

**АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ  
БАНК «ЕВРОФИНАНС МОСНАБАНК»  
(акционерное общество)**

**(АО АКБ «ЕВРОФИНАНС МОСНАРБАНК»)**

**УТВЕРЖДЕНО**

**Протокол заседания Правления Банка  
от «22» августа 2019 г. №38**

**СОГЛАШЕНИЕ  
об использовании электронной системы  
дистанционного банковского  
обслуживания**

**Москва  
2019 г.**

**Eurofinance Mosnarbank**

**APPROVED**

**Board Meeting Protocol  
dated august 22, 2019 No. 38**

**AGREEMENT  
on the use of an electronic system for  
remote banking services**

**Moscow  
2019**

## СОГЛАШЕНИЕ

### об использовании электронной системы дистанционного банковского обслуживания

Настоящее Соглашение об использовании электронной системы дистанционного банковского обслуживания (далее – Соглашение) является договором присоединения в соответствии со ст.428 Гражданского кодекса Российской Федерации, и заключается в порядке, установленном настоящим Соглашением.

#### **Термины и определения**

В настоящем Соглашении следующие определения имеют следующее значение.

**Акт признания Открытого ключа ЭП** - документ на бумажном носителе, выдаваемый Банком Клиенту/Уполномоченному представителю Клиента, в котором Стороны удостоверяют факт передачи Технологических ключей, Сертификата Технологического ключа.

**Банк** – АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «ЕВРОФИНАНС МОСНАРБАНК» (акционерное общество) (полное наименование), АО АКБ «ЕВРОФИНАНС МОСНАРБАНК» (сокращенное наименование), адрес: 121099, г. Москва, ул. Новый Арбат, д.29, официальный сайт в сети «Интернет»: [www.evrofinance.ru](http://www.evrofinance.ru), генеральная лицензия на проведение банковских операций №2402, выданная Банком России 23.07.2015.

**Владелец сертификата ключа проверки ЭП** – Клиент, на имя которого Банком выдан Сертификат Технологического ключа и Сертификат Рабочего ключа.

**Документация** - все руководства, инструкции, рекомендации о мерах безопасности при совершении электронного документооборота в Системе, технические описания и другая документация, касающаяся Системы, которые передаются Банком Клиенту в электронном виде по акту об оказании услуг по установке Системы.

## AGREEMENT

### on the use of an electronic system for remote banking services

This Agreement on the use of an electronic system for remote banking services (the Agreement) is a joinder agreement as per Article 428 of the Civil Code of the Russian Federation and is entered into in accordance with the procedure established hereby.

#### **Terms and definitions**

In this Agreement, the following definitions shall have the following meanings.

**Act of acknowledgement of an ES Public Key** – document on paper, issued by the Bank to the Client/Authorized Representative of the Client, in which the Parties confirm the fact of transfer of Technological Keys, Technological Key Certificate.

**Bank** – Evrofinance Mosnarbank, address: 29 Novy Arbat Street, Moscow, 121099, official website in the Internet: [www.evrofinance.ru](http://www.evrofinance.ru), general license for banking transactions No. 2402 issued by the Bank of Russia on 07.23.2015.

**Holder of the ES verification key certificate** – a Client, to whose name the Bank has issued a Technological Key Certificate and an Operational Key Certificate.

**Documentation** – all the manuals, instructions, recommendations on security matters for electronic document flow in the System, functional descriptions and other documentation, relating to the System, which are transferred by the Bank to the Client in electronic format under the act of System installation services.

**Договор об использовании ДБО** - договор об использовании электронной системы дистанционного банковского обслуживания (по форме Банка), заключенный между Клиентом и Банком, с помощью которого Клиент присоединяется к Соглашению в целом в соответствии со статьей ст.428 Гражданского кодекса Российской Федерации. Заключение Договора об использовании ДБО осуществляется в порядке, установленном Соглашением.

**Закрытый ключ ЭП** – уникальная последовательность символов, известная только Владельцу сертификата ключа проверки ЭП и Уполномоченному представителю Клиента, предназначенная для создания в Электронных документах ЭП и идентификации Уполномоченного представителя Клиента в Системе, и однозначно связанная с Открытым ключом ЭП.

**Квитанция** – электронное сообщение о приеме Электронного документа Стороны-отправителя Стороной-получателем или смене статуса документа Стороной-получателем в процессе обработки. Получение квитанции в Системе влечет за собой смену статуса документа в Системе Стороны-отправителя.

**Клиент** – юридическое лицо, заключившее с Банком Соглашение путем присоединения к нему.

**Ключ (и)** – совместно или, если указано особо, отдельно, Открытый ключ ЭП, Закрытый ключ ЭП, Секретный и открытый ключи шифрования.

**Кодовое слово** – последовательность символов, известная только Клиенту и Банку, используемая для идентификации Клиента при телефонном разговоре с Клиентом в целях подтверждения/неподтверждения возобновления исполнения операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента. Кодовое слово может использоваться многократно. Кодовое слово указывается в Договоре об использовании

**Contract on the Use of RBS** – a contract on the use of an electronic system for remote banking services (in the Bank’s format) between the Client and the Bank, whereby the Client joins the Agreement as a whole in accordance with Article 422 of the Civil Code of the Russian Federation. The Contract on the Use of RBS shall be entered into in accordance with the procedure established hereby.

**ES Private Key** – a unique symbol sequence known only to the Holder of the ES verification key certificate and the Authorized Representative of the Client and designed for generation of Electronic Signatures in the Electronic Documents and identification of the Authorized Representative of the Client in the System, and uniquely associated with the ES Public Key.

**Receipt confirmation** – an electronic message on the reception of the Electronic document sent by the Sending party and received by the Receiving party or the change of the document status by the Receiving party during processing. Reception of the receipt confirmation in the System entails a change in the document status in the System of the Sending party.

**Client** – a legal entity that has entered into the Agreement with the Bank by joining it.

**Key(s)** – jointly or, if specified so, separately, the ES Public Key, ES Private Key, Secret and Public Encryption Keys.

**Code word** – a symbol sequence known only to the Client and the Bank, used to identify the Client during a telephone conversation with the Client in order to confirm/not confirm the resumption of a transaction with signs of money transfer without the consent of the Client. The Code Word may be used more than once. The Code Word shall be specified in the Contract on the Use of RBS and may be changed in the procedure established by the Agreement.

ДБО и может быть изменено в порядке, предусмотренном Соглашением.

**Компрометация ключей** – возникновение подозрений в том, что используемые Ключи доступны лицам, не имеющим на то полномочий. К событиям, влекущим за собой Компрометацию ключей, относятся, включая,

- утрата носителей с Ключами;
- утрата носителей с Ключами с последующим обнаружением;
- доступ посторонних лиц (не Уполномоченных представителей Клиента) к Ключам, использование Ключей без согласия Клиента;
- другие события, которые, по мнению Сторон, свидетельствуют о наличии возможности Несанкционированного доступа третьих лиц к Ключам.

**Конфиденциальная информация** – любая информация (сведения), которой Стороны обмениваются в соответствии с настоящим Соглашением и которая носит частный, непубличный и конфиденциальный характер и имеет действительную или потенциальную ценность в силу ее неизвестности третьим лицам.

**Несанкционированный доступ** – доступ к Системе (в том числе, к Электронным документам), ее использование лицами, не имеющими на то полномочий.

**Открытый ключ ЭП** – уникальная последовательность символов, соответствующая Закрытому ключу ЭП, доступная любому пользователю Системы и предназначенная для проверки подлинности ЭП в Электронном документе и его целостности.

**Плановая смена рабочих ключей** – создание Уполномоченным представителем Клиента новых Рабочих ключей, которое осуществляется до истечения срока действия действующего Рабочего ключа.

**Подсистема** – одна из двух подсистем Системы:

- подсистема «Клиент-Банк», в соответствии с которой на персональный компьютер

**Key compromise** – suspicions that the used Keys are accessible to unauthorized third parties. Events entailing the Key Compromise include, but not limited to the following:

- loss of media with the Keys;
- loss of media with the Keys with their subsequent finding;
- access by third parties (other than the Authorized Representatives of the Client) to the Keys, use of the Keys without consent of the Client;
- other events, which according to the Parties evidence the possibility of Unauthorized Access of third parties to the Keys.

**Confidential information** – any information (data), which the Parties exchange in compliance to the present Agreement and which bears a private, non-public and confidential nature and has actual or potential value due to its obscurity to third parties.

**Unauthorized Access** – access to the System (including Electronic Documents), its use by the persons who do not have the authorization to do so.

**ES Public Key** – a unique symbol sequence, corresponding to the ES Private Key accessible to any user of the System and designed for verification of authenticity of the Electronic Signature within the Electronic Document, as well as a check on its entirety.

**Planned change of Operational Keys** – generation of new Operational Keys by the Client's Authorized Representative before the expiry of the current Operational Key.

**Subsystem** – one of two subsystems of the System:

- the Client-Bank subsystem, in accordance with which the Client program is installed on

Клиента устанавливается программа «Клиент», которая хранит все свои данные на этом персональном компьютере или на сетевых ресурсах Клиента;

- подсистема «Интернет клиент-банк», в соответствии с которой Клиент, используя стандартный браузер операционной системы своего персонального компьютера, получает доступ к указанной подсистеме и ее данным, размещенным на сервере Банка.

**Проверка ЭП Электронного документа** - проверка соотношения, связывающего хэш-функцию Электронного документа, ЭП такого документа и Открытого ключа ЭП подписавшего абонента. Если такая проверка, произведенная на Средствах защиты информации, даст положительный результат, то ЭП признается правильной, а сам Электронный документ – подлинным, без искажений, в противном случае Электронный документ считается ошибочным, а ЭП под ним - недействительной.

**Рабочий день** – рабочий день, признаваемый таковым применимым к деятельности Сторон законодательством каждой из Сторон.

**Рабочие ключи** – Ключи, предназначенные для подтверждения авторства, целостности и конфиденциальности Электронных документов, передаваемых в Системе. Рабочие ключи формируются Уполномоченным представителем Клиента самостоятельно посредством Системы. Срок действия Рабочих ключей составляет 36 месяцев с даты формирования запроса на создание Сертификата Рабочего ключа.

**Секретный и открытый ключи шифрования** – Ключи, используемые для процедуры шифрования и дешифрования Электронных документов. При шифровании используется открытый ключ Стороны-получателя, при расшифровании секретный ключ Стороны-получателя.

**Сертификат Рабочего ключа** - электронный документ с ЭП Банка, содержащий Открытый ключ ЭП и шифрования, а также сведения, идентифицирующие Уполномоченного

the Client's personal computer, which stores all of its data on such personal computer or in the Client's network;

- the Internet Client-Bank subsystem, whereby the Client uses the standard browser of the operating system of his/her personal computer to access the subsystem and its data placed on the Bank's server.

**Check of the Electronic Signature of an Electronic Document** – check on the interrelation between the Electronic document connecting the hash function, Electronic Signature of such document and an Electronic Signature Open Key of the signing subscriber. If such check, conducted with the information security product, provides a positive result, then the Electronic Signature is acknowledged as correct, and the Electronic document is found authentic, without distortions, otherwise the Electronic Document is found faulty, and the Electronic Signature thereto as invalid.

**Business day** – business day that is found as under the legislation, of each of the Parties, applicable to the operations of the Parties.

**Operational keys** – Keys provided for the confirmation of authorship, entirety and confidentiality of the Electronic Documents, transmitted within the System. Operational Keys are generated independently by the Client's Authorized Representative by means of the System. The validity period of Operational Keys is 36 months from the date of the request for an Operational Key Certificate.

**Secret and Public Encryption Keys** - Keys used for encrypting and decrypting Electronic Documents. When encrypting, the Public Key of the recipient Party is used. When decrypting, the Secret Key of the recipient Party is used.

**Operational Key certificate** – an electronic document with the Bank's ES containing ES Public and Encryption Keys, as well as the information, identifying the Authorized

представителя Клиента. Сертификат предназначен для подтверждения подлинности ЭП и идентификации Уполномоченного представителя Клиента в Системе.

**Сертификат Технологического ключа** - электронный документ с ЭП Банка, содержащий Открытые ключи ЭП и шифрования, а также сведения, идентифицирующие Уполномоченного представителя Клиента. Сертификат предназначен для создания Рабочих ключей Уполномоченного представителя Клиента в Системе. Выдается Банком Клиенту/Уполномоченному представителю Клиента в электронном виде и на бумажном носителе по Акту признания Открытого ключа ЭП.

**Система** – корпоративная информационная система дистанционного банковского обслуживания, организованная Банком, представляющая собой комплекс программно-технических средств и организационных мероприятий для создания, защиты, передачи и обработки Электронных документов по открытым каналам связи, в том числе с использованием сети «Интернет». Система используется как электронное средство платежа и обеспечивает создание ЭП в Электронном документе с использованием Закрытого ключа ЭП, подтверждение подлинности ЭП в Электронном документе с использованием Открытого ключа ЭП, создание Ключей.

**Средства защиты информации** – сертифицированные криптографические средства, обеспечивающие реализацию следующих функций: создание ЭП в Электронном документе с использованием Закрытого ключа ЭП, проверка ЭП Электронного документа с использованием Открытого ключа ЭП, создание Закрытых и Открытых ключей ЭП, а также создание и использование Секретных и открытых ключей шифрования, шифрование и расшифрование.

**Средства обработки и хранения информации** – программно-аппаратные средства, требования к которым приведены в

Representative of the Client. The Certificate is designed for confirmation of Electronic Signature authentication and identification of the Authorized Representative of the Client in the System.

**Technological Key certificate** – an electronic document containing ES Public and Encryption Keys, as well as the information, identifying the Authorized Representative of the Client. The Certificate is designed for generating Operational Keys of the Authorized Representative of the Client in the System. It is issued by the Bank to the Client/Authorized Representative of the Client in soft and hard versions under the Act of Acknowledgement of the ES Public Key.

**System** – a corporate IT system for remote banking services established by the Bank, which is a set of software and hardware and organizational measures for generating, protecting, transmitting, and processing Electronic Documents through open communication channels, including using the Internet. The System is used as electronic means of payment and provides for ES generation in an Electronic Document using the ES Private Key, confirmation of the ES authenticity in the Electronic Document using the ES Public Key, and generation of Keys.

**Information Security Products** – certified cryptographic tools providing for the following functions: ES generation in an Electronic Document using the ES Private Key, checking the ES of an Electronic Document using the ES Public Key, generation of ES Private and Public Keys, as well as generation and using of Secret and Public Encryption Keys, encryption and decryption.

**Products designed for processing and storage of information** – software and hardware, requirements for which are shown

Приложении №1 к Соглашению.

**Сторона (Стороны)** – Банк и/или Клиент.

**Счет** - счет, открытый Банком Клиенту на момент заключения настоящего Соглашения или счета, которые будут открыты Банком Клиенту в будущем, на основании соответствующих договоров банковского счета (далее – “ДБС”), заключенных между Сторонами.

**Тарифы** - размеры вознаграждения Банка за оказываемые по настоящему Соглашению работы и услуги. Тарифы устанавливаются Банком. Действующие на момент заключения настоящего Соглашения Тарифы доводятся до сведения Клиента при заключении настоящего Соглашения, а также по первому требованию Клиента. Тарифы могут быть изменены Банком в одностороннем порядке, о чем Банк уведомляет Клиента не позднее, чем за 5 (пять) Рабочих дней Банка до даты ввода в действие изменений путем размещения информации в операционном зале Банка, на официальном сайте Банка в сети «Интернет», а также путем передачи указанной информации посредством Системы.

**Технологические ключи** – Ключи Клиента, изготавливаемые Банком и предназначенные для технологической процедуры формирования (подписи) запроса на создание Сертификата Рабочего ключа и для самостоятельного формирования Рабочих ключей Уполномоченным представителем Клиента, действующие до даты формирования Клиентом Рабочего ключа, либо до истечения 36 месяцев с момента изготовления Банком Технологических ключей.

**Уполномоченный представитель Клиента** – физическое лицо, указанное в Данных о Владельце сертификата ключа проверки ЭП, наделенное Клиентом правом подписания Электронных документов ЭП для последующей передачи посредством Системы и/или входа в Систему, создания любых Электронных документов, установления защищенного соединения с Банком для приема и отправки любых

in Annex No. 1 to the Agreement.

**Party (Parties)** – Bank and/or Client.

**Account** – the account opened by the Bank for the Client at the time of the conclusion of the present Agreement or accounts which will be opened by the Bank for the Client in the future, based on the corresponding bank account agreements (hereinafter referred to as “BAA”), concluded between the Parties.

**Tariffs** – amount of remuneration of the Bank for the works and services rendered under the present Agreement. Tariffs are set by the Bank. Tariffs, that are valid at the time of entering into the present Agreement, are brought to the attention of the Client when entering into the present Agreement, as well as at the first request of the Client. Tariffs may be changed by the Bank in a unilateral manner, about which the Bank informs the Client no later than 5 (five) Business days of the Bank before the date of commissioning the changes through posting the information in the operating area of the Bank, on the official web-site of the Bank in the Internet, as well as through the transfer of the said information through the System.

**Technological keys** – the Client’s Keys generated by the Bank and designed for the technological process of generating (signing) a request to generate an Operational Key Certificate and for independent generation of Operational Keys by the Authorized Representative of the Client, valid until the Client generates an Operational Key or within 36 months from date of the Operational Key generation by the Bank.

**Authorized Representative of the Client** – an individual specified in the Information about the ES Verification Key Certificate Holder and empowered by the Client to sign Electronic Documents with an Electronic Signature for subsequent transfer by means of the System and/or logging in the System, to generate any Electronic Documents, to establish a secure connection with the Bank for reception and transmission of any

Электронных документов, подписанных ЭП Клиента, и владеющее Закрытым ключом ЭП, позволяющим создавать ЭП в Электронных документах (подписывать Электронные документы) и идентифицировать Уполномоченного представителя Клиента в Системе.

**Хэш-функция** – алгоритм вычисления контрольной последовательности для произвольных электронных сообщений с целью доказательной проверки их целостности.

**Шифрование** – преобразование данных исходных (открытых) сообщений таким образом, что их смысл становится недоступным для любого лица, не владеющего секретом обратного преобразования.

**Расшифрование** – операция обратная шифрованию.

**Электронная подпись (ЭП)** – реквизит Электронного документа, предназначенный для защиты данного Электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием Закрытого ключа ЭП и позволяющий идентифицировать Владельца сертификата ключа проверки ЭП и Уполномоченного представителя Клиента с правом подписи Электронных документов, а также удостовериться в целостности информации Электронного документа. Для выработки и проверки ЭП используются программные Средства защиты информации «OpenSSL». В рамках настоящего Соглашения под Электронной подписью понимается усиленная неквалифицированная электронная подпись.

**Электронный документ** – электронное сообщение, подписанное ЭП и переданное одной из Сторон другой Стороне посредством Системы, в котором информация представлена в электронной форме, равнозначное документу на бумажном носителе, подписанному собственноручной подписью (собственноручными подписями) уполномоченных лиц Сторон и скрепленному печатью (при ее наличии) в случае

Electronic Documents signed by the Client's Electronic Signature, and possessing a Private Electronic Signature Key, which allows to generate an Electronic Signature in Electronic Documents (to sign Electronic Documents) and to identify the Authorized Representative of the Client in the System.

**Hash function** – calculation algorithm of the control sequence for the random electronic messages for the purpose of evidentiary control of their entirety.

**Encryption** – transformation of the data of original (public) messages in such a way that their meaning becomes inaccessible to anyone who does not possess the secret of reverse transformation.

**Decryption** – reverse operation of encryption.

**Electronic Signature (ES)** – details of an Electronic Document, which are designed for the protection of the given Electronic Document against falsification, received as result of cryptographic transformation of information with the use of a ES Private Key and which allow to identify the ES Verification Key Certificate Holder and the Authorized Representative of the Client entitled to sign Electronic Documents, as well as to assure the entirety and integrity of the information contained in the Electronic Document. The OpenSSL information security software is used to generate and verify an Electronic Signature. For the purposes of this Agreement, an Electronic Signature means a reinforced unqualified electronic signature.

**Electronic Document** – an electronic message, which is signed with ES and transmitted by one of the Parties to the other Party via the System presenting information in an electronic form, and which is equivalent to a hard copy document signed with a handwritten signature (signatures) of the authorized representatives of the Parties and bearing a seal (if applicable), if required.



необходимости.

### **Статья 1. Предмет Соглашения.**

1.1. Стороны устанавливают между собой порядок и условия обмена Электронными документами по Системе в целях проведения на основании Электронных документов банковских операций (в том числе расчетных) по Счетам, а также осуществления депозитарных операций, заключения договоров банковского вклада (депозита), заключения иных сделок и осуществления других действий в соответствии с условиями заключенных между Сторонами ДБС и иных соглашений, осуществления Банком функций агента валютного контроля, предоставления в Банк документов, необходимых для осуществления Банком функций, установленных законодательством Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

1.2. Информационный обмен в рамках Системы осуществляется по открытым каналам связи, в том числе с использованием сети «Интернет».

1.3. Для обеспечения конфиденциальности Электронного документа при передаче по открытым каналам связи, а также для обеспечения авторства и целостности Электронного документа, в Системе используется Средство защиты информации «OpenSSL».

1.4. Клиент согласен с тем, что использование Средства защиты информации «OpenSSL» в качестве средства обеспечения конфиденциальности при передаче по открытым каналам связи, а также для обеспечения авторства и целостности Электронного документа, является достаточным, т.е. обеспечивающим защиту интересов Клиента.

1.5. Клиент отказывается от предъявления претензий к Банку, основанием которых является использование «OpenSSL» в качестве средства защиты Электронного документа от несанкционированного доступа при передаче по открытым каналам связи, а также для обеспечения авторства и целостности Электронного документа.

### **Article 1. The Subject-Matter of the Agreement.**

1.1. The Parties have established the procedure and the terms for the exchange of Electronic Documents within the System for the purposes of performing bank operations on the Accounts (including settlement operations) based on Electronic Documents, as well as custody transactions, concluding bank deposit agreements, concluding other transactions and performing other actions in compliance with the terms of BAAs concluded between the Parties, as well as other agreements, performance of the functions of a currency control agent by the Bank, submission to the Bank of the documents required for the Bank to perform the functions established by the laws of the Russian Federation on counteraction to legalization (laundering) of proceeds from criminal activities and terrorism funding.

1.2. Informational exchange within the System is made through open communication channels, and also through the use of the Internet.

1.3. In order to assure confidentiality of an Electronic document during the transfer through the open communications channel, as well as in order to assure the authorship and the entirety of an Electronic document, System engages information security products - «OpenSSL».

1.4. The Client agrees that the use of the information security product «OpenSSL» as means for the securing of the confidentiality during the transfer through the open communication channels, as well as to assure the authorship and entirety of an Electronic document, is sufficient, i.e. assuring the protection of Client's interests.

1.5. The Client refuses to file claims with the Bank, the motivation for which is the use of the «OpenSSL» as a product for the protection of an Electronic document from unsanctioned access during the transfer through the open communication channels, as well as to assure the authorship and entirety of an Electronic document.

## **Статья 2. Общие положения.**

2.1. Система будет использоваться для обмена Электронными документами в любом формате, за исключением архивных файлов, таких как: zip, 7z, arj, rar и аналогичных им. Формирование Электронных документов и обмен ими будет осуществляться в соответствии с требованиями Документации. Любая информация, передаваемая Сторонами по Системе, обрабатывается Средствами защиты информации.

2.2. Стороны признают, что используемые во взаимоотношениях между ними Электронные документы, подписанные ЭП, имеют равную юридическую силу с документами на бумажном носителе, подписанными собственноручными подписями уполномоченных лиц Сторон и скрепленными печатями в случае необходимости, и являются достаточным основанием для выполнения Банком операций, действий, а также для совершения Сторонами сделок, предусмотренных ДБС, Соглашением, иными соглашениями между Сторонами.

2.3. Стороны признают, что используемые ими по настоящему Соглашению способы доставки, указанные в Приложении №2 к Соглашению, Средства обработки и хранения информации достаточны для обеспечения надежной и эффективной работы по приему, передаче и хранению информации.

2.4. Электронный документ порождает обязательства Сторон по настоящему Соглашению, ДБС, а также иным соглашениям между Банком и Клиентом, является офертой или акцептом, если он оформлен передающей Стороной в соответствии с настоящим Соглашением, ДБС, иными соглашениями между Банком и Клиентом и Документацией, подписан ЭП и передан посредством Системы, а принимающей Стороной получен, и Проверка ЭП Электронного документа дала положительный результат.

Электронные документы не могут быть оспорены или отрицаться Сторонами и третьими лицами или быть признаны недействительными только на том основании, что они переданы в Банк с использованием Системы и способов доставки.

## **Article 2. General provisions.**

2.1. System will be used for the exchange of Electronic documents in any format except archive files, i.e. zip, 7z, arj, rar, etc. Formation of the Electronic documents and the exchange thereof will be conducted in compliance with the requirements of the Documentation. Any information, transmitted by the Parties through the system, shall be processed by the information security products.

2.2. Parties acknowledge, that the Electronic documents used in their mutual relations, which are signed with Electronic Signatures, have an equal legal force to the documents committed on paper, signed with the handwritten signatures of the authorized representatives of the Parties and are sealed if it is required, form a sufficient basis for the execution of operations and actions by the Bank, as well as for consummation by the Parties of the transactions contemplated by BAAs, the Agreement and other agreements between the Parties.

2.3. The Parties acknowledge that the methods of delivery used by them under the present Agreement and specified in Annex No. 2 hereto, and the Information Processing and Safekeeping Means are sufficient for the assurance of a secure and efficient work on the acceptance, transfer and safekeeping of information.

2.4. An electronic document is binding for the Parties under the present Agreement, BAAs, as well as other agreements between the Bank and the Client, and constitutes an offer or acceptance in case if it is drawn up by the transmitting Party in compliance with the present Agreement, BAAs, other agreements between the Bank and the Client and Documentation, is signed with an Electronic Signature and transferred through the System, and is received by the Receiving Party, and if the verification of the Electronic Signature on the Electronic Document resulted in a positive outcome.

Electronic documents may not be contested or denied by the Parties and third parties or be declared invalid only because they have been submitted to the Bank using the System and methods of delivery.

2.5. Банк и Клиент используют Систему для передачи Электронных документов друг другу в приоритетном порядке, при этом использование Системы не ограничивает права Клиента по предоставлению в Банк платежных, иных документов на бумажном носителе, составленных в соответствии с ДБС, Соглашением, иными соглашениями между Банком и Клиентом. Настоящим Стороны соглашаются с тем, что в случае поступления в Банк Электронного документа по Системе и соответствующего платежного, иного документа на бумажном носителе, содержащих идентичные условия проведения операции, осуществления соответствующих действий, в том числе, по Счету, счету депо, счету по вкладу (депозиту) либо поступления в Банк идентичных Электронных документов, Банк будет рассматривать каждый из указанных документов как самостоятельный платежный, иной документ, и осуществит все действия, необходимые для проведения операции, осуществления соответствующих сделок, действий, в том числе, по Счету, счету депо, счету по вкладу (депозиту), в соответствии с каждым из представленных/переданных Клиентом документов.

2.6. Внутренние процедуры использования Клиентом Системы и его внутренний документооборот устанавливаются Клиентом самостоятельно.

2.7. Клиент уведомлен о том, что информация, передаваемая Банком посредством Системы, не является информацией «в реальном времени».

### **Статья 3. Порядок подключения Клиента к Системе и Плановой смены Рабочих ключей.**

3.1. Для участия в обмене Электронными документами:

3.1.1. Клиент выполняет следующие действия:

а) заполняет заявку на установку Системы, где указывает необходимую Подсистему и передает ее в Банк на бумажном носителе;

б) назначает и наделяет соответствующими полномочиями физических лиц, ответственных за осуществление обмена Электронными документами, в том числе:

2.5. The Bank and the Client use the System for the transfer of Electronic documents to each other in a priority procedure, however the use of the System does limit the rights of the Client for the provision, to the Bank, of payment and other documents in physical format, drafted in compliance with BAAs, the Agreement and other agreements between the Bank and the Client. Hereby the Parties agree that in case the Bank receives an Electronic Document transferred through the System and the corresponding payment, other document on paper, containing identical conditions for the commission of an operation, performance of relevant actions, including operations on an Account, depot-account, deposit account or the reception by the Bank of identical Electronic documents, the Bank will consider each of the specified documents as an individual payment or other document, and will carry out all the actions, required for the commissioning of an operation, appropriate transactions and actions, including on the Account, depot-account, deposit account in compliance to each of the documents presented/transferred by the Client.

2.6. Internal procedures for the use of the System by the Client and its internal documentation management are established by the Client individually.

2.7. The Client is notified that the information, transferred by the Bank through the System is not “real time” information.

### **Article 3. Procedure for connecting the Client to the System and Planned change of Operational Keys.**

3.1. For participation in the exchange of Electronic Documents:

3.1.1. The Client performs the following actions:

a) fills out an application for installation of the System specifying the required Subsystem and submits it to the Bank on paper;

b) appoints and delegates the respective authorities to individuals responsible for the exchange of Electronic Documents including:

- Authorized Representative of the Client;
- System Administrator – a person,

- Уполномоченного представителя Клиента,  
- администратора Системы – лицо, ответственное за техническую поддержку Системы;

в) для каждого Уполномоченного представителя Клиента заполняет и представляет в Банк 2 (два) экземпляра Данных о Владельце сертификата ключа проверки ЭП (по форме Приложения №5 к Соглашению) с приложением заверенной Банком/нотариально (в случае необходимости с проставлением апостиля/при условии ее легализации) копии документа, удостоверяющего личность Уполномоченного представителя Клиента и/или документа, подтверждающего право лица на пребывание (проживание) в Российской Федерации и/или миграционной карты, – для иностранных граждан и лиц без гражданства. При этом Банк проставляет отметки о получении на каждом экземпляре Данных о Владельце сертификата ключа проверки ЭП.

Для Уполномоченных представителей Клиента с полномочиями «без права подписи» документ, удостоверяющий личность Уполномоченного представителя Клиента и/или документ, подтверждающий право лица на пребывание (проживание) в Российской Федерации и/или миграционная карта, – для иностранных граждан и лиц без гражданства - могут быть представлены в Банк в копиях, заверенных в порядке, установленном Банком.

Документы, представляемые Клиентом и составленные на иностранном языке, должны сопровождаться переводом на русский язык, за исключением случаев установленных законодательством Российской Федерации. Перевод на русский язык должен быть заверен в порядке, установленном законодательством Российской Федерации;

г) обеспечивает наличие и приведение оборудования, предназначенного для установки Системы, в соответствие с требованиями к аппаратно-программным средствам, приведенными в Приложении №1 к Соглашению.

3.1.2. Банк выполняет следующие действия:

а) изготавливает Технологические ключи на каждого Уполномоченного представителя Клиента в течение 5-и (пяти) Рабочих дней Банка со дня принятия Банком документов,

responsible for the technical support to the System;

c) fills out and submits to the Bank 2 (two) copies of Information on the Authorized Representative of the ES Verification Key Certificate Holder for each Authorized Representative of the Client (as per the form of Annex No. 5 to the Agreement) accompanied by a copy of an identification document of the Authorized Representative of the Client certified by the Bank/notarized (and apostilled, if necessary/subject to legalization) and/or a document certifying the person's right to stay (reside) in the Russian Federation and/or a migration card – for foreign nationals and persons destitute of nationality. The Bank confirms receipt thereof on each copy of the Information on the ES Verification Key Certificate Holder.

For the Authorized Representatives of the Client “without the right of signature”, an identification document of the Authorized Representative of the Client and/or a document confirming the person's right to stay (reside) in the Russian Federation and/or a migration card – for foreign nationals and persons destitute of nationality – may be submitted to the Bank as copies certified according to the procedure established by the Bank.

Documents submitted by the Client and drawn up in a foreign language must be accompanied by a translation into Russian, with the exception of cases provided for by the laws of the Russian Federation. Translation into Russian must be certified according to the procedure established by the laws of the Russian Federation;

c) ensures the availability and compliance of the equipment, required for the installation of the System, with the requirements for hardware and software stipulated in Annex No. 1 to the Agreement;

3.1.2. The Bank performs the following actions:

a) produces Technological Keys for each Authorized Representative of the Client within 5 (five) Business Days of the Bank from the

по форме и содержанию соответствующих подп. в) п.3.1.1 Соглашения;

б) передает Клиенту Технологические ключи; Акт признания Открытого ключа ЭП в двух экземплярах и один экземпляр Данных о Владельце сертификата ключа проверки ЭП с отметкой Банка, поставленной в соответствии с подпунктом в) п.3.1.1 Соглашения; пароль для входа в подсистему «Интернет клиент-банк» и информацию об адресе для входа в подсистему «Интернет клиент-банк» (при выборе Клиентом подсистемы «Интернет клиент-банк»), а также Документацию в электронном виде;

в) консультирует Клиента по вопросам установки Системы после проведения Клиентом подготовительных мероприятий, перечисленных в п.3.1.1 Соглашения. После завершения всех работ по подключению Клиента к Системе Стороны подписывают соответствующий акт на бумажном носителе;

г) по желанию Клиента, проводит в своем помещении занятия по обучению эксплуатации Системы с лицами, уполномоченными Клиентом, в согласованные Сторонами сроки.

3.2. Документы, указанные в п.3.1, п.3.4, п.3.6 Соглашения, а также документы, которые в соответствии с Соглашением Стороны обязаны предоставлять друг другу на бумажном носителе, Стороны вправе передавать друг другу через уполномоченного представителя или с помощью почтовой службы DHL, иной аналогичной почтовой службы.

3.3. После получения Клиентом Технологических ключей Стороны проводят мероприятия, в ходе которых проверяется (тестируется) следующее:

- наличие постоянной и устойчивой связи при работе Системы;
- работа всех основных функций программного обеспечения Системы;
- бесспорная работа Средств защиты информации;
- получение и передача Электронных документов, а также формирование архивов полученных и отправленных Электронных документов.

3.4. После успешного тестирования Системы:

date of the Bank's acceptance of the documents in the form and with the content complying with Sub-paragraph c) of Paragraph 3.1.1 of the Agreement;

b) provides the Client with the Technological Keys, two copies of the Act of acknowledgement of the ES Public Key and one copy of the Information on the ES Verification Key Certificate Holder with a Bank mark, applied in compliance with Sub-paragraph b) of Paragraph 3.1.1. of the present Agreement, as well as a password to enter the Internet Client-Bank subsystem, information about the address to enter the Internet Client-Bank subsystem (if the Internet Client-Bank subsystem is chosen by the Client), and the Documentation in an electronic format;

c) provides consultations to the Client on the System installation after the Client has completed the preparatory measures listed in paragraph 3.1.1 of the Agreement. After completion of the whole scope of work of connecting the Client to the System, the Parties shall sign the respective act on paper;

d) at the discretion of the Client, implements measures in own premises aimed at training for the use of the System with the persons authorized by the Client, within the terms agreed by the Parties.

3.2. Documents, specified in subparagraphs 3.1, 3.4, 3.6 of the Agreement, as well as the documents, which in compliance to the Agreement Parties must provide to each other on paper, can be transferred by the Parties to each other through an authorized representative or through the DHL postal service, or other similar postal service.

3.3. After the Client's receipt of the Technological Keys, the Parties take measures to check (test) the following:

- availability of a sustained and a stable connection during the operation of the System;
- operation of all the main functions of the System software;
- error free operation of the information security products;
- reception and transfer of Electronic documents, as well as the formation of archives for the received and sent Electronic documents.

3.4. After successful testing of the System:

- Клиент:
  - создает Рабочие ключи и электронный запрос на создание Сертификата Рабочего ключа;
  - направляет в Банк электронный запрос на создание Сертификата Рабочего ключа;
  - по каждому из Уполномоченных представителей Клиента заверяет собственноручной подписью уполномоченного лица Клиента и печатью Клиента (при ее наличии) либо собственноручной подписью Уполномоченного представителя Клиента в отношении Технологического ключа данного представителя (без проставления печати) полученный от Банка Акт признания Открытого ключа ЭП и передает один экземпляр указанного акта в Банк вместе с Актом признания открытого ключа (сертификата) для обмена сообщениями (по форме Приложения №6 к Соглашению), распечатанным из Системы, в двух экземплярах, подписанным собственноручными подписями уполномоченного лица Клиента и соответствующего Уполномоченного представителя Клиента и заверенным печатью Клиента (при ее наличии).
- Банк:
  - в течении двух Рабочих дней Банка с даты получения надлежащим образом оформленного со стороны Клиента Акта признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению), в двух экземплярах, изготавливает Сертификат Рабочего ключа на основании электронного запроса Клиента на создание Сертификата Рабочего ключа;
  - проставляет отметку о дате начала и окончания срока действия ключа на каждом экземпляре принятого от Клиента Акта признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению);
  - направляет Клиенту Сертификат Рабочего ключа.

3.5. Клиент принимает от Банка в Системе

- the Client shall:
  - create Operational Keys and an electronic request for the creation of an Operational key certificate;
  - send to the Bank the electronic request for the creation of an Operational key certificate;
  - for each of the Authorized Representatives of the Client, certify with a handwritten signature of the Client's authorized person and the seal of the Client (if any) or with a handwritten signature of the Authorized Representative of the Client in relation to the Technological Key of this representative (without affixing a seal) the Act of Acknowledgement of the ES Public Key received from the Bank and submit one copy of the above act to the Bank along with the Act of Acknowledgement of the Public Key (certificate) for message exchange (according to the form of Annex No. 6 to the Agreement) printed out from the System, in duplicate, bearing handwritten signatures of the authorized person of the Client and of the corresponding Authorized Representative of the Client and bearing the seal of the Client (if any).
- The Bank shall:
  - generate an Operational Key Certificate based on the Client's electronic request for a new Operational Key Certificate within two Business Days of the Bank from the date of the receipt of the Act of Acknowledgement of the Public Key (certificate) for message exchange (Annex No. 6 to the Agreement) duly executed by the Client in duplicate;
  - make a note on the date of the commencement and completion of the key validity period on each copy of the Act of Acknowledgement of the Public Key (certificate) for message exchange (Annex No. 6 to the Agreement) accepted from the Client;
  - send the Operational Key Certificate to the Client.

3.5. The Client accepts the Operational Key

Сертификат Рабочего ключа и отправляет в Банк извещение о начале передачи Электронных документов в рабочем режиме в виде Электронного документа, подписанного Рабочим ключом.

Банк начинает обслуживание Клиента с использованием Системы в рабочем режиме с момента получения от Клиента посредством Системы первого Электронного документа, подписанного Рабочим ключом.

3.6. При плановой смене Рабочих ключей:

- Клиент:
  - создает и направляет в Банк электронный запрос на создание нового Сертификата Рабочего ключа;
  - предоставляет в Банк на бумажном носителе Акт признания открытого ключа (сертификата) для обмена сообщениями (по форме Приложения №6 к Соглашению) в двух экземплярах;
  - принимает от Банка в Системе новый Сертификат Рабочего ключа.
- Банк:
  - в течение двух Рабочих дней Банка с даты получения надлежащим образом оформленного со стороны Клиента Акта признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению), в двух экземплярах, изготавливает новый Сертификат Рабочего ключа на основании электронного запроса Клиента на создание нового Сертификата Рабочего ключа;
  - проставляет отметку о дате начала и окончания срока действия ключа на каждом экземпляре принятого от Клиента Акта признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению);
  - направляет Клиенту новый Сертификат Рабочего ключа.

3.7. Банк, обладая соответствующими правами, предоставленными ему в соответствии с договором, заключенным между Банком и ООО «БСС», предоставляет Клиенту право на пользование Системой в течение действия настоящего Соглашения. Право на пользование предоставляется с учетом ограничений, предусмотренных

Certificate from the Bank in the System and sends to the Bank a notice of the beginning of Electronic Document transmission in the operational mode in the form of an Electronic Document signed with the Operational Key.

The Bank starts servicing the Client using the System in operational mode from the receipt of the first Electronic Document signed with the Operational Key from the Client in the System.

3.6. When Operational Keys must be changed according to the schedule:

- The Client shall:
  - create and submit to the Bank an electronic request for the creation of a new Operational Key Certificate;
  - submit to the Bank on paper the Act of Acknowledgement of the Public Key (certificate) for message exchange (Annex No. 6 to the Agreement) in duplicate;
  - accept a new Operational Key Certificate from the Bank in the System.
- The Bank shall:
  - generate a new Operational Key Certificate based on the Client's electronic request for a new Operational Key Certificate within two Business Days of the Bank from the date of the receipt of the Act of Acknowledgement of the Public Key (certificate) for message exchange (Annex No. 6 to the Agreement) duly executed by the Client in duplicate;
  - make a note on the date of the commencement and completion of the key validity period on each copy of the Act of Acknowledgement of the Public Key (certificate) for message exchange (Annex No. 6 to the Agreement) accepted from the Client;
  - send the new Operational Key Certificate to the Client.

3.7. The Bank, due to the corresponding rights granted to it under the contract concluded between the Bank and BSS, Ltd., grants to the Client the right to use the System during the validity term of the Agreement. The right to use is granted, subject to the restrictions provided by the law of the Russian Federation on the legal protection for computer software.

законодательством Российской Федерации о правовой охране программ для ЭВМ.

#### **Статья 4. Права и обязанности Сторон.**

##### **4.1. Взаимные права и обязанности Сторон.**

4.1.1. Стороны при обмене Электронными документами с использованием Системы обязуются руководствоваться правилами и требованиями, установленными законодательством Российской Федерации, ДБС, настоящим Соглашением, иными соглашениями между Банком и Клиентом.

4.1.2. Стороны обязуются не разглашать третьей стороне (за исключением случаев, предусмотренных законодательством Российской Федерации и настоящим Соглашением) информацию о Средствах защиты информации, используемых в Системе.

4.1.3. Каждая из Сторон обязуется немедленно информировать другую Сторону обо всех случаях Компрометации ключей, несанкционированного использования Системы, а также повреждениях/утраты программно-аппаратных средств обработки, хранения, передачи Электронных документов, Средств защиты информации, а также Ключей и не использовать Ключи при наличии оснований полагать, что они скомпрометированы.

4.1.4. Средства защиты информации Электронных документов, предоставленные Системой, признаются Сторонами достаточными для защиты информации от несанкционированного доступа, подтверждения авторства и подлинности Электронных документов.

4.1.5. Любые Электронные документы, передаваемые по Системе, подлежат шифрованию.

4.1.6. Любые Электронные документы, передаваемые по Системе должны быть заверены ЭП Стороны - отправителя.

4.1.7. Какие-либо ограничения полномочий Уполномоченного представителя Клиента, в т.ч. указанные в соответствующих Данных о Владельце сертификата ключа проверки ЭП, Банком не признаются и не контролируются, если иное не установлено соглашением между Клиентом и Банком. Банк не

#### **Article 4. Rights and obligations of the Parties.**

##### **4.1. Reciprocal rights and obligations of the Parties.**

4.1.1. Parties, during the exchange of the Electronic documents through the use of the System, undertake to be guided by the rules and requirements as set by the legislation of the Russian Federation, BAAs, this Agreement, and other agreements between the Bank and the Client.

4.1.2. Parties undertake not to disclose to a third party (except for cases, as under the legislation of the Russian Federation and this Agreement) the information about the Information Security Products used in the System.

4.1.3. Each Party undertakes to immediately inform the other Party about all the cases of Key compromise, unauthorized use of the System, as well as the damage to the software and hardware designed for processing, storage and transfer of Electronic documents, as well as the information security products and Keys, and not to use Keys if there are the reasons to assume that they are compromised.

4.1.4. Information protection products for Electronic Documents granted by the System are found as sufficient by the Parties for the protection of information from unauthorized access, confirmation of authorship and authenticity of Electronic Documents.

4.1.5. Any Electronic Documents transferred within the System, are subject to encryption.

4.1.6. Any Electronic Documents transferred within the System must be certified by an Electronic Signature of the Party - Sender.

4.1.7. The Bank shall not accept any limitations of the powers of the Authorized Representative of the Client including the ones (powers) stated in the corresponding Information on the Authorized Representative of the Key Certificate Holder, unless otherwise stipulated by a separate agreement



осуществляет контроль за суммами платежей, суммами сделок, осуществляемых Уполномоченными представителями Клиента в соответствии с ДБС, Соглашением, иными соглашениями между Сторонами.

4.1.8. Клиент уведомлен и согласен, что письмо, направленное Клиентом в Банк в соответствии с Соглашением по электронной почте (e-mail), считается полученным Банком с момента его регистрации как входящего документа во внутренней системе документооборота Банка.

#### **4.2. Права и обязанности Клиента.**

4.2.1. Клиент не имеет права тиражировать и передавать третьей стороне программное обеспечение, предоставляемое Банком по Соглашению и все конфиденциальные данные, относящиеся к Соглашению.

4.2.2. Клиент имеет право, при необходимости, воспользоваться помощью специалиста Банка для устранения неполадок, возникших в Системе, направив в Банк письменную заявку. По результатам работы специалиста Банка Стороны подписывают акт об оказании услуг на бумажном носителе.

4.2.3. Клиент обязуется в сроки, предусмотренные Соглашением, обеспечить на своем расчетном и/или иных счетах, открытых в Банке, остаток денежных средств в размере, необходимом для оплаты услуг Банка в соответствии с Соглашением и Тарифами.

4.2.4. Клиент обязуется обеспечивать сохранность и целостность установленной Системы, включая Средства защиты информации, а также выполнять требования к эксплуатации Системы, изложенные в Документации.

4.2.5. Клиент по требованию Банка обязан предоставить оригиналы документов на бумажном носителе, преобразованных в Электронные документы и переданных по Системе, в течение 14 (четырнадцати) календарных дней с момента направления ему требования. Документы на бумажном носителе должны быть подписаны уполномоченными лицами Клиента и заверены печатью Клиента (при ее наличии).

4.2.6. В случае смены руководителя

between the Client and the Bank. Accordingly, the Bank shall not control the amounts of payments, the amounts of transactions consummated by Authorized Representatives of the Client in accordance with BAAs, the Agreement and other agreements between the Parties.

4.1.8. The Client is aware and agrees that the letter sent by the Client to the Bank under this Agreement by e-mail shall be deemed received by the Bank upon its registration as an incoming document in the internal document management system of the Bank

#### **4.2. Rights and obligations of the Client.**

4.2.1. The Client has no right to replicate and transfer, to a third party, the software, granted by the Bank under the present Agreement and all the confidential information relating to the Agreement.

4.2.2. The Client has the right, if required, to use the assistance of an expert from the Bank in order to amend the errors, arising in the System, by directing a written request to the Bank. Upon the results of the work conducted by the expert, as in compliance with the Client's application, Parties sign a Service Performed Report on paper.

4.2.3. The Client within the term specified by the Agreement, undertakes to assure that its settlement account and/or other accounts opened with the Bank indicate a balance of funds in the amount, required for the payment of services rendered by the Bank as in compliance with the Agreement and Tariffs.

4.2.4. The Client undertakes to assure security and entirety of the installed System, including information security products, as well as implement the requirements for the operation of the System, as specified in the Documentation.

4.2.5. The Client, at the request of the Bank, shall present the original documents on paper, as transformed into Electronic documents and transmitted through the System, within a period of 14 (fourteen) calendar days from the moment the Bank sends such a requirement. Documents on paper must be signed by the authorized persons of the Client and certified by the Client's seal (if applicable).

4.2.6. In case the Client undergoes a change of

(единоличного исполнительного органа) Клиент обязан подтвердить права действующего Уполномоченного представителя Клиента.

4.2.7. В случае прекращения полномочий действующего Уполномоченного представителя Клиента, а также в случае несанкционированного доступа к Системе, Компрометации ключей, Клиент обязан незамедлительно направить в Банк письмо об аннулировании соответствующего комплекта Ключей (вложенным файлом) по адресу электронной почты (e-mail), указанному в Договоре об использовании ДБО, с последующим немедленным предоставлением в Банк оригинала вышеуказанного письма об аннулировании соответствующего комплекта Ключей на бумажном носителе.

Направление указанных документов по адресу электронной почты (e-mail) означает требование Клиента прекратить прием и исполнение любых Электронных документов, подписанных ЭП, сформированной на скомпрометированном/аннулируемом Ключе.

Для изготовления нового комплекта Технологических ключей Клиент предоставляет в Банк Данные о Владельце сертификата ключа проверки ЭП в двух экземплярах (Приложение №5 к Соглашению) с приложением необходимых документов.

4.2.8. В случае изменения фамилии, имени, отчества (при наличии) Уполномоченного представителя Клиента, а также наименования Клиента, Клиент предоставляет в Банк все документы, предусмотренные настоящим Соглашением для изготовления нового комплекта Технологических ключей, а также письмо об аннулировании соответствующего комплекта Ключей.

В целях изменения вида права подписи Электронных документов Уполномоченного представителя Клиента, Клиент обращается в Банк с письменным заявлением в произвольной форме.

В случае изменения иных данных Уполномоченного представителя Клиента, Клиент предоставляет в Банк Акт признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению), с приложением заверенной

the Director (sole executive body), the latter shall confirm the rights of the effective Authorized Representative of the Client.

4.2.7. In case of termination of the authorities of the current Authorized Representative of the Client, as well as in case of unauthorized access to the System, Key Compromise, the Client shall immediately send to the Bank a letter on cancellation of the corresponding set of Keys (as enclosure) to the e-mail address specified in the Contract on the Use of RBS, followed by immediate presentation of the original letter on cancellation of the corresponding set of Keys on paper to the Bank.

The fact of sending these documents by e-mail means the Client's request to stop receiving and executing any Electronic documents signed with the Electronic Signature generated using the compromised/canceled Key.

For the purposes of having a new set of Technological Keys generated, the Client provides the Bank with the information on the ES Verification Key Certificate Holder in two copies (Annex No. 5 to the Agreement) with documents attached thereto as required.

4.2.8. In case of changes in the surname, name, patronymic (if any) of the Authorized Representative of the Client, as well as the name of the Client, the Client shall provide the Bank with the documents specified herein for the purposes of generation of a new set of Technological Keys, as well as a letter on cancellation of the respective set of Keys.

To change the type of the right to sign Electronic Documents granted to the Authorized Representative of the Client, the Client shall file a written free-form application to the Bank.

In case of changes in other information on the Authorized Representative of the Client, the Client shall provide the Bank with the Act of acknowledgement of the Public Key (certificate) for message exchange (Annex No. 6 to the Agreement) accompanied by a copy

Банком/нотариально (в случае необходимости с проставлением апостиля/при условии ее легализации) копии документа, удостоверяющего личность Уполномоченного представителя Клиента и/или документа, подтверждающего право лица на пребывание (проживание) в Российской Федерации и/или миграционной карты – для иностранных граждан и лиц без гражданства.

Для Уполномоченных представителей Клиента с полномочиями «без права подписи» документ, удостоверяющий личность Уполномоченного представителя Клиента и/или документ, подтверждающий право лица на пребывание (проживание) в Российской Федерации и/или миграционная карта, – для иностранных граждан и лиц без гражданства могут быть представлены в Банк в копиях, заверенных в порядке, установленном Банком.

Документы, представляемые Клиентом и составленные на иностранном языке, должны сопровождаться переводом на русский язык, за исключением случаев установленных законодательством Российской Федерации. Перевод на русский язык должен быть заверен в порядке, установленном законодательством Российской Федерации.

4.2.9. Клиент обязан самостоятельно контролировать сроки действия Технологических ключей/Рабочих ключей и своевременно инициировать процедуру создания Рабочих ключей/Плановой смены рабочих ключей до истечения срока действия действующих Рабочих ключей. Соответствующие уведомления о Плановой смене рабочих ключей могут направляться Банком по Системе в течение месяца до истечения срока действия действующих Рабочих ключей. В случае, если в установленные Соглашением сроки Клиентом не направлен в Банк запрос на создание Сертификата Рабочего ключа и/или не предоставлены в Банк на бумажном носителе Акт признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению) и Акт признания Открытого ключа ЭП (в случае необходимости), а также в случае несоответствия полученных Банком от Клиента на бумажном носителе перечисленных документов условиям

of an identification document of the Authorized Representative of the Client certified by the Bank/notarized (and apostilled, if necessary/subject to legalization) and/or a document certifying the person's right to stay (reside) in the Russian Federation and/or a migration card – for foreign nationals and persons destitute of nationality.

For the Authorized Representatives of the Client “without the right of signature”, an identification document of the Authorized Representative of the Client and/or a document confirming the person's right to stay (reside) in the Russian Federation and/or a migration card – for foreign nationals and persons destitute of nationality – may be submitted to the Bank as copies certified according to the procedure established by the Bank.

Documents submitted by the Client and drawn up in a foreign language must be accompanied by a translation into Russian, with the exception of cases provided for by the laws of the Russian Federation. Translation into Russian must be certified according to the procedure established by the laws of the Russian Federation.

4.2.9. The Client must independently control the validity periods of Technological/Operational Keys and timely initiate the procedure of generating Operational Keys/Planned change of Operational Keys before expiry of the current Operational Keys. The respective notifications of the Planned change of Operational Keys may be sent by the Bank through the System within one month before expiry of the current Operational Keys. If the Client fails to send a request for a new Operational Key Certificate and/or an Act of acknowledgement of the public key (certificate) for message exchange (Annex No. 6 to the Agreement) and an Act of acknowledgement of the ES Public Key (if necessary) on paper to the Bank within the timing set out by the Agreement, or if the the above documents on paper received by the Bank from the Client do not comply with the Agreement and/or if the Client does not accept the Operational Key Certificate from the Bank in the System, the Technological/Operational Key shall become null and void.

Соглашения и/или непринятия Клиентом от Банка в Системе Сертификата Рабочего ключа, действие Технологического ключа/Рабочего ключа прекращается.

Порядок изготовления нового Технологического ключа/Рабочего ключа аналогичен порядку, установленному п.п.3.1, 3.2, 3.4, 3.6 Соглашения.

4.2.10. Клиент обязан информировать Банк об изменении информации, касающейся исполнения Сторонами Соглашения. По мере внесения соответствующих изменений, незамедлительно представлять в Банк документы, подтверждающие изменения данных сведений.

Все риски неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о произошедших изменениях, в том числе, указанных в п.п.4.2.6-4.2.8, п.5.5 Соглашения, несет Клиент.

4.2.11. При расторжении Соглашения Клиент обязуется уничтожить все предоставленное ему в пользование программное обеспечение (исполняемые и вспомогательные файлы) Системы.

4.2.12. Клиент обязуется не передавать третьим лицам свои права и обязанности по Соглашению без письменного (на бумажном носителе) согласия Банка.

4.2.13. Клиент обязан проверять наличие новых Электронных документов от Банка, направленных в адрес Клиента, ежедневно, за исключением официально установленных выходных и праздничных нерабочих дней Банка, а также ежедневно проверять SMS-сообщения, направленные Банком в связи с выявлением им операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента.

Клиент обязан не реже одного раза в 5 (пять) календарных дней знакомиться с информацией, публикуемой Банком в соответствии с п.12.6 Соглашения.

За убытки, возникшие в результате неисполнения Клиентом вышеуказанных обязанностей, Банк ответственности не несет.

4.2.14. Клиент обязуется по требованию и форме Банка предоставлять документы (как на бумажном носителе, так и с помощью Системы), подтверждающие данные об Уполномоченном представителе Клиента.

4.2.15. Клиент обязуется соблюдать требования по информационной

The procedure of a new Technological/Operational Key generation is the same as the procedure set out in Paragraphs 3.1, 3.2, 3.4, 3.6 of this Agreement.

4.2.10. The Client shall inform the Bank, in writing about any changes in the information relating to the performance of the Agreement and submit to the Bank documents confirming changes in said information as far as such changes are introduced.

All risks of adverse consequences associated with untimely notification of the Bank about any changes that have taken place, including those stated in Paragraphs 4.2.6-4.2.8, 5.5 of the Agreement, shall be borne by the Client.

4.2.11. In case of the termination of the Agreement, the Client undertakes to destroy all the software of the System granted to the latter for use (executable and auxiliary files).

4.2.12. The Client undertakes not to transfer its rights and obligations as under the present Agreement, to third parties without a written consent (on paper) of the Bank.

4.2.13. The Client shall check, on the daily basis, the availability of the new Electronic documents from the Bank, directed to the Client, except for the officially established holidays and weekends, as well as daily check SMS messages sent by the Bank in relation to any discovered transaction with signs of money transfer without the Client's consent.

The Client must at least once every five (5) calendar days review the information published by the Bank in accordance with Paragraph 12.6 of the Agreement.

The Bank shall not be liable for losses incurred as a result of the Customer's failure to fulfill the above obligations.

4.2.14. The Client undertakes to provide documents (both on paper and in the System) certifying data on the Authorized Representative of the Client on demand of the Bank.

4.2.15 The Client undertakes to comply with information safety requirements specified in

безопасности при работе с Системой, указанные в Приложении № 4 к Соглашению, а также направляемые Банком по Системе и размещаемые на официальном сайте Банка в сети «Интернет».

#### **4.3. Права и обязанности Банка.**

4.3.1. Банк не принимает к исполнению Электронные документы, оформленные с нарушением требований законодательства Российской Федерации, Соглашения, ДБС, иных соглашений между Сторонами.

4.3.2. Банк имеет право отказать Клиенту в приеме к исполнению Электронного документа, если Клиент заполнил поля Электронного документа с ошибками. В этом случае Клиенту направляется Квитанция с указанием причины отказа.

4.3.3. Банк не имеет права самостоятельно корректировать реквизиты Электронных документов Клиента.

4.3.4. В случае непредоставления Клиентом документов, указанных в п.4.2.7 Соглашения, Банк не будет нести ответственность за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Клиентом Электронного документа, подписанного Уполномоченным представителем Клиента, данные о котором были предоставлены Клиентом в Банк ранее.

4.3.5. Банк прекращает прием и исполнение любых Электронных документов, подписанных ЭП, сформированной на скомпрометированном/аннулируемом Ключе в сроки, предусмотренные в письме об аннулировании соответствующего комплекта Ключей, а в случае отсутствия указания на такие сроки – немедленно. Все Электронные документы, поступившие в Банк до получения Банком указанного письма, исполняются в порядке, установленном Соглашением или иными соглашениями между Сторонами.

В случае непредставления оригинала письма об аннулировании соответствующего комплекта Ключей Клиентом на бумажном носителе Банк не будет нести ответственность за убытки, причиненные Клиенту в результате прекращения приема и исполнения Электронных документов,

Annex No. 4 to the Agreement, distributed by the Bank in the System, and posted on the Bank's official website in the Internet in the course of working with the System.

#### **4.3. Rights and obligations of the Bank.**

4.3.1. The Bank does not accept Electronic documents for execution, drawn up in violation of the requirements of the legislation of the Russian Federation, the Agreement, BAAs, and other agreements between the Parties.

4.3.2. The Bank has the right to refuse the Client in the acceptance for execution of an Electronic Document, if the Client omitted mistakes when filling in such Electronic Document. In this case a Receipt confirmation is sent to the Client specifying the reason for refusal.

4.3.3. The Bank may not independently correct details of Electronic Documents of the Client.

4.3.4. If the Client fails to provide the documents specified in Paragraph 4.2.7 of the Agreement, the Bank shall not be liable for the consequences of performing transactions, other actions, deals on the basis of an Electronic Document duly executed by the Client, signed by the Authorized Representative of the Client, details of which were provided by the Client to the Bank earlier.

4.3.5. The Bank shall stop accepting and executing any Electronic Documents signed with the Electronic Signature generated using a compromised / canceled Key within the time limits specified in the letter on cancellation of the corresponding Key set, and in case no such time limits are specified - immediately. All the Electronic Documents received by the Bank prior to the receipt of such letter by the Bank shall be executed in accordance with the procedure established by the Agreement or other agreements between the Parties.

In case of the Client's failure to submit the original letter on cancellation of the respective Key set on paper, the Bank shall not be liable for any losses incurred on the Client as a result of the termination of acceptance and execution of the Electronic Documents signed with the Electronic Signature generated using a

подписанных ЭП, сформированной на соответствующем

скомпрометированном/аннулируемом Ключе.

4.3.6. Банк имеет право отказать Клиенту в приеме/приостановить исполнение любого Электронного документа по своему усмотрению, в том числе, но не ограничиваясь, в случае возникновения у него подозрений, что Электронный документ подписан не Уполномоченным представителем Клиента, Компрометации ключей, Несанкционированного доступа к Системе и/или в случае какого-либо нарушения Клиентом Соглашения, при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, при этом Клиент вправе передать в Банк соответствующий платежный, иной документ на бумажном носителе, составленный в соответствии с условиями ДБС, Соглашения, иных соглашений между Банком и Клиентом, законодательством Российской Федерации.

О своем отказе в приеме Электронного документа Банк обязуется уведомить Клиента не позднее Рабочего дня Банка, следующего за днем поступления Электронного документа в Банк, путем направления сообщения Клиенту по Системе.

4.3.7. Банк имеет право отказать Клиенту в приеме Электронных документов/приостановить их исполнение для проведения расчетных операций по Счету, счету по вкладу (депозиту), подписанных ЭП, в случаях, предусмотренных законодательством Российской Федерации, в том числе, в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

4.3.8. Банк имеет право запрашивать у Клиента подтверждение данных об Уполномоченном представителе Клиента.

4.3.9. Банк имеет право вносить в одностороннем порядке изменения в порядок функционирования Системы и сообщать об этом Клиенту в письменном уведомлении на бумажном носителе или посредством Системы.

4.3.10. Банк имеет право приостановить обслуживание Клиента с использованием

compromised / canceled Key.

4.3.6. The Bank has the right to refuse the Client in the acceptance/suspend execution of any Electronic Document at its own discretion, including, but not limited to, the cases when it suspects that the Electronic Document is signed by somebody other than the Authorized Representative of the Client, Key Compromise, Unauthorized Access to the System and/or in case of the Client's default hereunder, if the Bank discovers a transaction with signs of money transfer without the Client's consent, in which case the Client has the right to present the Bank with the corresponding payment, other document on paper, drawn up in compliance with the terms of BAAs, the Agreement, other agreements between the Bank and the Client, the legislation of the Russian Federation.

The Bank shall notify the Client about its refusal to accept the Electronic document no later than the day, following the day of reception of an Electronic document by the Bank, by sending a message to the Client via the System.

4.3.7. The Bank has the right to refuse the Client in the acceptance/suspend execution of Electronic Documents for carrying out settlement transactions on the Account, a deposit account signed with ES in cases provided for by the legislation of the Russian Federation, including in the field of countering the legalization (laundering) of criminal proceeds and terrorism funding.

4.3.8. The Bank has the right to require from the Client confirmation of data on the Authorized Representative of the Client.

4.3.9. The Bank shall have the right to amend unilaterally the procedure of the System functioning and inform the Client about it via a written notification or the System.

4.3.10. The Bank shall have the right to suspend services for the Client rendered with the use of the System, for duration of

Системы на время спорных ситуаций с уведомлением об этом Клиента.

4.3.11. Банк имеет право приостановить обслуживание Клиента с использованием Системы для выполнения неотложных, аварийных и регламентных работ, связанных с обслуживанием Системы.

4.3.12. Банк имеет право по своей инициативе блокировать действие Рабочих ключей при Компрометации ключей.

4.3.13. Банк обязуется в течение 7 (семи) Рабочих дней Банка от даты получения заявки на установку Системы и при условии выполнения Клиентом обязательств, в соответствии с п. 3.1.1 Соглашения, произвести работы и оказать услуги, предусмотренные п. 3.1.2 Соглашения.

4.3.14. Банк обязуется принимать от Клиента Электронные документы, подписанные Уполномоченным(и) представителем(лями) Клиента в соответствии с условиями настоящего Соглашения, требованиями законодательства Российской Федерации и осуществлять операции, сделки, иные действия на основании таких Электронных документов в сроки, предусмотренные ДБС, Соглашением, иными соглашениями между Сторонами.

В случае направления Электронного документа в нерабочие дни Банка, днем поступления Электронного документа является первый Рабочий день Банка, следующий за нерабочим днем. Стороны признают в качестве единой шкалы времени при работе с Системой местное время г. Москвы.

4.3.15. После подключения к Системе Банк информирует Клиента о совершении с использованием Системы или без ее использования каждой операции по Счету, счету депо путем предоставления Клиенту выписки по Счету, счету депо не позднее Рабочего дня Банка, следующего за днем совершения операции по Счету, счету депо, путем направления их только посредством Системы. Днем выдачи (получения) указанных выписок считается день их направления Банком по Системе. В случае, если доступ Клиента к Системе приостановлен, уведомление Клиента о совершении указанных операций осуществляется путем предоставления Клиенту выписки по Счету, счету депо по

disputable situations, upon a corresponding notice given to the Client.

4.3.11. The Bank shall have the right to suspend services for the Client rendered with the use of the System, for the performance of urgent, emergency and scheduled works associated with servicing of the System.

4.3.12. The Bank may on its own initiative block the operation of the Operational Keys in case of the Key Compromise.

4.3.13. Within a period of 7 (seven) Business days from the date of the System installation request, provided that the Client has executed the obligations as in compliance with Paragraph 3.1.1. of the Agreement, the Bank shall execute works and render services, as under Paragraph 3.1.2. of the Agreement.

4.3.14. The Bank undertakes to accept Electronic documents from the Client, which have been signed by the Authorized Representative(s) of the Client in compliance with the terms of the present Agreement and the requirements of the legislation of the Russian Federation and implement operations, transactions and other actions in time stipulated in BAAs, the Agreement and other agreements between the Parties, on the basis of such Electronic Documents.

If an Electronic Document is sent on non-business days of the Bank, the day of receipt of the Electronic Document shall be the first Business Day of the Bank following the non-business day. The Parties recognize the Moscow local time as the single time scale when working with the System.

4.3.15. After connection to the System the Bank shall inform the Client about each transaction on the Account effected using the System or without its use by providing to the Client statements of the Account and the depot account not later than the Bank's Business Day following the date of the transaction on the Account and depot account with said statements to be forwarded exclusively via the System. The date of issue (receipt) of said statements shall be the date of their forwarding by the Bank via the System. If the Client's access to the System is suspended, the Client shall be notified of the above transactions by way of sending the Client statements of the Account, depot account via the System immediately after recovery of the access

Системе незамедлительно после восстановления доступа к ней или другим способом и в сроки, предусмотренные соответствующим ДБС/договором счета депо. Направление Банком указанных выписок по Системе (или другим способом и в сроки, предусмотренные соответствующим ДБС/договором счета депо) является надлежащим уведомлением Клиента о совершении операции с использованием электронного средства платежа в соответствии с законодательством Российской Федерации, и не требует дополнительного направления Банком Клиенту каких-либо иных уведомлений.

4.3.16. Банк обязуется консультировать Клиента по вопросам работы с Системой (в Рабочие дни Банка с 10.00 до 16.00 московского времени), предоставлять Клиенту новые версии Системы, а также информировать Клиента обо всех изменениях порядка функционирования Системы в течение всего срока действия настоящего Соглашения.

4.3.17. Банк обязуется в случае невозможности устранить неполадки, возникшие в Системе, по месту нахождения Банка, направить специалиста к Клиенту в течение 15 (пятнадцати) календарных дней с момента получения письменной заявки от Клиента. Необходимость выезда к Клиенту определяется Банком с учетом возникших неполадок в Системе.

**Статья 5. Права и обязанности Сторон при выявлении Банком операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента.**

5.1. Банк при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, обязан до осуществления списания денежных средств со Счета приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, на срок, предусмотренный законодательством Российской Федерации.

5.2. О приостановлении исполнения распоряжения Клиента о совершении

thereto or in any other manner and within the terms fixed by corresponding BAA/depot account agreement.

The said statements forwarded by the Bank via the System (or in any other manner and within the terms fixed by the corresponding BAA/depot account agreement) shall be deemed the proper notification of the Client about the transaction using the electronic means of payment in accordance with the legislation of the Russian Federation, and shall not require any additional notification from the Bank to the Client.

4.3.16. The Bank undertakes to consult the Client on the issues of operations in the System (on Business Days of the Bank from 10 a.m. till 4 p.m. Moscow time), grant the Client with the new versions of the System, as well as inform the Client about all the changes in the functions of the System during the entire period of validity of the present Agreement.

4.3.17. In case of impossibility to correct errors arising in the System, at the location of the Bank, the Bank shall send an expert to the Client within 15 (fifteen) calendar days from the moment of reception of a written application from the Client. The need to visit the Client is defined by the Bank taking into account the arising errors in the System.

**Article 5. Rights and obligations of the Parties when the Bank discovers transactions with signs of money transfer without the consent of the Client.**

5.1. If the Bank discovers a transaction with signs of money transfer without the consent of the Client, the Bank shall suspend the order to perform the transaction with signs of money transfer without the consent of the Client before the withdrawal of funds from the Account for a term stipulated by the laws of the Russian Federation.

5.2. The Bank shall immediately notify the Client about the suspension of the Client's



операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента Банк обязуется уведомить Клиента незамедлительно путем направления сообщения Клиенту по своему усмотрению по Системе или по номеру мобильного телефона<sup>1</sup>, указанному Клиентом в Договоре об использовании ДБО или сообщенному Клиентом Банку в порядке, предусмотренном Соглашением.

Днем получения Клиентом сообщения об операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, является день направления Банком указанного сообщения по Системе или день направления Банком SMS-сообщения на номер мобильного телефона Клиента, указанный им в Договоре об использовании ДБО или сообщенный Клиентом Банку в порядке, предусмотренном Соглашением.

5.3. Клиент подтверждает/не подтверждает исполнение Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без согласия Клиента, по номеру телефона Банка, указанному на официальном сайте Банка в сети «Интернет», с произнесением Кодового слова Клиента.

При наличии технической возможности, подтвердить исполнение Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без согласия Клиента, Клиент может по Системе путем ввода кода – подтверждения, предварительно запрошенного Клиентом по Системе и полученного на мобильный номер телефона, указанный в Договоре об использовании ДБО или сообщенный Клиентом Банку в порядке, предусмотренном Соглашением. До подтверждения исполнения Банком соответствующего платежа Клиент обязан сверить реквизиты распоряжения, отправленного Клиентом, с реквизитами, указанными в уведомлении, направленном Банком по номеру мобильного телефона,

order to perform such transaction with signs of money transfer without the consent of the Client by sending a message to the Client at its own discretion via the System or to the mobile phone number<sup>1</sup> specified by the Client in the Contract on the Use of RBS or notified by the Client to the Bank in the procedure established by the Agreement.

The day of receipt of the message about a transaction with signs of money transfer without the consent of the Client by the Client shall be deemed the day of the above message sent by the Bank via the System or to the Client's mobile phone number specified by the Client in the Contract on the Use of RBS or notified by the Client to the Bank in the procedure established by the Agreement.

5.3. The Client confirms/does not confirm the performance by the Bank of the order suspended due to signs of money transfer without the Client's consent by calling on the Bank's phone number specified on the official web-site of the Bank in the Internet and using the Client's Code Word.

If technically possible, the Client may confirm the performance by the Bank of the order suspended due to signs of money transfer without the Client's consent, using the System and entering the confirmation code preliminarily requested by the Client via the System and received on the mobile phone number specified in this Contract on the use of RBS or advised by the Client to the Bank in the procedure established by the Agreement. Until confirmation of performance by the Bank of the corresponding payment, the Client shall check the details in the order sent by the Client against the details specified in the notification sent by the Bank to the mobile phone number specified by the Client in the Contract on the Use of RBS or otherwise advised by the Client to the Bank in the

<sup>1</sup> Клиентам, указавшим при заключении Договора об использовании ДБО два номера мобильных телефонов, SMS-сообщение направляется на номер мобильного телефона, указанный в первой строке пункта «Мобильный телефон клиента для приема сообщений в формате SMS-сообщений». / The Clients specifying two mobile phone numbers when entering the Contract on the Use of RBS, SMS messages shall be sent to the mobile phone number specified in the first line of "Mobile phone number of the client for SMS messages".

указанному Клиентом в Договоре об использовании ДБО или сообщенному Клиентом Банку в порядке, предусмотренном Соглашением.

При поступлении в Банк подтверждения исполнения Банком соответствующего платежа в течение операционного дня, указанного в ДБС, денежные средства списываются со Счета в текущий Рабочий день Банка. При поступлении вышеуказанного подтверждения после операционного дня, денежные средства списываются со Счета не позднее следующего Рабочего дня Банка.

В случае, если Клиент соглашается с сообщением Банка о том, что операция по Счету соответствует признакам осуществления перевода денежных средств без согласия Клиента, Клиент вправе незамедлительно направить в Банк отзыв соответствующего распоряжения.

При неполучении от Клиента соответствующего подтверждения, Банк возобновляет исполнение распоряжения по истечении срока, установленного законодательством Российской Федерации.

Клиент уведомлен о том, что все телефонные разговоры записываются и хранятся в Банке в течение срока, установленного законодательством Российской Федерации. Записи указанных телефонных разговоров могут быть использованы при разрешении любых споров, а также предоставлены в суд.

5.4. Банк вправе в одностороннем порядке изменить Кодовое слово Клиента, направив Клиенту уведомление на бумажном носителе с собственноручной подписью руководителя Банка (уполномоченного им лица) об изменении Кодового слова.

5.5. В случае утраты Клиентом контроля над номером мобильного телефона, а также утраты Клиентом уверенности в том, что Кодовое слово и/или номер мобильного телефона не могут быть использованы неуполномоченными лицами (далее – компрометация), Клиент обязан незамедлительно направить в Банк письмо о компрометации Кодового слова и/или номера мобильного телефона (вложенным файлом) по адресу электронной почты (e-mail), указанному в Договоре об использовании ДБО, с последующим немедленным

procedure established by the Agreement.

If the Client confirms the above payment to the Bank within the transaction hours specified in the BAA, funds shall be debited from the Account on the current Business Day of the Bank. If the above confirmation is received after the transaction hours, the funds shall be debited from the Account no later than on the next Bank's Business Day.

If the Client agrees with the Bank's message that the transaction on the Account bears signs of money transfer without the consent of the Client, the Client may immediately revoke the respective order from the Bank.

If the Customer fails to send the corresponding confirmation, the Bank shall resume the order after expiry of the term stipulated by the laws of the Russian Federation.

The Client is hereby notified that all telephone conversations shall be recorded and stored by the Bank within the period established by the laws of the Russian Federation. The recordings of such telephone conversations may be used when resolving any disputes and may be presented to court.

5.4. The Bank may unilaterally change the Client's Code Word by sending a notification to the Client on paper with a handwritten signature of the Bank Manager (his authorized representative) on the change of the Code Word.

5.5. If the Client loses control over the mobile phone number or loses confidence that the Code Word and/or mobile phone number cannot be used by unauthorized persons ("compromise"), the Client shall immediately send to the Bank a letter about the compromise of the Code Word and (or) mobile telephone number (as an enclosed file) to the e-mail address specified in the Contract on the use of RBS, subject to the subsequent immediate sending of the original of such letter to the Bank.

предоставлением в Банк оригинала вышеуказанного письма.

Все распоряжения Клиента о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, поступившие после получения Банком вышеуказанного письма по электронной почте и до принятия Банком от Клиента последующего уведомления на бумажном носителе с собственноручной подписью уполномоченного лица Клиента с указанием нового Кодового слова и/или номера мобильного телефона, считаются автоматически отозванными.

В случае замены Клиентом номера мобильного телефона и/или Кодового слова, Клиент обязан незамедлительно уведомить об этом Банк в письменном виде на бумажном носителе с собственноручной подписью уполномоченного лица Клиента с указанием нового Кодового слова и/или номера мобильного телефона.

До момента принятия Банком вышеуказанного уведомления Банк использует в соответствии с Соглашением ранее сообщенный Банку Клиентом номер мобильного телефона, ранее сообщенное Клиентом Банку/Банком Клиенту (в соответствии с п.5.4 Соглашения) Кодовое слово.

5.6. Банк не несет ответственности за ущерб, причиненный Клиенту вследствие несанкционированного использования третьими лицами (в том числе при компрометации) Кодового слова/номера мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.

5.7. Банк не несет ответственности за негативные последствия, в том числе убытки Клиента, которые могут возникнуть у Клиента вследствие неполучения уведомления от Банка об операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, в том числе, в связи с недостоверностью/неактуальностью информации, указанной Клиентом, а также в связи с недоступностью для Клиента указанных способов связи, а также по вине Клиента или мобильного оператора, в случае

All the Client's orders on the performance of the transaction having signs of funds transfer without the Client's consent which are delivered after the Bank receives the above e-mail and before the Bank accepts from the Client the subsequent notification on paper with a handwritten signature of the Client's authorized representative specifying the new Code Word and/or mobile phone number, shall be deemed automatically revoked.

If the Client changes the mobile phone number and (or) the Code Word, the Client shall immediately notify the Bank thereof in writing on a paper bearing the handwritten signature of the authorized person of the Client specifying a new Code Word and (or) mobile telephone number.

Until the Bank accepts the above notification, the Bank shall use the mobile phone number previously provided to the Bank by the Client and the Code Word previously provided to the Bank by the Client/to the Client by the Bank (as per Paragraph 5.4 of the Agreement) in accordance with the Agreement.

5.6. The Bank shall not be liable for damage caused to the Client due to unauthorized use by third parties (including in case of compromise) of the Code Word/mobile phone number, to which the Bank sends SMS messages about transactions with signs of money transfer without the consent of the Client.

5.7. The Bank shall not be liable for negative consequences, including losses of the Client, which the Client may suffer as a result of non-receipt of a notification from the Bank about a transaction with signs of money transfer without the consent of the Client including, but not limited to, for the reason of inaccuracy/outdated nature of the information specified by the Client, unavailability of the specified communication methods for the Client, fault of the Client or the mobile operator, loss of the Code Word/mobile phone number, to which the Bank sends SMS

утраты Клиентом Кодового слова/номера мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, их компрометации.

5.8. Банк не несет ответственности за убытки Клиента, возникшие в результате утраты (порчи, передачи, утери, разглашении) Клиентом Кодового слова/номера мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.

5.9. Банк не несет ответственности за убытки Клиента, возникшие вследствие несвоевременного сообщения Банку об утрате Клиентом контроля над номером мобильного телефона, а также утрате Клиентом уверенности в том, что Кодовое слово, номер мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, не могут быть использованы неуполномоченными лицами.

5.10. Клиент обязуется предоставить Банку действительный номер мобильного телефона и обеспечить постоянную доступность номера мобильного телефона для приема сообщений в формате SMS-сообщений на русском/английском языке.

5.11. Клиент несет ответственность за достоверность номера мобильного телефона, обязан не допускать создание дубликатов (клонов) sim-карты, а также не допускать получение, использование и замену sim-карты и/или номера мобильного телефона, Кодового слова неуполномоченными лицами.

5.12. Клиент обязуется обеспечить хранение информации о Кодовом слове способом, делающим Кодовое слово недоступным третьим лицам.

Банк обязуется принять все необходимые меры организационного и технического характера для обеспечения невозможности доступа неуполномоченных лиц к информации о Кодовом слове, номере мобильного телефона Клиента, находящейся в распоряжении Банка.

5.13. Клиент подтверждает, что ему известно

messages on transactions with signs of money transfer without the consent of the Client, by the Client or the compromise thereof.

5.8. The Bank shall not be liable for the Client's losses resulting from the loss (damage, transfer, disclosure) of the Code Word/mobile phone number, to which number the Bank sends SMS messages on transactions with signs of money transfer without the consent of the Client, by the Client.

5.9. The Bank shall not be liable for losses of the Client arising out of the late notification of the Bank about the loss of control over the mobile phone number by the Client, as well as the loss by the Client of confidence that the Code Word, mobile number, to which the Bank sends SMS messages on transactions with signs of money transfer without the consent of the Client, cannot be used by unauthorized persons.

5.10. The Client shall provide the Bank with a valid mobile phone number and ensure that the mobile phone number is always available for receiving SMS messages in Russian/English.

5.11. The Client shall be liable for the accuracy of the mobile phone number, shall prevent any duplication (cloning) of the SIM card, and prevent the receipt, use, and replacement of the SIM card and/or mobile phone number, the Code Word by unauthorized persons.

5.12. The Client shall ensure the safekeeping of information about the Code Word in a manner that makes the code word inaccessible to third parties.

The Bank shall take all the necessary measures of the organizational and technical nature to ensure that unauthorized persons cannot access the information on the Code Word and the Client's mobile phone number available to the Bank.

5.13. The Client is hereby aware of the risk of

о том, что в процессе передачи информации путем направления SMS-сообщения возможен риск несанкционированного доступа третьих лиц к такой информации и настоящим выражает свое согласие с тем, что Банк не несет ответственности за разглашение информации о Клиенте, операциях по его Счетам в случае такого несанкционированного доступа.

5.14. Клиент соглашается с тем, что Банк не несет ответственности за какие-либо аварии, сбои и перебои в обслуживании, связанные с оборудованием, системами передачи электроэнергии и/или линий связи, сети «Интернет», которые обеспечиваются, подаются, эксплуатируются и/или обслуживаются третьими лицами в связи с направлением Банком Клиенту SMS-сообщения, в том числе убытки, понесенные в связи с неправомерными действиями или бездействием третьих лиц. Банк не несет ответственность за доступность и работоспособность средств связи, с помощью которых Банк осуществляет уведомление Клиента.

#### **Статья 6. Конфиденциальность.**

6.1. Условия и информация, содержащаяся в Соглашении, а также вся переписка, связанная с его исполнением, считаются обеими Сторонами конфиденциальной информацией, составляющей, в том числе, банковскую и коммерческую тайну, которую Стороны не вправе разглашать третьим лицам без предварительного письменного согласия другой Стороны, за исключением случаев, предусмотренных Соглашением и законодательством Российской Федерации, предоставления такой информации независимым аудиторским организациям по их требованию в ходе проведения аудита бухгалтерского учета и финансовой (бухгалтерской) отчетности; когда она оказалась известной третьим лицам до того, как Стороны ее разгласили.

#### **Статья 7. Финансовые взаимоотношения.**

7.1. Порядок оплаты, стоимость работ и услуг, оказываемых Банком Клиенту по

unauthorized access by third parties to the information communicated by SMS messages and hereby agrees that the Bank shall not be liable for any disclosure of such information about the Client and transactions on the Client's Accounts in the event of such unauthorized access.

5.14. The Client hereby agrees that the Bank shall not be liable for any emergencies, malfunctions and interruptions in the services due to equipment, electricity systems and/or communication lines, the Internet, which are provided, supplied, operated and/or maintained by third parties, as related to the SMS messages sent by the Bank to the Client, including losses incurred due to illegal actions or inaction of third parties. The Bank shall not be liable for the availability and operability of the means of communication used by the Bank to notify the Client.

#### **Article 6. Confidentiality.**

6.1. Terms and information, contained in the present Agreement, as well as all the correspondence, relating to its execution, are considered as confidential by both Parties, constituting, inter alia, a bank and commercial secret, which the Parties have no right to disclose to third parties without preliminary written consent thereto of the other Party, only in case and in the manner, as under the present Agreement and the legislation of the Russian Federation and provision of such kind of information to independent audit organizations on their demand in the process of audit of accounting and financial (accounting) reports; when it has been disclosed to the third parties before it was disclosed by the Parties.

#### **Article 7. Mutual financial relations.**

7.1. Manner of payment, price of works and services, rendered by the Bank to the Client as

настоящему Соглашению, устанавливаются Тарифами<sup>2</sup> и настоящим Соглашением. Расчеты производятся в рублях путем списания Банком (без дополнительных распоряжений Клиента) денежных средств с расчетного и/или иных счетов Клиента, открытых в Банке, с которых такое списание допускается законодательством Российской Федерации, предварительно полностью до оказания услуг. Если денежные средства списываются со счета Клиента в иностранной валюте, а сумма, причитающаяся Банку в соответствии с Тарифами, выражена в рублях, Банк самостоятельно производит конверсию указанных средств по курсу Банка России на день совершения операции и направляет полученную сумму для оплаты услуг Банка.

7.2. В случае, если остаток денежных средств на расчетном и/или иных счетах Клиента не позволяет Банку в срок и в размере, определенных Соглашением и действующими Тарифами, произвести списание платы за услуги Банка, Банк имеет право не оказывать запрашиваемые Клиентом услуги и/или приостановить обслуживание Клиента по Системе до момента полной оплаты задолженности Клиентом, соответственно уведомив об этом Клиента не менее чем за 5 (пять) Рабочих дней Банка. Клиент отказывается от любых претензий к Банку за возникновение в этом случае возможных убытков, включая реальный ущерб и упущенную выгоду, связанных с задержками в проведении Клиентом операций по Счету, счету депо, счету по вкладу (депозиту), осуществления иных действий, сделок.

7.3. В случае расторжения Клиентом Соглашения в одностороннем порядке, Клиент обязан не позднее 3 (трех) Рабочих дней Банка от даты направления уведомления о расторжении оплатить стоимость оказанных услуг.

7.4. Клиент настоящим дает согласие (заранее данный акцепт) на исполнение (в том числе

under the present Agreement, are set by the Tariffs<sup>2</sup> and the present Agreement. Settlements are conducted in rubles through the direct debiting by the Bank (without additional Client's orders) of the funds from the settlement and/or other accounts held by the Client in the Bank, from which such debiting is permitted by the legislation of the Russian Federation, preliminarily in full prior to the provision of services. If the funds are debited from a foreign currency account of the Client, and the amount due to the Bank, as in compliance to the Tariffs, is expressed in rubles, Bank individually converts the specified funds at the exchange rate of the Bank of Russia as at the day of the commission of the operation and directs the received amount for payment for the Bank's services.

7.2. In case if the balance of funds in the settlement and/or other accounts of the Client does not allow the Bank, within the term and in the amount set by the Agreement and the effective Tariffs, to debit the amount of payment for the services of the Bank, the Bank shall have the right not to render the services requested by the Client and/or suspend the servicing of the Client in the System until the full payment of the Client's debt has been made, correspondingly notifying the Client of such at least 5 (five) Business Days of the Bank in advance. The Client refuse to file any claims with the Bank for the occurrence, in such case, of possible losses, including real damage and lost profits, related to the delays in commissioning Client operations on the Account, depot account, deposit account, or other actions or transactions.

7.3. In case the Client terminates the Agreement in a unilateral manner, Client shall no later than 3 (three) Business Days of the Bank from the date of the sending of the notification about the termination, cover the cost of rendered services.

7.4. Hereby the Client gives his consent (pre-authorization) to the execution (including

<sup>2</sup> Тарифы не включают расходы на выезд за пределы г. Москвы к месту проведения работ по установке и обслуживанию Системы, которые оплачиваются Клиентом дополнительно на основании представленных Банком документов, подтверждающих эти расходы и списываются Банком со счета Клиента без дополнительных распоряжений Клиента. / Tariffs shall not include travel expenses outside Moscow to the place of installation and maintenance of the System, which are to be additionally paid by the Client on the basis of support documents provided by the Bank and shall be debited by the Bank from the Client's account without additional orders from the Client.

частичное) Банком, в полной сумме платежных требований/инкассовых поручений Банка или иных документов, установленных Банком России, для осуществления прав, предусмотренных п.7.1 Соглашения, в течение срока действия Соглашения.

### **Статья 8. Ответственность Сторон.**

8.1. За неисполнение и/или ненадлежащее исполнение обязательств по Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации.

8.2. Клиент несет ответственность за сохранность и целостность установленного программного обеспечения, включая Средства защиты информации, за выполнение требований к эксплуатации Системы, изложенных в Соглашении и Документации, за надлежащее выполнение условий Соглашения, а также за использование Ключей только Уполномоченным представителем Клиента, указанным в соответствующих Данных о Владельце сертификата ключа проверки ЭП (Приложение №5 к Соглашению).

8.3. Банк несет ответственность перед Клиентом в соответствии с законодательством Российской Федерации, при наличии вины за реальный ущерб, но не за упущенную выгоду, с учетом ограничений, предусмотренных п.8.4 Соглашения, за точное, своевременное и полное исполнение поручений и инструкций Клиента по проведению банковских, депозитарных операций, по совершению иных действий, сделок, на основании надлежащим образом оформленных и своевременно переданных по Системе Электронных документов Клиента.

8.4. Банк не несет ответственности:

- за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Клиентом Электронного документа, признанного верным и принятого Банком к исполнению (любой Электронный документ, подписанный Уполномоченным представителем Клиента в соответствии с Соглашением и полученный Банком по Системе, в любом случае признается

partial execution) by the Bank of Bank's payment requests/collection orders or other documents stipulated by the Bank of Russia, in full, for the implementation of rights specified in the p. 7.1 of the Agreement within the validity period of the Agreement.

### **Article 8. Liability of the Parties.**

8.1. The Parties shall be held liable for non-performance and/or improper performance of the duties under the Agreement, as in compliance to the legislation of the Russian Federation.

8.2. The Client shall be responsible for the security and entirety of the installed software, including the information security products, for the observance of the requirements for the operation of the System, specified in the Agreement and the Documentation, for due execution of the terms of the Agreement, as well as for the use of Keys only by the Authorized Representative of the Client specified in the corresponding Information on the ES Verification Key Certificate Holder (Annex No. 5 to the Agreement).

8.3. The Bank shall be held liable before the Client, as in compliance to the legislation of the Russian Federation, in case of its fault for real damage, but not for lost profits, in light of the restrictions, as under Paragraph 8.4 of the Agreement, for the exact, timely and full execution of the orders and instructions presented by the Client for the commission of banking operations, custody transactions and other actions or transactions on the basis of the duly drawn up and timely transferred, within the System, Electronic Documents of the Client.

8.4. The Bank shall not be liable for the following:

- for the consequences of operations, other actions or transactions on the basis of a duly drafted Electronic Document from the Client, acknowledged as accurate and accepted by the Bank for execution (any Electronic Document signed by the Authorized Representative of the Client in compliance to the Agreement and received by the Bank through the System, is in any case found as an Electronic Document received from the Client, which excludes

Электронным документом, исходящим от Клиента, что не допускает отказ Клиента от того, что такой документ направлен с его стороны, ни при каких обстоятельствах);

- за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Клиентом Электронного документа, подписанного прежним Уполномоченным представителем Клиента, до получения от Клиента письма об аннулировании соответствующего комплекта Ключей;

- за последствия отказа Банка в соответствии с п.п. 4.3.2, 4.3.5 - 4.3.7 Соглашения от приема к исполнению Электронного документа, переданного Клиентом по Системе;

- за последствия использования Системы, установленной у Клиента, посторонними, а также неуполномоченными на это лицами;

- за последствия разглашения Клиентом информации о порядке работы Системы, включая порядок использования Средств защиты информации;

- за нарушение работы Системы и возникновение трудностей в осуществлении операций, иных действий посредством Системы в результате ошибок и неточностей, допущенных Клиентом;

- за нарушение работы Системы в результате неисправности Средств обработки и хранения информации Клиента, используемых для доступа к Системе;

- за нарушение работы Системы в результате действий третьих лиц;

- за последствия нарушения Клиентом требований и правил, приведенных в Соглашении и Документации;

- за последствия нарушения работоспособности телекоммуникационных линий связи, сети «Интернет»;

- за убытки Клиента, возникшие вследствие несвоевременного сообщения Банку о Компрометации ключей;

- за убытки, возникшие в результате утраты (порчи, передачи, утери, разглашении) Клиентом применяемых в Системе паролей, Ключей, Конфиденциальной информации и/или программного обеспечения;

- за убытки, возникшие в результате использования Системы в нарушение каких-либо требований законодательства

Client's refusal from the fact that such document was sent on its behalf, under any circumstances);

- for the consequences of operations, other actions or transactions on the basis of a duly drafted Electronic Document from the Client, signed by the former Authorized Representative of the Client, until the date of receipt of a letter on cancellation of the respective Key set from the Client;

- for the consequences of the Bank's refusal, in compliance to Paragraphs 4.3.2, 4.3.5 - 4.3.7 of the Agreement, to accept for execution an Electronic document, transferred by the Client via the System;

- for the consequences of use of the System, installed for the Client, by third parties, as well as by persons not authorized for such use;

- for the consequences of the disclosure by the Client of the information on the procedure of operation of the System, including the procedure for the use of information security products;

- for the malfunction of the System and occurrence of difficulties in the commission of operations in the System as a result of errors inaccuracies, admitted by the Client;

- for the malfunction of the System as a result of an error in the products designed for processing and storage of information of the Client, used to access the System;

- for the malfunction of the System as a result of actions of third parties;

- for the consequences of Client's violation of rules and requirements, as presented in the Agreement and the Documentation;

- for the consequences of malfunctions in the telecommunication lines and the Internet;

- for the losses sustained by the Client, arising as a result of untimely message to the Bank about the Key compromise;

- for the losses, arising a result of loss (damage, transfer, loss, disclosure) by the Client of the passwords used in the System, Keys, Confidential Information and/or software;

- for the losses, arising as a result of the use of the System in violation of any requirements of the legislation of the Russian Federation,



Российской Федерации, применимого к деятельности Клиента.

### **Статья 9. Порядок разрешения споров.**

9.1. Стороны примут все меры к разрешению всех споров и разногласий, связанных с толкованием Сторонами Соглашения и его выполнением путем переговоров.

9.2. В случае, если Стороны не придут к взаимоприемлемому решению путем переговоров, Сторона, предъявившая претензию, официально вручает другой Стороне уведомление о претензии в письменном виде на бумажном носителе. Сторона, получившая уведомление, проводит расследование по факту претензии в течение 7 (семи) календарных дней от даты получения уведомления, по истечении которых на бумажном носителе уведомляет другую Сторону о результатах расследования.

9.3. В случае, если результаты расследования не удовлетворяют Сторону, предъявившую претензию, либо если такое уведомление не получено Стороной, предъявившей претензию, Стороны формируют техническую комиссию для разбора конфликтной ситуации в течение 15 (пятнадцати) календарных дней с момента истечения срока, указанного в п. 9.2 Соглашения. Целью работы комиссии является установление правомерности и обоснованности претензии. Порядок разбора конфликтной ситуации приведен в Приложении №3 к Соглашению. В состав комиссии включаются в равном количестве представители Банка и представители Клиента, а также представители организации–разработчика Системы и, в случае необходимости, независимые эксперты. Состав комиссии согласовывается Сторонами в акте. Их полномочия подтверждаются доверенностями. Срок действия комиссии составляет не более 14 (четырнадцать) календарных дней.

9.4. Работа комиссии проходит на территории Банка.

9.5. В случае отсутствия у одной из Сторон каких-либо материалов, требуемых для установления правомерности и

applicable to the operations of the Client.

### **Article 9. Settlement of disputes.**

9.1. The Parties shall undertake all the possible measures for the resolution of all the disputes and disagreements, relating to the interpretation, by the Parties, of the Agreement and its execution, through negotiations.

9.2. In case if Parties will fail to reach a mutually beneficial solution through negotiations, Party, which has filed the claim, will officially present the other Party with a notification on the claim submitted in writing on paper. Party that received the notification shall conduct an investigation on the fact of the claim, within a period of 7 (seven) calendar days from the date of reception of the notification, upon the expiry of which it shall notify the other Party, on paper, about the results of the investigation.

9.3. If the results of the investigation will not satisfy the Party which has filed the claim, or if such notification was not received by the Party, which filed the claim, Parties shall organize a technical committee for the for the resolution of the conflict situation, within a period of 15 (fifteen) calendar days from the moment of the expiration of the term specified in Paragraph 9.2. of the Agreement. Work objective of the committee is the establishment of legitimacy and justification of the claim. Procedure for the resolution of the conflict situation is shown in Annex No. 3 to the Agreement. The committee shall include, equally, the representatives of the Bank and the representatives of the Client, as well as representatives of the System developer company, and if such is required, independent experts. Composition of the committee is agreed by the Parties with an Act. Their authorities are substantiated by power of attorneys. Validity period of the committee constitutes a maximum of 14 (fourteen) calendar days.

9.4. Work of the committee takes place on the territory of the Bank.

9.5. In case one of the Parties lacks any materials, required for the establishment of legality and justification of the claim (list of

обоснованности претензии (перечень материалов приведен в Приложении №3 к Соглашению), спор решается в пользу другой Стороны.

9.6. Результат работы комиссии оформляется актом, в котором определяются последующие действия Сторон.

9.7. В случае, если техническая комиссия не будет создана в сроки, предусмотренные Соглашением, либо, если в течение 14 (четырнадцать) календарных дней с момента создания технической комиссии, ее работа не даст результата, либо, если Стороны не придут к взаимоприемлемому решению, спор передается на рассмотрение в Арбитражный суд г. Москвы в соответствии с законодательством Российской Федерации.

9.8. Стороны признают, что Электронные документы, направленные Сторонами друг другу по Системе или хранящиеся в Банке в соответствии с Соглашением, а также соответствующие протоколы почтовых серверов и(или) сведения из баз данных, протоколирующих отправку каждого уведомления с его содержанием, сформированные на бумажных носителях, подписанные уполномоченным лицом и скрепленные печатью, записи телефонных разговоров между Сторонами являются достаточным доказательством соответствующего факта и могут быть представлены в качестве надлежащего доказательства в суд в случае рассмотрения спора, возникшего в результате применения Системы, а также при рассмотрении споров в досудебном порядке в соответствии с Соглашением.

#### **Статья 10. Срок действия Соглашения.**

10.1. Соглашение вступает в силу с момента подписания Договора об использовании ДБО уполномоченными представителями Сторон.

10.2. Соглашение действует до момента прекращения обязательств по всем ДБС.

10.3. Банк вправе отказаться от исполнения настоящего Соглашения полностью в одностороннем порядке, письменно уведомив об этом Клиента, в случае, если по истечении 6 (шести) месяцев с даты заключения Соглашения Банком от Клиента посредством

materials in presented in Annex No. 3 to the Agreement), the dispute shall be resolved in favor of the other Party.

9.6. The result of the work conducted by the committee is documented by a report, which defines the follow-up actions of the Parties.

9.7. If the technical committee will not established within the terms, as defined by the Agreement, or if during 14 (fourteen) calendar days from the moment of the establishment of the technical committee its operations will not provide any results, or, if the Parties fail to reach a mutually acceptable solution, the dispute shall be transferred for consideration by the Arbitration court of Moscow as in compliance to the legislation of the Russian Federation.

9.8. The Parties acknowledge that the Electronic documents, directed by the Parties to each other through the System or the ones stored in the Bank in compliance to the Agreement, as well as the corresponding protocols of mail servers and (or) information from the databases recording the sending of each notification with its content on paper signed by the authorized person and sealed, records of telephone conversations between the Parties shall be sufficient evidence of the respective fact and may be presented as an adequate evidence before the court, in case of the consideration of the dispute, arising as a result of the application of the System, as well as during the consideration of disputes in a pre-trial proceedings as in compliance with the Agreement.

#### **Article 10. Validity period of the Agreement.**

10.1. The Agreement shall enter into force from the moment of the Contract on the Use of RBS signing by the authorized representatives of the Parties.

10.2. The Agreement shall remain valid until the end of the obligations under all BAAs.

10.3. The Bank shall have the right to fully repudiate this Agreement unilaterally upon a written notice to the Client, if following six (6) months after the date of signing of the Agreement by the Bank no Electronic Document has been received from the Client

Системы в течение указанного времени не будет получен Электронный документ в соответствии с п.3.5 Соглашения или в течение указанного времени Клиент не устанавливал защищенное соединение с Банком для приема и отправки любых Электронных документов.

10.4. Соглашение может быть расторгнуто по письменному заявлению одной из Сторон (односторонний отказ от исполнения Соглашения полностью).

В случае расторжения Соглашения по инициативе Банка, Банк уведомляет об этом Клиента не позднее, чем за 14 (четырнадцать) календарных дней до даты расторжения.

В случае расторжения Соглашения по инициативе Клиента, Клиент в письменной форме на бумажном носителе уведомляет об этом Банк не позднее, чем за 3 (три) Рабочих дня Банка до даты расторжения.

Расторжение Соглашения до истечения срока его действия не освобождает Стороны от выполнения обязательств, предусмотренных Соглашением и не исполненных до даты его расторжения, и не лишает Сторону, чьи права по Соглашению нарушены в результате невыполнения обязательств другой Стороной, требовать защиты своих прав в соответствии с законодательством Российской Федерации и Соглашением.

#### **Статья 11. Обстоятельства непреодолимой силы.**

11.1. Стороны освобождаются от ответственности за неисполнение и/или ненадлежащее исполнение обязательств по Соглашению, если такое неисполнение явилось результатом действий или обстоятельств непреодолимой силы (далее - Форс-мажор), то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств.

11.2. Под термином Форс-мажор понимаются наводнение, пожар, землетрясение, ураган, взрыв, оседание почвы, эпидемии и иные подобные явления, а также война или военные действия в месте нахождения Банка или Клиента, забастовки в отрасли или регионе, принятие органом законодательной, исполнительной или судебной власти акта, повлекшие за собой невозможность надлежащего исполнения Соглашения

in accordance with Paragraph 3.5 of the Agreement or if the Client has failed to establish, during said period, a secured connection with the Bank for reception and transmission of any Electronic Documents.

10.4. The Agreement may be terminated under the written application of one of the Parties (a unilateral repudiation of the Agreement in its entirety).

In case of the Agreement termination at the Bank's initiative, the Bank shall notify the Client thereof no later than 14 (fourteen) calendar days prior to the date of termination.

In case of the Agreement termination at the Client's initiative, the Client shall notify the Bank thereof no later than 3 (three) Bank's Business Days prior to the date of termination in writing on paper.

Termination of the Agreement prior to the end of its validity does not free the Parties from the execution of the obligations, as under the Agreement and which were left un-executed before the date of its termination, and does not deprive the Party, whose rights under the Agreement have been violated as a result of the non-execution of the obligations by the other Party, of the right to demand protection of its rights as in compliance to the legislation of the Russian Federation and the Agreement.

#### **Article 11. Force Majeure.**

11.1. The Parties shall be freed from liability for non-performance and/or improper performance of the obligations under the Agreement, if such non-performance was a result of the actions or effect of force majeure (hereinafter the Force Majeure), i.e. extraordinary and unavoidable, in the given conditions, circumstances.

11.2. Force Majeure is understood as a flood, fire, earthquake, hurricane, explosion, soil shrinkage, epidemic and other similar occurrences, as well as war or military actions at the location of the Bank or the Client, strikes in the industry or the region, adoption of an act by the authority of legislative, enforcement or judicial power entailing the impossibility of execution of the Agreement by the Parties.

Сторонами.

11.3. Сторона, для которой возникли обстоятельства непреодолимой силы, обязана в течение 7 (семи) Рабочих дней от даты возникновения Форс-мажора уведомить другую Сторону о наступлении таких обстоятельств, с приложением соответствующих доказательств. Доказательством Форс-мажора может служить официальный документ компетентной организации, подтверждающий факт наступления обстоятельств непреодолимой силы.

11.4. В случае наступления обстоятельств непреодолимой силы срок выполнения Сторонами обязательств по Соглашению переносится соразмерно времени, в течение которого действуют такие обстоятельства и их последствия. После прекращения действия Форс-мажора обязательства Сторон возобновляются.

#### **Статья 12. Заключительные положения.**

12.1. Настоящее Соглашение является типовым. Для заключения Соглашения Клиент предоставляет в Банк Договор об использовании ДБО (по форме Банка), который заполняется, подписывается и предоставляется в Банк в двух экземплярах. Соглашение составлено на русском и английском языках. В случае противоречий между версиями Соглашения на русском и английском языке, преимущественную силу имеет версия Соглашения на русском языке.

12.2. Если отдельное положение Соглашения теряет силу или становится неисполнимым, это не приводит к недействительности других его положений.

12.3. С даты заключения Соглашения вся переписка и договоренности между Сторонами, касающиеся условий Соглашения и предшествующие его заключению, теряют силу.

12.4. Вся переписка в рамках исполнения Соглашения осуществляется Сторонами на русском/английском/испанском языке и может быть осуществлена посредством Системы.

12.5. Банк вправе в одностороннем порядке вносить изменения в Соглашение, уведомив об этом всех лиц, присоединившихся к

11.3. The Party, who is faced with the Force Majeure, shall within a period of 7 (seven) Business Days from the date of occurrence of the Force Majeure, inform the other Party about the occurrence of such circumstances, with an annex of the corresponding evidence. Evidence of Force Majeure can be an official document from a competent organization, confirming the fact of occurrence of the Force Majeure circumstances.

11.4. In case of occurrence of the Force Majeure circumstances the term for the execution of the obligations by the Parties as under the Agreement shall be transferred commensurate to the time, during which such circumstances and their consequences take effect. After the end of the Force Majeure the obligations of the Parties resume.

#### **Article 12. Final Provisions.**

12.1. This Agreement is a standard agreement. For the purposes of entering into the Agreement, the Client shall submit to the Bank the Contract on the Use of RBS (in the format of the Bank), which shall be filled out, signed, and submitted to the Bank in duplicate. The Agreement is executed in Russian and English. In the event of a conflict between the Russian and English versions of the Agreement, the Russian version of the Agreement shall prevail.

12.2. If a separate provision of the Agreement becomes invalid or unenforceable, this shall not invalidate other provisions of the Agreement.

12.3. From the date of the Agreement, all the correspondence and arrangements between the Parties concerning the terms and conditions of the Agreement before the above date shall become null and void.

12.4. All the correspondence within the framework of the execution of the Agreement shall be carried out by the Parties in Russian/English/Spanish and may be carried out through the System.

12.5. The Bank may unilaterally amend the Agreement upon notification of all the persons who have joined the Agreement no later than

Соглашению, не позднее чем за 10 (десять) календарных дней до вступления в силу указанных изменений. Указанный в настоящем пункте срок уведомления может быть уменьшен Банком в случае внесения изменений в Соглашение в связи с изменением законодательства Российской Федерации.

В случае изменения законодательства Российской Федерации Соглашение, до момента его изменения Банком применяется в части, не противоречащей требованиям законодательства Российской Федерации.

12.6. Банк с целью ознакомления Клиентов с Соглашением публикует его на официальном сайте Банка в сети «Интернет» по адресу: [www.evrofinance.ru](http://www.evrofinance.ru).

Банк уведомляет всех лиц, присоединившихся к Соглашению, о внесении в него изменений путем публикации информационного письма, а также полного текста изменений на официальном сайте Банка в сети «Интернет» по адресу: [www.evrofinance.ru](http://www.evrofinance.ru). Дополнительно к указанному способу уведомления Банк по своему усмотрению может использовать иные способы информирования Клиента.

Моментом публикации Соглашения, Тарифов и информации для ознакомления Клиентов, а также моментом ознакомления Клиента с опубликованными Соглашением, Тарифами и информацией для ознакомления Клиентов считается момент их первого размещения на официальном сайте Банка в сети «Интернет» по адресу: [www.evrofinance.ru](http://www.evrofinance.ru).

12.7. Действие изменений, внесенных в Соглашение, и вступивших в силу, распространяется на всех лиц, присоединившихся к Соглашению, независимо от даты присоединения к Соглашению (даты заключения Договора об использовании ДБО). В случае несогласия с изменениями, вносимыми в Соглашение, Клиент вправе расторгнуть Соглашение в одностороннем порядке до вступления таких изменений в силу в порядке, установленном в п.10.4 Соглашения.

12.8. В случае, если до вступления в силу опубликованных Банком изменений и/или дополнений, внесенных в Соглашение, Соглашение не расторгнуто, Стороны

10 (ten) calendar days before the amendment effective date. The notification period specified herein may be reduced by the Bank in the event of amendments to the Agreement due to changes in the laws of the Russian Federation.

In the event of changes in the laws of the Russian Federation, the Agreement shall apply to the extent it does not contradict the laws of the Russian Federation until amended by the Bank.

12.6. To make the Agreement available to the Clients for review, the Bank shall publish it on the Bank's official website in the Internet at: [www.evrofinance.ru](http://www.evrofinance.ru).

The Bank shall notify all the persons who have joined the Agreement of any amendments hereto by publishing an information letter, as well as the full text of the amendments on the official website of the Bank in the Internet at: [www.evrofinance.ru](http://www.evrofinance.ru). In addition to the above notification method, the Bank may, at its own discretion, use other ways to inform the Client.

The moment of publishing the Agreement, Tariffs, and information for the Clients' reference, as well as the moment of the Client's review of the Agreement, Tariffs, and information for the Clients' reference shall be deemed the time when they are first posted on the Bank's official website in the Internet at: [www.evrofinance.ru](http://www.evrofinance.ru).

12.7. Effective amendments to the Agreement shall apply to all the persons who have joined the Agreement, regardless of the date when they joined the Agreement (date of the Contract on the Use of RBS). In case the Client disagrees with the amendments to the Agreement, the Client may terminate the Agreement unilaterally before such changes take effect in the accordance with the procedure established by p. 10.4 of the Agreement.

12.8. If the Agreement is not terminated before the effective date of the amendments and/or supplements to the Agreement published by the Bank, the Parties shall deem

<p>признают, что указанные изменения и/или дополнения в Соглашение приняты Клиентом.</p> <p>12.9. Банк не несет ответственности, если информация об изменении и/или дополнении Соглашения, опубликованная в порядке и в сроки, установленные Соглашением, не была получена и/или изучена и/или правильно истолкована Клиентом.</p> <p>12.10. Список Приложений, являющихся неотъемлемой частью Соглашения:</p> <ul style="list-style-type: none"> <li>- Приложение №1 «Требования к аппаратно-программным средствам».</li> <li>- Приложение №2 «Способы доставки информации».</li> <li>- Приложение №3 «Порядок разбора конфликтных ситуаций».</li> <li>- Приложение №4 «Требования по информационной безопасности».</li> <li>- Приложение №5 «Данные о Владельце сертификата ключа проверки ЭП».</li> <li>- Приложение №6 «Акт признания открытого ключа (сертификата) для обмена сообщениями».</li> </ul>	<p>such amendments and/or supplements to the Agreement accepted by the Client.</p> <p>12.9. The Bank shall not be liable if the information on the amendments and/or supplements to the Agreement published in the manner and within the period established by the Agreement has not been received and/or studied and/or correctly interpreted by the Client.</p> <p>12.10. List of Annexes, constituting an integral part of the Agreement:</p> <ul style="list-style-type: none"> <li>- Annex No. 1 «Requirements to hardware and software».</li> <li>- Annex No. 2 «Means for the delivery of information».</li> <li>- Annex No. 3 «Procedure for the resolution of conflict situations».</li> <li>- Annex No. 4 «Information safety requirements».</li> <li>- Annex No. 5 «Information on the ES Verification Key Certificate Holder ».</li> <li>- Annex No. 6 «Act of acknowledgement of the public key (certificate) for message exchange».</li> </ul>
---	--

<p style="text-align: center;"><b>Приложение №1</b> <b>к Соглашению об использовании электронной</b> <b>системы дистанционного банковского</b> <b>обслуживания</b></p> <p>№ _____ от « ____ » _____ 20__ г.</p> <p style="text-align: center;"><b>ТРЕБОВАНИЯ К АППАРАТНО-ПРОГРАММНЫМ СРЕДСТВАМ</b></p> <ol style="list-style-type: none"> <li>1. Операционная система Windows 7 и выше.</li> <li>2. Браузер Internet Explorer версии 9.0 или выше (только для установки рабочего места Клиента подсистемы «Интернет Клиент-банк»).</li> <li>3. Наличие подключенного сетевого или локального принтера.</li> <li>4. Наличие подключения к сети Internet.</li> <li>5. Microsoft Word версии не ниже 97 или OpenOffice версии не ниже 2.3.0.</li> <li>6. Перед установкой системы необходимо установить программное обеспечение Средства защиты информации.</li> <li>7. При обмене информацией с бухгалтерскими системами (далее - БС) «1С», «Парус», БЭСТ-4 и с другими БС, в которых есть возможность экспорта документов в текстовый формат, необходимо, чтобы формат дат и чисел импортируемых документов соответствовал форматам дат и чисел, задаваемых в региональных настройках операционной системы компьютера.</li> <li>8. В региональных настройках операционной системы компьютера формат дат должен использоваться ДД.ММ.ГГГГ.</li> <li>9. В региональных настройках операционной системы компьютера в качестве десятичного разделителя чисел и сумм должна использоваться точка («.»).</li> <li>10. ODBC-драйвер MS Access (только для установки рабочего места Клиента подсистемы «Клиент-банк»).</li> </ol>	<p style="text-align: center;"><b>Annex No. 1</b> <b>To the Agreement on the use of an electronic system</b> <b>for remote banking services</b></p> <p>No. _____ dated _____ 20__</p> <p style="text-align: center;"><b>REQUIREMENTS FOR THE SOFTWARE AND HARDWARE.</b></p> <ol style="list-style-type: none"> <li>1. Operating system Windows 7 or higher.</li> <li>2. Browser Internet Explorer v. 9.0 or higher (only for installation of the Internet Client-Bank subsystem on the Client's workstation).</li> <li>3. Availability of connected network or local printer.</li> <li>4. Internet connection.</li> <li>5. Microsoft Word 97 or higher, or OpenOffice 2.3.0 or higher.</li> <li>6. The Information Security Products software must be installed before installing the System.</li> <li>7. When exchanging information with accounting systems (ASs) "1C", "Parus", BEST-4, and with other ASs, in which it is possible to export documents in text format, the format of dates and numbers of imported documents must coincide with the formats of dates and numbers set in the regional settings of the computer operating system.</li> <li>8. The date format in the regional settings of the computer operating system must be DD.MM.YYYY.</li> <li>9. In the regional settings of the computer operating system, a dot (.) must be used as a decimal separator in numbers and sums.</li> <li>10. ODBC-driver MS Access (only for installation of the Client-Bank subsystem on the Client's workstation).</li> </ol>
--	---

<p style="text-align: center;"><b>Приложение №2</b> <b>к Соглашению об использовании</b> <b>электронной системы дистанционного</b> <b>банковского обслуживания</b> № _____ от « _____ » _____ 20 ____ г.</p> <p style="text-align: center;"><b>СПОСОБЫ ДОСТАВКИ ИНФОРМАЦИИ</b></p> <p><b>1. Работа осуществляется через выделенное подключение к своему провайдеру услуг сети «Интернет» – способ доставки информации на русском языке.</b> Параметры подключения в случае использования - подсистемы «Клиент-Банк»: открытые TCP порты 1024, 1400 на IP адрес 91.227.169.45 - подсистемы «Интернет Клиент-Банк»: открытые TCP порты 80, 443 на сайт <a href="https://online.efbank.ru">https://online.efbank.ru</a> или IP адрес 91.227.169.146 Параметры подключения могут быть изменены и сообщены Клиенту в письменном уведомлении или направлены Клиенту посредством Системы.</p> <p><b><u>Настройка Клиентом данной транспортной схемы осуществляется на рабочем месте самостоятельно согласно требованиям провайдера.</u></b></p> <p><b>2. Работа осуществляется через выделенное подключение к своему провайдеру услуг сети «Интернет» – способ доставки информации на английском языке.</b> Параметры подключения: открытые TCP порты 80, 443, 8443 на сайт <a href="https://dbo.efbank.ru/online">https://dbo.efbank.ru/online</a> или IP адрес 91.227.169.132 Параметры подключения могут быть изменены и сообщены Клиенту в письменном уведомлении или направлены Клиенту посредством Системы.</p> <p><b><u>Настройка Клиентом данной транспортной схемы осуществляется на рабочем месте самостоятельно согласно требованиям провайдера.</u></b></p>	<p style="text-align: center;"><b>Annex No. 2</b> <b>To the Agreement on the use of an electronic</b> <b>system for remote banking services</b> No. _____ dated _____ 20 ____</p> <p style="text-align: center;"><b>MEANS OF DELIVERY OF INFORMATION</b></p> <p><b>1. Work is carried out through a dedicated connection to your Internet service provider – means of delivery of information in Russian.</b> Connection parameters when using - Client-Bank subsystem: open TCP ports 1024, 1400 to IP address 91.227.169.45 - Internet Client-Bank subsystem: open TCP ports 80, 443 to website <a href="https://online.efbank.ru">https://online.efbank.ru</a> or IP address 91.227.169.146 Connection parameters may be changed and communicated to the Client by a written notification or sent to the Client via the System.</p> <p><b><u>The Client shall set this delivery mechanism independently at the workstation according to the provider's requirements.</u></b></p> <p><b>2. Work is carried out through a dedicated connection to your Internet service provider – means of delivery of information in English.</b> Connection parameters: open TCP ports 80, 443, 8443 to website <a href="https://dbo.efbank.ru/online">https://dbo.efbank.ru/online</a> or IP address 91.227.169.132 Connection parameters may be changed and communicated to the Client by a written notification or sent to the Client via the System.</p> <p><b><u>The Client shall set this delivery mechanism independently at the workstation according to the provider's requirements.</u></b></p>
--	---



<p style="text-align: right;"><b>Приложение №3</b></p> <p style="text-align: center;"><b>к Соглашению об использовании электронной системы дистанционного банковского обслуживания</b></p> <p style="text-align: right;">№ _____ от « _____ » _____ 20__ г.</p> <p style="text-align: center;"><b>ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ</b></p> <p><b><u>1. Общие положения</u></b></p> <p>1.1. Ниже приведен перечень конфликтных ситуаций по поводу исполнения Электронных документов (далее - «Документов»), рассматриваемых технической комиссией, действующей в соответствии с порядком, предусмотренным Соглашением:</p> <ul style="list-style-type: none"> <li>- Документ исполнен, а Клиент утверждает, что Документ не посылал и не подписывал;</li> <li>- Клиент утверждает, что он направил Документ, а Документ не исполнен, причем, по утверждению Клиента, от Банка получена Квитанция об исполнении;</li> <li>- Клиент утверждает, что он направил один Документ, а исполнен другой Документ;</li> <li>- другие конфликтные ситуации.</li> </ul> <p>1.2. При разрешении спорных ситуаций Стороны обязуются руководствоваться следующими принципами:</p> <ul style="list-style-type: none"> <li>- Сторона-получатель обязуется признать подлинным и действительным Документ, переданный ей посредством Системы и имеющий ЭП, сформированную на закрытых ключах Стороны-отправителя, при условии положительного результата проверки ЭП на соответствующих открытых ключах;</li> <li>- Сторона-отправитель обязуется признать подлинным (переданным ею посредством Системы) и действительным Документ, имеющий ЭП, сформированную на ее закрытых ключах, при условии положительного результата проверки ЭП на соответствующих открытых ключах;</li> <li>- ответственность возлагается на Сторону-отправителя, при получении Стороной-получателем ложного Документа с успешно подделанной ЭП,</li> </ul>	<p style="text-align: right;"><b>Annex No. 3</b></p> <p style="text-align: center;"><b>To the Agreement on the use of an electronic system for remote banking services</b></p> <p style="text-align: right;">No. _____ dated _____ 20__</p> <p style="text-align: center;"><b>PROCEDURE FOR THE RESOLUTION OF CONFLICT SITUATIONS</b></p> <p><b><u>1. General Provisions</u></b></p> <p>1.1. Below is the list of conflict situations regarding the execution of Electronic documents (hereinafter the «Documents»), considered by the technical committee, acting in compliance to the procedure, as under the Agreement:</p> <ul style="list-style-type: none"> <li>- The document was performed, and the Client insists that the Document was not sent and was not signed by the latter;</li> <li>- The Client asserts that he directed the Document but the Document was not performed, however, according to the Client, Bank provide a confirmation receipt for the above document;</li> <li>- The Client asserts, that he sent one Document, but a different Document was performed;</li> <li>- other conflict situations.</li> </ul> <p>1.2. During the resolution of conflict situations Parties undertake to be guided by the following principles:</p> <ul style="list-style-type: none"> <li>- Receiving party undertakes to acknowledge, as authentic and valid, the Document transferred thereto through the System and which has a Electronic Signature, formed on the closed keys of the Sending party, subject to the positive result of the Electronic Signature verification on the corresponding open keys;</li> <li>- Sending party undertakes to acknowledge as authentic (transferred thereto through the System) and valid the Document which has an Electronic Signature, formed under its private keys, subject to the positive result of the Electronic Signature verification on the corresponding open keys;</li> <li>- the responsibility is borne with the Sending party in case the Receiving party receives a false document with successfully falsified Electronic signature, as in this case</li> </ul>
--	--

так как в этом случае Сторона-отправитель не обеспечила сохранность Закрытых ключей ЭП.

1.3. Стороны признают, что математические свойства алгоритма ЭП гарантируют невозможность подделки значения ЭП любым лицом, не обладающим закрытым ключом подписи.

1.4. Стороны должны представить комиссии следующие материалы:

- носители информации с файлами, содержащими выгруженные из Системы путем использования функционала «Выгрузка данных для проверки подписи» спорный Документ, а также распечатанный из Системы спорный Документ или Квитанцию на него. Описание процедуры выгрузки данных для проверки подписи приведено в Документации;
- подписанные собственноручными подписями уполномоченных лиц Клиента и Банка оригиналы Актов признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению);
- носитель с Ключами Средств защиты информации.

1.5. Проверка подлинности Электронного документа осуществляется посредством программы OpenSSL.exe. Описание программы приведено в документации на официальном сайте разработчика в сети «Интернет»: <http://openssl.org/docs/>.

## **2. Процедура проверки подлинности Электронных документов**

2.1. Для разбора конфликтных ситуаций техническая комиссия выполняет следующие действия:

- проверяет подлинность ЭП под выгруженным спорным Документом с использованием Открытого ключа ЭП Стороны-отправителя данного Документа;
- проверяет соответствие

the Sending party did not assure the security of the Private Electronic signature keys.

1.3. Parties agree that the mathematical features of the Electronic signature algorithm, guarantee impossibility of falsification of the Electronic Signature value by any person, who does not possess the private signature key.

1.4. Parties must present the following materials to the committee:

- data carriers with the files, containing the disputed Document downloaded from the System through the use of the function «Downloading of data for the verification of the signature», as well as the Disputed document printed from the system or the Receipt received for it. Description of the procedures for the downloading of data for the verification of the signature is provided in the Documentation;
- original copies of the Acts of acknowledgement of the public key (certificate) for message exchange (Annex No. 6 to the Agreement) signed with the handwritten signatures of the authorized persons of the Client and the Bank;
- carrier with the Keys for the Information Security Products.

1.5. Verification of the authenticity of an Electronic document is conducted through the OpenSSL.exe application. Description of the application is shown in the documentation at the official website of the developer, on the Internet: <http://openssl.org/docs/>.

## **2. Procedure for the verification of the authenticity of the Electronic documents.**

2.1. For the resolution of conflict situations the technical committee performs the following:

- verification of authenticity of the Electronic Signature on the downloaded disputed Document with the use of a Public Electronic Signature Key of the Sending party of the given Document;
- verification of conformity of the

<p>экземпляров Актов признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению) предоставленных Сторонами в соответствии с п.1.4. Порядка разбора конфликтных ситуаций;</p> <ul style="list-style-type: none"> <li>– сверяет соответствие ключевых полей открытого ключа из Актов признания открытого ключа (сертификата) для обмена сообщениями с распечаткой протокола проверки ЭП, полученной при помощи программы OpenSSL.exe.</li> </ul> <p>2.2. Результаты работы технической комиссии отражаются в акте, подписанном всеми членами технической комиссии. Члены технической комиссии, не согласные с выводами большинства, подписывают акт с возражениями, который прилагается к основному акту.</p>	<p>copies of the Acts of acknowledgement of the public key (certificate) for message exchange (Annex No. 6 to the Agreement) provided by the Parties as per p. 1.4 of the Procedure for the Resolution of Conflict Situations;</p> <ul style="list-style-type: none"> <li>– reconciliation of the key fields of the public key from the Acts of acknowledgement of the public key (certificate) for message exchange with the printed out ES verification protocol from OpenSSL.exe.</li> </ul> <p>2.2. Results of the measures undertaken by the technical committee are documented in the report, signed by all the members of the committee. Members of the technical committee, who disagree with the conclusions made by the majority, sign a report of objection, which is annexed to the main report.</p>
---	--

<p style="text-align: center;"><b>Приложение №4</b> <b>к Соглашению об использовании электронной</b> <b>системы дистанционного банковского</b> <b>обслуживания</b> № _____ от « ____ » _____ 20__ г.</p> <p style="text-align: center;"><b>ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ</b> <b>БЕЗОПАСНОСТИ</b></p> <p>Для минимизации рисков несанкционированного доступа к Счетам, счету по вкладу (депозиту) Клиента со стороны злоумышленников и компрометации ключевой информации, Банк настоятельно просит Клиентов соблюдать следующие меры информационной безопасности:</p> <ul style="list-style-type: none"> <li>• Выделить компьютер, который не будет использоваться в иных целях, кроме как для работы в Системе; не осуществлять, а при наличии технической возможности, запретить выход в сеть «Интернет» с этого компьютера на иные адреса, за исключением адресов серверов Банка.</li> <li>• Ограничить или полностью запретить удаленный доступ к выделенному компьютеру с других компьютеров локальной сети. Не использовать средства удаленного администрирования на выделенном компьютере. При наличии технических средств, поместить выделенный компьютер в отдельную сеть, контролируруемую межсетевым экраном и системами обнаружения атак.</li> <li>• Заменить все стандартные пароли, заданные при установке Системы, на уникальные собственные, производить периодическую смену паролей (не реже одного раза в три месяца).</li> <li>• Использовать на постоянной основе антивирусное программное обеспечение с последней актуальной версией баз.</li> <li>• Регулярно (не реже одного раза в неделю) выполнять антивирусную проверку для своевременного обнаружения вредоносных программ.</li> <li>• Использовать на компьютере исключительно лицензионное программное обеспечение.</li> <li>• Регулярно (не реже одного раза в месяц или по факту публикации) устанавливать обновления операционной системы.</li> </ul>	<p style="text-align: center;"><b>Annex No. 4</b> <b>To the Agreement on the use of an electronic system</b> <b>for remote banking services</b> No. _____ dated _____ 20__</p> <p style="text-align: center;"><b>INFORMATION SAFETY REQUIREMENTS</b></p> <p>In order to minimize the risks of unauthorized access to the Client's Accounts by law violators and the compromise of key data, the Bank strongly recommends its Clients to comply with the following information safety measures:</p> <ul style="list-style-type: none"> <li>• To choose a computer that shall be used solely for the purpose of working with the System; not to access the Internet from such a computer and, if possible, to prevent all Internet connection from such a computer, except for the connection with the Bank services.</li> <li>• To limit or prohibit remote access to such a computer from all other computers of the local network. Not to use remote administration tools on such a computer. Technical assets permitting, to create a specified network controlled by a network firewall and an intrusion detection system for such a computer.</li> <li>• To replace all default passwords set out at the moment of System installation with unique passwords; to change passwords regularly (not less than once in three months);</li> <li>• To constantly use anti-virus software with the latest versions of databases;</li> <li>• To carry out anti-virus checks on a regular basis (not less than once a week) in order to timely detect malicious software;</li> <li>• To use only licensed software on the computer;</li> <li>• To update the operating system regularly (not later than once a month or upon launching);</li> </ul>
--	--

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• Проверить группу «Администраторы» на выделенном компьютере, исключить всех рядовых пользователей из этой группы, не работающих с Системой.</li> <li>• При наличии технической возможности, для пользователей, работающих с Системой, создать отдельную групповую политику, разрешающую запуск только определенных приложений.</li> <li>• Для доступа к серверам Банка использовать только заведомо известные Вам адреса интернет серверов Банка.</li> <li>• В случае отсутствия возможности подключения к серверу Банка незамедлительно сообщать об этом Банку.</li> <li>• Хранить в безопасном месте (в сейфе) и никому не передавать носители с ключевой информацией, обеспечив к ним доступ только уполномоченных лиц.</li> <li>• Никогда не осуществлять копирование закрытых (секретных) ключей электронной подписи на локальный жесткий диск компьютера, даже с последующим его удалением.</li> <li>• Регулярно (не реже одного раза в месяц) проверять целостность ключевых носителей, проводя проверку наличия на них файлов электронной подписи.</li> <li>• Своевременно (в соответствии с условиями Соглашения) проводить Плановую смену рабочих ключей.</li> <li>• Не оставлять носители с ключевой информацией без присмотра, подключать их к компьютеру только на время использования и незамедлительно их отключать после проведения банковских операций. При оставлении рабочего места Системы без присмотра всегда блокировать экран с последующим вводом пароля для его разблокировки.</li> <li>• Производить незамедлительную замену ключей электронной подписи в случае их компрометации или подозрении на компрометацию.</li> <li>• Своевременно устанавливать все обновления Системы.</li> <li>• Не устанавливать обновления, а также не открывать ссылки в почтовых сообщениях, полученных от имени Банка по электронной почте; получив такое сообщение, незамедлительно сообщать</li> </ul> | <ul style="list-style-type: none"> <li>• To check the Administrator's group on the selected computer and to remove all users that do not operate the System;</li> <li>• Technical assets permitting, develop a separate group policy for the users working with the System and allow the use of specific applications only.</li> <li>• To use only known Internet addresses of Bank servers to access them.</li> <li>• To inform the Bank immediately, in case Bank servers are unavailable.</li> <li>• To store data carriers with key information in a safe place (a vault), never to transfer them to third parties, to limit access to them only to authorized persons;</li> <li>• Never to copy private (secret) digital signature keys on the local hard drive of the computer, even in case the copies are deleted immediately;</li> <li>• Timely (according to the terms and conditions of the Agreement) perform the Planned change of Operational Keys;</li> <li>• To check the integrity of key carriers and the presence of digital signature files on them on a regular basis (not later than once a month);</li> <li>• Not to let the carriers of key information unattended; to connect them to the computer only for the time of use and immediately disconnect after the completion of banking operations. In case a work place with the System is left unattended, to block the screen and to use a password for its further unlocking;</li> <li>• To immediately replace digital signature keys in case of their actual or alleged compromise;</li> <li>• Timely update the System;</li> <li>• Not to install updates and not to open links received in the e-mail from the Bank; to inform the Bank about receiving any such e-mails;</li> </ul> |
|---|--|

<p>об этом Банку.</p> <ul style="list-style-type: none"> <li>• Ежедневно, в течение операционного дня Банка и по окончании Рабочего дня, осуществлять дополнительный вход в Систему для контроля перечня исходящих документов за текущий день. При обнаружении подозрительных документов, незамедлительно обращаться в Банк.</li> <li>• В случае подозрений на замедление работы компьютера отключить компьютер физически от локальной сети и сети «Интернет» и обратиться к системному администратору с просьбой о необходимости проведения полной антивирусной проверки сканированием всех файлов и памяти компьютера.</li> <li>• В случае, если инцидент информационной безопасности все же произошел, ни в коем случае не выключать компьютер, а отключить его физически только от локальной сети и сети «Интернет», незамедлительно обратиться к системному администратору и сообщить об инциденте в Банк для проведения оперативного расследования и принятия необходимых мер для сбора доказательств.</li> <li>• В случае выявления Клиентом подозрительных операций в Системе незамедлительно сообщать об этом в Банк.</li> </ul>	<ul style="list-style-type: none"> <li>• To access the System additionally in order to check the list of the documents for the current day in a daily basis during a banking day and at its end. In case of detection of any suspicious documents, to inform the Bank immediately;</li> <li>• In case of suspicious delays in the computer's operations, to physically disconnect the computer from the local network and the Internet and to request complete anti-virus scanning of all files and computer memory from the system administrator;</li> <li>• In case of a breach of information security, never to turn the computer off, but to disconnect it physically from the local network and the Internet, to address the system administrator immediately and to inform the Bank about the incident in order to carry out on-the-spot investigation and take measures to collect evidence.</li> <li>• In case the Client detects suspicious operations with the System, he should immediately inform the Bank about it.</li> </ul>
---	--

**Приложение № 5**  
**к Соглашению об использовании электронной системы**  
**дистанционного банковского обслуживания**  
 № \_\_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**Annex No. 5**  
**To the Agreement on the use of an electronic system for remote banking**  
**services**  
 No. \_\_\_\_\_ dated \_\_\_\_\_ 20\_\_

**ФОРМА**  
**FORM**

**ДАННЫЕ О ВЛАДЕЛЬЦЕ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭП**  
**INFORMATION ON THE ES VERIFICATION KEY CERTIFICATE HOLDER**

Наименование организации – Владельца сертификатов ключей Organization – Key Certificate Holder	
Уполномоченный представитель Клиента - Фамилия Имя Отчество Authorized Representative of the Client - Full name	
Паспорт/удостоверение личности Passport/ identity card	№ _____ выдан _____ Серия _____ Номер _____ series number issued on
кем выдан паспорт/удостоверение личности Issued by/ID	
дата выдачи Date of issue	место и дата рождения place and date of birth
адрес места жительства (регистрации) Residence address (registration)	
Гражданство Citizenship	идентификационный номер налогоплательщика (ИНН) (при его наличии, при его отсутствии - указать «отсутствует») taxpayer's identification number (INN) (if available, if not available - indicate «not available»)

данные миграционной карты: \_\_\_\_\_  
 Migration card information

Логин (6-10 символов): \_\_\_\_\_  
 Login (6-10 symbols)

Право подписи документов: единственная, первая, вторая, без права подписи  
 (ненужное зачеркнуть)  
 Right to sign the documents: single, first, second, without the right to sign documents  
 (delete as applicable)

**Полномочия при наличии права подписи: подписание ЭП всех Электронных документов, предусмотренных Соглашением, направляемых Клиентом в Банк посредством Системы.**

**Authorities, in case of availability of the right of signature: signing with the Electronic signature of all the Electronic documents, as provided for by the Agreement, directed by the Client to the Bank through the System.**

**Полномочия «без права подписи»: вход в Систему, создание любых Электронных документов, предусмотренных Соглашением, установление защищенного соединения с Банком для приема и отправки любых Электронных документов, подписанных Уполномоченными представителями Клиента.**

**Authorities «without right of signature»: log-in the System, creation of any Electronic documents, provided by this Agreement, establishment of protected connection with the Bank for receiving and sending of any Electronic documents signed by the Authorized Representatives of the Client.**

---

(подпись Уполномоченного  
представителя Клиента)  
(signature of the Authorized  
Representative of the Client)

Руководитель  
Director:

---

(подпись) / (Ф.И.О.)  
(signature) (Full name)

М.П.  
Stamp here

---

**Отметки Банка**  
**Bank mark**

Администратор (заместитель администратора) СЗИ Банка  
IPF Administrator (deputy administrator) of the Bank

---

(подпись) / (Ф.И.О.)  
(signature) (Full name)

---

(дата получения Данных)  
(date of receipt of the Information)



**Приложение № 6**  
**к Соглашению об использовании электронной системы**  
**дистанционного банковского обслуживания**  
 № \_\_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

**Annex No. 6**  
**To the Agreement on the use of an electronic system for remote banking**  
**services**  
 No. \_\_\_\_\_ dated \_\_\_\_\_ 20 \_\_\_\_

**ФОРМА**  
**FORM**

**АКТ**  
**признания открытого ключа (сертификата)**  
**для обмена сообщениями**  
**АКТ**  
**of acknowledgement of the public key (certificate)**  
**for message exchange**

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г. \_\_\_\_\_

Настоящим Актом признаётся ключ проверки электронной подписи и открытый ключ шифрования, принадлежащий уполномоченному представителю Клиента:  
 The electronic signature verification key and public encryption key of the authorized representative of the Client is acknowledged by this Act.

**Сведения о Клиенте:**  
**Details of the Client:**

1. Наименование: \_\_\_\_\_  
Name
2. Место нахождения: \_\_\_\_\_  
Location
3. Тел. \_\_\_\_\_ 4. Факс \_\_\_\_\_  
Tel. Fax

**Сведения об Уполномоченном представителе Клиента:**  
**Details of the Authorized Representative of the Client:**

1. Фамилия, имя, отчество: \_\_\_\_\_  
Full name
  2. Удостоверение личности/паспорт: серии \_\_\_\_\_ № \_\_\_\_\_,  
ID/passport: series  
выдан « \_\_\_\_ » \_\_\_\_\_ г. \_\_\_\_\_  
issued on
  3. Место и дата рождения; \_\_\_\_\_  
Place and date of birth
  4. Адрес места жительства (регистрации): \_\_\_\_\_  
Residence (registered) address
  5. Гражданство: \_\_\_\_\_  
Citizenship
- ИНН (при его наличии, при его отсутствии – указать «отсутствует») \_\_\_\_\_  
 Taxpayer Identification Number (INN) (if available, if not – specify “none”)  
 данные миграционной карты \_\_\_\_\_  
 Migration card information

Личная подпись Уполномоченного представителя Клиента \_\_\_\_\_  
 Personal signature of the Authorized Representative of the Client

**Параметры ключа:**

**Parameter of the Key:**

Алгоритм: (указывается алгоритм)

Algorithm (algorithm is specified)

Начало срока действия: « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_

Valid from

Окончание срока действия: « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_

Valid till

**Текст открытого ключа:****Open Key text:**

--

**Дополнительные поля открытого ключа (сертификата)****Additional lines of the Open Key (certificate):**

Имя владельца ключа: Name of the key owner: Код страны: Country code: Страна: Country: Город: City: Наименование клиента: Name of the Client: Идентификатор клиента в системе/identifier of the Client in the System Данные об издателе/Information about the issuer:
--

**Ключ зарегистрирован и может использоваться для обмена сообщениями.****The Key is registered and may be used for message exchange.**

Администратор/Заместитель  
 администратора СКЗИ БАНКА/  
 Administrator/Deputy  
 Administrator of the BANK's  
 information cryptosecurity software

Руководитель КЛИЕНТА  
 Director of the CLIENT

---

М.П.  
 Stamp here

---

М.П.  
 Stamp here