

УТВЕРЖДЕНО
APPROVED

Приказом от «20» марта 2009 года №299
by Order No. 299 dated March 20, 2009
Вступает в действие с «01» апреля 2009 года
Takes effect since April 1, 2009

**Положение
Regulation
об использовании системы «Интернет-Банк IBANK2»
АКБ «Абсолют Банк» (ЗАО)
Версия 5.0
on the use of the Internet-Bank IBANK2 system
of Commercial Bank «Absolut Bank»
Version 5.0**

1. Общие положения и применяемые термины General Provisions and Applicable Terms	3
2. Процедура генерации ключей и действия при их компрометации Key Generation and Key Compromise Procedures	7
3. Срок действия ключей Effective Term of EDS Keys	8
4. Хранение и использование ключей Storing and Using EDS Keys	9
5. Порядок работы в Системе и создания электронных документов Клиентом Procedure of Operation and Electronic Documents to Be Created by the Customer in the System.....	9
6. Порядок передачи Клиентом и приема Банком электронных документов Procedure for Electronic Document Transfer by the Customer and Receipt by the Bank.....	11
7. Порядок разрешения споров Dispute Resolution Procedure	12
8. Прочие условия Miscellaneous	15

1. Общие положения и применяемые термины

1.1. Настоящее Положение о порядке использования системы «Интернет – Банк iBank2» АКБ «Абсолют Банк» (ЗАО) (далее по тексту – «Положение») определяет порядок обмена в электронном виде расчетными и иными документами между Акционерным коммерческим банком «Абсолют Банк» (закрытое акционерное общество) (далее по тексту – «Банк») и клиентами Банка – физическими лицами, юридическими лицами, индивидуальными предпринимателями и физическими лицами, занимающимися частной практикой (далее по тексту – «Клиент») при помощи системы «Интернет – Банк iBank2» на основании заключенных Договора о порядке обмена документами в электронном виде с использованием системы «Интернет – Банк iBank2», либо Договора о порядке обмена документами в электронном виде с использованием системы «Интернет – Банк iBank2» (с физическим лицом) (далее по тексту – «Договор»).

1.2. Термины, применяемые в Положении

1.2.1. Система «Интернет – Банк iBank2» (далее по тексту – «Система») – электронная банковская система, позволяющая Клиенту с использованием глобальной информационно-телекоммуникационной сети «Интернет» (далее по тексту – «Интернет») передавать в Банк в электронном виде расчетные и иные документы, отслеживать текущий статус этих документов, а также получать из Банка выписки по счетам, сообщения и иные документы.

1.2.2. Составляющими Системы являются:

- Центральный абонентский пункт Банка (далее по тексту – «ЦАП Банка») – сервер системы дистанционного банковского обслуживания, который обрабатывает всю передаваемую Клиентом в Банк информацию, а также размещает необходимую информацию на Интернет-сервере Системы;
- Абонентский пункт Клиента - оборудованный подсистемой защиты персональный компьютер Клиента, подсоединенный к Интернету, с которого Клиент осуществляет работу в Системе.

Абонентский пункт Клиента должен быть оборудован персональным компьютером, отвечающим следующим требованиям:

- цветной дисплей поддерживающий разрешение от 800x600 точек при шестнадцатибитном цвете;
- установленный и настроенный Интернет-браузер с поддержкой Java;
- настроенный канал доступа в Интернет.

1.2.3. *Электронные документы* – документы, в которых информация представлена в электронно-цифровом формате.

1. General Provisions and Applicable Terms

1.1. This Regulation on the Use of Internet – Bank iBank2 System of Commercial bank “Absolut Bank” (hereinafter referred to as the “Provisions”) shall define the procedure of exchange by electronic settlement and other electronic documents between Absolut Bank (hereinafter referred to as the “Bank”) and the Bank’s customers – individuals, legal entities, individual entrepreneurs and privately practicing individuals (hereinafter referred to as the “Customer”) using the Internet – Bank iBank2 System under the Agreement on the Procedure of Electronic Exchange of Documents by means of Internet – Bank iBank2 System entered between the Customer and the Bank or the Agreement on the Procedure of Electronic Exchange of Documents by means of Internet – Bank iBank2 System entered between the Customer (an individual) and the Bank (hereinafter referred to as the “Agreement”).

1.2. Terms Used in the Provisions

1.2.1. *The Internet – Bank iBank 2 System* (hereinafter referred to as the “System”) – an electronic banking system which allows the Customer to use the Internet, a global information and telecommunications system, to transfer settlement and other documents in the electronic form to the Bank, monitor the current status of these documents and receive account statements, messages and other documents from the Bank.

1.2.2. The System’s components include:

- Central subscriber terminal of the Bank (hereinafter referred to as the “CST of the Bank”) – a remote banking server which will process all information transferred by the Customer to the Bank and also post the necessary information to the Internet server of the System;
- User terminal of the Customer – a personal workstation of the Customer equipped with a data protection sub-system and connected to the Internet, which the Customer will use to work in the System.

The user terminal of the Customer should be based on a workstation meeting the following requirements:

- 16-bit color display supporting minimum screen resolution of 800x600;
- installed and customized Internet browser with Java support;
- customized Internet access channel.

1.2.3. *Electronic documents* – documents presenting information in an electronic digital format.

1.2.3.1. *Расчетный электронный документ* – расчетный документ в электронном виде, созданный Клиентом в Системе и оформленный в соответствии с требованиями действующего законодательства РФ.

1.2.3.2. *Иной электронный документ* – любой документ в электронном виде, кроме расчетного, созданный Клиентом или Банком в Системе.

1.2.4. *ЭЦП* – электронно-цифровая подпись - реквизит электронного документа, добавляемый к Электронному документу, полученный в результате криптографического преобразования информации, который позволяет получателю Электронного документа удостовериться в его авторстве и неизменности его содержания, в том числе в отсутствии подделки или искажения Электронного документа со стороны получателя или третьих лиц. Процедуры создания и проверки ЭЦП на базе асимметричного криптографического алгоритма с применением функции хэширования выполнены в соответствии с требованиями ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94.

1.2.5. *Ключ ЭЦП* (далее – «Ключ») – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всех возможных для данного алгоритма преобразований. Ключ состоит из открытого и закрытого ключей, которые связаны между собой с помощью особого математического соотношения.

1.2.5.1. *Открытый ключ ЭЦП* – криптографический ключ (уникальная последовательность символов, соответствующая закрытому ключу ЭЦП), известный помимо Владельца ключа другим пользователям Системы и предназначенный для проверки подлинности ЭЦП. Открытый ключ ЭЦП позволяет установить авторство и неизменность содержания Электронного документа, но не позволяет вычислить закрытый ключ ЭЦП. Открытый ключ ЭЦП считается принадлежащим Клиенту, если такой ключ был зарегистрирован в каталоге открытых ключей Центра регистрации ключей (далее по тексту «ЦРК») Банка в соответствии с порядком, установленным в разделе 2 Положения (Зарегистрированный ключ ЭЦП).

1.2.5.2. *Закрытый ключ ЭЦП* – криптографический ключ (уникальная последовательность символов), известный только Владельцу ключа (Клиенту или Банку соответственно) и хранимый Владельцем в тайне. Закрытый ключ ЭЦП используется для формирования ЭЦП.

1.2.6. *Каталог открытых ключей ЭЦП* – база данных Банка, элементами которой являются: наименования/ Ф.И.О. Клиентов - пользователей Системы, действующие открытые ключи ЭЦП Клиентов и идентификаторы открытых ключей ЭЦП

1.2.3.1. *Electronic payment document* – a settlement document in an electronic form created by the Customer in the System and executed in accordance with requirements of the laws and regulations of the Russian Federation currently in force.

1.2.3.2. *Other electronic document* – any document in an electronic form (except a payment document) created by the Customer or the Bank in the System.

1.2.4. *EDS* – electronic digital signature – a requisite of an electronic document to be added to the Electronic Document as a result of encryption transformation of the information which allows the recipient of the Electronic Document to identify the document's drafter (authorship) and ensures the integrity of its contents, including protection against fraud or distortion of the Electronic Document by the recipient or any third party. The procedures for creation and authentication of EDS based on an asymmetric encryption algorithm using the hash function are implemented in accordance with requirements of GOST R 34.10-94 and GOST R 34.11-94.

1.2.5. *EDS key* (hereinafter referred to as the “Key”) – a specific secret status of certain parameters of the data encryption algorithm which ensures selection of one transformation from a set of all transformations possible under this algorithm. The Key includes a public (open) key and a private (closed) key which are interrelated by way of a specific mathematical ratio.

1.2.5.1. *Public EDS Key / Open EDS Key* – an encryption key (a unique sequence of symbols corresponding to a private EDS key) which, apart from the Key Owner, is known to other users of the System and designed to authenticate an EDS. A public EDS key allows to identify the drafter and ensure the integrity of contents of an Electronic Document but does not allow to derive a private EDS key. A public EDS key is deemed to be owned by the Customer where such key has been registered in a public key catalog of the Key Registration Center (hereinafter referred to as the “KRC”) of the Bank under a procedure established by Section 2 of these Provisions (The Registered EDS Key).

1.2.5.2. *Private EDS Key / Closed EDS Key* – an encryption key (a unique sequence of symbols) known only to the Key Owner (the Customer or the Bank, respectively) and held confidential by the Owner. A private EDS key is used to generate an EDS.

1.2.6. *Catalog of Public EDS Keys* – a database of the Bank including business/family names of Customers who are the System users, effective public EDS keys of Customers and identifications of public EDS keys of Customers.

Клиентов.

1.2.7. *Сертификат открытого ключа ЭЦП* – документ, содержащий информацию об открытом ключе ЭЦП Клиента: собственно открытый ключ ЭЦП и его идентификатор.

Сертификаты открытого ключа ЭЦП оформляются по форме, указанной в Приложении № 1 к Положению, подписываются Клиентом (уполномоченным лицом Клиента) и заверяются его печатью (при наличии). По одному экземпляру сертификата открытого ключа ЭЦП хранится в Банке и у Клиента.

1.2.8. *Компрометация ключа* – событие, связанное с утратой доверия к тому, что используемые ключи обеспечивают возможность установления авторства и неизменности содержания Электронного документа. К таким событиям относятся в том числе:
– утрата носителей информации с ключами;
– утрата носителей информации с ключами с последующим обнаружением;
– увольнение сотрудников Клиента-юридического лица, имевших доступ к закрытым ключам, и иные события, в результате которых используемый ключ в целом или его часть (открытый либо закрытый ключи) могут стать известны или доступны третьим лицам, не уполномоченным на пользование ими.

1.2.9. *Блокировочное слово* - слово, которое Клиент указывает при первоначальной регистрации на сайте Банка, запоминает и использует в качестве пароля при обращении по телефону в Банк для временного блокирования работы Клиента в Системе в случае компрометации ключа ЭЦП.

1.2.10. *USB-токен «iBank 2 Key»* — аппаратное USB-устройство генерации и хранения ключей ЭЦП, состоящее из PC/SC-совместимого USB-картридера и SIM-карты, в которой реализованы все российские криптоалгоритмы и имеется защищенная область памяти, позволяющая хранить до 64-х секретных ключей ЭЦП.

1.2.11. *Статус Электронного документа* – состояние Электронного документа в базе данных ЦАП Банка, однозначно соответствующее стадии обработки документа в Банке.

1.2.12. *Инструкция на проведение операции с Электронным документом* – команда, посылаемая Клиентом по Системе для изменения статуса Электронного документа.

1.2.13. *События в системе «Интернет-Банк» (или «События»)* - автоматическое обновление доступной Клиенту информации в Системе «Интернет – Банк iBank2», которое позволяет Клиенту получать оперативные уведомления в соответствии с пунктами 1.2.13.1 и 1.2.13.2 Положения:

1.2.13.1 для Клиентов – юридических лиц,

1.2.7. *Certificate of a public EDS key* – a document containing information on the public EDS key of a Customer: the public EDS key itself and the identification thereof.

Certificates of public EDS keys shall be documented in a form specified in Annex No. 1 to the Provisions, signed by the Customer (an authorized representative of the Customer) and sealed with its seal (if any). The Bank and the Customer shall each store one certificate of a public EDS key.

1.2.8. *Key compromise* – an event related to a loss of confidence that the used keys allow to identify the drafter and ensure the integrity of an Electronic Document. These events shall include, in particular:
– loss of data carriers containing the keys;
– loss of data carriers containing the keys which were subsequently recovered;
– dismissal of employees of a corporate Customer who had access to private keys, and other events as a result of which the used key may fully or partially (the public or private key) become known or available to any third party not authorized to use these keys.

1.2.9. *Lock word* – a word specified by the Customer at the time of the original registration in the website of the Bank, which he should remember and use as a password when requesting the Bank by phone to temporarily block the Customer's operations in the System in the event of an EDS key compromise.

1.2.10. *USB-token "iBank 2 Key"* – a hardware USB device for generation and storage of EDS keys, consisting of a PC/SC-compatible USB card reader and a SIM-card which comprises all the Russian cryptographicalgorithms and has a protected memory area allowing to store up to 64 secret EDS keys.

1.2.11. *Status of an Electronic Document* – status of an Electronic Document in the database of the Bank's CST which directly corresponds to the document's processing stage at the Bank.

1.2.12. *Electronic Document transaction instruction* – a command sent by the Customer via the System to change the status of an Electronic Document.

1.2.13. *Events in the system "Internet-Bank" (or "Events")* – automatic updating of information available to Client in the System "Internet-Bank iBank2", which allows Client to receive timely notifications in compliance with clauses 1.2.13.1 and 1.2.13.2 of the Regulations:

1.2.13.1 For Clients being legal entities, individual entrepreneurs and individuals engaged in private

индивидуальных предпринимателей и физических лиц, занимающихся частной практикой доступно информирование по Событиям:

- Вход в систему
- О поступлении в банк документа
- Отвержение документа
- Входящие банковские письма
- Движение средств по счету
- О текущих остатках
- Выписка по счету

1.2.13.2 для Клиентов – физических лиц доступно информирование по Событиям:

- Вход в систему
- Входящие банковские письма
- Движение средств по счету

1.2.14. *Информирование о Событиях в системе* – автоматическая отправка Клиенту сообщения о Событии в Системе «Интернет – Банк iBank2», в соответствии с п.1.2.13 Положения. Отправка сообщений может осуществляться по электронной почте и/или на мобильный телефон.

1.2.15. *Владелец ключа ЭЦП Клиента* – уполномоченное лицо Клиента, осуществляющее от имени Клиента работу в Системе, на имя которого оформлен Сертификат открытого ключа ЭЦП, и которое владеет соответствующим закрытым ключом ЭЦП.

Для Клиентов – физических лиц Владелец ключа ЭЦП может быть только сам Клиент.

Владелец ключа ЭЦП должен отвечать следующим требованиям:

- обладает правом подписи расчетных документов,
- указан в карточке с образцами подписей и оттиска печати Клиента.

Если в действующей карточке с образцами подписей и оттиска печати указаны лица, обладающие второй подписью, то владельцев ключей ЭЦП Клиента должно быть не менее двух – по одному с первой и второй группой подписи.

Каждый Владелец ключа ЭЦП Клиента, может являться владельцем не более одного действующего ключа ЭЦП первой или второй группы подписи данного Клиента.

1.2.15.1. *Функции Владелец ключей ЭЦП Клиента:*
– заверение Электронных документов ЭЦП при помощи ключей;
– ответственное хранение ключей;
– своевременное извещение Банка о случаях компрометации ключей;
– контроль за соблюдением Клиентом при работе с Абонентского пункта Клиента установленных процедур работы в Системе;

practice, informing about the listed below Events is available, and namely:

- Access to the system
- About document coming to the Bank
- Document rejection
- Incoming bank letters
- Funds movement on account
- About current balances
- Statement of account

1.2.13.2 For Clients being individuals informing about the listed below Events is available, and namely:

- Access to the system
- Incoming bank letters
- Funds movement on account

1.2.14. *Informing about Events in the system* – automatic sending of message to Client about Event in the System “Internet-Bank iBank2”, in compliance with clause 1.2.13 of the Regulations. Messages may be sent via electronic mail and/or to mobile phone.

1.2.15. *Customer EDS key owner* – an authorized representative of the Customer who performs operations in the System on behalf of the Customer, in whose name the Certificate of the public EDS key is issued, and who owns the respective private EDS key.

For individuals – a EDS key owner can only be the client himself.

The EDS key owner should meet the following requirements:

- have the right of signature in respect of payment documents,
- be specified in the Customer’s card containing samples of signatures and seal prints.

If the effective signature sample card contains signatures of persons having the right of the second signature, there should be at least two Customer EDS key owners – one having the first and one having the second signature right.

Any EDS key owner of the client can be an owner of not more than one active EDS key of the first or second signature group of this particular client.

1.2.15.1. *The functions of Customer EDS Key Owners shall include the following:*

- certifying Electronic Documents using EDS keys;
- custody of (storing) EDS keys;
- timely advice to the Bank of the keys being compromised;
- control of compliance by the Customer with the established operation procedures of the System when using the Customer’s user terminal;

– контроль за своевременностью обновления ключей по требованию Банка; – организация регулярных сеансов связи с Банком (не реже одного раза в неделю) для своевременного получения из Банка выписок и служебных сообщений, а также иной информации, в т.ч. о текущем состоянии Электронных документов;
– осуществление регулярного просмотра корреспонденции в Системе.

1.3. От имени Банка работу в Системе осуществляют:

- Администратор ЦРК Банка;
- Администратор ЦАП Банка.

1.4. Клиент – юридическое лицо, физическое лицо, занимающееся частной практикой, индивидуальный предприниматель, вправе ограничить список IP адресов, с которых Клиентом будет осуществляться доступ к Системе, путем заключения с Банком Соглашения об IP фильтрации по форме Приложения № 2 к Положению.

2. Процедура генерации ключей и действия при их компрометации

2.1. Процесс генерации ключей осуществляется Клиентом на персональном компьютере Клиента с использованием *USB-токена «iBank 2 Key»*. Полученные в ходе генерации сертификаты открытых ключей ЭЦП Клиента подписываются и передаются Клиентом в Банк на бумажном носителе.

2.2. Регистрация открытых ключей ЭЦП Клиента в Каталоге открытых ключей осуществляется Администратором ЦРК Банка не позднее, чем на следующий рабочий день после передачи Клиентом в Банк подписанных сертификатов открытых ключей ЭЦП, при условии соблюдения Клиентом требований п.1.2.15 Положения и корректного заполнения сертификатов.

2.3. Плановая регенерация ключей производится по истечении срока действия ключа согласно п.3.1. Положения или по инициативе любой из Сторон.

2.4. Если плановая регенерация ключей производится по инициативе Банка, Банк обязан проинформировать об этом Клиента по Системе за одну неделю до предполагаемой даты регенерации. С указанной Банком даты прежние ключи Клиента считаются недействительными.

2.5. Если плановая регенерация ключей производится по инициативе Клиента, Клиент обязан проинформировать об этом Банк по Системе за одну неделю до предполагаемой даты регенерации. При этом прежние ключи Клиента независимо от

– control of timely update of the keys upon request of the Bank;

– organization of regular communication sessions with the Bank (at least once a week) for the purpose of timely receipt of statements and service messages as well as other information (including as may be related to the current status of Electronic Documents) from the Bank;

– regular review of messages in the System.

1.3. The following persons shall work in the System on behalf of the Bank:

- KRC Administrator of the Bank;
- CST Administrator of the Bank.

1.4. A corporate customer, privately practicing individual, individual entrepreneur shall have the right to restrict the list of IP-addresses to be used by the Customer for accessing the System by way of an IP-Filtration Agreement to be entered with the Bank in the form specified in Annex No. 2 to these Provisions.

2. Key Generation and Key Compromise Procedures

2.1. The process of key generation shall be performed by the Customer on the Customer's workstation using *USB-token "iBank 2 Key"*. Certificates of public keys of the Customer's EDS shall be signed and delivered by the Customer to the Bank in a hard copy.

2.2. Public keys of the Customer EDS shall be registered with the Public Key Catalog by the KRC Administrator of the Bank not later than the next business day following the delivery of the signed public EDS key certificates by the Customer to the Bank provided, however, that the Customer has complied with requirements of clause 1.2.15 of the Provisions and has correctly completed the certificates.

2.3. A scheduled re-generation of keys shall be performed upon expiry of the effective term of the key in accordance with requirements of clause 3.1 of these Provisions or upon the initiative of any of the Parties.

2.4. If the Bank has initiated a scheduled re-generation of keys the Bank shall advise the Customer accordingly via the System one week before the proposed re-generation date. Previous keys of the Customer shall be deemed void from the date specified by the Bank.

2.5. If the Customer has initiated a scheduled re-generation of keys the Customer shall advise the Bank accordingly via the System one week before the proposed re-generation date. In this case, previous keys of the Customer shall be deemed void from the

факта регенерации считаются недействительными с даты и времени, указанных Клиентом в соответствующем сообщении.

2.6. При компрометации ключа Клиент немедленно сообщает об этом Администратору ЦРК Банка (с учетом установленного режима работы - с понедельника по пятницу с 8-00 ч до 19-00 ч московского времени):

- при личной явке Клиента (уполномоченного представителя Клиента) в Банк путем предоставления письменного сообщения, заверенного подписями уполномоченных лиц и оттиском печати (при наличии), указанными в карточке, или

- по телефону, используя блокировочное слово, с последующим предоставлением в Банк письменного сообщения, заверенного подписями уполномоченных лиц и оттиском печати (при наличии), указанными в карточке.

ЦРК Банка фиксирует факт компрометации ключа, и Банк временно блокирует работу Клиента в Системе. По письменному требованию Клиента, заверенному подписями уполномоченных лиц и оттиском печати (при наличии), указанными в карточке, Банк отменяет исполнение Расчетных электронных документов, принятых к исполнению до момента поступления заявления о компрометации, если Банк имеет технологическую возможность такой отмены.

Регенерация ключей производится Клиентом в соответствии с п.п. 2.1., 2.2. Положения.

2.7. Банк вправе блокировать работу Клиента в Системе при наличии подозрений в компрометации ключа Клиента без уведомления последнего. Возобновление работы Клиента происходит после регенерации Ключа в соответствии с п.п. 2.1 , 2.2. Положения.

2.8. Исключение открытых ключей ЭЦП Клиента из Каталога открытых ключей ЦРК Банка производится на основании прекращения действия Договора, а также в случаях регенерации ключей.

2.9. После исключения открытых ключей ЭЦП Клиента из Каталога открытых ключей ЦРК Банка сертификаты открытых ключей ЭЦП Клиента хранятся в Банке не менее пяти лет.

3. Срок действия ключей

3.1. Срок действия ключа ЭЦП определяется сроком полномочий Владельца ключа распоряжаться средствами на счете Клиента с правом первой или второй подписи, но не превышает 1 (Один) год с даты начала действия ключа.

3.2. Банк уведомляет Владельца ключа о предстоящем истечении срока действия ключа по Системе 30 календарных дней до даты окончания

date and time specified by the Customer in the relevant notice, irrespective of whether re-generation was effected or not.

2.6. If a key has been compromised, the Customer shall promptly advise the KRC Administrator of the Bank accordingly (taking into account the established business hours from 8 a.m. to 7 p.m. Moscow time, Monday through Friday):

- if the Customer (an authorized representative of the Customer) has personally delivered a notice in writing certified by signatures of authorized persons and seal prints (if any) specified in the sample card,

- via phone using the lock word with further delivering to the Bank of a written notice certified by the signatures of authorized representatives and the seal (if any) specified in the sample card.

The KRC of the Bank shall register the fact of a key compromise, and the Bank shall temporarily block operations of the Customer in the System.

Upon the Customer's written request approved by signatures of authorized persons and seal prints (if any) specified in the sample card, the Bank shall cancel execution of Electronic Payment Documents accepted for execution prior to the time of delivery of a key compromise notice, if the Bank has a technical ability to carry out such cancellation.

Re-generation of keys shall be performed by the Customer in accordance with clauses 2.1 and 2.2 of these Provisions.

2.7. The Bank may block the Customer's operations in the System without a notice being served to the latter if a compromise of the Customer's key is suspected. The Customer's operations shall be resumed after the Key has been re-generated under clauses 2.1., 2.2 of these Provisions.

2.8. The Customer's public EDS keys shall be de-registered from the Public Key Catalog of the Bank's KRC in the event of termination of the Agreement, as well as in the event of re-generation of keys.

2.9. The Bank shall store the certificates of the Customer's public EDS keys for at least five years from the date they have been de-registered from the Public Key Catalog of the Bank's KRC.

3. Effective Term of EDS Keys

3.1. The effective term of an EDS key shall be determined by the term during which the EDS Key Owner with the right of the first or second signature is authorized to dispose of the Customer's funds but shall not in any case be more than 1 (one) year from the start date of the key.

3.2. The Bank shall advise the EDS Key Owner via the System of the forthcoming expiry of the key term in 30 calendar days prior its expiry.

срока.

3.3. По окончании срока действия ключи подлежат обязательной регенерации Клиентом в соответствии с п.п. 2.1., 2.2. Положения, при этом прежние ключи Клиента, по которым истек срок действия, считаются недействительными с даты, следующей за датой окончания срока их действия.

4. Хранение и использование ключей

4.1. Способ хранения Клиентом закрытых ключей и паролей к ключам должен исключать их утрату и использование неуполномоченными лицами. Клиент обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение закрытых ключей.

4.2. В ЦРК Банка хранятся только открытые ключи Клиента. Закрытые ключи Клиента третьим лицам и Банку не известны.

4.3. Ответственность за все возможные последствия использования ключей Клиента неуполномоченными лицами несет Клиент.

5. Порядок работы в Системе и создания электронных документов Клиентом

5.1. Инициатором передачи Расчетных электронных документов в Банк, а также получения от Банка информации, переданной по Системе, является Клиент. Для получения по Системе от Банка интересующей его информации Клиент формирует соответствующие Интернет-запросы, в ответ на которые Банк предоставляет запрашиваемую информацию.

5.2. Клиент самостоятельно устанавливает соединение с Интернет-сервером Системы и следит за поддержанием сеанса связи во время работы в Системе.

5.3. После осуществленной Системой идентификации Клиента последний получает доступ к Системе и начинает работу в ней.

5.4. Клиент заполняет или редактирует формы Электронных документов в формате, определенном в экранной форме клиентской части Системы, и заверяет созданные Электронные документы своей (своими) ЭЦП. ЭЦП подтверждает авторство созданного в Системе Электронного документа и является средством проверки неизменности его содержания, так как любое изменение Электронного

3.3. Upon expiry of the effective term, the keys shall be subject to mandatory re-generation by the Customer in accordance with clauses 2.1 and 2.2 of these Provisions, with the Customer's previous keys which have their effective terms expired to be deemed void from the date following the date of expiry of their effective term.

4. Storing and Using EDS Keys

4.1. The Customer shall store private EDS keys and the passwords to the keys in a way as to prevent their loss and unauthorized use. Moreover the Customer shall undertake to ensure the security, non-disclosure and non-dissemination of private EDS keys.

4.2. The KRC of the Bank shall store only public EDS keys of the Customer. The Customer's private EDS keys shall be unknown to third parties and the Bank.

4.3. The Customer shall assume responsibility for all possible consequences of unauthorized use of the Customer's EDS keys.

5. Procedure of Operating in the System and Creation of Electronic Documents by the Customer

5.1. Any transfer of Electronic Payment Documents to the Bank and receipt of information transmitted via the System from the Bank shall be initiated by the Customer. In order to receive relevant information from the Bank via the System, the Customer shall generate Internet queries in response to which the Bank shall provide the requested information.

5.2. The Customer himself establishes connection with the System's Internet server and monitors the operation of the communications session while operating in the System.

5.3. After the System has identified the Customer, the System shall become accessible to the Customer to start his operations.

5.4. The Customer shall complete or edit the forms of Electronic Documents in a format determined on the screen of the Customer's part of the System, and shall authenticate the created Electronic Documents by his EDS(s). EDS will identify the drafter of an Electronic Document created in the System and provide a means for ensuring its integrity since any modification of the Electronic Document authenticated by EDS will violate

документа после заверения его ЭЦП нарушает целостность ЭЦП.

Электронный документ должен быть заверен ЭЦП в строгом соответствии с действующей карточкой с образцами подписей и оттиска печати:

- при наличии лиц, обладающих правом второй подписи, документ заверяется двумя ЭЦП - по одной ЭЦП из первой и второй группы подписей.

5.5. Система автоматически отображает сведения о текущем этапе обработки Клиентом и/или Банком Электронного документа посредством присвоения Электронному документу определенного статуса в Системе.

Система присваивает Электронным документам следующие статусы:

- «новый»: присваивается вновь созданному в Системе Электронному документу;
- «подписан»: присваивается Электронному документу, заверенному необходимым количеством ЭЦП Клиента (по одной ЭЦП из каждой группы подписей, указанной в карточке с образцами подписей и оттиска печати);
- «доставлен»: присваивается Электронному документу, успешно прошедшему проверку в соответствии с п. 6.2. Положения;
- «отвергнут»: присваивается Электронному документу, не прошедшему проверку в соответствии с п. 6.2. Положения, либо последующую проверку по причине его несоответствия требованиям, установленным действующим законодательством РФ или Положением, а также в иных случаях на усмотрение Банка;
- «на исполнении»: присваивается Расчетному электронному документу, находящемуся на этапе исполнения Банком;
- «на обработке»: присваивается Расчетному электронному документу, исполнение которого требует дополнительного контроля со стороны Банка;
- «исполнен»: присваивается Расчетному электронному документу - после получения Банком выписки по соответствующему корреспондентскому счету Банка, подтверждающей исполнение такого документа, - если платеж исполнялся через корреспондентский счет, и непосредственно после отражения документа в балансе Банка – если платеж был исполнен внутри Банка.

5.6. Банк передает Клиенту по Системе следующие виды Электронных документов:

- выписки по счетам Клиента;
- расшифровки поступлений по счетам Клиента (кредитовые расчетные документы);
- справочную и иную информацию (в том числе формы учета по валютным операциям и документы подтверждающие операции торгового финансирования и сделки на срочном рынке).

5.7. Информация, переданная Банком Клиенту по

the integrity of EDS.

An Electronic Documents shall be authenticated by EDS strictly in compliance with the effective sample card with signatures and seal prints:

- in the event persons have the right of the second signature, the document shall be certified by two EDSs, one for the first and one for the second group of signatures.

5.5. The System shall automatically represent information on the current status of an Electronic Document processed by the Customer and/or the Bank by assigning a specific status to the Electronic Document in the System.

The System shall assign the following status to Electronic Documents:

- “new”: to be assigned to an Electronic Document newly created in the System;
- “signed”: to be assigned to an Electronic Document certified by the necessary number of the Customer’s EDSs (one EDS for each of the signature groups specified in the sample card with signatures and seal prints);
- “delivered”: to be assigned to an Electronic Document that successfully passed the control procedure in accordance with clause 6.2 of these Provisions;
- “denied”: to be assigned to an Electronic Document which has failed to pass the control procedure in accordance with clause 6.2 of these Provisions, or any subsequent control procedure because of its non-compliance with requirements of the effective legislation of the Russian Federation or these Provisions or for other reasons at the Bank’s discretion;
- “for execution”: to be assigned to an Electronic Document, which is being executed by the Bank;
- “processing”: to be assigned to an Electronic Payment Document to be additionally controlled by the Bank;
- “executed”: to be assigned to an Electronic Payment Document upon receipt by the Bank of the relevant correspondent account statement to confirm execution of such document if the payment has been effected via a correspondent account, and immediately after the document was posted to the Bank’s books if the payment has been executed internally.

5.6. The Bank shall deliver the following types of Electronic Documents to the Customer via the System:

- account statements in respect of the Customer’s accounts;
- breakdown of funds received in the Customer’s accounts (credit settlement documents);
- reference and other information (including reporting forms for foreign exchange transactions and documents confirming trade finance operations and term market deals).

5.7. Information sent by the Bank to the Customer via

Системе, считается доведенной до сведения Клиента по истечении одной недели с даты ее передачи Банком (начиная со дня передачи), независимо от фактического восприятия такой информации Клиентом.

5.8. Все справочники, шаблоны Электронных документов, Электронные документы после их сохранения, а также выписки по счетам и иная информация находятся в ЦАП Банка и доступны Клиенту только во время проведения авторизованных сеансов связи с Банком по Системе.

5.9. Клиент самостоятельно устанавливает параметры информирования о Событиях в Системе в соответствии п.1.2.13 и п.1.2.14 Положения. Информирование о Событиях в Системе позволяет Клиенту оперативно контролировать операции в Системе и, в соответствии с п.2.6. Положения, предпринимать своевременные действия для обеспечения защиты от несанкционированных действий злоумышленников и хищения денежных средств со счетов, а также является информационным сервисом по текущим операциям Клиента.

6. Порядок передачи Клиентом и приема Банком электронных документов

6.1. Созданный Клиентом Электронный документ может быть передан Клиентом в Банк по Системе как вместе с инструкцией на его исполнение, так и без такой инструкции.

При получении Банком инструкции на исполнение Электронного документа Банк осуществляет проверку Электронного документа и принимает его к исполнению при условии положительного результата проверки.

6.2. Результат проверки Электронного документа считается положительным, если Электронный документ оформлен в соответствии с действующим законодательством РФ и требованиями, установленными Положением, заверен надлежащей (надлежащими) ЭЦП и прошел в Банке проверку ЭЦП.

6.3. После проверки Банком Электронного документа Система присваивает ему статус «доставлен» или «отвергнут» соответственно.

Статус каждого Электронного документа, однозначно отражающий текущий этап его обработки Банком, автоматически отслеживается программными средствами ЦАП Банка во время сеансов связи, проводимых Клиентом. Свидетельством того, что Электронный документ принят к исполнению Банком, является присвоение ему в Системе статуса «доставлен».

the System shall be deemed received by the Customer upon expiry of one week from and including the date it was sent by the Bank, irrespective of whether such information was actually perceived by the Customer or not.

5.8. All manuals, template Electronic documents, saved Electronic Documents, account statements and other information shall be maintained by the CST of the Bank and shall be accessible to the Customer only during authorized communications sessions with the Bank via the System.

5.9. Client independently sets parameters of informing about Events in the System in compliance with clauses 1.2.13 and 1.2.14 of the Regulations. Informing about Events in the System allows Client to timely control transactions in the System and, in compliance with clause 2.6 of the Regulations, to take timely measures to protect against unauthorized actions of intruders and against funds theft from accounts, it as well is used as information service for current transactions of Client.

6. Procedure of Electronic Documents Transfer by the Customer and their Receipt by the Bank

6.1. An Electronic Document created by the Customer may be transmitted by the Customer to the Bank via the System either with an attached execution instruction or without such instruction.

When the Bank has received the instruction to execute an Electronic Document, the Bank shall verify the Electronic Document and accept it for execution, given a positive result of verification.

6.2. The result of verification of an Electronic Document shall be deemed positive if the Electronic Document is completed in compliance with requirements of the effective laws and regulations of the Russian Federation and requirements of these Provisions, authenticated with proper EDS(s) and passed an EDS control at the Bank.

6.3. Once the Bank has verified the Electronic Document, the System shall assign to it the status of either “delivered” or “denied” respectively.

The status of each Electronic Document unambiguously reflecting the current stage of its processing by the Bank shall be automatically monitored by the CST software at the time of communications sessions performed by the Customer. The status of “delivered” assigned to the Electronic Document by the System shall evidence that the Electronic Document has been accepted by the Bank for execution.

6.4. Информация об Электронных документах, не принятых Банком к исполнению по причине их оформления с нарушением требований п. 6.2. Положения или по иным основаниям, размещается Банком на Интернет-сервере Системы в течение рабочего дня (с учетом установленного режима работы Банка), следующего за днем получения инструкции на исполнение Электронного документа, с указанием причины, по которой документ не принят к исполнению.

7. Порядок разрешения споров

7.1. Стороны в рабочем порядке урегулируют все споры, возникающие между ними в ходе работы в Системе, за исключением споров, указанных в п. 7.2. Положения.

7.2. Споры Сторон по поводу авторства и неизменности содержания Электронных документов рассматриваются Экспертной комиссией, формируемой сторонами (далее по тексту – «Комиссия»). Процедура рассмотрения спора состоит из следующих этапов:

- предъявление претензии одной из Сторон другой Стороне;
- формирование Комиссии для рассмотрения спора;
- разрешение Комиссией спора по существу.

7.3. Претензия предъявляется соответствующей Стороной в письменной форме путем официального вручения под расписку другой Стороне или направления по почте телеграммой либо заказным письмом с уведомлением о вручении.

7.4. Получив претензию, соответствующая Сторона официально в письменной форме информирует другую Сторону о результатах ее рассмотрения в течение 5 (Пяти) рабочих дней с даты получения претензии.

7.5. Сторона, предъявившая претензию, в течение 5 (Пяти) рабочих дней после получения результатов рассмотрения претензии от другой Стороны должна рассмотреть представленные объяснения и письменно уведомить другую Сторону о снятии претензии или о несогласии с представленными объяснениями.

7.6. Если Сторона не согласна с представленными объяснениями, Стороны обязаны в течение 5 (Пяти) рабочих дней с даты уведомления о несогласии сформировать Комиссию для рассмотрения и разрешения указанного спора по существу.

7.7. До передачи спора на рассмотрение Комиссии Сторонам следует удостовериться, что причиной возникновения спора не является нарушение

6.4. Information on Electronic Documents not accepted by the Bank for execution because of them being completed with violations of requirements of clause 6.2 of the Provisions or for other reasons shall be posted by the Bank to the System's Internet server during the next business day (taking into account the established business hours of the Bank) following the day when the instruction for execution of this Electronic Document was received, specifying the reason why the document was not accepted for execution.

7. Dispute Resolution Procedure

7.1. The Parties shall resolve in course of usual business relations all disputes arising between them in the course of the System's operation, except the disputes specified in clause 7.2 of the Provisions.

7.2. Disputes between the Parties relating to the identity of the drafter (authorship) and integrity (unchanged contents) of Electronic Documents shall be considered by a Commission of Experts to be formed by the Parties (hereinafter referred to as the "Commission"). The dispute resolution procedure shall include the following stages:

- a claim to be made by one Party against the other Party;
- a Commission to be formed to consider the dispute;
- resolution of the dispute by the Commission.

7.3. A claim shall be made by the relevant Party in writing and shall be officially serviced to the other Party against receipt, or shall be served by mail or telegram or registered letter with advice of delivery.

7.4. Upon receipt of the claim the relevant Party shall formally advise the other Party in writing of the results of its consideration within 5 (five) business days from the date of receipt of the claim.

7.5. Within 5 (five) business days from the date of receipt of the consideration results, the claiming Party shall consider the presented explanations and advise the other Party in writing that the claim is to be removed or that it does not accept the presented explanations.

7.6. If the claiming Party does not accept the presented explanations, within 5 (five) business days from the date of the non-acceptance advice the Parties shall form a Commission to consider and resolve the said dispute on its merits.

7.7. Before the dispute is referred to the Commission for consideration, the Parties shall make sure that the dispute does not relate to violation of integrity of the

<p>целостности программного обеспечения, произошедшее в результате сбоев аппаратуры, воздействия компьютерных вирусов, в том числе полученных через Интернет, и т.п. В этом случае Стороны руководствуются п. 7.1. Положения.</p> <p>7.8. В состав Комиссии включается равное количество представителей Банка и Клиента. При необходимости в состав Комиссии могут быть включены независимые эксперты, в частности, представители компании - разработчика Системы. Максимальное количество членов Комиссии не должно превышать 6 (Шести) человек.</p> <p>7.9. Полномочия представителей Сторон для участия в Комиссии должны подтверждаться оформленными надлежащим образом доверенностями.</p> <p>7.10. Заседание Комиссии проводится не позднее 2 (Двух) рабочих дней со дня ее формирования.</p> <p>7.11. При рассмотрении спора об авторстве и неизменности содержания Электронного документа Комиссия устанавливает следующие факты:</p> <ul style="list-style-type: none"> – предмет спора Сторон; – перечень Электронных документов, относящихся к предмету спора; – идентичность созданного Клиентом Электронного документа документу на бумажном носителе, распечатанному Банком и хранящемуся в документах дня Банка; – принадлежность ЭЦП Электронного документа Клиенту. <p>7.12. При рассмотрении спора Комиссия использует следующие данные в качестве эталонных:</p> <ul style="list-style-type: none"> – данные имеющегося в Банке архива отправленных/принятых Электронных документов; – сертификат(ы) открытого ключа ЭЦП Клиента, подписанный(ые) Клиентом и хранящийся(я) в Банке (Эталонный(е) сертификат(ы)). <p>7.13. Разрешение споров осуществляется на основании результатов проверки ЭЦП Клиента в спорном Электронном документе.</p> <p>7.14. Комиссия осуществляет свою работу на территории Банка с использованием персонального компьютера, свободного от вирусов и программных закладок, с установленными на нем эталонными DLL-библиотеками СКЗИ, предоставляемыми ООО «БИФИТ».</p> <p>7.15. Для рассмотрения спора Комиссией Администратор ЦРК Банка предоставляет Эталонный(е) сертификат(ы).</p> <p>7.16. Клиент для рассмотрения спора Комиссией предоставляет сертификат(ы) открытого ключа ЭЦП Клиента, хранящийся(я) у Клиента.</p>	<p>software caused by a hardware failure, effect of computer viruses, including those received via the Internet, and etc. In this case, the Parties shall act according to clause 7.1 of these Provisions.</p> <p>7.8. The Commission shall include representatives of the Bank and those of the Customer in equal proportion. If necessary, the Commission may include independent experts, e.g. representing the company, which developed the System. The maximum number of members in the Commission shall not exceed 6 (six).</p> <p>7.9. Due authorization of the Parties' representatives to participate in the Commission shall be confirmed by duly drawn powers of attorney.</p> <p>7.10. The Commission shall hold its meeting not later than 2 (two) business days from the date it was formed.</p> <p>7.11. In considering a dispute relating to the identity of the drafter and integrity of the Electronic Document, the Commission shall establish the following facts:</p> <ul style="list-style-type: none"> – subject of the dispute between the Parties; – list of Electronic Documents relating to the subject of the dispute; – whether the Electronic Document created by the Customer is identical to the paper document printed out by the Bank and maintained in the Bank's day file; – whether the Customer owns the EDS of the Electronic Document. <p>7.12. In considering the Dispute, the Commission shall use the following data as reference data:</p> <ul style="list-style-type: none"> – data from the archive of outgoing/incoming Electronic Documents maintained by the Bank; – public key certificate(s) of the Customer EDS signed by the Customer and maintained by the Bank (Reference Certificate(s)). <p>7.13. Disputes shall be resolved on the basis of verification results of the Customer EDS in the disputed Electronic Document.</p> <p>7.14. The Commission shall carry out its activities on the territory of the Bank using a workstation free of viruses and software bookmarks and with installed reference DLL-libraries of the DES to be made available by ООО BIFIT.</p> <p>7.15. For the dispute to be considered by the Commission, the KRC Administrator of the Bank shall make available Reference Certificate(s).</p> <p>7.16. For the dispute to be considered by the Commission, the Customer shall provide public key certificate(s) of the Customer EDS maintained by the</p>
---	---

<p>7.17. Если инициатором рассмотрения спора является Клиент, Комиссией устанавливается актуальность открытых ключей ЭЦП Клиента на момент передачи Электронного документа, являющегося объектом спора. Открытые ключи ЭЦП Клиента считаются актуальными, если они были зарегистрированы в Каталоге открытых ключей в соответствии с п. 2.2. Положения и действовали в момент, когда спорный Электронный документ был передан Клиентом в Банк.</p> <p>7.18. Принимая во внимание математические свойства алгоритма ЭЦП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94, гарантирующими невозможность подделки значения сертифицированной ЭЦП любым лицом, не обладающим закрытым ключом ЭЦП, Стороны признают, что рассмотрение спора в отношении авторства и неизменности содержания Электронного документа заключается в доказательстве принадлежности ЭЦП конкретного Электронного документа конкретной Стороне.</p> <p>7.19. Рассмотрение Комиссией спора об авторстве и неизменности содержания Электронного документа проводится с использованием АРМ «Операционист» Системы «iBank2».</p> <p>7.20. В целях формирования Протокола проверки ЭЦП Администратор ЦАП Банка в присутствии Комиссии осуществляет следующие действия: – выводит на печать сертификат открытого ключа ЭЦП Клиента из Каталога открытых ключей, используя АРМ «Администратор» Системы «iBank2»; – сравнивает распечатанный сертификат открытого ключа ЭЦП Клиента из Каталога открытых ключей с Эталонным сертификатом, предоставленным Комиссии Администратором ЦРК Банка, а также с аналогичным сертификатом, хранящимся у Клиента и представленным Комиссии Клиентом. Значения открытого ключа ЭЦП Клиента, содержащиеся в Каталоге открытых ключей, в Эталонном сертификате и в хранящемся у Клиента сертификате, должны совпасть. В случае их несовпадения верным признается Эталонный сертификат; – с помощью АРМ «Операционист» находит спорный документ и, используя меню «Проверить ЭЦП», формирует результат проверки ЭЦП, в котором указываются идентификаторы ключей ЭЦП, участвовавшие в подписи документа, авторство которого оспаривается; – выводит на печать Документ со списком идентификаторов подписавших его ключей ЭЦП. В случае, если спорный Электронный документ был подписан несколькими ЭЦП, данная процедура повторяется применительно к каждой ЭЦП.</p> <p>7.21. Принадлежность ЭЦП Клиенту и авторство</p>	<p>Customer.</p> <p>7.17. If the Customer has initiated consideration of the dispute, the Commission shall establish effectiveness of public keys of the Customer EDS at the time the Electronic Document subject to dispute was transmitted. Public keys of the Customer EDS shall be deemed effective if they were registered with the Public Key Catalog in accordance with clause 2.2 of these Provisions and were in force at the time when the disputed Electronic Document was transmitted by the Customer to the Bank.</p> <p>7.18. Taking into account the mathematical properties of the EDS algorithm implemented in accordance with the standards of the Russian Federation (GOST R 34.10-94 and GOST R 34.11-94) and ensuring that the value of certified EDS can not be fraudulently imitated by any person not possessing the private EDS key, the Parties recognize that consideration of a dispute relating to the identity of the drafter and integrity of the Electronic document shall be limited to proving that EDS of the given Electronic Document is owned by the given Party.</p> <p>7.19. The Commission shall consider a dispute relating to the identity of the drafter and integrity of an Electronic Document using the Teller Account of the iBank2 System.</p> <p>7.20. In order to draft an EDS Verification Protocol, the CST Administrator of the Bank shall perform the following actions in presence of the Commission: – print out the public key certificate(s) of the Customer EDS from the Public Key Catalog using the Administrator Account of the iBank2 System; – compare the printed copy of the public key certificate(s) of the Customer EDS with the Reference Certificate(s) provided to the Commission by the KRC Administrator of the Bank, and with the identical certificate maintained by the Customer and made available to the Commission by the Customer. The values of the public key of the Customer EDS as indicated in the Public Key Catalog, the Reference Certificate and the certificate maintained by the Customer should match. Where they do not match, the Reference Certificate shall be recognized as true and correct; – find the disputed Electronic Document using a Teller Account and, using the Verify EDS menu, print to the screen the result of EDS verification specifying identifications of EDS keys found in the Electronic Document with the disputed identity of the drafter; – print out the Electronic Document with a list of identifications of EDS keys found in it. Where the disputed Electronic Document was signed by more than one EDS, this procedure shall be repeated for each EDS.</p> <p>7.21. The Customer's ownership of the EDS and</p>
---	---

Электронного документа считается установленным, если идентификаторы открытых ключей ЭЦП, содержащихся в списке идентификаторов, подписавших Документ, и Эталонном сертификате совпадают, в Документе сформирована запись «ЭЦП Корректна», и распечатанный сертификат открытого ключа ЭЦП Клиента из Каталога открытых ключей совпадает с Эталонным сертификатом.

7.22. Заключение Комиссии оформляется письменно в двух экземплярах – по одному для каждой из Сторон - и подписывается всеми членами Комиссии.

7.23. Заключение Комиссии является окончательным, пересмотру во внесудебном порядке не подлежит и является обязательным для участвующих в рассмотрении спора Сторон.

7.24. Если Стороны не могут урегулировать спор в рабочем порядке, не согласны с Заключением Комиссии, или если одна из Сторон уклоняется от создания Комиссии в случаях, когда в соответствии с Положением Комиссия должна быть создана, возникший спор передается на рассмотрение и разрешение по существу суду, определенному Сторонами в Договоре.

Все иные споры Сторон, связанные с обменом Электронными документами по Системе, также передаются на рассмотрение указанного в настоящем пункте суда.

8. Прочие условия

8.1. Положение составлено на русском и английском языках. При этом в случае любого разночтения преимущественную силу имеет текст на русском языке.

identity of the drafter of an Electronic Document shall be deemed established where identifications of public EDS keys contained in the list of identifications found in the Electronic Document match those found in the Reference Certificate, the Electronic Document is marked “EDS correct”, and the certificate of the Customer’s public EDS key printed out from the Public Key Catalog matches the Reference Certificate.

7.22. The Commission’s opinion shall be documented in writing in two duplicates, one for each of the Parties, to be signed by all members of the Commission.

7.23. The Commission’s opinion shall be final and binding on all Parties involved in consideration of the dispute, and shall not be subject to revision under an extrajudicial procedure.

7.24. Where the Parties failed to resolve the dispute in course of usual business relations, disagree with the Commission’s opinion, or if one of the Parties evades from forming a Commission where such Commission has to be formed in accordance with these Provisions, the dispute in question shall be referred to a court determined by the Parties in the Agreement which shall consider and resolve the dispute on its merits.

All other disputes between the Parties relating to Electronic Documents exchange via the System shall be likewise referred for consideration to the court specified in this clause.

8. Miscellaneous

8.1. The Regulation is made in Russian and English languages. In the event of any discrepancies, the Russian language shall prevail.

Приложение № 1
Annex No. 1

к Положению об использовании системы «Интернет-Банк iBank2»

to the Regulation on the Use of the Internet-Bank iBank2 System

АКБ «Абсолют Банк» (ЗАО)
of Commercial bank "Absolut Bank"

СЕРТИФИКАТ ОТКРЫТОГО КЛЮЧА ЭЦП КЛИЕНТА
PUBLIC KEY CERTIFICATE OF CUSTOMER EDS
В СИСТЕМЕ «Интернет Банк iBank2»
IN INTERNET BANK IBANK2 SYSTEM
АКБ «Абсолют Банк (ЗАО)
OF ABSOLUT BANK

1. Наименование/ ФИО Клиента / Business/Full name of Customer

2. Местонахождение/адрес регистрации по месту жительства Клиента / Location/registered residence address of Customer

3. Почтовый адрес Клиента / Postal address of Customer

4. Наименование документа о регистрации, кем и когда выдан / Name of registration document, issuing authority and date of issue

5. Тел. / Tel. _____ 6. ИНН / TIN _____ 7. КПП / KPP _____

8. Факс / Fax _____ 9. E-mail _____

10. Сведения о владельце открытого ключа ЭЦП / Details of public EDS key owner
Фамилия, Имя, Отчество / Full name

Должность / Position

Документ, удостоверяющий личность / Personal identification document
серия / series _____, номер / number _____
кем выдан / issuing authority

_____ дата выдачи / date of issue «___» _____
года.

11. Примечания / Comments

Открытый ключ ЭЦП клиента / Public Customer EDS Key

Идентификатор / Identification _____

Дата начала действия / Start date «___» _____ 200__ г.

Дата окончания действия / Termination date «___» _____ 200__ г.

Представление открытого ключа ЭЦП в шестнадцатеричном виде / Hex representation of public EDS key:

FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Группа подписи / Signature group _____

Сертификат открытого ключа ЭЦП клиента в системе Интернет Банк iBank2 действует в рамках договора на обслуживание в системе Интернет Банк iBank2 / This public customer EDS certificate in the Internet Bank iBank2 System shall be in effect in accordance with Internet Bank iBank2 System Service Agreement № ___ от _____ 200__ г.

**Достоверность приведенных данных подтверждаю
I confirm that the above data is true and accurate**

Личная подпись владельца ЭЦП / Personal signature of EDS owner

Руководитель организации
CEO of Customer Entity

Уполномоченный представитель Банка
Authorized representative of the Bank

Оттиск печати
Seal print

Оттиск печати Банка
Bank seal print

Приложение № 2
Annex No. 2

к Положению об использовании системы «Интернет-Банк iBank2»

to the Regulation on the Use of the Internet-Bank iBank2 System

АКБ «Абсолют Банк» (ЗАО)
of Commercial bank “Absolut Bank”

СОГЛАШЕНИЕ
об IP фильтрации
IP filtration AGREEMENT

г. _____

« _____ » _____ 200__ года

<p>Акционерный коммерческий банк «Абсолют Банк» (закрытое акционерное общество), именуемый в дальнейшем «Банк», в лице _____</p> <p>_____, действующего на основании доверенности от «__» _____ 200__ года № _____, с _____ одной стороны, и _____</p> <p>_____ (Полное фирменное наименование Клиента)</p> <p>именуем _____ в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, заключили настоящее соглашение (далее по тексту – «Соглашение») о нижеследующем:</p>	<p>Commercial bank “Absolut Bank”, hereinafter referred to as the “Bank”, represented by _____</p> <p>_____, acting on the basis of the Power of attorney dated «__» _____ 200__ No. _____, on the one part, and _____</p> <p>_____ (Full business name of the Customer)</p> <p>hereinafter referred to as the “Customer”, represented by _____</p> <p>_____, acting on the basis of _____, on the other part, have hereby entered into this Agreement (hereinafter referred to as the “Agreement”) as follows:</p>
--	---

1. Разрешить Клиенту доступ к системе «Интернет-Банк iBank2» только со следующих IP адресов:
 The Customer shall be allowed to access Internet Bank iBank2 System from the following IP-addresses only:

№ п/п / Item No.	IP адрес / IP-address			
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

1. Соглашение действует в рамках договора на обслуживание в системе Интернет Банк iBank2 №___ от _____ 200__ г. (далее по тексту – Договор) и утрачивает силу при заключении нового соглашения о IP-фильтрации или расторжении Договора.
2. Настоящее соглашение составлено в двух экземплярах – по одному для каждой из Сторон, и считается действительным при наличии подписей Сторон и печати Банка.

МЕСТО НАХОЖДЕНИЯ И РЕКВИЗИТЫ СТОРОН.

Реквизиты Банка:

Акционерный коммерческий банк «Абсолют Банк» (закрытое акционерное общество).

Место нахождения: 127051, г. Москва, Цветной бульвар, д. 18.

Место нахождения Филиала: _____ (указывать только филиалам)

Кор. _____ счет: _____

_____, БИК _____ ИНН 7736046991.

Счет в долларах США (USD) - № 18301701 with KBC BANK NV, 1177 Avenue of the Americas, New York, NY 10036, USA, SWIFT: KREDUS33;

Счет в Евро (EUR) - № 488591799660 with KBC BANK NV, B – 1080 Brussels, Belgium, SWIFT: KREDBEBB.

Absolut Bank, Moscow, Russia; SWIFT: ABSLRUMM.

2. The Agreement shall apply under Internet Bank iBank2 System Service Agreement No.____ dated _____ 200__ (hereinafter referred to as the Service Agreement) and shall terminate at making a new IP filtration agreement or at termination the Service Agreement.
3. This Agreement is made in two duplicates, one for each of the Parties, and shall be deemed valid if signed by the Parties and sealed with the Bank's seal.

ADDRESSES AND DETAILS OF THE PARTIES.

Details of the Bank:

Commercial bank "Absolut Bank".

Address: 18, Tsvetnoy Boulevard, Moscow 127051.

Branch location address: _____

(to be filled in by branches only)

Correspondent _____ account: _____

_____, BIC _____ TIN 7736046991.

USD account No. 18301701 with KBC BANK NV, 1177 Avenue of the Americas, New York, NY 10036, USA, SWIFT: KREDUS33;

EURO account No. 488591799660 with KBC BANK NV, B – 1080 Brussels, Belgium, SWIFT: KREDBEBB.

Absolut Bank, Moscow, Russia; SWIFT: ABSLRUMM.

Telephone: _____. Fax: _____.

Телефон: _____. Факс: _____. Реквизиты Клиента: Наименование: _____ _____ _____ Место _____ нахождения: _____ _____ _____ ИНН, _____ КПП, _____ ОКПО: _____ _____ Платежные _____ реквизиты: _____ _____ _____ _____ Телефон: _____ _____ _____	Details of the Customer: Business _____ name: _____ _____ Registered _____ address: _____ _____ _____ TIN, _____ KPP, _____ ОКПО: _____ _____ Bank account details: _____ _____ _____ _____ Telephone: _____ _____ _____
--	--

ПОДПИСИ СТОРОН / SIGNATURES OF THE PARTIES
