agreement, if not all of the persons specified in the SSC of the Client shall have the ED signature right in the System;
- List of Users in the form of Annex no. 6 to the Agreement and the proxy notice (in hard

доверенности (на бумажном носителе) по форме Приложения № 5 к Соглашению для подключения Операторов, Контролеров и Ревизоров и Подписантов ВК;

6.2. Банк в течение 10 (Десяти) Рабочих дней с даты вступления Соглашения в силу передает Клиенту установочный пакет со Средствами доступа, в состав которого входят:

- конверты с Регистрационными данными для каждого Пользователя Клиента;
- Устройства USB-token;
- Руководство «Быстрый старт»;
- Инструкция по работе с Устройством USB-token;
- 2 (Два) экземпляра Акта приема-передачи (составляется по форме Банка).

6.3. Уполномоченный представитель Клиента проверяет соответствие содержимого установочного пакета перечню Пользователей, которым предоставляется право работать в Системе:

- соответствие Ф.И.О. Уполномоченных лиц, перечисленных в КОП;
- соответствие конверта с Регистрационными данными данным Пользователя;
- соответствие уникального номера Устройства USB-token данным Пользователя.

После сверки уполномоченный представитель Клиента подписывает Акт приема-передачи и один экземпляр передает Банку.

6.4. Для подключения к Системе Подписант, Подписант ВК, Контролер, Ревизор:

- получает персональный конверт с Регистрационными данными (Именем пользователя и Паролем);
- *применимо для Подписантов, Подписантов ВК, Контролеров, Ревизоров, которым предоставляется персональное Устройство USB-token для подписания ЭД УЭП:* получает персональное Устройство USB-token, меняет стандартный пароль на Устройстве USB-token на персональный Пароль согласно Инструкции по работе с устройством USB-Token (запрос на смену Пароля будет выдан автоматически при подключении Устройства USB-token к компьютеру);
- проверяет наличие прав «Локального администратора» на компьютере;
- выполняет вход на сайт Системы в сети Интернет <http://elbrus.raiffeisen.ru>;
- в форме запроса авторизации вводит выданные Банком Имя пользователя и

copy) in the form of Annex 5 to the Agreement to connect Operators, Controllers, Auditors and CC Signatories;

6.2. The Bank provides the Client with the installation package with the means of access within 10 (ten) working days from the date of entry into force of the Agreement, which includes:

- envelopes with registration data for each User of the Client;
- USB-token Devices;
- «Quick Start» Manual;
- USB-token device manual;
- 2 (two) copies of the acceptance and transfer certificate (drawn up according to the form of the Bank).

6.3. An authorized representative of the Client checks the contents of the installation package according to the list of Users who are granted with the right to work in the System:

- Correctness of the names of the authorized persons listed in SSC;
- Conformity of the envelope with the registration data with the data of the User;
- Conformity of the unique number of the USB-token device with the User data.

After the verification, the authorized representative of the Client signs the acceptance and transfer certificate, and sends one copy to the Bank.

6.4. To connect to the System, a Signatory, a CC Signatory, Controller, Auditor:

- receives an envelope with personal registration data (username and password);
- *applicable to Signatories, CC Signatories, Controllers, Auditors who receive a personal USB-token device for signature of ED with an EDS:* receives a personal USB-token device, change the default password on the USB-token Device to a personal password according to the instructions on the USB-Token device (a request to change the password will be issued automatically when you connect the USB-token device to your computer);
- checks for the rights of a «local administrator» on the computer;
- logs on System's website on the Internet <http://elbrus.raiffeisen.ru>;
- enters the username and the password for the first login issued by the Bank in the form of

- Пароль для первого входа в Систему;
 - меняет Пароль, выданный Банком, на персональный Пароль для работы в Системе (далее Система будет запрашивать смену персонального Пароля каждые 180 (Сто восемьдесят) календарных дней);
 - *применимо для Подписантов, Подписантов ВК, Контролеров, Ревизоров, которым предоставляется персональное Устройство USB-token:* подключает к компьютеру Устройство USB-token для создания и хранения Закрытого ключа;
 - *применимо для Подписантов, Подписантов ВК, Контролеров, Ревизоров, которым не предоставляется Устройство USB-token:* подключает к компьютеру USB-флэш-накопитель для создания и хранения Закрытого ключа; проходит процедуру регистрации в Системе и отправляет в Банк ЭД «Запрос на новый сертификат»;
 - проверяет получение ЭД «Запрос на новый сертификат» статуса «Обработан»;
 - распечатывает 2 (Два) экземпляра «СЕРТИФИКАТА ключа УЭП для Системы Банк-Клиент «ELBRUS» АО Райффайзенбанк», заверяет собственноручной подписью, подписью руководителя Клиента и печатью Клиента (при наличии);
 - передает оба экземпляра «СЕРТИФИКАТА ключа УЭП для Системы Банк-Клиент «ELBRUS» АО Райффайзенбанк» Банку;
- 6.5.** Для подключения к Системе Оператор:
- получает персональный конверт с Регистрационными данными (Именем пользователя и Паролем);
 - выполняет вход на сайт Системы в сети Интернет <http://elbrus.raiffeisen.ru>,
 - в форме запроса авторизации вводит выданные Банком Имя пользователя и Пароль для первого входа в Систему;
 - меняет Пароль, выданный Банком, на персональный Пароль для работы в Системе (далее Система будет запрашивать смену персонального Пароля каждые 180 (Сто восемьдесят) календарных дней);
- 6.6.** Для изменения права подписи Подписанта в Системе:
- При изменении прав подписи Подписантов согласно новой КОП, принятой Банком, и/или принятой Банком в работу доверенности по форме Приложения № 5 к настоящему Соглашению, если Подписант ранее относящийся ко II группе подписей, согласно
- authorization request;
 - changes Password issued by the Bank to a personal password to work in the System (the System will request a personal password change every 180 (one hundred eighty) calendar days);
 - applicable to Signatories, CC Signatories, Controllers, Auditors who receive a personal USB-token device:* connects the USB-token device to computer to generate and store the private key;
 - applicable to Signatories, CC Signatories, Controllers, Auditors who do not receive the USB-token device:* connects the USB flash drive to the computer to create and store the private key; completes the registration procedure in the System and sends an ED «Request for a new certificate» to the Bank;
 - checks that the ED «Request for a new certificate» gets the status «Processed»;
 - prints two (2) copies of the «EDS key certificate» for the «ELBRUS Internet» Bank-Client System of AO Raiffeisenbank, certifies with a handwritten signature, signature of the executive of the Client and Client's seal (if any);
 - sends both copies of the «EDS key certificate» of the «ELBRUS Internet» Bank-Client System of AO Raiffeisenbank to the Bank;
- 6.5.** To connect to the System the Operator:
- receives an envelope with personal registration data (username and password);
 - logs on to the System's website on the Internet <http://elbrus.raiffeisen.ru>,
 - enters the username and the password for the first login issued by the Bank in the form of authorization request;
 - changes Password issued by the Bank to a personal password to work in the System (the System will request a personal password change every 180 (one hundred eighty) calendar days);
- 6.6.** To change the rights of signatories' signatures in the System:
- If you change the signing rights of Signatories under the new SSC accepted by the Bank and/or the proxy notice accepted by the Bank according to Annex no. 5 to this Agreement, if the signatory previously belonging to II group of signatures under the new SSC and/or the new proxy notice

новой КОП и/или новой доверенности по форме Приложения № 5 к настоящему Соглашению, обладает подписью из I группы подписей или единственной подписью, то Имя Пользователя и персональный Пароль действуют без изменений.

Подписант, Подписант ВК, Контролер, Ревизор с правом подписания ЭД УЭП:

для изменения права подписи в Системе осуществляет следующие действия:

- получает персональное Устройство USB-token, меняет стандартный пароль на Устройство USB-token на персональный Пароль согласно Инструкции по работе с устройством USB-Token (запрос на смену Пароля будет выдан автоматически при подключении Устройства USB-token к компьютеру);
- подключает к компьютеру Устройство USB-token для создания и хранения Закрытого ключа УЭП;
- отправляет в Банк ЭД «Запрос на новый сертификат»;
- проверяет получение ЭД «Запрос на новый сертификат» статуса «Обработан»;
- распечатывает 2 (Два) экземпляра «СЕРТИФИКАТА ключа УЭП для Системы Банк-Клиент «ELBRUS» АО Райффайзенбанк», заверяет собственноручной подписью, подписью руководителя Клиента и печатью Клиента (при наличии);
- передает оба экземпляра «СЕРТИФИКАТА ключа УЭП для Системы Банк-Клиент «ELBRUS» АО Райффайзенбанк» Банку.

6.7. После проверки в Банке полученного от Пользователя «СЕРТИФИКАТА ключа УЭП для Системы Банк-Клиент «ELBRUS» АО Райффайзенбанк» и сверки с ЭД «Запрос на сертификат», документ подписывается со стороны Банка, Клиенту возвращается 1 (Один) экземпляр, а Пользователю предоставляется доступ к выполнению операций в Системе.

6.8. Банк в течение 2 (Двух) Рабочих дней после получения «СЕРТИФИКАТА ключа УЭП» для Системы Банк-Клиент «ELBRUS» выполняет регистрацию и активацию Открытого ключа УЭП.

После активации Открытого ключа УЭП в Системе Пользователь может подписывать ЭД УЭП.

6.9. После окончания процедуры регистрации и активации Открытого ключа УЭП в Банке, Пользователь с правом подписи, а также с

accepted by the Bank according to Annex no. 5 to this Agreement, has the signature of the I group of signatures or an exclusive signature, the User Name and personal Password are unchanged.

Signatory, CC Signatory, Controller, Auditor with the right to sign ED with EES:

to change the signature rights in the System the following actions should be performed:

- receives a personal USB-token device, change the default password on the USB-token Device to a personal password according to the instructions on the USB-Token device (a request to change the password will be issued automatically when you connect the USB-token device to your computer);
- connects the USB-token device to a PC for creation and storage of the private EDS key;
- sends ED «Request for a new certificate» to the Bank;
- checks that the ED «Request for a new certificate» gets the status «Processed»;
 - prints two (2) copies of the «EDS certificate key» to the «ELBRUS Internet» Bank-Client System of AO Raiffeisenbank, authenticates with a handwritten signature, signature of the executive of the Client and Client's seal (if any);
 - sends both copies of the «EDS certificate key» to the «ELBRUS Internet» Bank-Client System of AO Raiffeisenbank Bank.

6.7. After checking by the Bank of the «EDS certificate key» for the «ELBRUS Internet» Bank-Client System of AO Raiffeisenbank received from the User and checking with the «Request a certificate» ED, the document is signed by the Bank, one (1) copy is returned to the User and the User is given access to the procedures in the System.

6.8. The Bank performs the registration and activation of the Public EDS key within 2 (two) working days after receiving the «EDS key certificate» for «ELBRUS Internet» Bank-Client System.

After the activation of the Public EDS key in the System the User can sign ED with an EDS.

6.9. After the registration and activation of the Public EDS key in the Bank, the User with the signature rights, as well as access rights CC

правами доступа Подписант ВК, Контролер, Ревизор: Signatory, Controller, Auditor:

- выполняет вход в Систему;
- получает выписки о движении денежных средств по Счету;
- формирует, подписывает и передает в Банк ЭД через поле «Письмо в Банк» с информацией о завершении установки Системы в соответствии с образцом (см. ниже), которое является подтверждением ввода Системы в эксплуатацию.

- logs on to the System;
- receives statements on the movement of funds on the Account;
- generates, signs and submits to the Bank EDs through the "Letter to the bank" field with the information about the completion of the installation of the System in accordance with the sample (see. below), which is a confirmation of the commissioning of the System.

Образец сообщения:

«_____ (указать полное наименование Клиента) сообщает, что подключение к Системе прошло успешно».

6.10. По завершении работы Пользователь выполняет выход из Системы и извлекает Устройство USB-token (при его наличии).

6.11. Для подключения/отключения Пользователей или изменения параметров Услуги «ELBRUS mobile» Подписант:

- выполняет вход в Систему;
- выбирает раздел «Дополнительные услуги»;
- выбирает раздел «Mobile»;
- создает запрос на новую услугу. В запросе будет указано наименование организации Клиента;
- подтверждает созданную услугу подписью, тем самым активируя услугу.

Запрос на подключения/отключение Услуги «ELBRUS mobile» подписывает Подписант I группы подписей или обладающий единственной подписью согласно КОП.

6.12. Для подключения/отключения Пользователей или изменения параметров Услуги «SMS для Бизнеса» Пользователь:

- выполняет вход в Систему;
- выбирает раздел «Дополнительные услуги»;
- выбирает наименование организации;
- канал доставки – номер телефона и/или адрес электронной почты;
- формирует запрос в Банк.

Запрос на подключения/отключение Пользователей или изменения параметров Услуги «SMS для Бизнеса» подписывает Подписант I группы подписей или обладающий единственной подписью согласно КОП.

6.13. Для подключения/отключения Пользователей или изменения параметров Услуги «SMS-ОТП» Пользователь, обладающий правом подписи:

Sample message:

«_____ (Insert the full name of the Client) reports that the connection to the System was successful».

6.10. Upon the completion of the work the User exits the System and removes the USB-token device (if any).

6.11. To connect/disconnect users or modify the parameters of the «ELBRUS mobile» Services, a Signatory:

- logs on to the System;
- selects the «Additional services» section;
- select «Mobile» section;
- makes a request for a new service. The request will indicate the name of the organization of the Client;
- It confirms the created service with a signature thereby activating the service.

The request for activation/deactivation of the «ELBRUS mobile» service is signed by a Signatory of I Group of signature or having an exclusive signature or the signature according to the SSC.

6.12. To connect/disconnect Users or modify the parameters of «SMS for Business» service, a User:

- logs on to the System;
- selects the «Additional services» section;
- selects the name of the organization;
- delivery channel - the telephone number and/or e-mail address;
- generates a request to the Bank.

A request for connecting/disconnecting of Users or changing the settings of the «SMS for business» services is signed by a Signatory of I Group of signatures or having an exclusive signature according to the SSC.

6.13. To connect/disconnect Users or modify the parameters of the «SMS-OTP» service, a User with the right to sign:

- выполняет вход в Систему;
- выбирает раздел «Дополнительные услуги»;
- выбирает раздел «SMS-ОТР»;
- создает запрос на новую услугу. В запросе необходимо указать Уполномоченное лицо, которому подключается «SMS-ОТР»;
- подтверждает созданную услугу подписью, тем самым активируя услугу.

7. ОБСЛУЖИВАНИЕ КЛИЕНТА.

7.1. Режим обслуживания Клиента:

Банк осуществляет прием ЭД, передаваемых по Системе с 08:00 до 20:00 МСК по Рабочим дням.

7.2. Банк оставляет за собой право отключать Систему для проведения профилактических работ:

- в Рабочие дни: с 20:00 до 08:00 МСК;
- в дни, не являющиеся Рабочими днями.

7.3. Банк осуществляет исполнение ЭД Клиента в сроки, установленные Сроками предоставления расчетных документов (распоряжений) и документов валютного контроля для исполнения текущим рабочим днем, размещенными на сайте Банка в сети Интернет по адресу <http://www.raiffeisen.ru>.

7.4. Временем получения Банком ЭД Клиента является время присвоения конкретному ЭД статуса «Принят».

Временем исполнения Банком ЭД Клиента является время присвоения конкретному ЭД статуса «Исполнен».

7.5. В целях исполнения требований Федерального Закона № 173-ФЗ от 10.12.2003 г. «О валютном регулировании и валютном контроле» и нормативных актов Банка России в области валютного регулирования и валютного контроля, Клиент посредством Системы предоставляет в Банк документы для целей валютного контроля в виде подписанных ЭП ЭД, в т.ч. содержащих прикрепленные Скан-копии обосновывающих документов. При этом датой получения указанных ЭД Банком является дата присвоения документу в Системе статуса «Принят», при условии, что ЭД и прикрепленные Скан-копии обосновывающих документов получены Банком в Рабочий день.

В том случае, если указанные выше документы переданы Клиентом через Систему в Банк в день, не являющийся Рабочим днем, то документы считаются принятыми Банком в первый Рабочий день, следующий за днем их передачи Клиентом через Систему, не

- logs on to the System;
- selects the «Additional services» section;
- chooses «SMS-ОТР» section;
- makes a request for a new service. The request must specify the Authorized person to whom «SMS-ОТР» connects;
- It confirms the created service with a signature, thereby activating the service.

7. CLIENT SERVICE.

7.1. Client service mode:

The Bank receives EDs transmitted over the System from 08:00 to 20:00 Moscow time on weekdays.

7.2. The Bank reserves the right to turn off the System for maintenance:

- on weekdays: from 20:00 to 08:00 Moscow time;
- during non-working days.

7.3. The Bank shall execute the Client's ED in the prescribed period of presenting settlement documents (orders) and currency control documents for the execution of the current working day, placed on the Bank's website on the Internet at <http://www.raiffeisen.ru>.

7.4. The time of receipt of by the Bank of the Client's EDs is the time of assigning to a particular ED of the «Accepted» status.

The time of execution by the Bank of the Client's EDs is the time of assigning to a particular ED of the «Executed» status.

7.5. In order to fulfil the requirements of Federal Law 173-FZ of 10.12.2003 «On Currency Regulation and Currency Control» and normative acts of the Bank of Russia in the field of currency regulation and currency control, the Client provides the Bank with the documents for currency control purposes in the form of EDs signed with a ED via the System, including containing attached scanned copies of supporting documents. In this case the date of receipt of the said EDs by the Bank is the date of assigning to the document in the System of the «Accepted» status, provided that the EDs and the attached scanned copies of supporting documents are received by the Bank on the Working Day.

In the event that the above documents are sent by the Client through the System to the Bank on the day that is not a Working Day, the documents are considered accepted by the Bank on the first Working Day following the date of their transfer by the Client through the System, that was not a

являвшимся Рабочим днем. Время получения документов Банком фиксируется в соответствии со временем по месту нахождения Банка (филиала Банка), в котором открыты соответствующие Счета Клиента. Датой принятия Документов ВК Банком в целях исполнения валютного законодательства РФ является дата присвоения в Системе статуса «Обработан ВК». Датой отказа в приеме Документов ВК Банком является дата присвоения в Системе статуса «Отказан ВК».

7.6. Временем получения Клиентом ЭД, направленного Банком Клиенту, является присвоение документу в Системе статуса «Принят» (вне зависимости от того, когда Клиент осуществлял вход в Систему).

8. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА.

8.1. Контакты Службы поддержки клиентов, использующих функционал Системы Банк-Клиент «ELBRUS Internet»:

Телефоны: +7 (495) 225-9192
8 (800)700-99-95 (звонок
бесплатный по России)

График работы: ежедневно с 09:00 до 18:00 МСК, кроме дней, не признаваемых Рабочими днями.

8.2. Служба поддержки осуществляет консультации по настройке и работе с Системой:

Электронная почта: elbrus@raiffeisen.ru
Форма обратной связи на сайте Системы:
<http://elbrus.raiffeisen.ru/>, меню «Обратная связь».

Working Day. The time of reception by the Bank of the documents is registered in accordance with the time at the location of the Bank (Bank branch), where the relevant Client's Accounts are opened. The date of reception of the CC document by the Bank to abide the currency legislation of the Russian Federation is the date of the assignment in the System of the «Processed by the CC» status. The date of the refusal to accept the CC documents by the Bank is the date of the assignment in the System of the «Denied by the EC» status.

7.6. The time of reception of an ED sent the Bank by the Client is the time of assignment to a document in the System of the «Accepted» status (regardless of the time the client logs on to the System).

8. TECHNICAL SUPPORT.

8.1. Contacts of the Client support for the clients using the software and hardware of the«ELBRUS Internet» Bank-Client System:

Telephones: +7 (495) 225-9192
8 (800)700-99-95 (toll-free in
Russia)

Working hours: daily from 09:00 to 18:00 Moscow time, except for the days that are not recognized as weekdays.

8.2. Client support provides advice on setting up or working with the System:

Email: elbrus@raiffeisen.ru
The feedback form on the System website:
<http://elbrus.raiffeisen.ru/>, the menu «Contact Us».

**Порядок разрешения разногласий при
обмене (в связи с обменом) электронными
документами (далее – «ЭД»), заверенными
электронной подписью (далее – «ЭП»).**

**Procedure for settlement of disputes in the
exchange (in connection with the exchange) of
electronic documents (hereinafter – «ED»),
certified with a digital signature
(hereinafter – «DS»).**

1. Согласительная комиссия (далее – **Комиссия**) создается с целью разрешения разногласий, возникших между Банком и Клиентом при обмене (в связи с обменом) ЭД, установления фактических обстоятельств, послуживших основанием возникновения разногласий, а также для проверки целостности и подтверждения подлинности ЭД.

1. The Conciliation Commission (hereinafter - **the Commission**) is created in order to resolve disputes arising between the Bank and the Client in the exchange (in connection with the exchange) of EDs, establishing the facts that gave rise to the dispute, as well as to verify the integrity and confirmation of the authenticity of EDs.

2. При возникновении разногласий при обмене (в связи с обменом) ЭД Сторона, заявляющая о наличии разногласия (далее – **Сторона-инициатор**), обязана направить другой Стороне заявление в свободной форме о разногласиях, подписанное уполномоченным лицом, с подробным изложением причин разногласий и предложением создать Комиссию. Заявление должно содержать реквизиты представителей Стороны-инициатора, которые будут участвовать в работе Комиссии, место, время и дату сбора Комиссии (не позднее 7 (Семи) календарных дней со дня отправления заявления).

2. In the event of disagreements during the exchange (in connection with the exchange) of EDs the party claiming the existence of disagreements (hereinafter - **the Initiating Party**), is obliged to send to the other party an application in a free form on the disagreements signed by an authorized person, detailing the reasons for the disagreements, and the proposal to create the Commission. The application must contain details of the representatives of the Initiating Party who will participate in the work of the Commission, the place, time and date of the Commission's gathering (not later than 7 (seven) calendar days from the date of sending of the application).

***Примечание:** До подачи заявления Стороне-инициатору рекомендуется убедиться в целостности своего программного обеспечения, Открытых и Закрытых ключей, а также отсутствии несанкционированных действий со стороны лиц, уполномоченных Клиентом выполнять определенные действия в Системе.*

***Note:** Before submitting the application to the Party-initiator it is recommended to ensure the integrity of the software, public and private keys, as well as the absence of unauthorized actions on the part of the persons authorized by the Client to perform certain actions in the System.*

3. В состав Комиссии должно входить равное количество представителей каждой Стороны (не менее 3 (Трех) человек, включая представителей службы безопасности, юридической службы и иных), а также, в случае необходимости, независимые эксперты. Члены Комиссии от каждой Стороны назначаются приказами, изданными соответствующей Стороной.

3. The Commission shall be composed of an equal number of representatives of each Party (not less than three (3) persons, including members of the security service, legal department and other), as well as, if necessary, independent experts. Members of the Commission shall be appointed by each Party by the orders issued by the corresponding Party.

В случае необходимости привлечения независимых экспертов, эксперт считается назначенным только при согласии обеих Сторон, выраженном в письменной форме. Порядок оплаты работы независимых экспертов в Комиссии определяется по предварительному согласованию Сторон. Эксперты не обладают правом голоса при принятии решения

If it is necessary to involve independent experts, the expert considered designated only with the consent of both parties, expressed in writing. The salary of independent experts of the Commission is determined by a prior agreement between the Parties. Experts do not have a voting right in the decision-making process of the Commission.

Комиссией.

4. Комиссия создается на срок до 15 (Пятнадцати) Рабочих дней. В исключительных случаях, по согласованию Сторон, срок работы Комиссии может быть продлен до 30 (Тридцати) Рабочих дней.

5. Стороны обязуются способствовать работе Комиссии и не допускать отказа от представления необходимых документов.

6. Стороны обязуются предоставить Комиссии возможность ознакомления с условиями и порядком работы своих Аппаратных средств и программного обеспечения, используемых для работы с Системой.

7. В ходе работы Комиссии каждая Сторона обязана доказать, что она исполнила обязательства по настоящему Соглашению надлежащим образом. Результатом деятельности Комиссии является определение Стороны, несущей ответственность по фактам, вызвавшим разногласия.

8. К разногласиям, связанным с корректностью использования ЭП относятся разногласия, возникающие в связи с непризнанием одной из Сторон факта принадлежности ЭП по ЭД конкретному Подписанту и/или содержимого ЭД, подписанного ЭП.

8.1. Действия комиссии при использовании Ключей УЭП

Комиссии при необходимости передаются: Открытые ключи УЭП Банка и Открытые ключи УЭП Подписантов Клиента. Распечатки Открытых ключей УЭП Банка и Подписантов Клиента сравниваются с соответствующими Сертификатами ключа подписи. При положительном результате сравнения, проверенные Открытые ключи принимаются к использованию в дальнейшей работе Комиссии. Комиссия осуществляет подтверждение подлинности оспариваемого ЭД путем проверки УЭП Подписанта(ов) с помощью СКЗИ, используемого в Системе.

Если в результате проверки все проверяемые УЭП для оспариваемого ЭД верны, все проверяемые УЭП используются в соответствии со сведениями, указанными в Сертификатах ключа подписи и Сертификаты ключа подписи действительны, считается установленным, что

- ✓ проверяемый оспариваемый ЭД был сформирован в соответствии с правилами и требованиями использования Системы;
- ✓ проверяемый ЭД был подписан Закрытым ключом УЭП, соответствующим Сертификату ключа подписи, использовавшемуся при

4. The Commission is established for a period of 15 (fifteen) working days. In exceptional cases, by agreement of the Parties, the period of work of the Commission may be extended for up to thirty (30) working days.

5. The Parties undertake to assist the work of the Commission and to prevent non-submission of the required documents.

6. The Parties undertake to provide the Commission with the opportunity to familiarize with the conditions and operation procedure of its hardware and software used to operate in the System.

7. During the work of the Commission, each party is required to prove that it has fulfilled its obligations under this Agreement as appropriate. The goal of the Commission is to identify the parties responsible for the facts that caused the disagreements.

8. The disagreements related to the correct use of DS include the disagreements arising in connection with the non-recognition by one of the Parties of the fact that a particular DS on an ED belongs to a specific Signatory and/or the content of an ED signed with a DS.

8.1. Commission actions when using EDS keys

If necessary the Commission is given: Public EDS Bank keys and public EDS keys of the Client's Signatories. Printouts of Public EDS keys of the Bank and the Client's Signatories are compared with the corresponding Signature key certificates. If the result of the comparison is favourable, the checked Public keys are accepted for use in the further work of the Commission.

The Commission carries out authentication by verifying the disputed ED by verifying of Signatories' EDS(s) using the CIPF used in the System.

If all the examined EDS for the disputed ED are true, all the examined EDS are used in accordance with the information stated in the Signature key certificates and the Signature key certificates are valid, it is deemed established that

- ✓ the examined disputed ED was generated in accordance with the rules and requirements of the System operation;
- ✓ the examined ED was signed with a private EDS key corresponding to the Signature key certificate used in the examination;

- проведении проверки;
- ✓ владельцами Сертификатов ключа подписи являются полномочные Пользователи, зарегистрированные в Системе.

8.2. Действия комиссии при использовании ПЭП:

Комиссия осуществляет подтверждение подлинности оспариваемого ЭД путем проверки корректности ПЭП с помощью вычисления значения Хэш-функции по алгоритму ГОСТ Р 34.11-94 реквизитов ЭД: пароля клиента в Системе и Хэш-функции дайджеста документа⁶ содержащего Одноразовый код, идентификатора ПЭП действовавшего на момент подписания (предоставляется Банком). Значение Хэш-функции сравнивается с полем hash дайджеста документа выгруженного из интерфейса Системы.

Если в результате проверки все проверяемые ПЭП для оспариваемого ЭД верны, считается установленным, что

- ✓ проверяемый оспариваемый ЭД был сформирован в соответствии с правилами и требованиями использования Системы;
- ✓ проверяемый ЭД был подписан ПЭП уполномоченного Пользователя, зарегистрированного в Системе.

9. По результатам работы Комиссия оформляет акт, содержащий:

- фактические обстоятельства, послужившие основанием возникновения разногласий;
- порядок работы членов Комиссии;
- вывод о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого ЭД и соответствующее обоснование.

Акт составляется в 2 (Двух) экземплярах, подписывается всеми членами Комиссии. Каждой из Сторон Комиссия направляет по одному экземпляру акта для принятия решения. Члены Комиссии, не согласные с мнением большинства, подписывают акт с особым мнением, которое прикладывается к акту.

10. В случае если на предложение Стороны-инициатора о создании Комиссии ответ другой стороны не был получен, или получен отказ от участия в работе Комиссии, или если другой Стороной чинились препятствия в работе Комиссии, Сторона-инициатор вправе составить акт в одностороннем порядке с указанием причины его составления. В акте приводится обоснование выводов о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого ЭД. Указанный

- ✓ the Signature key certificate holders are the authorized Users registered in the System.

8.2. Commission Actions in case of use of SES:

The Commission carries out authentication of the disputed ED by verifying the correctness of SDSs by calculating the hash value according to the GOST R 34.11-94 algorithm of the ED details: client's password in the System and hash function of the document digest⁶ containing the one-time code, SDS ID in force at the time of signing (provided by the Bank). The hash value is compared with the hash digest field of the document uploaded from the System interface.

If in the course of the examination it is established that all the examined SDSs for the disputed ED are true, it is considered established that

- ✓ the examined disputed ED was generated in accordance with the rules and requirements of the System operation;
- ✓ the examined ED was signed with SDSs of authorized users registered in the System.

9. The Commission draws up an act on the results containing:

- The facts that were the basis of a dispute;
- order of work of the Commission members;
- The conclusion on the authenticity (falsity, reception, transfer, revocation, etc.) of the disputed ED and corresponding justification.

The certificate is made in 2 (two) copies signed by all members of the Commission. The Commission shall send each of the Parties one copy of the act to make a decision. Commission members who disagree with the majority opinion, sign the act with the dissenting opinion, which is attached to the act.

10. If a proposal of the Initiating Party on the creation of the Commission receives no response from the other party, or gets a refusal to participate in the work of the Commission, or if the other Party have hampered the work of the Commission, the Initiating Party has the right to unilaterally draw up an act indicating the reasons for its drawing up. The act provides a rationale for the conclusions about the authenticity (falsity, reception, transfer, revocation, etc.) of the disputed ED. This act is made in two copies, signed by an authorized officer

⁶ Набора подписываемых полей ЭД.
Set of signed ED fields.

акт составляется в двух экземплярах, подписывается уполномоченным должностным лицом Стороны-инициатора, и один экземпляр направляется другой Стороне.

11. Акт Комиссии является основанием для принятия Сторонами окончательного решения, которое должно быть подписано Сторонами не позднее 10 (Десяти) Рабочих дней со дня окончания работы Комиссии.

12. В случае непринятия Сторонами решения в установленный срок, а также в случае непредставления другой Стороной ответа на Акт, составленный Стороной-инициатором, Сторона-инициатор вправе обратиться в суд в соответствии с положениями Соглашения.

of the Initiating Party, and one copy is sent to the other Party.

11. The Commission's Act is the basis for the Parties to make the final decision, which shall be signed by the parties no later than 10 (ten) working days from the end of the work of the Commission.

12. In the event of failure of the Parties to make a decision within the prescribed period and in the case of non-response by the other Party on the Act, drawn up by the Initiating Party, the Initiating Party shall have the right to apply to court in accordance with the provisions of the Agreement.

Приложение № 4
к Соглашению об общих правилах и условиях
предоставления банковских услуг
с использованием системы
Банк-Клиент «ELBRUS Internet»

Annex no. 4
to the Agreement on general terms and conditions
of banking services
with the use of the «ELBRUS Internet»
Bank-Client System

**ИНФОРМАЦИОННАЯ КАРТОЧКА
КЛИЕНТА**

CLIENT INFORMATION CARD

Наименование
юридического
лица/филиала или
представительства/
ФИО индивидуального
предпринимателя:

Name of the legal
entity/branch or
representative office/
Name of the individual
entrepreneur:

ИНН/КИО _____

TIN/FCC _____

Список Подписантов Клиента

Client's Signatories List

№ п/п/ No. item	Ф.И.О. уполномоченного лица/ Name of the authorized person	Группа, к которой Клиентом отнесена подпись/The group to which the Client assigned the signature ⁷
		« »
		« »
		« »
		« »
		« »
		« »
		« »
		« »

Руководитель _____

(Должность, подпись, ФИО)

Executive _____

(Position, signature, name)

Дата подписания

« ____ » _____ 20 ____ г.

М.П.

Date of signing

« ____ » _____ 20 ____ г.

L.S.

⁷ Указывается «1», если Подписант относится к I группе подписей или может подписывать ЭД единственной подписью согласно КОП; указывается «2», если Подписант относится ко II группе подписей согласно КОП.

«1» is indicated if the signatory belongs to I group or signatures or may sign EDs only with the exclusive signature according to the SSC; «2» is indicated if the signatory belongs to II group of signatures according to the SSC.

Приложение № 5
к Соглашению об общих правилах и условиях
предоставления банковских услуг
с использованием системы
Банк-Клиент «ELBRUS Internet»

Annex no. 5
to the Agreement on general terms and conditions
of banking services
with the use of the «ELBRUS Internet»
Bank-Client System

ДОВЕРЕННОСТЬ

PROXY NOTICE

г. _____, «__» _____ 20__ года.

the city of _____, _____, 20__.

_____ (наименование
Клиента), в _____ лице
_____ (должность
руководителя), действующего на основании
_____, уполномочивает

_____ (*Client's name*),
represented by _____
(*position of the executive*), acting on the basis of
_____, authorizes

_____ (фамилия,
имя, отчество полностью), паспорт серии
_____ № _____, выдан
_____ (когда, кем),
проживающего(-ую) по адресу:
_____, телефон
_____.

_____ (*Name,*
surname, patronymic), passport series _____ No.
_____, issued by _____
_____ (*when, by*
whom), residing at:
_____, telephone
_____.

в рамках заключенного между АО
«Райффайзенбанк» как Банком и
_____ (наименование
Клиента) как Клиентом Соглашения об общих
правилах и условиях предоставления
банковских услуг с использованием Системы
Банк-Клиент «ELBRUS Internet» от «__»
_____ 20__ г. (далее – Соглашение)
совершать действия⁸ в Системе Банк-Клиент
«ELBRUS Internet» (далее – Система):

under the Agreement on general terms and
conditions of banking services using the «ELBRUS
Internet» Bank-Client System, concluded between
АО «Raiffeisenbank» as the Bank and
_____ (*Client's name*) as the
Client dated _____, 20__
(hereinafter – Agreement) to operate⁸ in the
«ELBRUS Internet» Bank-Client System
(hereinafter – System):

- с правом доступа «Оператор», создавать и просматривать электронные документы;
- с правом доступа «Контролер», создавать, просматривать и подписывать электронной подписью электронные документы ;
- с правом доступа «Ревизор», создавать и просматривать электронные документы, создавать и подписывать шаблоны электронных документов, что блокирует возможность Пользователям создавать ЭД не по шаблону;
- с правом доступа «Подписант документов ВК», принимать от Банка, составлять, просматривать, подписывать и направлять в Банк Документы ВК;
- с правом доступа «Подписант», создавать, просматривать и подписывать электронные документы [подписью, относящейся к первой группе подписей] [подписью, относящейся ко второй группе подписей] [единственной подписью] (*один Подписант не может быть уполномочен и на подпись, относящуюся и к первой, и ко второй группе подписей*) с использованием Электронной подписи, без

- with the «Operator» authorization access, create, and view electronic documents ;
- with the «Controller» authorization access, create, view and sign electronic documents with the electronic signature ;
- with the «Auditor» authorization access, create, and view electronic documents, create and sign templates of electronic documents that blocks a possibility to create E-Documents by Users other than template;
- with the «CC Signatory» authorization access, accept from the Bank, create, view, sign and send CC Documents to the Bank;
- with the «Signatory» authorization access, create, view and sign electronic documents [signature belonging to the first group of signatures] [signature belonging to the second group of signatures] [exclusive signature] (*one Signatory cannot be authorized on the signature, belonging to both the first and the second group of signatures*) with the use of a Digital signature, without right of signing of paper based documents,

⁸ Подробное описание ролей Пользователей и Уровня доступа, а также терминов, используемых по тексту настоящей Доверенности, описаны в Соглашении.

Detailed description of Users' roles and Access level as well as terms used in the text of this Proxy notice are described in Agreement.

права подписи документов на бумажном носителе, используя собственноручную подпись.

with personal handwritten signature.

Доверенность выдана без права передоверия.

The Proxy notice is issued without the right of delegation.

Срок действия доверенности по «__» ____
20__ г. включительно.

The Proxy notice expires on _____
____, 20__ inclusive

_____/_____/_____
(Должность) (подпись) (ФИО)
М.П.

_____/_____/_____
(Position) (signature) (Name)
L.S.

Приложение № 6
к Соглашению об общих правилах и условиях
предоставления банковских услуг
с использованием системы
Банк-Клиент «ELBRUS Internet»

Annex no. 6
to the Agreement on general terms and conditions
of banking services
with the use of the «ELBRUS Internet»
Bank-Client System

З А Я В Л Е Н И Е

APPLICATION

НА ПОДКЛЮЧЕНИЕ / ОТКЛЮЧЕНИЕ/
ПОЛЬЗОВАТЕЛЕЙ ОТ СИСТЕМЫ БАНК-КЛИЕНТ
«ELBRUS Internet» / НА ВЫДАЧУ УСТРОЙСТВА USB-
token / РЕГИСТРАЦИОННЫХ ДАННЫХ (ПИН-
конвертов)

FOR CONNECTING / DISCONNECTING OF USERS
TO/FROM THE «ELBRUS Internet» BANK-CLIENT
SYSTEM / FOR OBTAINING A USB-token DEVICE /
REGISTRATION DATA (PIN envelopes)

Наименование
юридического
лица/филиала или
представительства/
ФИО индивидуального
предпринимателя: _____

Name of the legal
entity/branch or a
representative office/
Name of the individual
entrepreneur: _____

ИНН/КИО

TIN/FCC

Прошу Банк:

I hereby request the Bank to perform the following actions:

№ п/п/ No. item	Ф.И.О. уполномоченного лица/ Name of the authorized person	Паспортные данные уполномоченного лица/ Passport data of the authorized person	Право доступа/ right of access	Подключить к Системе/ Connect to the System	Отключить от Системы/ Disconnect from the System	Выдать Устройство USB-token/ Hand out the USB-token device	Выдать Регистрацион ные данные/ Hand out the registration data
			Оператор / Operator	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
			Подписант ВК/ CC Signatory	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			Контролер / Controller	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			Ревизор / Auditor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			Подписант (I группа подписей или единственная подпись) / Signatory (I group of signatures or an exclusive signature)	<input type="checkbox"/> ⁹	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			Подписант (II группа подписей)/ Signatory (II group of signatures)	<input type="checkbox"/> ⁹	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Руководитель
(Должность)

Executive
(Position)

_____)

_____)

Дата и
печать

Date and
stamp

⁹ Графа «Подключить к Системе» заполняется для Подписанта I, II группы подписей или единственной подписи в случае, если право подписи предоставляется на основании Доверенности (Приложение 5 к данному Соглашению).
The field «Connect to the System» is filled out for Signatory of I, II group of signatures or an exclusive signature in case of the right of signing is provided on the basis of the proxy notice (Annex no. 5 to the Agreement).

Приложение № 7
к Соглашению об общих правилах и условиях
предоставления банковских услуг
с использованием системы
Банк-Клиент «ELBRUS Internet»

Annex no. 7
to the Agreement on general terms and conditions of
banking services
with the use of the «ELBRUS Internet»
Bank-Client System

ДОВЕРЕННОСТЬ

PROXY NOTICE

г. _____ «__» _____ 20__ года.

the city of _____, «__» _____ 20__.

_____ (*наименование Клиента*),
в лице _____ (*должность*
руководителя), действующего на основании
_____, уполномочивает

_____ (*Client's*
name), represented by _____
(*position of the executive*), acting on the basis of
_____, authorizes

_____ (*фамилия, имя,*
отчество полностью), паспорт серии _____ № _____
выдан _____ (*когда, кем*),
проживающего(-ую) по адресу:
_____, телефон _____,
_____.

_____ (*Name, surname,*
patronymic), passport series _____ No. _____,
issued by _____ (*when,*
by whom), residing at:
_____, telephone _____,
_____.

получать в АО «Райффайзенбанк» (далее – Банк)
Устройства USB-token и запечатанные ПИН-
конверты, содержащие Средства доступа для входа
в Систему Банк-Клиент «ELBRUS Internet».

to receive in AO Raiffeisenbank (hereinafter - the
Bank) USB-token devices and sealed PIN-envelopes
containing Access Means to access the «ELBRUS
Internet» Bank-Client System

_____/_____
(*Должность*) (*подпись*) (*ФИО*)

_____/_____
(*Position*) (*signature*) (*Name*)

М.П.

L.S.

Приложение № 8
к Соглашению об общих правилах и условиях
предоставления банковских услуг
с использованием системы
Банк-Клиент «ELBRUS Internet»

Annex no. 8
to the Agreement on general terms and conditions
of banking services
with the use of the «ELBRUS Internet»
Bank-Client System

**Согласие Пользователя на передачу его
идентификаторов
в АО «Райффайзенбанк» при подключении
услуги «SMS-ОТР»
(в случае, когда Оператором сотовой связи
Пользователя является ПАО МегаФон)**

**User Consent to the transfer of his identifiers
to AO Raiffeisenbank when enabling
«SMS-ОТР» services
(In the case where the User's mobile phone
operator is PJSC MegaFon)**

Настоящим даю согласие ПАО «МегаФон» (место нахождения: Россия, 115035, г. Москва, Кадашёвская набережная, д. 30; ОГРН 1027809169585, ИНН 7812014560) (далее – Оператор связи) на передачу:

I hereby give my consent to PJSC MegaFon (location: Russia, 115035, Moscow, Kadashevskaya embankment, 30.; OGRN1027809169585, INN 7812014560) (hereinafter - the Service Provider) to the transfer:

- Закрытое акционерное общество «МегаЛабс» (далее – ЗАО «МегаЛабс»; 119180, г. Москва, 2-ой Казачий переулок, 11 строение 1, ОГРН 1057747083767, ИНН 7713556058);
 - Общество с ограниченной ответственностью «ОСК» (далее – ООО «ОСК»; 115114, г. Москва, ул. Летниковская, д.10, стр.1, ОГРН 1057746705631, ИНН 7705658056);
 - Акционерное общество «Райффайзенбанк» (далее – АО «Райффайзенбанк»; 129090, Москва, ул. Троицкая, д. 17, стр. 1, ОГРН 1027739326449, ИНН 7744000302).
- Closed Joint Stock Company MegaLabs (hereinafter - CJSC MegaLabs, 119180, Moscow, 2-oy Kazachiy Lane, 11 Building 1, OGRN 1057747083767, INN 7713556058);
 - Limited Liability Company «OSK» (hereinafter - LLC «OSK», 115114, Moscow, Letnikovskaya street, 10, building 1, OGRN 1057746705631, INN 7705658056);
 - Joint Stock Company Raiffeisenbank (hereinafter - AO Raiffeisenbank, 129090, Moscow, Troitskaya street, 17, building 1, OGRN 1027739326449, INN 7744000302).

В целях предоставления мне услуги «SMS-ОТР» для обеспечения проведения безопасности платежей, осуществляемых с использованием Системы и/или мобильного приложения «ELBRUS Mobile» на условиях настоящего Соглашения, следующих данных:

In order to provide «SMS-ОТР» service to me to ensure the security of the payments made using the System and/or «ELBRUS Mobile» mobile application on the terms of this Agreement, the following data:

- фактическое место нахождения моего абонентского устройства с установленной в нём SIM-картой Оператора связи, для абонентского номера, указанного мною в заявлении на подключение Услуги (далее – Абонентское устройство);
 - факт замены моего Абонентского устройства;
 - факт замены SIM-карты в моём Абонентском устройстве;
 - факт наличия вирусного программного обеспечения в моём Абонентском устройстве;
- the actual location of my subscriber device with installed Operator's SIM-card for the subscriber number, stated by me in the application on the connection of the Service (hereinafter - Subscriber device);
 - the fact of replacement of my Subscriber device;
 - the fact of the replacement of the SIM-card in my Subscriber device;
 - existence of virus software in my Subscriber device;

– факт нахождения Абонентского устройства в сети связи Оператора связи.

– the fact the subscriber device location in the Operator's telecommunications network.

Подтверждаю, что уведомлен о том, что отзыв настоящего согласия возможен путем направления в адрес ПАО «МегаФон» письменного уведомления или посредством интерфейсов, указанных Оператором связи на сайте www.megafon.ru.

I confirm that I am aware that a revocation of the present consent is possible by sending on the address of PJSC MegaFon a written notice or via the interfaces listed by the Operator on www.megafon.ru.

Настоящее согласие является действительным до момента его отзыва¹⁰.

This consent is valid until its revocation¹⁰.

(Должность) _____
()

Дата и
печать

(Position) _____
()

Date and
stamp

¹⁰ В случае отзыва Подписантом настоящего Согласия на передачу идентификаторов в АО «Райффайзенбанк», Банк производит отключение услуги «SMS-ОТР» для данного Пользователя. Также услуга «SMS-ОТР» прекращает предоставляться, если к ней был подключен единственный номер мобильного телефона Подписанта, который отозвал Согласие.
In case of withdrawal by the Signatory of this consent to transfer the identifiers to AO Raiffeisenbank, the Bank disables the «SMS-ОТР» service for the User. Also, «SMS-ОТР» service is no longer provided, if it was connected to the only mobile phone number of the Signatory, who withdrew consent.