Приложение № 4
к Общим условиям использования электронных документов/ Annex No. 4
to General Terms and Conditions of Use of Electronic Documents

ИНСТРУКЦИЯ
О ПОРЯДКЕ ВЗАИМОДЕЙСТВИЯ СТОРОН ПО ОСУЩЕСТВЛЕНИЮ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ[1]/ INSTRUCTION
ON INTERACTION OF THE PARTIES IN COURSE OF EXCHANGE OF ELECTRONIC DOCUMENTS[1]

1. Обмен Электронными документами/ Exchange of electronic documents

1.1. Для работы в Системе Пользователь Системы использует программно-технические средства, удовлетворяющие требованиям, приведенным в Списке технических и программных средств, необходимых для работы подсистемы “Клиент” (далее – Список).	1.1. For the purpose of working in the System, a System User uses the hardware and software which meet the requirements specified in the List of Hardware and Software necessary for operation of the *Client* subsystem (hereinafter referred to as the List).
1.2. В процессе работы Пользователь Системы выполняет в Системе следующие действия: o Регистрация в Системе – формирование специального ЭД “регистрация”, подписанного ЭП Клиента (далее – ЭПК). Работа в Системе возможна только после успешной проверки ЭПК сервером Системы. o Работа с ЭД, исходящими от Клиента, предполагает формирование новых ЭД на основе ЭД, имеющихся в Системе и предусмотренных в Заявлении. Для каждого типа ЭД в Системе имеется соответствующая экранная форма. Для документов “Платежное поручение” возможен импорт в Систему файлов определенного Банком формата. Описание структуры файла импорта имеется на сервере Банка.	1.2. In the course of operation, a System User is obliged to perform the following actions within the System: o Registration in the System, which means generation of a special Electronic Document “Registration” signed by the Client’s electronic signature (hereinafter referred to as CES). It is only possible to work in the System following successful authorization of CES by the System server. o Working with ED originated by the Client implies generation of new EDs on the basis of EDs stored in the System and specified in the Application. With regard to each type of ED a relevant display form exists in the System. With regard to *Payment Order* documents it is possible to import in the System files of the format determined by the Bank. A description of the structure of file import is available on the server of the Bank.

[1] Настоящая Инструкция определяет порядок взаимодействия Сторон при использовании Клиентом подсистемы «ИКБ».

○ Проставление для каждого ЭД одной или нескольких ЭПК. Количество ЭПК для каждого типа ЭД определено в Заявлении. После подписания ЭД всеми необходимыми ЭПК в соответствии с Заявлением происходит автоматическая пересылка ЭД в Банк для исполнения. ○ Просмотр, печать, сохранение в файл поступивших из Банка ЭД. ○ Выход из Системы.	○ Provision of one or several CESs for each ED. The number of CESs for each type of ED is specified in the Application. Following the signing of ED by all necessary CESs in compliance with the Application, ED is automatically remitted to the Bank for execution. ○ Viewing, printing, storing and filing of EDs which arrive from the Bank. ○ Logging out of the System.
1.3. Процедура обработки ЭД сервером Системы происходит следующим образом: ○ По окончании формирования ЭД Пользователи Системы проставляют ЭПК в количестве, определенном в Заявлении и отправляют ЭД в Банк. ○ Сервер Банка получает ЭД и проверяет корректность всех имеющихся в нем ЭПК. ○ Основанием для принятия Банком ЭД, переданного Клиентом по Системе, является наличие в количестве, установленном в соответствии с Заявлением, и корректность всех ЭПК в ЭД. При положительном результате проверки сервер Банка проставляет в документе отметку о времени приема ЭД и ЭП Банка (далее – ЭПБ), свидетельствующую о получении Банком ЭД, и сохраняет данный ЭД в Системе. При отрицательном результате проверки ЭПК ЭПБ в ЭД не проставляется, Клиент получает сообщение об ошибке средствами Системы. Ключи проверки электронной подписи Банка и копии соответствующих Сертификатов ключей размещаются на сервере системы https://www.bankline.ru. Сертификат Ключа проверки электронной подписи Банка подписывается только уполномоченным представителем Банка. Срок действия Комплекта ключей Банка составляет 5 лет.	1.3. The following procedure for ED processing by the System server is now in place: ○ Following generation of ED by the System User, CESs are fixed in the number specified in the Application, and ED is then sent to the Bank. The server of the Bank receives ED and verifies all CESs contained in ED. Availability of all CESs in the number determined by the Application and authenticity of all CESs in ED constitute the ground for the Bank to accept ED communicated by the Client via the System. In the event of a successful verification, the server of the Bank puts a mark in the document regarding the time of acceptance of ED and ES of the Bank (hereinafter referred to as BES), which confirms the Bank's acceptance of ED. and stores such ED in the System. In the event of a negative result of verification of CES no BES is fixed in ED, and the Client is given an authorization error message via the System. Keys of verification of the Bank's electronic signature and copies of relevant Key Certificates are stored on the System Server at https://www.bankline.ru. The key of authorization of the electronic signature of the Bank is only signed by an authorized representative of the Bank. The set of keys of the Bank is valid for five years.
1.4. Процедуры, описанные в п.1.3 настоящей Инструкции, представляют собой единый и неделимый на части процесс получения Банком ЭД, не могут быть	1.4. The procedures described in paragraph 1.3 of this Instruction constitute a single and indivisible process of acceptance of EDs by the Bank and may not be performed in another

выполнены в другой последовательности и рассматриваться независимо друг от друга.	sequence and may not be viewed separately from each other.
1.5. Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл должен содержать ЭПК, отметку о времени приема документа Банком и ЭПБ. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.	1.5. A document is deemed to be delivered by the Client to the Bank, if saved in the archive of the Client's documents on the Bank's server. The Client is entitled to save any outgoing document in a file with a view to keep its own archive. The file is to carry CES, a mark about the time of acceptance of the document by the Bank and BES. Files stored on the Bank's server and in the Client's archive may be subsequently used in the course of dispute settlement between the Parties.
1.6. Переданный Клиентом в Банк ЭД в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус ЭД изменяется Банком. Клиент имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк ЭД. Сервер Банка присваивает полученным от Клиента ЭД следующие статусы: Рублевые платежные поручения: ○ получен банком ○ документ отправлен на исполнение ○ Рассчитана комиссия за РКО xx.xx. ○ Принято или «обработано с ошибкой» с указанием причины, по которой документ отвергнут; ○ Отправлен на валютный контроль ○ Включен в рейс для РКЦ ○ Исполнен Остальные типы документов: ○ получен банком ○ документ отправлен на исполнение ○ Принят к исполнению или “обработано с ошибкой” с указанием причины, по которой документ отвергнут; ○ Реестр к росписи ○ Реестр расписан или частично расписан в случае частичной росписи ○ Сообщение отправлено в филиал ○ Документ получен сотрудником валютного контроля.	1.6. ED handed over by the Client to the Bank at each point of time has a relevant status on the Bank's server with a note of time of its receipt. ED status may be modified by the Bank. The Client enjoys an opportunity to receive on a continuous basis information from the Bank's server concerning status modification (including the time of its modification) of the electronic document handed over to the Bank. The server of the Bank assigns the following statuses to electronic documents received from the Client: Payment order in rubles: ○ Accepted by the bank ○ Document sent for execution ○ Cash and settlement service fee charged in the amount of xx.xx. ○ Accepted or processed with error, with indication of the reason underlying rejection of the document; ○ Sent to foreign exchange control ○ Put on the dispatch list for delivery to cash settlement center ○ Settled Other types of documents: ○ Received by the Bank ○ Document sent for execution ○ Accepted for execution or processed with error, with indication of the reason underlying rejection of the document; ○ Register breakdown ○ Register broken down or partially broken down in the event of partial breakdown ○ Message sent to subsidiary

Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться присвоение Банком ЭД Клиента статуса “документ отправлен на исполнение”, а при работе в Депозитарном модуле Системы - получение Клиентом документа типа «Статус обработки распоряжения/запроса», в котором указано, что статус обработки соответствующего ЭД Клиента «Принято к исполнению». Банк информирует Клиента об исполнении каждого ЭД Клиента путем направления Клиенту соответствующего уведомления посредством Системы. Примечание: Перечень и описание статусов ЭД, присваиваемых сервером Банка в Депозитарном модуле Системы, приведены в руководстве пользователя Депозитарного модуля Системы.	○ Document accepted by foreign-exchange control officer. The Parties acknowledge that assigning of the Client’s *Document Sent for Execution* status will constitute the Bank’s appropriate notification of the Client about acceptance of the Client’s document for execution, and with regard to working in the Depository Module of the System – receipt by the Client of the document with the *Status of Processing of an Order/Request* type which specifies that the status of processing of a relevant ED of the Client is *Accepted for Execution*. The Bank notifies the Client about execution of every ED of the Client by forwarding to the Client a relevant notification via the System. Note: The list and description of statuses of EDs assigned by the Bank’s server in the Depository Module of the System are given in the User Manual in the Depository Module of the System.
1.7. При формировании ЭД для Клиента Банк проставляет в нем ЭПБ. ЭД считается переданным Банком Клиенту, если он подписан ЭПБ и выложен на сервер Банка, то есть имеется в списке входящих ЭД Клиента на сервере Банка. Клиент может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.	1.7. When generating ED for the Client, the Bank will fix its electronic signature in such document. ED is deemed transmitted to the Client by the Bank, if signed by BES and placed on the Bank’s server, i.e. such ED is on the list of the Client’s incoming electronic documents on the Bank’s server. The Client may save any incoming document in a file for maintaining its own archive. Archive files may consequently be used in the course of dispute settlement.
1.8. Банк фиксирует электронные архивы полученных от Клиента ЭД, содержащих ЭПК и ЭПБ, и доставленных Клиенту ЭД, содержащих ЭПБ, и хранит их способом, обеспечивающим Клиенту доступ к данным ЭД на сервере Банка.	1.8. The Bank will record the electronic archives of electronic documents obtained from the Client, which carry CESs and BESs and EDs delivered to the Client which carry CESs and kept in a mode which provides the Client with access to EDs with BES on the Bank’s server.
1.9. Клиент с помощью программы проверки ЭП CryptoManager.exe, установленной на Персональном компьютере, имеет возможность в любой момент времени проверить ЭПБ и ЭПК любого файла архива. Вышеуказанная программа проверки ЭП позволяет выполнять проверку типов ЭП (раздел 3 настоящей Инструкции), разрешенных для использования в Системе.	1.9. Based on the use of *CryptoManager.exe* verification program installed in PC, the Client may at any point of time verify BES and CES fixed in any archive file. The above ES verification software provides for verifying ES types (section 3 of this Instruction), allowed for use in the System.
1.10. Программу проверки ЭП CryptoManager.exe можно получить у фирмы-	1.10. *CryptoManager.exe* ES verification software may be obtained from the manufacturer of

разработчика Системы – ЗАО “ИНИСТ” (Лицензия ФСБ России № 12818Н от 16.04.2013), зарегистрированной по адресу 115035, г. Москва, Космодамианская наб., д.40-42, стр.3.	the System CJSC INIST (License issued by the Federal Security Service (FSB) of Russia No.12818N on April 16, 2013) registered at 115035, Moscow, 40-42 bldg 3 Kosmadamianskaya embankment.

2. Порядок получения, замены и хранения ключей/ Procedure for receiving, replacing and storaging of keys

2.1. Для Комплектов ключей, сгенерированных для работы на Персональном компьютере Клиентами, относящимися к корпоративному сегменту:	2.1. With regard to sets of keys generated for operation of PCs by business segment Clients:
2.1.1. Клиент может генерировать Комплекты ключей своих Пользователей Системы согласно Заявлению с помощью программных средств, предоставленных Банком, на USB-токенах с использованием своих технических средств.	2.1.1. The Client may generate sets of keys for its System Users on the basis of an Application with use of the software provided by the Bank, on USB tokens on the basis of its own technical facilities.
2.1.2. Первый Ключ проверки электронной подписи каждого Пользователя Системы регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе.	2.1.2. The first Electronic Signature verification key of each System User shall be registered by the Bank on the basis of the Key Certificate signed by the Parties and executed in hard copy.
2.1.3. Второй и последующий Ключи проверки электронной подписи регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе, или на основании электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, являющегося единоличным исполнительным органом Клиента и направленного в Банк с использованием Системы. При этом, Банк вправе запрашивать, а Клиент обязан по запросу Банка предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя, в том числе являющимися единоличным исполнительным органом.	2.1.3. The second and subsequent Electronic Signature verification keys shall be registered by the Bank on the basis of the Key Certificate signed by the Parties executed in hard copy, or on the basis of a request for release of the Key Certificate to be signed by the System User’s electronic signature effective at the date of signing, which System User acts as a sole executive body of the Client, and thereafter to be sent to the Bank via the System. In such case the Bank shall be entitled to request, and the Client shall be obliged pursuant to such request to submit documents to the Bank (in the form of the originals or duly certified copies thereof), which confirm the powers of the User, including those of the sole executive body.
2.1.4. Срок действия Комплекта ключей указывается в Сертификате ключа. Срок действия Комплекта ключей не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его	2.1.4. The period of validity of the set of keys is specified in the Key Certificate. The said period may not exceed the term of authority of a System User pursuant to the documents which confirm his/her authority. In cases where based on the documents provided by the Client it is deemed

полномочия. В случае если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Системы, срок действия Комплекта ключей не может превышать трех лет. До истечения установленного срока Клиент обязан инициировать процедуру смены Комплектов ключей. По заявлению Клиента, направленному в Банк в произвольной форме средствами Системы до окончания срока действия Комплекта ключей, его действие может быть продлено на срок не более 3 месяцев. По инициативе Клиента Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.	impossible to determine the term of effect of the System User's authority, the period of validity of ф set of keys may not exceed three years. Prior to expiration of the established period, the Client is obliged to initiate the procedure of replacement of sets of keys. Based on the Client's application submitted to the Bank in a free format via the System facilities prior to expiration of the term of validity of a set of keys its effect may be extended for a term not exceeding three months. At the initiative of the Client, a set of keys may be replaced at any point of time of its effect. Each new key certificate signed by the Parties will automatically supersede the effect of the previously issued key certificate of a particular System User.
2.1.5. Оформленные со стороны Банка Сертификаты ключей Клиента вручаются УПК либо направляются Клиенту посредством почтовой связи по адресу Клиента, указанному в Договоре. Сертификаты ключей должны храниться у каждой из Сторон не менее пяти лет после окончания их срока действия.	2.1.5. The Client's key certificates generated by the Bank are to be handed to ARC, or mailed to the Client's address specified in the Agreement. Key certificates are to be kept by each of the Parties for not less than five years following expiration of the term of their validity.
2.1.6. При поступлении электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, Банк направляет Клиенту с использованием Системы Сертификат ключа, подписанный электронной подписью уполномоченного представителя Банка. При этом Клиент вправе обратиться в Банк с целью получения копии Сертификате ключа на бумажном носителе, заверенной Банком как удостоверяющим центром.	2.1.6. Upon arrival of an electronic request for issuance of a Key Certificate signed by the System User's Electronic Signature effective at the date of signing, the Bank shall send via the System the Key Certificate signed by the electronic signature of an authorized representative of the Bank. In such case the Client is entitled to apply to the Bank for a hard copy of the Key Certificate certified by the Bank as a certification center.
2.1.7. В случае информирования Банком Клиента в Системе о необходимости осуществить замену USB-токена соответствующего типа, Клиент обязан осуществить замену USB-токена. С момента информирования Банком Клиента в Системе о необходимости осуществить замену USB-токена, генерация Комплектов ключей с помощью USB-токена, подлежащего замене, не осуществляется.	2.1.7. In case the Bank notifies the Client via the System about the need to replace a USB token of a relevant type, the Client is obliged to replace the USB token. As from the date of such notification, no key sets may be generated with the help of the USB token subject to replacement.
2.2. Для Комплектов ключей, сгенерированных для работы на Персональном	2.2. With regard to the key sets generated for operation of PCs by business segment Clients:

компьютере Клиентами, относящимися к сегменту предпринимателей:	
2.2.1. Клиент может генерировать Комплекты ключей своих Пользователей Системы согласно Заявлению с помощью программных средств, предоставленных Банком, на USB-токенах или иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств.	2.2.1. The Client may generate sets of keys for its System Users based on the Application with the help of the software provided by the Bank, on USB tokens or other information media (hard disks, removable media (flash disks, external hard disks), etc.) with use of its own technical facilities.
2.2.2. Первый Ключ проверки электронной подписи каждого Пользователя Системы регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе.	2.2.2. The first ES verification key of each System User is to be registered by the Bank on the basis of the key certificate signed by the Parties and executed in a hard copy.
2.2.3. Второй и последующий Ключи проверки электронной подписи регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе, или на основании электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, и направленного в Банк с использованием Системы. Указанный запрос также может быть подписан простой электронной подписью Пользователя Системы, сформированной на основании предъявленного клиентом SMS-кода, ранее направленного Банком на номер телефона данного Пользователя Системы, указанный в Заявлении и/или предоставленный Банку Пользователем Системы в процессе обслуживания в Системе. Пользователь Системы должен обладать полномочиями на направление в Банк соответствующего электронного запроса. При использовании Клиентом Системы при наличии открытого расчетного счета подпись такого Пользователя должна быть включена в карточку с образцами подписей и оттиска печатей, действующей к счету Клиента, обслуживаемому в рамках Договора, в случае ее оформления. При этом, Банк вправе запрашивать, а Клиент обязан по запросу Банка предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя по направлению в Банк электронного запроса на выдачу Сертификата ключа.	2.2.3. The second and subsequent ES verification keys are to be registered by the Bank on the basis of the key certificate signed by the Parties and executed in a hard copy, or on the basis of an electronic application for issuance of a key certificate signed by an electronic signature of the System User effective as at the date of signing by the System Users of ES and forwarded to the Bank via the System. The above application may also be signed by a System User's basic electronic signature generated on the basis of the SMS code previously sent by the Bank to the telephone number of such System User specified in the Application and/or provided by the System User to the Bank in the course of service in the System. A System User is to be authorized to send to the Bank a relevant electronic request. In case where the Client uses the System in in conjunction with a current account, the signature of such User is be recorded in the banking sample signatures and seal card which are attached to the Client's account serviced within the framework of the Agreement, if such card is in place. In such case the Bank has the right to request, and the Client is obliged following the Bank's request, to submit to the Bank the documents (in the form of originals or duly certified copies), which confirm the User's authority to forward to the Bank an electronic request for issuance of a key certificate.

2.2.4. Срок действия Комплекта ключей определяется Банком и указывается в Сертификате ключа. Срок действия Комплекта ключей не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае, если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Системы, срок действия Комплекта ключей не может превышать трех лет. До истечения установленного срока действия Комплекта ключей Клиент обязан инициировать процедуру смены Комплектов ключей. При этом, до окончания срока действия Комплекта ключей Клиент может продлить его действие на срок не более 3 (трех) месяцев, направив в Банк заявление посредствами Системы. По инициативе Клиента Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Банком, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.	2.2.4. The term of validity of a set of keys is to be determined by the Bank and specified in the key certificate. The said term may not exceed the period of validity of the authority of a System User in accordance with the documents which confirm the User's authority. In cases where it is deemed impossible to identify the term of validity of the System User's authority, the term of effect of a set of keys may not exceed three years. Prior to expiration of the established term of a set of keys the Client is obliged to initiate the procedure of substitution of a set of keys. In such case, prior to expiration of the term of validity of a set of keys the Client may extend the term of not more than 3 (three) months by forwarding to the Bank a relevant application via the System. At the initiative of the Client, a set of keys may be replaced at any point of time of its effect. Each new key certificate signed by the Bank automatically supersedes the effect of the previously issued key certificate of a particur System User.
2.2.5. Оформленные со стороны Банка Сертификаты ключей Клиента на бумажных носителях вручаются уполномоченному представителю Клиента либо направляются Клиенту посредством почтовой связи по адресу Клиента, указанному в Договоре. Сертификаты ключей должны храниться у каждой из Сторон не менее пяти лет после окончания их срока действия.	2.2.5. The Client's key certificates executed by the Bank in hard copies are to be handed to an authorized representative of the Client, or mailed to the Client's address specified in the Agreement. The Parties are obliged to keep key certificates for not less than five years following expiration of their validity.
2.2.6. При поступлении электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, Банк направляет Клиенту с использованием Системы Сертификат ключа, подписанный электронной подписью уполномоченного представителя Банка. При этом Клиент вправе обратиться в Банк с целью получения копии Сертификата ключа на бумажном носителе, заверенной Банком как удостоверяющим центром.	2.2.6. Upon arrival of an electronic application for issuance of a key certificate signed by the System User's electronic signature effective as at the date of signing, the Bank is to send to the Client via the System a key certificate with an electronic signature of an authorized representative of the Bank. In such case the Client has the right to request to the Bank to issue a hard copy of the key certificate certified by the Bank acting as a certification authority.
2.2.7. В случае информирования Банком Клиента в Системе о прекращении действия имеющегося у Клиента USB-токена соответствующего типа, Клиент должен	2.2.7. In the event that the Client is notified by the Bank about termination of the effect of the Client's USB token of a relevant type, the Client is obliged to perform the procedure of replacement of the sets of keys of its System Users:

осуществить процедуру смены Комплектов ключей своих Пользователей Системы: • путем генерирования Комплектов ключей своих Пользователей Системы на иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств, либо • путем осуществления замены USB-токена, посредством обращения в подразделение Банка.	• By way of generating sets of keys of its System Users on other media (hard disks, removable media (flash disks, external hard disks), etc.) with use of its own technical facilities, or • By way of replacing a USB token following a relevant request to the Bank.
2.3. Для Комплекта ключей, сгенерированного посредством Мобильного приложения:	2.3. With regard to the set of keys generated with the help of a mobile application:
2.3.1. Пользователь вправе генерировать Комплект ключей для Мобильного приложения с помощью программных средств, предоставленных Банком, при наличии действующего Комплекта ключей, сгенерированного для работы на Персональном компьютере.	2.3.1. The User has the right to generate a set of keys for a mobile application with the help of the software provided by the Bank in the existence of an effective set of keys generated for working on PC.
2.3.2. Срок действия Комплекта ключей указывается в Сертификате ключа. Срок действия Комплекта ключей, сгенерированного посредством Мобильного приложения, не может превышать срок действия Комплекта ключей Пользователя, сгенерированного для работы на Персональном компьютере. До истечения установленного срока Клиент обязан инициировать процедуру смены Комплектов ключей. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.	2.3.2. The term of validity of a set of keys is specified in the key certificate. The term of validity of a set of keys generated with the use of a mobile application may not exceed the term of validity of the User's set of keys generated for working on PC. Prior to expiration of the established period, the Client is obliged to initiate the procedure of replacement of a set of keys. Each new key certificate signed by the Parties will automatically supersede the effect of the previously issued key certificate of such System User.
2.3.3. Статус ЭП Пользователя Системы, сгенерированной посредством Комплекта ключей для Мобильного приложения, соответствует Статусу ЭП Пользователя Системы, указанному в Заявлении, при генерации Комплекта ключей на USB-токенах или иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.)	2.3.3. The status of ES of a System User generated with the use of a set of keys for a mobile application corresponds to the status of the electronic signature of a System User specified in the Application upon generation of a set of keys on USB tokens or other media (hard disks, removable media (flash disks, external hard disks), etc.).
2.3.4. Обязательная замена Комплекта ключей проводится в следующих случаях: • истек срок действия Комплекта ключей; • произошла Компрометация ключей.	2.3.4. It is required to replace a set of keys in the following cases: • The term of validity of a set of keys has expired; • The keys have been compromised.

2.4. В случае лишения Клиентом Пользователя Системы права подписывать ЭП ЭД соответствующие Комплекты ключей выводятся из действия на основании письменного заявления Клиента или ЭД свободного формата, направленного в Банк посредством Системы и подписанного уполномоченным лицом Клиента.	2.4. In case the Client denies a System User the right to sign an electronic document with ES the relevant key sets are be disabled pursuant to a written application of the Client or an electronic document of a free format sent to the Bank via the System and signed by an authorized representative of the Client.
2.5. Банк вправе аннулировать Сертификат ключа в следующих случаях: • не подтверждено, что владелец Сертификата ключа владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате; • установлено, что содержащийся в Сертификате ключ проверки ЭП уже содержится в ином ранее созданном Сертификате ключа; • вступило в силу решение суда, которым, в частности, установлено, что Сертификат ключа содержит недостоверную информацию. Информация о прекращении действия Сертификата ключа вносится Банком в соответствующий реестр сертификатов в срок, установленный действующим законодательством Российской Федерации.	2.5. The Bank has the right to revoke a key certificate in the following cases: • There is no confirmation that a certificate holder possesses the ES key which corresponds to the ES verification key specified in such certificate; • It is established that the ES verification key specified in the certificate already exists in another previously generated key certificate; • A court decision came into effect, which in particular established that the key certificate contains unreliable information. The Bank records information concerning revocation of a key certificate in a relevant certificate register within the term established by the applicable law of the Russian Federation.

3. Обеспечение безопасности процедуры обмена документами/ Maintenance of security of document exchange procedure

3.1. Безопасность обмена ЭД достигается за счет применения следующих средств:	3.1. Security of ED exchange is ensured via use of the following facilities:
3.1.1. Для Персонального компьютера: Средство криптографической защиты информации (СКЗИ) на базе Программного комплекса «Бикрипт 5.0.» (вариант исполнения 2), разработанного ООО Фирма «ИнфоКрипт» (сертификат соответствия ФСБ РФ СФ/114-3021 от 30 декабря 2016 года). Клиент, относящийся к сегменту предпринимателей, имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (жесткий диск, съемные носители (оптические диски, флеш-память, внешний винчестер) и т.п.). Клиент уведомлен	3.1.1. With regard to personal computers: Cryptographic information protection facilities (CIPFs) on the basis of the software solution Bicrypt 5.0. (version 2) developed by InfoCrypt LLC (certificate of conformity issued by the Federal Security Service (FSB) of the Russian Federation (FSB) No. SF/114-3021 oof December 30, 2016). For the purpose of safe-keeping electronic signature keys, a business segment Client is entitled to use information media instead of USB tokens (hard discs, removable media (optical discs, flash memory, external hard discs), etc.). The Client is notified by the Bank that

Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов. Использованием СКЗИ «Криптотокен ЭП 2» в составе USB-токенов JaCarta ГОСТ/JaCarta-2 ГОСТ, разработанных ЗАО «Алладин Р.Д.» (сертификат соответствия ФСБ России № СФ/124-3473 от 10.08.2018 г и № СФ/124 – 3502 от 11.09.2018 г.). Ключ электронной подписи никогда не покидает внутренней защищенной памяти USB-токена. Генерация и хранение Ключа электронной подписи, а также подписание документов производится во внутренней защищенной памяти USB-токена. Доступ к Ключу электронной подписи осуществляется с использованием пароля. Клиент, относящийся к сегменту предпринимателей, имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.). Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов. Шифрования данных в телекоммуникационных каналах с использованием СКЗИ КриптоПро CSP версии 4.0 и выше. Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v. 1.2, RFC 2246 и выше2). Удостоверения принадлежности сервера Системы ПАО РОСБАНК с помощью сертификата, выданного ПАО РОСБАНК аккредитованным Удостоверяющим центром ООО "КРИПТО-ПРО".	utilization of other information media in lieu of USB tokens significantly reduces the level of security in the course of ED exchange, and therefore is fully aware of resulting risks. The Bank recommends to abstain from using any information media other than USB tokens. Utilization of CIPF Cryptotoken ES 2 in conjunction with USB tokens JaCarta GOST/JaCarta-2 GOST developed by CJSC Alladin R.D. (certificate of conformity issued by the Federal Security Service (FSB) of the Russian Federation (FSB) No. SF/124-3473 of August 10, 2018 and SF/124 – 3502 of September 11, 2018). An electronic signature key is never detached from the internal protected memory of a USB token. ES keys are generated and signing of documents is performed inside the internal protected memory of a USB token. Access to ES key is obtained with use of a password. A business segment Client has the right to use other information media in lieu of USB tokens when safe-keeping ES keys (hard discs, removable media (flash memory, external hard discs), etc.). The Client is notified by the Bank that utilization of other information media in lieu of USB token seriously affects the level of security in the course of ED exchange, and is fully aware of resulting risks. The Bank recommends to abstain from using any information media other than USB tokens. Data encryption in telecommunication channels with use of CIPF CryptoPro CSP of version 4.0 and higher. With a view to protect data from unauthorized access in telecommunication channels, protocol Transport Layer Security (TLS v. 1.2, RFC 2246 and above 3) is recommended for use. Certification of appurtenance of the System server of PJSC ROSBANK with the help of a certificate issued to PJSC ROSBANK by the Certification Authority of CRYPTO-PRO LLC.
3.1.2. Для Мобильного приложения:	3.1.2. With regard to mobile apps:

[2] Рекомендуется использовать версию TLS v.1.2.

[3] It is recommended to use version *TLS v.1.2*.

Средства криптографической защиты информации с использованием алгоритма RSA для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v.1.2, RFC 2246), применяются криптографические международные алгоритмы шифрования RSA (3072 bit), обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с SHA 512. Симметричное шифрование AES с длиной ключа 256 bit., генерация и хранение Ключа электронной подписи, а также подписание ЭД производится во внутренней защищенной памяти Мобильного устройства. Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации, предназначенных для генерации и хранения ключа ЭП, за исключением USB-токенов.	Cryptographic information protection facilities with use of RSA algorithm for the purpose of protecting data from unauthorized access in telecommunication channels protocol Transport Layer Security (TLS v.1.2, RFC 2246) is used, as well as international cryptographic encryption algorithms RSA (3072 bit), exchange of keys on the basis of the Diffie-Hellman algorithm and hashing in accordance with SHA 512. AES symmetric encryption with the key length of 256 bit., generation and safe-keeping of ES keys, as well as signing with the help of ES are performed in the internal protected memory a mobile device. The Client is notified by the Bank that utilization of other information media in lieu of USB token seriously affects the level of security in the course of ED exchange, and is fully aware of resulting risks. The Bank recommends to abstain from using any information media for generating and safe-keeping ES keys other than USB tokens.
3.2. Клиенту рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих требований безопасности:	3.2. The Client is recommended to arrange a comprehensive set of organizational and technical measures designed to meet the following security requirements:
3.2.1. Для работы на Персональном компьютере: Организовать выделенный компьютер подсистемы «Клиент», предназначенный исключительно для работы с Банком; Генерацию и хранение ключевой информации, а также подписание документов производить с использованием USB-токенов JaCarta ГОСТ/JaCarta -2 ГОСТ; В случае генерации Клиентом, относящимся к сегменту предпринимателей, Ключей электронной подписи своих Пользователей на носители, отличные от USB-токенов, осуществлять эксплуатацию рабочего места и обеспечение его безопасности организационными и техническими мерами в соответствии с требованиями эксплуатационной документацией для СКЗИ «Бикрипт 5.0» для класса КС1: «Средство криптографической защиты информации «Бикрипт 5.0». Правила пользования» (ИНФК.11485466.4012.027.31). Данный	3.2.1. With regard to PC operation: To allocate a dedicated PC of the Client subsystem intended exclusively for communicating with the Bank; Generation and safe-keeping of key information, as well as signing of documents shall only be performed with use of USB tokens JaCarta GOST/JaCarta -2 GOST; In case a business segment Client generates ES keys for its Users on information media other than USB tokens, it is necessary to operate workstations and ensure their security with reliance on organizational and technical measures in compliance with the operating document requirements for CIPF Bicrypt 5.0 for class KS1: Cryptographic information protection facility Bicrypt 5.0. Directions for Use (INFK.11485466.4012.027.31). The said document is available on the official web-site of the Bank at http://www.rosbank.ru. To introduce restriction of network interconnection of the Client subsystem PC

документ размещен на официальном сайте Банка в сети Интернет по адресу http://www.rosbank.ru. Ввести ограничение сетевого взаимодействия компьютера подсистемы «Клиент» только с необходимым доверенным перечнем IP-адресов; Проверять, что установлено защищенное TLS-соединение с официальным ресурсом сервиса https://www.bankline.ru Средствами подсистемы «Клиент» закрепить за Пользователями Системы IP-адрес/список IP-адресов компьютеров подсистемы «Клиент» в целях обеспечения контроля на стороне Банка; Обеспечить на выделенном компьютере наличие средств защиты от вредоносного программного обеспечения, их работоспособность и регулярное обновление; Исключить на выделенном компьютере открытие писем с вложениями, полученными от неизвестных или недоверенных источников; Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы; Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы; Исключить использование средств удаленного администрирования; Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана; Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.); Контролировать соблюдение требований безопасности.	exclusively with the required trusted list of IP addresses; To verify whether a TLS protected connection with the official resource https://www.bankline.ru service is in place; To assign, based on the Client subsystem facilities, to System Users an IP address/list of IP addresses of the Client subsystem PCs with a view to ensure control on the side of the Bank; To provide for availability on a dedicated PC of malware protection facilities, as well as to ensure their operability and regular updating; To preclude opening on dedicated PCs of letters with enclosures received from unknown or untrusted sources; To make use exclusively of licensed software and operating system; To organize regular installation of software and operating system protection updates; To rule out use of remote administration tools; To put in place a licensed network firewall (it is allowed to use personal network firewalls); To carry out a set of organizational arrangements to ensure information security (operating system security settings, restriction of right to access an information system, pass-wording, preparation of incident response procedures, etc.); To monitor security requirements compliance.
3.2.2. Для работы с Мобильным устройством: Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;	3.2.2. With regard to a mobile device operation: To make use exclusively of licensed software and operating systems; To arrange regular software and operating system updating;

Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы; Исключить использование средств удаленного администрирования; Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты); Контролировать соблюдение требований безопасности; Обеспечить наличие антивирусного программного обеспечения.	To preclude use of remote administration tools; To perform a set of organizational measures to ensure information security (operating system security settings, restriction of right to access an information system, pass-wording); To monitor security requirements compliance; To roll out anti-virus software.
3.3. Пользователи Системы, уполномоченные использовать Систему Клиентами, относящимися к сегменту предпринимателей, должны в Системе ввести номер телефона сотовой связи для получения на указанный номер информационных сообщений в соответствии с Договором.	3.3. System Users authorized by business segment Clients to use the System are obliged to enter into the System a mobile phone number in order to receive to such phone number information messages in accordance with the Agreement.
3.4. Клиент обязан: Исключить появление на Персональном компьютере или Мобильном устройстве подсистемы “Клиент” вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение подсистемы, скомпрометировать ключи Пользователя Системы посредством применения лицензионных средств защиты от вредоносного кода и регулярного их обновления; Исключить возможность несанкционированных Банком изменений в технических и программных средствах Клиента, определенных в Списке; Исключить возможность Компрометации ключей в процессе их транспортировки, эксплуатации и хранения.	3.4 The Client is obliged: To eliminate penetration of viruses and other destructive software into PCs or mobile devices of the Client subsystem which may destroy or modify the subsystem software, compromise the System Users’ keys, which protection should rely on application of licensed malware protection facilities and regular updating thereof; To rule out a possibility to introduce unauthorized modifications in the Clients’ hardware and software specified in the List not authorized by the Bank; To preclude a possibility of compromise of keys in the course of their transportation, operation and safe-keeping.
3.5. Стороны обязаны: обеспечивать конфиденциальность Ключей электронных подписей, в частности не допускать использование принадлежащих им Ключей электронных подписей без их согласия; уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в	3.5. The Parties are obliged: To ensure confidentiality of ES keys. In particular, it is not allowed to use the Parties’ ES keys without their consent; To notify the other Party about violation of confidentiality of an ES key (Key Compromise) within not more than one business day following

течение не более чем одного рабочего дня со дня получения информации о таком нарушении; не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.	the receipt of information concerning such violation; Not to use ES key, if there are reasons to believe that confidentiality of a key was breached.
3.6. Банк вправе в одностороннем порядке заблокировать Ключ электронной подписи Пользователя Системы в случае появления обоснованных подозрений в наличии на Персональном компьютере и/или Мобильном устройстве Пользователя Системы вирусов или других программ деструктивного действия. Блокировка Ключа электронной подписи. Пользователя Системы снимается Банком по факту получения от Клиента подтверждения об удалении с Персонального компьютера и/или Мобильного устройства Пользователя Системы вирусов или других программ деструктивного действия.	3.6. The Bank has the right to unilaterally lock a System User's ES key in case there is reasonable suspicion of virus infection or penetration of other malware in a PC and/or mobile device. ES key locking is realized by the Bank following receipt by the Client of confirmation on removal of viruses and other malware from a PC and/or a System User's mobile device.
3.7. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон. Если произошла Компрометация ключей любого Пользователя Клиента, последний обязан: В случае доступности Комплекта ключей (подозрение на несанкционированное копирование) немедленно послать в Банк ЭД "Блокировка ключа". При этом Система автоматически заблокирует возможность использования данного Комплекта ключей Пользователя Системы; В случае недоступности (утрата, хищение и т.п.) Комплекта ключей сообщить Администратору Системы по телефону (телефон и электронный адрес Администратора системы указаны на сайте www.bankline.ru, а также в Заявлении, используя для авторизации кодовую фразу, приведенную в Сертификате ключа, о факте Компрометации ключей; В случае утраты Пользователем Системы кодовой фразы Администратор Системы вправе произвести дополнительные действия по авторизации Пользователя Системы (обратный звонок по указанному в Заявлении телефону, запрос на предоставление дополнительной информации:	3.7. In case there is a threat of a Key Compromise, the following response sequence of the Parties is established. In case of a compromise of keys of any User of the Client, the latter is obliged: If a set of keys is available (suspicion of unauthorized copying), to immediately send to the Bank a Key Locking electronic message, following which the System will automatically block a possibility for System Users to use the compromised set of keys; If a set of keys is not available (as a result of loss, theft, etc.), to notify the System Administrator via phone (the System Administrator's phone number and electronic address are available on the web-site at www.bankline.ru, as well as in the Application, by using a code phrase for authorization specified in the Key Certificate with a view to report a Key Compromise; In case of loss by a System User of a code phrase, the System Administrator is entitled to undertake additional actions on a System User's authorization (dial back the phone number specified in the Application, send a request for additional information, i.e. full name of the Client's curator on the side of the Bank/authorized Bank officer, number of users, etc.). In case unreliable information is furnished, the System Administrator is to notify the Client's curator on the side of the

о фамилии куратора Клиента в Банке/уполномоченного сотрудника Банка, количестве пользователей и т.п.). В случае предоставления необъективной информации Администратор ставит в известность куратора Клиента в Банке/уполномоченного сотрудника Банка и по согласованию с ним решает вопрос о продолжении/блокировании работы Клиента в Системе; В случае компрометации (утраты, разглашения) SMS-кода незамедлительно проинформировать Банк по любому каналу связи; В срок не более трех рабочих дней после сообщения по телефону о факте Компрометации ключей направить в Банк на бланке Клиента письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Клиента (при наличии). В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены Комплекта ключей; В случае принятия решения о замене Комплекта ключей, сгенерированного для Персонального компьютера, сгенерировать новый Комплект ключей самостоятельно и направить своего представителя в Банк для его регистрации. В случае принятия решения о замене Комплекта ключей, сгенерированного посредством Мобильного приложения, сгенерировать новый Комплект ключей самостоятельно в соответствии с Инструкцией. Если произошла Компрометация ключей Банка, последний обязан: Известить Клиента о факте компрометации Комплекта ключей Банка, продолжении\приостановлении работы Системы и смене Комплекта ключей Банка посредством Системы с указанием даты и точного времени смены вышеуказанного Комплекта ключей; Произвести внеплановую смену Комплекта ключей Банка, опубликовать новый Ключ проверки электронной подписи и копию Сертификата ключа Банка, содержащего новый Ключ проверки электронной подписи Банка, на сервере Системы.	Bank/authorized Bank officer, and to take a decision based on the latter's consent, to continue/block the Client's work in the System; In case of a compromise (loss, disclosure) of SMS-code, it is necessary to immediately notify the Bank via any communication channel; Within not more than three business days following the phone call on a key compromise, to submit to the Bank a written account of the incident executed on the Client's letterhead duly certified by the signatures of authorized persons and the Client's seal attached (if available). The said written statement is to carry an instruction to the Bank to suspend further processing of electronic documents pending elimination of the reasons underlying the incident and/or to replace the keys; In the event a decision is taken to replace the set of keys generated for a PC, to independently regenerate a new set of keys and send its representative to the Bank with a view to register such new set of keys. In the event a decision is taken to replace the set of keys generated with use of a mobile application, to independently regenerate a new set of keys in accordance with the Instruction. In case of a compromise of a set of keys of the Bank, the latter is obliged: To notify the Client about the compromise of the Bank's set of keys, continuation/suspension of operation of the System and replacement of the set of keys of the Bank by using the System facilities with indication of the date and exact time of such replacement; To carry out an unscheduled replacement of the Bank's set of keys, to publish a new ES verification key and a copy of the Bank's Key Certificate with a new ES verification key of the Bank on the System server.
3.8. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного по	3.8. When notified by the Client authorized with use of a code phrase via the phone about a threat of a compromise of keys, the Bank will

кодовой фразе Клиента Банк немедленно приостанавливает использование Системы данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде. Дальнейшее использование Системы Клиентом возможно только после устранения угрозы Компрометации ключей Клиента.	immediately suspend such Client's work in the System. Thereafter operations may only be performed on the basis of paper documents. Further use of the System by the Client is only possible following elimination of a threat of compromise of the Client's keys.

4. Порядок проверки ЭД и ЭП при разногласиях/ Procedure for verification of ED and ES in the event of dispute

4.1. Для разрешения споров относительно подлинности ЭД по заявлению заинтересованной Стороны, полагающей, что ее права нарушены, Сторонами в двухнедельный срок с даты подачи заявления создается Согласительная комиссия, в присутствии которой производятся все операции по подготовке и проведению процедуры разрешения спора. В состав Согласительной комиссии включаются представители Банка в количестве двух человек и представители Клиента в количестве двух человек, а в случае необходимости (по соглашению Сторон) – независимые эксперты. Представителями Банка и Клиента могут быть назначены как сотрудники этих организаций, так и иные компетентные лица, полномочия которых подтверждаются соответствующими доверенностями.	4.1. With a view to settle disputes regarding ED authenticity following an application of the Party concerned, which claims a breach of its rights, the Parties shall, within two weeks following such application, set up a Conciliation Commission, in the presence of which arrangements will be made to prepare and conduct the procedure of dispute settlement. The Conciliation Commission is to comprise two representatives of the Bank and two representatives of the Client, and if necessary (subject to the Parties' consent) independent experts may be invited to sit on the Commission. Representatives of the Bank and the Client may be appointed from the number of the personnel of such entities, as well as other competent persons whose authority is to be certified by relevant powers of attorney.
4.2. Спорным ЭД является ЭД, в отношении которого одна Сторона предъявляет претензии по его подлинности другой Стороне.	4.2. An ED is deemed to be disputable with regard to which one Party challenges its authenticity to the other Party.
4.3. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка.	4.3. The procedure of verification of authenticity of an electronic document is to be conducted with use of the Bank's equipment and premises.
4.4. В присутствии членов Согласительной комиссии Банк обязан на свободном от программного обеспечения компьютере установить операционную систему Windows7 и выше и предоставленную фирмой-разработчиком ЗАО "ИНИСТ" программу проверки ЭП, указанную в п.1.10 настоящей Инструкции	4.4. In the presence of the members of the Conciliation Commission, the Bank is obliged to install an operating system Windows 7 and higher on a software-free computer, as well as ES verification program provided by its manufacturer CJS INIST specified in paragraph 1.10 of this Instruction.

4.4.1. Сторона, отстаивающая подлинность спорного ЭД, обязана предоставить спорный ЭД, действовавшие в момент создания спорного ЭД Сертификаты ключей Стороны, подписавшей спорный ЭД, Банк обязан предоставить сами Ключи проверки электронной подписи, записанные на съемном носителе в виде файлов в формате, применяемом Системой (в случае если Клиент не предоставляет спорный ЭД, он предоставляется Банком).	4.4.1. The Party which upholds the authenticity of a disputed ED is obliged to provide the arguable document, the key certificates of the Party, which signed the disputed document, effective as at the date of generation thereof, and the Bank is obliged to submit the ES verification keys properly recorded on a removable media on files in the format accepted by the System (in case the Client fails to submit an arguable electronic document, the Bank is obliged to furnish such document).
4.4.2. Стороны обязаны предоставить все имеющиеся в их распоряжении Сертификаты ключей, информацию о проведенных плановых и внеплановых сменах Комплекта ключей Сторон и документы, удостоверяющие факты смены Комплекта ключей. Стороны также обязаны предоставить служебные ЭД Системы, в которых указаны факты получения ЭД из каналов связи и результаты их обработки (проверки).	4.4.2. Both Parties are obliged to submit all available key certificates, information regarding scheduled and unscheduled replacements of sets of keys and the documents which certify the fact of replacement of sets of keys. The Parties are also obliged to provide internal electronic documents of the System, which contain reference to receipt of ED via communication channels and results of their processing (verification).
4.5. Члены Согласительной комиссии должны выполнить следующие действия:	4.5. The Conciliation Commission members are obliged to carry out the following steps:
4.5.1. Произвести с помощью программы проверки ЭП, указанной в п.1.10 настоящей Инструкции, и каждого Ключа проверки электронной подписи, использованного при подписании спорного ЭД, операцию проверки ЭП;	4.5.1. To perform verification of ES with use of the ES verification software specified in paragraph 1.10 of this Instruction and each ES verification key utilized in the course of signing of the disputed ED;
4.5.2. Создать Протокол установления подлинности ЭД – документ на бумажном носителе, создаваемый Системой в качестве результата проверки ЭП спорного ЭД (далее - Протокол). Протокол должен содержать распечатанные на бумажном носителе Ключи проверки электронной подписи, использованные для установления подлинности ЭП, и заключение об итогах проверки ЭП спорного ЭД. Протокол должен быть подписан собственноручно всеми членами Согласительной комиссии;	4.5.2. To generate a Protocol of ED verification on paper media created by the System as a result of verification of ES of the arguable document (hereinafter referred to as the Protocol). The Protocol is to carry electronic signature verification keys printed out on paper media employed for ES authentication, as well as to submit findings on verification of the disputed ED. The Protocol is to be signed in hand by all members of the Conciliation Commission;
4.5.3. Сравнить Ключи проверки электронной подписи, содержащиеся в Сертификатах ключей, с соответствующими Ключами проверки электронной подписи, зафиксированными в Протоколе установления	4.5.3. To compare the ES verification keys contained in the Key Certificates with relevant ES verification keys specified in the Protocol on authentication of ES of the arguable ED, as well as determine their identity, make a relevant record in

подлинности ЭП спорного ЭД, и установить, тождественны ли они, внести об этом запись в Протокол (данная запись заверяется подписями членов Согласительной комиссии);	the Protocol (such record is to be certified by the signatures of the members of the Conciliation Commission);
4.5.4. Установить, являлись ли Ключи проверки электронной подписи действующими на момент выработки ЭП спорного ЭД, и внести запись об этом в Протокол (данная запись заверяется подписями членов Согласительной комиссии). Ключ проверки электронной подписи признается действующим на момент создания ЭП спорного ЭД в случае, если дата создания спорного ЭД приходится на период действия Ключа проверки электронной подписи. В противном случае Ключ проверки электронной подписи признается недействующим на момент создания ЭП.	4.5.4. To determine whether the electronic signature verification keys were effective as at the time of generation of the disputed electronic document, and make a relevant record in the Protocol (such record is to be certified by the signatures of the members of the Conciliation Commission). An ES verification key is deemed effective as at the date of generation of ES of the disputed electronic document, provided that the date of creation of the disputed document falls within the period of the effect of the ES verification key, failing which the ES verification key is to be deemed invalid as at the time of ES generation.
4.6. Согласительная комиссия признает ЭД подлинным, если одновременно выполнены условия: Ключи проверки электронной подписи в Сертификатах ключей и в Протоколе совпадают, Все результаты проверки ЭП в Протоколе положительны, Согласительная комиссия признала все Ключи проверки электронной подписи, содержащиеся в Протоколе, действующими на момент выработки ЭП. В противном случае Согласительная комиссия признает ЭД недействительным.	4.6. The Conciliation Commission will recognize ED as authentic, provided all of the following conditions are met simultaneously: ES verification keys specified in the Key Certificates and the Protocol are identical, All findings on ES verification recorded in the Protocol are positive, The Conciliation Commission recognized all ES verification keys listed in the Protocol as valid as at the time of ES generation. Elsewise the Conciliation Commission is to hold the electronic document invalid.