

**Правила обмена электронными
документами при обслуживании
корпоративных клиентов АО КБ «Ситибанк»**

**Rules for the Exchange of Electronic
Documents in the Process of Servicing
Corporate Customers of AO Citibank**

*Утверждено Заседанием Правления АО КБ
«Ситибанк» на основании Протокола № 6
от 28 мая 2024 года*

*Approved by AO Citibank Management Board
based on Protocol 6 dated May 28, 2024*

1. Термины и определения

Авторизатор – уполномоченный представитель Клиента, имеющий право распоряжаться денежными средствами на соответствующем счете Клиента и совершать иные действия, предусмотренные уполномочивающими документами, путем направления в Банк Электронного документа.

Администратор Системы CitiDirect BE – лицо, назначенное Клиентом выполнять функции Управляющего по безопасности (как это предусмотрено Процедурами безопасности, содержащимися в Приложении 7 к настоящим Правилам), действия которого описаны в Приложении 5 к настоящим Правилам.

Оператор без права авторизации платежей – уполномоченный представитель Клиента, обладающий полномочиями на просмотр информации по соответствующим счетам Клиента, на создание платежных распоряжений, сервисных запросов, документов валютного контроля и иных документов, доступных для работы в Системе; на выгрузку, загрузку и просмотр данных Клиента о проведенных операциях; совершать иные действия доступные в Системе.

Администратор Системы CitiManager лицо, имеющее полномочия и обязанности, содержащиеся в договоре на обслуживание корпоративных карт и в настоящих Правилах, включая Приложения 9 к Правилам, назначенное Клиентом отвечать за:

- a) управление и администрирование обеспечения безопасности в ходе передачи Электронных документов через Систему CitiManager в рамках договора на обслуживание корпоративных карт;
- b) подключение Держателя Карты к Системе CitiManager и управление доступом Держателя Карты к доступным средствам на счете корпоративных карт Клиента посредством корпоративной карты;

1. Terms and Definitions

Authorizer - an authorized representative of the Customer who has the right to dispose of funds in the relevant account of the Customer and perform other actions stipulated by the authorizing documents by sending an Electronic Document to the Bank.

CitiDirect BE System Administrator - a person appointed by the Customer to perform the functions of the Security Manager (as provided for by Security Procedures contained in Annex 7 to this Rules), which actions are described in Annex 5 hereto).

Operator without the right to authorize payments - an authorized representative of the Customer, who has the authority to view information on the relevant accounts of the Customer, to create payment orders, service messages, currency control documents and other documents available for work in the System; to upload, download and view the Customer's transaction data; and make actions available in the System

CitiManager System Administrator is a person who has the authority and obligations contained in the Corporate Cards Agreement; and in these Rules, including the Annexes 9 to the Rules, assigned by the Customer to be responsible for:

- a) managing and administering security during the transfer of Electronic Documents through the CitiManager System in accordance with the Corporate Cards Agreement;
- b) providing access for the Cardholder to CitiManager System and managing the Cardholder's access to the available funds in the Customer's corporate cards account via a corporate card;
- c) approval on behalf of the Customer of the Application for the Cardholder's

- с) одобрение от лица Клиента Заявления о присоединении Держателя Карты к Договору на обслуживание корпоративных (далее - **Заявление на Карту**), форма которого устанавливается договором на обслуживание корпоративных карт.

Держатель Карты означает каждое лицо, уполномоченное Клиентом на получение корпоративной карты в рамках договора на обслуживание корпоративных карт, который имеет доступ к Системе CitiManager и присоединился к настоящим Правилам на основании Приложения 10 к Правилам или иной форме.

Банк - Акционерное общество коммерческий банк "Ситибанк" (АО КБ «Ситибанк»), расположенное по адресу Россия, 125047, Москва, ул. Гашека, 8-10, стр. 1. Генеральная лицензия на осуществление банковских операций Банка России № 2557 от 5 ноября 2001г.

Владелец Сертификата – лицо, надлежащим образом уполномоченное Клиентом или Банком на подписание от имени соответственно Клиента или Банка Электронных документов, которому выдается Сертификат ключа проверки электронной подписи.

Клиент – юридическое лицо, являющееся клиентом АО КБ «Ситибанк», в том числе в рамках договора банковского счета.

Ключ электронной подписи (Ключ усиленной ЭП) – уникальная последовательность символов, известная владельцу сертификата ключа проверки ЭП и предназначенная для создания Электронной подписи.

Ключ проверки электронной подписи (Ключ проверки усиленной ЭП) – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности электронной подписи.

Правила – настоящие Правила обмена электронными документами при обслуживании корпоративных клиентов АО КБ «Ситибанк» со всеми приложениями.

Пользователь – Администратор, Авторизатор или Оператор без права авторизации платежей.

Сертификат ключа проверки электронной подписи (Сертификат) – электронный

accession to the Corporate Cards Agreement (hereinafter - **Card Application**), the template of which is established by the Corporate Cards Agreement.

Cardholder means each person authorized by the Customer to receive a corporate card under a corporate cards agreement who has access to the CitiManager System and has joined these Rules on the basis of the Annex 10 to the Rules or any other form.

Bank – Joint Stock Company Commercial Bank Citibank (AO Citibank), located at: 8-10 Gasheka street, bldg. 1, Moscow, 125047, Russia. Bank of Russia General License to conduct banking operations No. 2557 dated November 5, 2001.

Certificate Holder – a person duly authorized by the Customer or the Bank to sign Electronic documents on behalf of the Customer or the Bank, accordingly, and to which an Electronic Signature Verification Key Certificate is issued.

Customer – a legal entity that is a customer of AO Citibank, including within the framework of a bank account agreement.

Electronic Signature Key (Enhanced ES Key) – a unique sequence of characters that is known to an ES verification key certificate holder and designed to create an Electronic signature.

Electronic Signature Verification Key (Enhanced ES Verification Key) – a unique sequence of characters that is uniquely associated with an ES key and designed to authenticate an electronic signature.

Rules – these Rules for the Exchange of Electronic Documents in the Process of Servicing Corporate Customers of AO Citibank together with all annexes.

User means Administrator, Authorizer or Operator without the right to authorize payments.

Electronic Signature Verification Key Certificate (Certificate) – the electronic document, issued

документ, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки электронной подписи.

Система – информационная система обмена электронными документами, состоящая из Системы CitiDirect BE (включая CitiDirect BE Mobile App), Системы CitiConnect, Системы CitiManager, а также иного программного и информационного обеспечения (в том числе, для обмена электронными документами по электронной почте (включая использование программного обеспечения группы компаний «Сигнал-КОМ»)), позволяющая производить обмен электронными документами с использованием Электронной подписи между Участниками Системы и осуществлять дистанционное банковское обслуживание в соответствии с действующим законодательством Российской Федерации и настоящими Правилами.

Система CitiDirect BE – информационная система (включая CitiDirect BE Mobile App), которая представляет собой совокупность программного и информационного обеспечения, позволяющая производить обмен Электронными документами между ее участниками и осуществлять дистанционное банковское обслуживание в соответствии с действующим законодательством Российской Федерации и настоящими Правилами.

Система CitiConnect – информационная система, позволяющая производить автоматизированный обмен Электронными документами между ее участниками и осуществлять дистанционное банковское обслуживание в соответствии с действующим законодательством Российской Федерации и настоящими Правилами.

Система CitiManager – информационная система, которая представляет собой совокупность программного и информационного обеспечения, позволяющая производить обмен электронными документами между ее участниками и осуществлять дистанционное банковское обслуживание программы корпоративных карт в соответствии с действующим законодательством Российской

by the certification authority or by a person authorized by the certification authority and confirming that an ES verification key belongs to the electronic signature verification key certificate holder.

System – the information system for the exchange of electronic documents comprising the CitiDirect BE System (including CitiDirect BE Mobile App), CitiConnect, CitiManager and other software and data support (including for the exchange of electronic documents via e-mail (including usage of software from the Signal-COM group)) enabling the exchange of electronic documents with the use of electronic signatures among System Participants and the implementation of remote banking services in accordance with applicable Russian Federation laws and the System rules.

CitiDirect BE System – the information system (including CitiDirect BE Mobile App) that corresponds to the totality of software and data support enabling the exchange of electronic documents among its participants and the implementation of remote banking services in accordance with applicable Russian Federation laws and these Rules.

CitiConnect System is an information system that allows automated exchange of Electronic Documents between its participants and remote banking services in accordance with the current legislation of the Russian Federation and these Rules.

CitiManager system is an information system that is a combination of software and information support that allows exchanging electronic documents between its participants and providing remote banking services for the corporate cards program in accordance with the current legislation of the Russian Federation, the Rules and the Bank's corporate cards agreement.

Федерации, Правилами и договором на обслуживание корпоративных карт Банка.

Удостоверяющий центр – юридическое лицо (подразделение юридического лица), индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронной подписи, а также иные функции, предусмотренные действующим законодательством РФ.

Удостоверяющим центром может являться:

- **Удостоверяющий центр Банка** – подразделение Банка, выполняющее функции удостоверяющего центра в соответствии с настоящими Правилами и внутренними документами Банка;
- **Внешний Удостоверяющий центр** – независимое по отношению к Банку юридическое лицо, осуществляющее в соответствии с договором между ним и Банком функции удостоверяющего центра для Клиентов Банка и действующее в рамках собственного Регламента Удостоверяющего центра.

Участники Системы – Банк, Клиент и Держатели Карт, а также Владельцы сертификатов ключа проверки ЭП, в лице которых Банк и Клиент осуществляют обмен Электронными документами посредством Системы в рамках заключенных между Банком и Клиентом договоров.

Электронная подпись (ЭП) – 1) Простая электронная подпись (Простая ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию; **2) Усиленная электронная подпись (Усиленная ЭП)** – информация в электронной форме, которая создается с использованием средств электронной подписи и присоединена к электронному документу или иным образом связана с ним, позволяет определить лицо, подписавшее электронный документ, и обнаружить факт внесения изменений в электронный документ после момента его подписания. Электронный документ, подписанный Усиленной электронной подписью, признается

Certification Authority – the legal entity (division of a legal entity), individual entrepreneur or state body or local government, handling the functions of creating and issuing electronic signature verification key certificates, along with other functions as contemplated by applicable laws of the Russian Federation.

The Certification Authority may be:

- **Bank's Certification Authority** – a division of the Bank that is functioning as the certification authority in accordance with these Rules and internal documents of the Bank;
- **Third-Party Certification Authority** – a legal entity that is independent from the Bank and functioning as a certification authority for the Bank's Customers pursuant to an agreement between the former and the Bank and operating within the framework of its own Certification Authority Regulations.

System Participants – the Bank, Customer and Cardholders, along with ES Verification Key Certificate Holders, through which the Bank and Customer exchange Electronic documents via the System within the framework of the agreements concluded between the Bank and the Customer.

Electronic Signature (ES) – 1) Simple Electronic Signature (Simple ES) – electronic data that is associated with other electronic data (the data being signed) or otherwise related to such data and which is used to identify the person signing the data; **2) Enhanced Electronic Signature (Enhanced ES)** – electronic data that is created with the use of electronic signature tools and is associated with an electronic document or otherwise related thereto, making it possible to identify the person who signed the electronic document and to detect changes made to the electronic document after it has been signed. An electronic document signed with an Enhanced Electronic Signature shall be recognized by the System Participants as equivalent to a document in hard copy executed with the handwritten signature of the Certificate Holder and authenticated with the seal of the respective legal entity (the Bank or the Customer).

Участниками Системы равнозначным документу на бумажном носителе, подписанному собственноручной подписью Владельца Сертификата и заверенному печатью соответствующего юридического лица (Банка или Клиента). Электронная подпись формируется исключительно по правилам, описанным в настоящих Правилах. Никакие иные правила, включая описанные в Процедурах безопасности, для правил формирования Электронной подписи не применяются в отношениях между Банком и Клиентом.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме, подписанный Электронной подписью.

Процедуры безопасности (Приложение 7 к настоящим Правилам) – документ, на который ссылаются Условия договора банковского счета АО КБ «Ситибанк», являющийся частью Договора банковского счета, заключенного между Банком и Клиентом, опубликованный на официальном сайте Банка, и регулирующий Способы аутентификации, Ответственность Клиента, Целостность данных и защищенную связь, а также Администратора безопасности и соответствующие функции. Способы аутентификации, включенные в Процедуры безопасности, применяются только в порядке, не противоречащем российскому законодательству, внутренним правилам и процедурам Банка и договорам между Банком и Клиентом.

2. Статус Правил и договоров

2.1 Настоящие Правила устанавливают порядок обмена документами и информацией в электронном виде между Банком и Клиентом, а также Держателями Карт (когда применимо), права и обязанности участников такого обмена, условия использования ЭП, а также вопросы ответственности Участников Системы. Настоящие Правила являются неотъемлемой частью Договора о порядке обмена документами и информацией в электронном виде при обслуживании корпоративных клиентов, заключенного между Банком и Клиентом или между Банком и Держателем карт (далее – «**Договор**»).

Electronic Signature shall be formed only according to the rules described in the Rules. No other rules for forming Electronic Signature, including those referred to in Security Procedures, shall not be applied to the relations between the Bank and Customer

Electronic Document – a document in which information is presented in electronic/digital form, signed with Electronic Signature.

Security Procedures (Annex 7 to the Rules) – a document referred to by the Bank Account Conditions of AO Citibank, which is a part of Bank Account Agreement, concluded between the Bank and the Customer, published on official Bank website, which regulates Authentication Methods, Customer Responsibilities, Data Integrity and Secured Communications Security Manager and Related Functions. Authentication Methods included in Security Procedures shall be applied only in a way that such methods do not contradict Russian legislation, Bank internal rules and policies and agreements concluded between the Bank and the Customer.

2. Status of the Rules

2.1 These Rules establish the procedures for the exchange of electronic documents and data between the Bank, Customer and Cardholders, the rights and obligations of the participants in such exchange, the terms and conditions for ES use, and matters of the liability of System Participants. These Rules are an integral part of the Agreement on the Exchange of Electronic Documents and Data concluded between the Bank and the Customer or between the Bank and the Cardholder (hereinafter – “**Agreement**”).

2.2 В случае противоречия условий Договора и положений настоящих Правил, подлежат применению условия Договора.

2.3 Порядок определения полномочий лиц и подписания ими соответствующих документов на бумажных носителях устанавливается в соответствии с внутренними правилами Банка.

2.4 Действующая редакция Правил публикуется Банком в сети Интернет и доступна по адресу <http://www.citibank.ru/russia/corporate/rus/edm.htm>. Банк обязуется хранить все недействующие редакции Правил в электронном виде и предоставлять Клиенту любую недействующую редакцию Правил по его запросу.

2.5 Настоящие Правила могут быть изменены Банком в одностороннем порядке при условии уведомления Клиента и Держателя карты не позднее, чем за 30 (тридцать) дней до вступления в силу таких изменений (в случае внесения изменений в сами Правила), или не позднее, чем за 5 (пять) рабочих дней (в случае внесения изменений в любое из приложений к настоящим Правилам).

Банк уведомляет Клиента и Держателя карты о внесении изменений в настоящие Правила путем размещения информационного письма и текста изменений на сайте Банка <http://www.citibank.ru/russia/corporate/rus/edm.htm> и/или любым иным доступным способом.

2.6 Сфера применения Системы и использования Электронных документов и Электронной подписи определяется в настоящих Правилах и Приложениях к ним и(или) договорах об обмене Электронными документами определенного вида, заключенных между Банком и Клиентом, при этом, в случае противоречия условий указанных договоров настоящим Правил, подлежат применению условия договоров об обмене Электронными документами определенного вида.

3. Система и её компоненты

В процессе действия Правил Система и её компоненты будут совершенствоваться Банком и претерпевать определенные последовательные изменения,

2.2 In case of discrepancies between the terms of the Agreement and the provisions of these Rules, the terms of the Agreement shall apply.

2.3 The procedures for determining the powers of individuals and their signature of the respective documents in hard copy shall be established in accordance with the Bank's internal rules.

2.4 The current version of the Rules is published by the Bank on the Internet and is available at <http://www.citibank.ru/russia/corporate/rus/edm.htm>. The Bank shall undertake to store all inactive versions of the Rules electronically and to provide the Customer with any inactive version of the Rules upon its request.

2.5 These Rules may be changed by the Bank on a unilateral basis subject to a notification of the Customer and Cardholder not later than 30 (thirty) days prior to the effectiveness of such changes (in case the changes are made to the Rules) and not later than 5 (five) business days (in case the changes are made to one of the annexes to these Rules).

The Bank notifies the Customer and Cardholder on the amendments/annexes to the Rules by posting an information notice and the text of amendments/annexes at the Bank's web-site <http://www.citibank.ru/russia/corporate/rus/edm.htm> and/or by any other available means.

2.6 The scope of usage of the System, the Electronic Documents and Electronic Signatures shall be determined in these Rules and Annexes and/or in the agreements on exchange of the Electronic Documents of certain kind concluded between the Bank and the Customer, that being said, in case of contradiction between the terms of specified agreements and the terms of these Rules the terms of agreements on exchange of the Electronic Documents of certain kind shall be applied.

3. The System and its components

In the course of the Rules, the System and its components will be improved by the Bank and undergo certain successive changes due to the introduction of new organizational and technical

обусловленные внедрением новых организационных и технических мер по инициативе Банка, при этом переход к использованию новых технологических возможностей не лишает Клиента, Банк и Держателя карты (где применимо) права продолжать использовать технические возможности Системы предыдущего этапа, если Банк не примет решения об отказе от использования таких технических возможностей с обязательным внесением соответствующих изменений в настоящие Правила. Ответственность за организацию новых организационных и технических мер в рамках Системы, а также за своевременное доведение новых требований к использованию Системы до сведения Клиента, а также Держателя карты (где применимо), и содействие в обеспечении Клиента, а также Держателя карты (где применимо), всеми необходимыми программными и аппаратными средствами возлагается на Банк. Банк взимает плату за предоставление таких программных и аппаратных средств.

3.1 Система CitiDirect BE

Система CitiDirect BE является системой дистанционного банковского обслуживания Клиент-Банк и используется Банком и Клиентом в качестве одного из способов обмена Электронными документами.

Клиент, присоединившийся к Системе CitiDirect BE, в том числе в рамках договора банковского счета, заключенного между Банком и Клиентом, должен использовать Систему CitiDirect BE в строгом соответствии с настоящими Правилами, а также руководством по установке, настройке и работе в системе CitiDirect BE, правилами администрирования системы CitiDirect BE, а также иными письменными и устными пояснениями, инструкциями и рекомендациями, которые Банк может время от времени предоставлять Клиенту.

Технические условия использования и содержание настоящих Правил определяются Банком и своевременно доводятся до сведения Клиента.

Банк имеет право ограничить доступ Клиента в систему CitiDirect BE в случаях, предусмотренных в Приложении 7 к настоящим Правилам.

measures initiated by the Bank, while the transition to the use of new technological capabilities does not deprive the Customer, the Bank and the Cardholder (if applicable) of the right to continue to use the technical capabilities of the previous stage, if the Bank does not decide to refuse to use such technical capabilities with the obligatory change of these Rules. Responsibility for managing new organizational and technical measures within the System, as well as for timely bringing new requirements for using the System to the Customer's and Cardholder's (if applicable) attention and assisting in providing the Customer and Cardholder (if applicable) with all the necessary software and hardware, rests with the Bank. The bank charges for the provision of such software and hardware.

3.1 CitiDirect BE System

The CitiDirect BE system is Customer-Bank remote banking service system which is used by the Bank and the Customer as one of the means of exchanging Electronic Documents.

The Customer, having acceded to the CitiDirect BE System, including in the context of a bank account agreement concluded between the Bank and the Customer, must use the CitiDirect BE System in strict accordance with the Rules and the CitiDirect BE Installation, Configuration and Operation Manual, CitiDirect BE System Administration Rules, and other written and oral explanations, instructions and recommendations that the Bank may provide to the customer from time to time.

Specifications for the use and maintenance of the Rules shall be defined by the Bank and brought to the notice of the Customer in a timely manner.

The bank is entitled to restrict Customer access to CitiDirect BE in the cases provided for in Appendix 7 to the Rules.

3.2 Система CitiConnect

Доступ к Системе CitiConnect, каналу связи, логины, пароли, сертификаты, иные средства и способы идентификации авторизованного доступа к каналу связи организуются на этапе интеграции.

Клиент, присоединившийся к Системе CitiConnect, в том числе в рамках договора банковского счета, заключенного между Банком и Клиентом, должен использовать Систему CitiConnect в строгом соответствии с настоящими Правилами.

Технические условия использования и содержание Правил определяются Банком и своевременно доводятся до сведения Клиента.

Банк имеет право ограничить доступ Клиента в систему CitiConnect в случаях, предусмотренных в Приложении 7 к настоящим Правилам.

3.3 Система CitiManager

Система CitiManager является системой дистанционного банковского обслуживания Интернет-Клиент и используется Банком, Клиентом и Держателем Карты в качестве одного из способов обмена Электронными документами в рамках программы корпоративных карт.

Доступ к Системе CitiManager осуществляется посредством логина, пароля и иных способов идентификации авторизованного доступа, которые предоставляются в рамках регистрации пользователя в Системе CitiManager.

Описание порядка регистрации Администратора Системы CitiManager и/или Держателя Карты в Системе CitiManager, а также права и ответственность пользователей описаны в Приложении 9 к настоящим Правилам.

4. Электронная подпись

При обмене Электронными документами в Системе, а также при обмене Электронными документами по электронной почте, Банк и Клиент, а также Держатель карты (где применимо), обязуются использовать Простую ЭП или Усиленную ЭП в установленном настоящими Правилами порядке и в соответствии со сферой использования ЭП, определенной в настоящих Правилах и Приложениях к ним и(или) в договорах об обмене Электронными

3.2 Система CitiConnect

Access to CitiConnect System, communication channel, logins, passwords, certificates, other means and methods for identification of authorized access to the communication channel are organized at the integration stage.

The Customer who joined the CitiConnect System (including within the framework of the bank account agreement concluded between the Bank and the Customer) must use the CitiConnect System in strict accordance with these Rules.

The technical conditions of use and the content of the Rules are determined by the Bank and promptly communicated to the Customer.

The bank is entitled to restrict Customer access to CitiDirect BE in the cases provided for in Appendix 7 to the Rules.

3.3 CitiManager System

CitiManager System is a Customer-facing web-based remote banking service system, which is used by the Bank, the Customer and the Cardholder as one of the ways to exchange Electronic Documents under corporate cards program.

Access to the CitiManager System is provided by means of a login, password and other methods of identifying authorized access, which are provided as part of the user registration in the CitiManager System.

A description of the registration procedure for CitiManager System Administrator and / or the Cardholder in the CitiManager System, as well as the rights and responsibilities of users are described in the Appendix to 9 this Regulation.

4. Electronic Signature

When exchanging Electronic Documents in the System (including via e-mail), the Bank, the Customer and the Cardholder (where applicable) undertake to use Simple ES or Enhanced ES in accordance with the procedure established by these Rules and in compliance with the ES scope of use, defined in these Rules and Annexes and (or) other agreements on Electronic Documents Exchange concluded between the Bank and the Customer.

документами определенного вида, заключенных между Банком и Клиентом. Банк вправе установить требование, что обмен определенными Электронными документами из перечня в Приложении 6 к настоящим Правилам осуществляется только с использованием Простой ЭП. Банк уведомит Клиента о таком решении не позднее чем за 30 (тридцать) дней до даты его вступления в силу. Несоответствие Электронных документов указанному требованию Банка будет основанием для отказа в приеме согласно пункту 6.6 Правил.

The Bank is entitled to set a requirement that exchange of certain Electronic Documents from Annex 6 to these Rules is made only with the use of Simple DS. The Bank will notify the Client about such decision not later than 30 (thirty) days prior to its effective date. Non-compliance of Electronic Documents with this Bank's requirement will constitute a ground for refusal to accept under clause 6.6 of the Rules.

4.1 Порядок использования Простой электронной подписи

4.1.1 Обмен Электронными документами происходит посредством:

- (а) направления файлов через соответствующий модуль для предоставления документов определенного вида, предусмотренный Системой;
- (б) заполнения и отправки данных в онлайн-формах соответствующего модуля для предоставления документов данного вида, предусмотренного Системой, в том числе с приложением необходимых файлов, при этом и данные, и файлы подписываются Электронной подписью отправителя и/или Авторизатора.

4.1.2 Электронные документы, полученные или переданные указанным способом, являются равнозначными документам на бумажных носителях, подписанных собственноручной подписью лиц, уполномоченных Участниками Системы, благодаря использованию Простой ЭП в соответствии с положениями настоящих Правил.

4.1.3 Лицо, подписывающее Электронный документ со стороны Клиента, определяется: **В Системе CitiDirect BE:** с помощью ввода регистрационного идентификационного кода в целях создания запроса на вход в Систему CitiDirect BE. В результате данных действий Система CitiDirect BE создает запрос на вход в Систему CitiDirect BE, который требует ввода одноразового пароля пользователем. Одноразовый пароль генерируется благодаря аппаратному аутентификатору SafeWord Card, MobilePass, CitiDirect BE Mobile App или иными средствами, которые предоставляются

4.1 Simple Electronic Signature usage

4.1.1 The exchange of Electronic Documents shall take place by:

- (a) sending the files via the relevant module for delivery of documents of a particular type, as contemplated by the System;
- (b) filling in and sending data in the online forms of the relevant module for the provision of documents of this type provided by the System, including the attachment of the necessary files while the data and the files are to be signed with the ES of the sender and/or **Authorizer**.

4.1.2 Electronic Documents received or sent by the mentioned means are equivalent to documents in hard copy executed with the handwritten signature of persons authorized by System Participants, by virtue of using Simple ES according to these Rules.

4.1.3 The person signing an Electronic Document on behalf of the Customer is determined: **In CitiDirect BE System:** through the requirements for entering a unique login name in order to generate a CitiDirect BE System login request. As a result of these actions, the CitiDirect BE System creates a CitiDirect BE System login request, which requires the user to enter a one-time password. The one-time password is generated courtesy of the SafeWord Card authentication device MobilePass, CitiDirect BE Mobile App or other tools, which are provided to each user of the CitiDirect BE System. Following the automatic verification and

каждому пользователю Системы CitiDirect BE. После автоматической проверки и подтверждения введенных данных осуществляется вход в Систему CitiDirect BE.

В Системе CitiDirect BE Mobile App: с использованием хранимого в приложении динамического ключа ассоциированного с уникальным регистрационным идентификационным кодом пользователя. Динамический ключ первично формируется на этапе первоначальной установки приложения и содержится в защищенном хранилище приложения. В дальнейшем, доступ в приложение CitiDirect BE Mobile App и использование динамического ключа осуществляется с использованием персонального регистрационного идентификационного кода пользователя и персонального пароля пользователя. По желанию пользователя доступ к приложению и использованию динамического ключа может быть защищен встроенными в устройство пользователя технологиями “Touch ID” (Google INC) или “Face ID” (Apple INC) (где доступны). Приложение CitiDirect BE Mobile App не собирает, не хранит и не передает биометрические данные пользователя используемые указанными выше технологиями.

В результате автоматического обмена ключами между приложением клиента и Системой CitiDirect BE и подтверждения данных осуществляется вход в Систему CitiDirect BE.

В Системе CitiConnect: с помощью:

- (а) ввода идентификационного имени и пароля в целях доступа к автоматизированному хранилищу данных;
- (б) использования совокупности закрытого ключа, известного Клиенту, и его открытой части (сертификата) известного Клиенту и Банку в целях доступа к автоматизированному хранилищу данных.

После автоматической проверки и подтверждения введенных данных осуществляется доступ в Систему CitiConnect для передачи и получения Электронных документов.

В Системе CitiManager:

с помощью ввода уникального имени пользователя и пароля Держателем Карты и/или Администратором Системы

confirmation of the data entered, the login to the CitiDirect BE System is carried out.

In the CitiDirect BE Mobile App System:

using a dynamic key stored in the application associated with a unique registration identification code of the user.

The dynamic key is first generated during the initial installation of the application and is stored in the application's secure storage. Further, access to the CitiDirect BE Mobile App and use of the dynamic key is carried out using the user's personal registration identification code and user's personal password. At the request of the user, access to the application and the use of a dynamic key can be protected by the “Touch ID” (Google INC) or “Face ID” (Apple INC) technologies built into the user's device (where available). The CitiDirect BE Mobile App does not collect, store or transmit user biometric data used by the above technologies.

As a result of the automatic key exchange between the client application and the CitiDirect BE System and data confirmation, the user logs into the CitiDirect BE System.

In CitiConnect System thanks to the requirements, such as:

- (a) entering an identification name and password in order to access the automated data repository;
- (b) using the set of the private key known to the Customer and its public part (certificate) known to the Customer and to the Bank in order to access the automated data repository.

After automatic verification and confirmation of the entered data, access is provided to CitiConnect System for sending and receiving Electronic Documents.

In CitiManager:

By entering a unique username and password of Cardholder and/or CitiManager System Administrator, created in accordance with Annex

CitiManager, созданных в соответствии с Приложением 9 к настоящим Правилам, в целях доступа в Систему CitiManager.

После автоматической проверки и подтверждения введенных данных осуществляется доступ в Систему CitiManager для передачи и получения Электронных документов.

Клиент и Держатель карты (если применимо) обязаны использовать уникальные идентификаторы пользователя, идентификаторы отправителя, цифровые сертификаты, коды доступа, пароли и другие средства идентификации, которые Банк выдал Клиенту и Держателю карты или каким-либо другим образом определил для Клиента и Держателя карты в соответствующий момент времени для доступа и (или) использования Системы. Использование описанных в Правилах условий для доступа в Систему является необходимым и достаточным условием, позволяющим достоверно определить, что (а) сообщение, полученное Банком посредством Системы, исходит от Клиента или Держателя карты (если применимо) и (б) Клиент или Держатель карты выразил волю на направление такого Электронного документа в Банк и безусловное принятие Клиентом и Держателем карты на себя правовых последствий направления такого Электронного документа.

4.1.4 Для аутентификации в Системе CitiDirect BE и Системе CitiConnect используются исключительно методы, описанные в настоящих Правилах. Никакие иные методы, включая методы, изложенные в Процедурах безопасности, не применяются.

4.1.5 Уполномоченные представители Клиента обязаны соблюдать конфиденциальность ключей Простой ЭП и не вправе предоставлять другим лицам свои пароли, регистрационные коды, имена и иную конфиденциальную информацию, связанную с использованием Системы, а также предоставлять в пользование третьим лицам аппаратные или программные аутентификаторы, генераторы паролей, приложения или устройства, содержащие данные используемые при идентификации/авторизации пользователя.

9 of these Rules, in order to access CitiManager System.

After automatic verification and confirmation of the entered data, access is provided to the CitiManager System for sending and receiving Electronic documents.

The Customer and the Cardholder (if applicable) are required to use unique user identifiers, sender IDs, digital certificates, access codes, passwords and other means of identification that the Bank issued for the Customer and the Cardholder or in any other way determined for the Customer and the Cardholder at the appropriate time for access and (or) use of the System. The use of the conditions for access to the System described in these Rules is a necessary and sufficient condition to reliably determine that (a) the message received by the Bank through the System comes from the Customer or the Cardholder (if applicable) and (b) the Customer or the Cardholder has expressed the will to send such Electronic document to the Bank and unconditional acceptance by the Customer and the Cardholder of the legal consequences of sending such an Electronic Document.

4.1.4 For authentication in CitiDirect BE System and CitiConnect System shall be use only those methods, which are described in the Rules. No other methods, including those described in Security Procedures, shall not be applied.

4.1.5 The Customer's authorized representatives are obligated to maintain the confidentiality of Simple ES keys and may not give out their passwords, login codes, user names and other confidential information related to the use of the System, as well as may not provide hardware or software authenticators for use by third parties, password generators, applications or devices containing data used for user identification/authorization.

4.1.6 Благодаря использованию системы регистрации действий пользователя, вошедшего в Систему в указанном выше порядке, Участники Системы имеют возможность определить, какие действия и каким пользователем были произведены, и в том числе, кем были подписаны Электронные документы. Использование указанных в пункте 4.1.1 настоящих Правил средств и процедур позволяет подтвердить формирование Простой ЭП определенным пользователем – уполномоченным представителем Клиента или Держателем Карты (если применимо).

4.1.6 Due to the use of a system for logging user actions logged into the System in the aforesaid manner, System Participants are able to determine which actions were taken by which user, including who signed the Electronic Documents. The use of the means and procedures specified in clause 4.1.1 of these Rules allows you to confirm the formation of a Simple ES by a specific user - an authorized representative of the Customer or by the Cardholder (if applicable).

4.2 Использование Усиленной ЭП

4.2.1 Обмен Электронными документами, подписанными Усиленной ЭП, происходит посредством:

- (а) направления файлов через соответствующий модуль для предоставления документов определенного вида, предусмотренный Системой CitiDirect BE и Системой CitiConnect;
- (б) заполнения и отправки данных в онлайн-формах соответствующего модуля для предоставления документов данного вида, предусмотренного Системой CitiDirect BE и Системой CitiConnect, в том числе с приложением необходимых файлов, при этом и данные, и файлы подписываются Усиленной Электронной подписью отправителя;
- (в) направления подписанных Усиленной ЭП файлов по электронной почте - для предоставления документов определенного вида.

4.2.2 Электронные документы, подписанные Усиленной ЭП, полученные или переданные указанным способом, а также посредством электронной почты, являются равнозначными документам на бумажных носителях, подписанным собственноручной подписью лиц, уполномоченных Участниками Системы, благодаря формированию и использованию Усиленной электронной подписи в соответствии с положениями настоящих Правил.

4.2.3 В случае использования неквалифицированной ЭП Банк осуществляет функции доверенного лица и регистрационного центра Внешнего Удостоверяющего центра. Наряду с

4.2 Enhanced Electronic Signature

4.2.1 The exchange of Electronic Documents, signed with Enhanced ES, shall take place by means of:

- (a) sending files via the relevant module for delivery of documents of a particular type, as specified by the CitiDirect BE System and CitiConnect System;
- (b) filling in and sending data in the online forms of the relevant module for the provision of documents of this type provided by the CitiDirect BE System and CitiConnect System, including the attachment of the necessary files, and the data and files are signed with the Enhanced Electronic Signature of the sender;
- (c) sending files signed with Enhanced ES via e-mail to provide certain types of documents.

4.2.2 Electronic Documents, signed with Enhanced ES, received or delivered by the said means, as well as via e-mail, shall be equivalent to documents in hard copy executed with the handwritten signature of persons authorized by Participants of the System, by virtue of the generation and use of an Enhanced electronic signature according to the provisions of the Rules.

4.2.3 In the case of unqualified Electronic Signature, the Bank performs the functions of an attorney and registration center of the Third-party Certification Authority. Along with the Rules regarding the use of the relevant

Правилами в отношении использования соответствующих Сертификатов и Электронных подписей Участниками Системы действует регламент Внешнего Удостоверяющего центра (далее – «Регламент»).

Certificates and Electronic Signatures, the System Participants shall also be subject to the regulations of the Third-party Certification Authority (hereinafter – “**Regulations**”).

5 Порядок формирования Усиленной Электронной Подписи

5.1 Порядок формирования Неквалифицированной Усиленной ЭП

5.1.1 Для формирования, использования и проверки Усиленной неквалифицированной ЭП Электронных документов используется сертифицированный ФСБ России программно-аппаратный комплекс Удостоверяющего центра «Notary-PRO», разработанный группой компаний «Сигнал-КОМ». Справка о данном программно-аппаратном комплексе и об иных используемых программных продуктах группы компаний «Сигнал-КОМ» приведена в Приложении 1 к настоящим Правилам.

5.1.2 Банк обязуется предоставить уполномоченному представителю Клиента в порядке, определенном Банком, программное обеспечение и аппаратные средства, разработанные группой компаний «Сигнал-КОМ», вместе с необходимыми инструкциями по эксплуатации, необходимые для генерации Ключа Усиленной ЭП, Ключа проверки Усиленной ЭП и запроса на Сертификат, после получения подписанного со стороны Клиента экземпляра договора об обмене Электронными документами определенного вида (если вид такого Электронного документа не включен в Приложение 6 к настоящим Правилам) и доверенности, выданной Клиентом на имя будущих Владельцев Сертификата и составленной по форме Банка.

5.1.3 Банк уполномочен предоставлять Клиентам лицензию на использование программного обеспечения группы компаний «Сигнал-КОМ» на основании договора, заключенного между Банком и ООО «Сигнал-КОМ».

5 Procedures for Enhanced Electronic Signature generation

5.1 Procedures for Enhanced Unqualified Electronic Signature generation

5.1.1 For the formation, use and verification of Enhanced unqualified electronic signature of the Electronic Documents, the hardware and software of Notary-PRO Certification Authority is used which is developed by the Signal-COM group and certified by the Federal Security Service of Russia. Information on this software and hardware complex and on other used software products of the Signal-COM group is given in Annex 1 to these Rules.

5.1.2 The Bank shall undertake to provide to the Customer’s authorized representative, in accordance with the procedures defined by the Bank, the software and hardware developed by the Signal-COM group, together with the required operating instructions, needed to generate an Enhanced ES Key, Enhanced ES Verification Key, and Certificate request, upon receipt of the agreement signed by the Customer on exchange of the Electronic Documents of certain kind (if the type of such Electronic Document is not included in Appendix 6 to these Rules) and the power of attorney issued by the Customer in the name of the future Certificate Holders and drawn up in accordance with the Bank’s template.

5.1.3 The Bank is authorized to provide Customers with a license to use the software from the Signal-COM group pursuant to an agreement concluded between the Bank and ООО Signal-COM.

5.1.4 Клиент обязуется произвести установку необходимого программного обеспечения самостоятельно. При возникновении вопросов в отношении установки программ Клиент вправе получить консультацию Службы технической поддержки Банка, направив запрос по адресу электронной почты ru.cdhd@citi.com или обратившись по номеру телефона +7 495 725 67 95.

5.1.5 Для формирования Ключей Усиленной неквалифицированной ЭП, Ключей проверки Усиленной неквалифицированной ЭП и изготовления Сертификата Удостоверяющим центром Клиенту необходимо присоединиться к Регламенту Внешнего Удостоверяющего центра, предоставив подписанное уполномоченным лицом и заверенное печатью Клиента заявление о присоединении к Регламенту (заявление о присоединении к Регламенту Удостоверяющего центра e-Notary - Приложение 2 к Правилам), а также направить Запрос на Сертификат по общей процедуре направления Запроса на Сертификат.

5.1.6 Для формирования Ключей Усиленной неквалифицированной ЭП, Ключей проверки Усиленной ЭП и изготовления Сертификата Удостоверяющим центром Банка Клиенту необходимо направить Запрос на Сертификат по общей процедуре направления запроса на Сертификат, предусмотренной настоящими Правилами. Форма Запроса на Сертификат приведена в Приложении 3 к настоящим Правилам.

5.1.7 Запрос на Сертификат в электронном виде передается Клиентом в Банк по адресу электронной почты cert.ru@citi.com а также распечатывается в двух экземплярах и передается в Банк. Экземпляры Запроса на Сертификат на бумажных носителях должны быть заверены подписью руководителя или иного уполномоченного представителя Клиента и печатью Клиента, подписью уполномоченного лица, которому должен быть выдан Сертификат, а также подписью уполномоченного лица, осуществляющего идентификацию лица, которому должен быть выдан Сертификат в момент подачи заявления.

5.1.4 The Customer shall undertake to carry out the installation of the necessary software independently. Should questions arise in relation to installing the programs, the Customer may obtain advice from the Bank's Technical Support Department by sending a request to the e-mail address ru.cdhd@citi.com or by calling the phone number +7 495 725 67 95.

5.1.5 For the generation of Enhanced nonqualified ES Keys and Enhanced nonqualified ES Verification Keys and the production of a Certificate by the Third-Party Certification Authority, the Customer is required to accede to the Regulations of the Third-Party Certification Authority by providing a declaration of accession to the Regulations of the Certification Authority, signed by an authorized representative and authenticated with the seal of the Customer (see Application for Accession to the Regulations of the certification authority - Annex 2 to the Rules), as well as to forward a Certificate Request according to the general procedure on sending the Request for a Certificate.

5.1.6 For the generation of Enhanced nonqualified ES Keys and Enhanced ES Verification Keys and the production of a Certificate by the Bank's Certification Authority, the Customer is required to send a Certificate Request according to the general procedure for forwarding a Certificate Request as contemplated by these Rules. The form for a Certificate Request to the Bank's Certification Authority is provided in Annex 3 to these Rules.

5.1.7 An electronic Certificate Request shall be sent by the Customer to the Bank at the e-mail address cert.ru@citi.com, and also printed in two copies and sent to the Bank. Copies of the Request for Certificate on paper shall be certified by the signature of the manager or other authorized representative of the Customer and by the Customer's seal, as well as by the signature of the authorized person to whom the Certificate is to be issued, as well as the signature of an authorized person who identifies the person to whom the Certificate is to be issued at the time of application.

Банк обязуется проверить соответствие Запроса на Сертификат в электронном виде предоставленным экземплярам на бумажных носителях, а также подписей и оттиска печати на бумажных носителях в соответствии с карточкой образцов подписей и оттиска печати или с другими документами Клиента. В случае подтверждения соответствия всех экземпляров Запроса на Сертификат, а также подписей и оттиска печати, содержащихся на бумажных носителях, Банк приступает к обработке Запроса на Сертификат и организует самостоятельно либо с привлечением Внешнего Удостоверяющего центра выдачу Сертификата Удостоверяющим центром.

5.1.8 Информация о созданном Сертификате помещается Удостоверяющим центром в реестр выпущенных Сертификатов. Банк обязуется передать Клиенту копию Сертификата в электронном виде по адресу электронной почты, указанному в Запросе на Сертификат.

Направление копии Сертификата в электронном виде по адресу электронной почты, указанному в Запросе на Сертификат, означает, что владельцем Сертификата является уполномоченный представитель, направивший Запрос на Сертификат в Банк, ключ проверки Электронной подписи принадлежит такому владельцу Сертификата.

5.2 Срок действия Сертификата

5.2.1 Срок действия Сертификата составляет 3 (три) года с даты выдачи Сертификата. Даты начала и окончания действия Сертификата указываются в самом Сертификате.

5.2.2 Действие Сертификата может быть приостановлено или аннулировано Удостоверяющим центром:

- по заявлению Владельца Сертификата, поданному в Банк. Действие Сертификата может быть возобновлено также по заявлению Владельца Сертификата, поданному в Банк.
- по инициативе Банка путем предоставления распоряжения Внешнему Удостоверяющему центру. Действие Сертификата может быть возобновлено по распоряжению Банка после устранения

The Bank undertakes to verify the compliance of the Request for Certificate in electronic form with the provided copies on paper, as well as signatures and an imprint of a seal on paper in accordance with the signature sample and seal imprint card or other documents of the Customer.

In case of confirmation of the conformity of all counterparts of the Certificate Request as well as signatures and seal imprints contained on paper, the Bank proceeds to processing the Certificate Request and arranges for the Certificate Authority to issue the Certificate independently or with the assistance of the External Certification Center.

5.1.8 Information on the Certificate produced shall be placed by the Certification Authority in the register of issued Certificates.

The Bank shall undertake to deliver to the Customer an electronic copy of the Certificate to the e-mail address indicated in the Certificate Request.

Sending a copy of the Certificate in electronic form to the email address specified in the Certificate Request means that the owner of the Certificate is an authorized representative who sent the Certificate Request to the Bank, the Electronic Signature verification key belongs to this Certificate owner.

5.2 Certificate period of validity

5.2.1 The period of validity for a Certificate shall be three (3) years from the Certificate issue date. The validity start and end date for a Certificate must be indicated in the Certificate itself.

5.2.2 The effect of a Certificate may be suspended or cancelled by the Certification Authority:

- pursuant to a request from the Certificate Holder, submitted to the Bank. The Certificate may also be reinstated pursuant to a request from the Certificate Holder, filed with the Bank.
- at the Bank's initiative by way of giving an instruction to the Third-Party Certification Authority. The Certificate may be reinstated by instruction of the Bank upon elimination of the causes serving as grounds for the suspension of the Certificate.

причин, послуживших основанием для приостановления Сертификата.

- по инициативе Банка в случае прекращения Банком использования услуг Внешнего Удостоверяющего центра.
- по инициативе Удостоверяющего центра в соответствии с Регламентом Удостоверяющего центра. Действие Сертификата может быть возобновлено после устранения причин, послуживших основанием для приостановления Сертификата.

5.3 Условия признания равнозначности Усиленной электронной подписи собственноручной подписи

5.3.1 Передаваемые и полученные при помощи Системы либо иных способов обмена Электронные документы, подписанные корректной Усиленной ЭП, юридически равнозначны документам, составляемым на бумажных носителях и заверяемым собственноручными подписями уполномоченных лиц и оттиском печати Банка и Клиента, и являются надлежащим основанием для возникновения соответствующих прав и обязанностей Банка и Клиента в рамках существующих между ними договорных отношений.

5.3.2 Усиленная ЭП признается равнозначной собственноручной подписи лица, уполномоченного Клиентом, при условии присоединения Клиента к настоящим Правилам и наличия действующего Сертификата.

5.4 Осуществление контроля целостности и полноты электронного сообщения

5.4.1 Программные и аппаратные средства, используемые для обмена Электронными документами, обеспечивают систему защиты информации с помощью шифрования и ЭП, гарантируют конфиденциальность, подтверждают авторство, подлинность и целостность Электронных документов.

5.4.2 При каком-либо изменении Электронных документов после подписания данного документа посредством Усиленной ЭП, ЭП становится некорректной, что подтверждается путем проверки подписи с Ключом проверки Усиленной ЭП автора

- at the Bank's initiative in case of the Bank ceasing to use the services of the Third-Party Certification Authority.

- at the Certification Authority's initiative in accordance with the Regulations of the Certification Authority. The Certificate may be reinstated upon elimination of the causes serving as grounds for the suspension of the Certificate.

5.3 Conditions for recognition of an Enhanced Electronic Signature and handwritten signature as equivalent

5.3.1 Electronic Documents sent and received with the use of the System, when signed with a valid Enhanced ES, are legally equivalent to documents executed in hard copy and certified with the handwritten signatures of authorized representatives and authenticated with the seal impression of the Bank and the Customer, and shall be appropriate grounds for the creation of the respective rights and obligations of the Bank and the Customer in the context of the existing contractual relationship between them.

5.3.2 Enhanced ES shall be recognized as equivalent to the handwritten signature of a person authorized by the Customer, subject to the Customer's accession to these Rules and the availability of a valid Certificate.

5.4 Controlling the integrity and completeness of electronic messages

5.4.1 Software and hardware which are using for the exchange of Electronic Documents provide a data security system using encryption and ES, guarantee confidentiality, and confirm the authorship, authenticity, and integrity of Electronic Documents.

5.4.2 In case of any change in Electronic Documents after a given document is signed via an Enhanced ES, the ES becomes invalid, which is confirmed by way of verifying the signature with the Enhanced ES Verification Key from the document's author, which will give a negative result.

документа, которая дает отрицательный результат.

6. Порядок обмена Электронными документами

6.1 Обмен документами и информацией осуществляется в электронном виде с момента присоединения к настоящим Правилам или с момента присоединения к настоящим Правилам при условии подписания Клиентом договора об обмене Электронными документами определенного вида (если вид такого Электронного документа не предусмотрен в Приложении 6 к настоящим Правилам).

6.2 При невозможности осуществления обмена в электронном виде с помощью Системы вследствие сбоев в работе аппаратных или программных средств, отсутствия технической возможности или особенностей реализации решений Банк и Клиент могут обмениваться документами и информацией по контактными адресам электронной почты с применением программного обеспечения File-PRO, разработанного группой компаний «Сигнал-КОМ» (далее – «File-PRO»).

6.3 При невозможности обмена документами по электронной почте с применением File-PRO Банк и Клиент обмениваются документами на бумажных носителях. Во всех указанных случаях сбоев в порядке обмена документами и информацией в электронном виде Банк и Клиент обязуются незамедлительно уведомлять друг друга любым доступным способом о невозможности использования предпочтительного способа обмена документами и информацией. При первой возможности Банк и Клиент должны оперативно вернуться к порядку обмена с помощью Системы, известив друг друга о своей готовности возобновить такой порядок обмена.

6.4 Банк обязуется принимать к исполнению Электронные документы, соответствующие установленным требованиям и подписанные корректной ЭП, в обычном порядке в соответствии с условиями договоров и соглашений между Банком и Клиентом.

6.5 Порядок приема и подтверждения приема Электронных документов Банком

6. Electronic Document exchange process

6.1 The exchange of documents and information is carried out in electronic form from the moment of accession to these Rules or from the moment of accession to these Rules provided that the Client signs an agreement on the exchange of certain types of Electronic Documents (if the type of such Electronic Document is not provided for in Annex 6 to these Rules).

6.2 When it is impossible to make an exchange using the System due to hardware or software malfunctions or technical inability or specific of the technical implementation, the Bank and the Customer shall exchange documents and data via their contact e-mail addresses using the File-PRO software developed by the Signal-COM group (hereinafter – “File-PRO”).

6.3 When it is impossible to exchange documents via e-mail using File-PRO, the Bank and the Customer shall exchange documents in hard copy. In all such cases of failures in the process of exchanging electronic documents and data, the Bank and the Customer shall undertake to promptly notify one another by any available means of the failure of the preferred means of exchanging documents and data. At the first opportunity, the Bank and the Customer must promptly return to the exchange process using the System, having notified one another of their readiness to resume such exchange process.

6.4 The Bank shall undertake to accept Electronic Documents for execution that conform to the established requirements and are signed with a valid ES, on a routine basis in accordance with the terms and conditions of the agreements and arrangements between the Bank and the Customer.

6.5 Procedures for the acceptance and confirmation of acceptance of Electronic

определяется в заключенных между Клиентом и Банком договорах об обмене Электронными документами определенного вида (если вид такого Электронного документа не предусмотрен Приложением 6 к настоящим Правилам).

6.6 Банк вправе отказать в приеме Электронных документов в случае несоответствия их оформления требованиям, установленным действующим законодательством и Банком, а также в случае отсутствия ЭП или ее некорректности, возникновения угрозы несанкционированного доступа к программным-аппаратным средствам Клиента и утраты конфиденциальности обмена документами и информации между Банком и Клиентом. Банк уведомляет Клиента любым доступным способом об отказе в приеме документов с указанием причины отказа.

7. Внешний Удостоверяющий центр

7.1 Внешним Удостоверяющим центром, который вправе в соответствии с положениями настоящих Правил и Договора выдавать Сертификаты для обмена Электронными документами между Банком и Клиентом, является Удостоверяющий центр e-Notary (<https://www.e-notary.ru/>) – корпоративный удостоверяющий центр, выполнение функций которого обеспечивает группа компаний «Сигнал-КОМ». Удостоверяющий центр e-Notary предоставляет полномочия регистрационного центра Банку на основании Доверенности, выданной АО «Сигнал-КОМ» на имя Банка. (Приложение 4 к настоящим Правилам). Возможность и/или необходимость работы с иными Внешними Удостоверяющими центрами, необходимость присоединения к соответствующим Регламентам, а также необходимые формы, документы и процедуры определяются Банком и Внешними Удостоверяющими центрами и своевременно доводятся до сведения Клиента.

7.2 Регламент Удостоверяющего центра e-Notary опубликован на сайте группы компаний «Сигнал-КОМ» по адресу <https://www.e-notary.ru/articles/view/id/3>.

7.3 Клиент обязуется заполнить и передать в Банк заявление о присоединении к

Documents by the Bank shall be defined in the agreement on exchange of the Electronic Documents of certain kinds concluded between the Customer and the Bank (if the type of such an Electronic Document is not provided for in Annex 6 to this Regulation).

6.6 The Bank shall be entitled to refuse to accept Electronic Documents if they are prepared in a way that does not conform to the requirements set by applicable laws and by the Bank, or if there is no ES or the ES is invalid, or if there is a threat of unauthorized access to the Customer's software and hardware and the loss of confidentiality in the exchange of documents and data between the Bank and the Customer. The Bank shall notify the Customer by any available means of the refusal to accept documents, stating the reason for the refusal.

7. Third-Party Certification Authority

7.1 Third-Party Certification Authority, which is entitled in accordance with the provisions of the Rules and the Agreement to issue Certificates for the exchange of Electronic Documents between the Bank and the Customer, shall be the Certification Authority e-Notary (<https://www.e-notary.ru/>) – a corporate certification authority whose functioning is supported by the Signal-COM group. The Certification Authority e-Notary grants the Bank authority as a registration center on the basis of the Power of Attorney issued by AO Signal-COM in favor of the Bank. (Annex 4 to these Rules).

The possibility and / or need to work with other Third-Party Certification Authorities, the need to join the relevant Regulations, as well as the necessary forms, documents and procedures are determined by the Bank and the Third-Party Certification Authorities and communicated to the Customer in a timely manner.

7.2 The Regulations of the Certification Authority are published on the Signal-COM group's website at: <https://www.e-notary.ru/articles/view/id/3>.

7.3 The Customer undertakes to complete and deliver to the Bank an application for

Регламенту Удостоверяющего центра e-Notary по форме, приведенной в Приложении 2 «Заявление о присоединении к Регламенту Удостоверяющего центра e-Notary» к настоящим Правилам.

7.4 Внешний Удостоверяющий центр может быть заменен по инициативе Банка на другой удостоверяющий центр в одностороннем порядке с уведомлением об этом Клиента не менее чем за 30 (тридцать) дней до даты замены.

7.5 Клиент обязуется в течение 10 (десяти) дней с момента замены удостоверяющего центра получить новый Сертификат от определенного Банком Внешнего Удостоверяющего центра, присоединившись к его Регламенту и оформив иные необходимые для этого документы, формы которых обязуется предоставить Банк.

7.6 Если срок ранее выданного Сертификата не истек после получения Клиентом нового Сертификата, ранее выданный Сертификат досрочно прекращает действовать по распоряжению Банка об аннулировании ранее выданного Сертификата.

8. Права и обязанности Участников Системы

8.1 Права и обязанности Клиента

8.1.1 Клиент обязан соблюдать конфиденциальность Ключа ЭП, обеспечить доступность Ключа только уполномоченным лицам, указанным в качестве Владельца Сертификата.

8.1.2 При смене уполномоченных лиц, обладающих правом подписи Электронных документов, утрате Ключей ЭП и в иных случаях, влекущих угрозу несанкционированного доступа к Ключам ЭП и программным средствам Клиента, Клиент обязан незамедлительно подать в Банк и\или Удостоверяющий Центр заявление об аннулировании Сертификата. При получении данного уведомления Банк и\или Удостоверяющий Центр организуют самостоятельно или с помощью Внешнего Удостоверяющего центра аннулирование действия Сертификатов.

8.1.3 Клиент обязан выполнять эксплуатационные требования Систем,

accession to the Regulations of the Certification Authority e-Notary in the form provided in Annex 2 “Application for accession of the Certification Authority e-Notary” to this Agreement.

7.4 The Third-Party Certification Authority may be replaced with another certification authority unilaterally at the Bank’s discretion with notification of the Customer at least 30 (thirty) days before the replacement date.

7.5 The Customer undertakes within 10 (ten) days from the moment of replacing the certifying authority to obtain a new Certificate from the Third-Party Certification Authority identified by the Bank, by joining its Regulations and issuing other necessary documents for this, the forms of which the Bank shall undertake to provide.

7.6 If a previously issued Certificate has not expired upon the Customer’s receipt of a new Certificate, the previously issued Certificate shall be prematurely terminated upon the Bank’s order to cancel the previously issued Certificate.

8. Rights and obligations of System Participants

8.1 the Customer’s rights and obligations

использования программного обеспечения и

8.1.1 The Customer is obligated to keep the ES Key confidential, and to ensure that the Key is accessible only by the authorized persons who are designated as a Certificate Holder.

8.1.2 In case of a change in the authorized persons with the right to sign Electronic Documents, the loss of ES Keys, and in other cases entailing a threat of unauthorized access to the Customer's ES Keys and software, the Customer shall be obligated to promptly file a Certificate cancellation request with the Bank and/or Certification Authority. When receiving such notification, the Bank and/or Certification Authority shall arrange for, either itself or with the assistance of the Third-Party Certification Authority, cancellation of the effect of the Certificates.

8.1.3 The client is obliged to fulfill the operational requirements of the Systems, the

ЭП в строгом соответствии с предоставленными инструкциями и руководствами.

8.1.4 Клиент обязан за свой счет обеспечивать работоспособность принадлежащих ему программных и аппаратных средств для работы в Системе, в том числе необходимые средства антивирусной защиты, а также их обновление в соответствии с указаниями Банка.

8.1.5 Клиент обязан предоставить по требованию Банка надлежащим образом оформленные Электронные документы путем их представления на бумажных носителях.

8.1.6 Клиент обязан формировать и поддерживать в течение 3 (трех) лет архивы всех переданных и принятых Электронных документов. Если действующим законодательством РФ установлены более продолжительные сроки хранения для аналогичных документов на бумажных носителях, применяются данные сроки.

8.1.7 Клиент обязан поддерживать работоспособность адресов электронной почты, выделенных для обмена Электронными документами, и обеспечивать невозможность их использования неуполномоченными на то лицами.

8.1.8 Клиент обязан формировать Ключ Усиленной ЭП, Ключ проверки Усиленной ЭП и Запрос на Сертификат в соответствии с настоящими Правилами.

8.1.9 Клиент обязан предварительно получить в надлежащей форме согласие своих уполномоченных лиц на обработку их персональных данных в связи с процессом выдачи Сертификатов и использования Системы.

8.1.10 Клиент вправе требовать приостановления или аннулирования Сертификатов своих уполномоченных лиц в порядке, предусмотренном пунктом 8.1.2 настоящих Правил.

8.1.11 Клиент вправе получать необходимые консультации по вопросам эксплуатации Систем, используемого программного обеспечения и ЭП от Службы технической поддержки Банка.

8.1.12 Клиент вправе направлять отказ от приема документа от Банка при отсутствии ЭП Банка или при некорректности ЭП.

use of software and ES in strict accordance with the instructions and manuals provided.

8.1.4 The Customer shall be obligated, at its expense, to ensure the operability of the software and hardware belonging to it for working within the System, including the necessary antivirus software and updates thereto according to the Bank's instructions.

8.1.5 The Customer shall be obligated to provide, upon the Bank's request, duly executed Electronic Documents via the submission thereof in hard copy.

8.1.6 The Customer shall be obligated to create and maintain for a period of three (3) years an archive of all Electronic Documents sent and received. If applicable the Russian Federation laws specify longer storage periods for similar documents in hard copy, the given periods shall apply.

8.1.7 The Customer shall be obligated to maintain the operability of the e-mail addresses designated for the exchange of Electronic Documents, and to ensure that it is impossible for unauthorized persons to use them.

8.1.8 The Customer shall be obligated to generate the Enhanced ES Key, Enhanced ES Verification Key, and Certificate Request in accordance with these Rules.

8.1.9 The Customer is obligated to obtain the prior consent in the appropriate form of its authorized representatives to the processing of their personal data in connection with the process of issuing Certificates and the use of the System.

8.1.10 The Customer shall have the right to request the suspension or cancellation of the Certificates of its authorized representatives in the manner contemplated by clause 8.1.2 of these Rules.

8.1.11 The Customer shall have the right to obtain the necessary advice on matters of the operation of the System, the software and ES from the Bank's Technical Support Department.

8.1.12 The Customer shall have the right to forward a refusal to accept a document from the Bank in the absence of the Bank's ES or in case of an invalid ES.

8.1.13 Клиент обязан назначить минимум двух Администраторов Системы CitiDirect BE, совершающих действия, предусмотренные в Приложении 5 к настоящим Правилам.

8.1.14 Клиент обязан установить (для случаев, где установление лимитов в системе технически возможно) и/или контролировать в Системе CitiDirect BE, Системе CitiConnect, Системе SwiftNet, CitiManager и иных системах лимиты для Уполномоченных лиц Клиента на совершение определенных видов действий (включая, но, не ограничиваясь, перевод денежных средств, размещение депозитов, совершение конверсионных операций, и т.п.).

8.1.13 The Customer is obliged to appoint at least two CitDirect BE System Administrators who perform the actions provided for in the Annex 5 to these Rules.

8.1.14 The Client is obliged to set (for cases where setting limits in the system is technically possible) and / or control in the CitiDirect BE System, CitiConnect System, SwiftNet System, CitiManager and other systems the limits for the Customer's Authorized Persons to perform certain types of actions (including, but not limited to, funds transfer, deposit placement, conversion operations, etc.).

8.2 Права и обязанности Банка

8.2.1 Банк обязан предоставить Клиенту программные и аппаратные средства, обеспечивающие авторизованный доступ к Системе, генерацию Ключей ЭП и Ключей проверки ЭП, формирование запросов на Сертификаты, формирование и проверку ЭП, защиту передаваемых по открытым каналам связи документов, а также собственные Ключи ЭП и копию собственных Сертификатов на бумажном носителе, где это необходимо. Служба технической поддержки Банка консультирует Клиентов в отношении использования ЭП и Системы.

8.2.2 Банк обязан формировать и поддерживать архивы всех переданных и принятых Электронных документов в соответствии с требованиями законодательства. При этом Банк обязуется соблюдать специальные сроки хранения документов, установленные требованиями действующего законодательства РФ для аналогичных видов документов, составленных на бумажных носителях.

8.2.3 Банк уведомляет Клиента о необходимости обновления программного обеспечения.

8.2.4 Банк обязан поддерживать работоспособность адресов электронной почты, выделенных для обмена Электронными документами, и обеспечивать невозможность их использования неуполномоченными на то лицами.

8.2.5 Банк обязан обеспечить выдачу своим сотрудникам Сертификатов и обеспечить использование ими Системы, необходимое для выполнения участия Банка в обмене

8.2 Rights and obligations of the Bank

8.2.1 The Bank is obligated to provide the Customer with software and hardware providing for authorized access to the System, the generation of ES Keys and ES Verification Keys, the creation of Certificate requests, ES generation and verification, the security of documents sent via public communication channels, along with its own ES Keys and copies of the respective Certificates in hard copy where required.

The Bank's Technical Support Department shall advise Customers on issues of the use of ES and the System.

8.2.2 The Bank shall be obligated to create and maintain archives of all Electronic Documents sent and received in accordance with legislative requirements. That being said, the Bank shall undertake to comply with the special storage periods for documents as stipulated by the requirements of applicable RF laws for similar types of documents prepared in hard copy.

8.2.3 The Bank shall notify the Customer of the need to update software.

8.2.4 The Bank shall be obligated to maintain the operability of the e-mail addresses designated for the exchange of Electronic Documents, and to ensure that it is impossible for unauthorized persons to use them.

6.2.5 The Bank shall be obligated to ensure that Certificates are issued to its employees and to provide for their use of the System as necessary to accomplish the Bank's participation

документами и информацией в электронном виде.

8.2.6 Банк вправе прекратить прием и исполнение Электронных документов в случае выявления признаков нарушения безопасности Системы, при условии незамедлительного уведомления Клиента любым доступным способом о данном факте и необходимости принятия соответствующих мер.

8.2.7 Банк вправе в любой момент потребовать у Клиента предоставления надлежащим образом оформленных документов на бумажных носителях, соответствующих Электронным документам, и не приступать к исполнению до предоставления требуемых документов.

8.2.8 Банк вправе отказать или приостановить исполнение какого-либо Электронного документа, подписанного корректной ЭП, если исполнение такового, по мнению Банка, является нарушением законодательства или может привести к нарушению законодательства, в частности, законодательства по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, до тех пор, пока Клиент не предоставит, к полному удовлетворению Банка, дополнительные объяснения и/или документы, которые будут запрошены Банком.

8.2.9 Банк вправе производить замену программного обеспечения Системы, устанавливать новые требования к ЭП, средствам защиты передаваемой информации, изменять форматы и список Электронных документов при условии уведомления Клиента не менее чем за 10 (десять) дней до подобных изменений.

8.2.10 Банк вправе разрешать или запрещать Клиенту использование Сертификатов, выданных другими удостоверяющими центрами.

8.2.11 Банк вправе запросить у Клиента документы, подтверждающие, что Клиент получил согласие его уполномоченных лиц на обработку персональных данных в связи с процессом выдачи Сертификатов.

8.2.12 Банк вправе в одностороннем порядке изменять настоящие Правила в соответствии с пунктом 2.5 настоящих Правил.

in the exchange of electronic documents and data.

8.2.6 The Bank shall have the right to cease the acceptance and execution of Electronic Documents in case of detecting signs of a breach in System security, subject to prompt notification of the Customer by any available means of this fact and of the need to take the appropriate measures.

8.2.7 The Bank shall have the right, at any time, to request the Customer's provision of duly executed documents in hard copy conforming to the Electronic Documents, and not to proceed with execution until the requested documents are provided.

8.2.8 The Bank shall have the right to deny or suspend the execution of any Electronic Document signed with a valid ES if the execution of such, in the Bank's opinion, would constitute a violation of the law or could lead to a violation of the law, in particular, the laws on anti money laundering and the financing of terrorism, until such time as the Customer provides, to the reasonable satisfaction of the Bank, the additional explanations and/or documents which the Bank shall request.

8.2.9 The Bank shall have the right to replace the software for the System, to impose new requirements on ES and the security measures for the data being sent, and to change the formats and list of Electronic Documents, subject to notification of the Customer at least ten (10) days prior to such changes.

8.2.10 The Bank shall have the right to permit or prohibit the Customer from using Certificates issued by other certification authorities.

8.2.11 The Bank shall have the right to request documents from the Customer confirming that the Customer has obtained the consent of its authorized representatives to the processing of personal data in connection with the process of issuing Certificates.

8.2.12 The Bank shall have the right, on a unilateral basis, to change these Rules in accordance with clause 2.5 of these Rules.

8.2.13 Банк, действуя в качестве регистрационного центра Внешнего Удостоверяющего центра, обладает следующими правами и несет следующие обязанности:

- идентифицировать и аутентифицировать физических лиц – будущих Владельцев Сертификатов;
- принимать и регистрировать Запросы на сертификаты;
- предоставлять Владельцам Сертификатов изготовленные Сертификаты в электронной форме;
- изготавливать копии Сертификатов на бумажных носителях;
- аннулировать, приостанавливать и возобновлять действие Сертификатов по заявлениям Владельцев Сертификатов и по собственной инициативе;
- аутентифицировать Владельцев Сертификатов, запрашивающих аннулирование, приостановление и возобновление действия Сертификатов.

8.2.14 Банк, действуя в качестве собственного Удостоверяющего центра, обладает следующими правами и несет следующие обязанности, помимо указанных в пункте 8.2.13 настоящих Правил:

- формировать Ключи ЭП и Ключи проверки ЭП Удостоверяющего центра (уполномоченных лиц Удостоверяющего центра);
- контролировать уникальность Ключей ЭП в регистрируемых запросах;
- изготавливать на основании принятых Запросов на Сертификаты электронные Сертификаты;
- вести реестр выпущенных и аннулированных Сертификатов;
- публиковать реестр выпущенных и аннулированных сертификатов в общедоступном сетевом справочнике;
- подтверждать подлинность электронных подписей в документах, представленных в электронной форме, по запросам пользователей Удостоверяющего центра;
- хранить запросы и сертификаты Ключей ЭП в реестре сертификатов в течение 5 (пяти) лет для проведения (в

8.2.13 The Bank, acting as the registration center for the Third-Party Certification Authority, possesses the following rights and assumes the following obligations:

- to identify and authenticate the individuals who are future Certificate Holders;
- to accept and record Certificate Requests;
- to provide Certificate Holders with the produced Certificates in electronic form;
- to produce hard copies of Certificates;
- to cancel, suspend, and reinstate Certificates pursuant to requests from Certificate Holders and at its own initiative;
- to authenticate the Certificate Holders requesting the cancellation, suspension, and reinstatement of Certificates.

8.2.14 The Bank, acting as its own Certification Authority, possesses the following rights and assumes the following obligations, in addition to those indicated in clause 8.2.13 of these Rules:

- to generate the ES Keys and ES Verification Keys of the Certification Authority (authorized representatives of the Certification Authority);
- to check for the uniqueness of the ES Keys in the requests recorded;
- to produce electronic Certificates on the basis of accepted Certificate Requests;
- to keep a register of issued and cancelled Certificates;
- to publish the register of issued and cancelled certificates in a public network directory;
- to authenticate the electronic signatures in documents submitted electronically, pursuant to requests from the Certification Authority's users;
- to store requests and ES Key certificates in the register of certificates for a period of five (5) years in order to parse (as

случае необходимости) разбора конфликтных ситуаций, связанных с их применением.

necessary) conflict situations relating to the use thereof.

9. Ответственность Участников Системы

9.1 Банк и Клиент самостоятельно несут ответственность за убытки вследствие разглашения или передачу третьим лицам Ключей ЭП и любых иных фактов компрометации ЭП. Банк не несет ответственности за убытки Клиента, возникшие вследствие несанкционированного использования Ключа ЭП неуполномоченными лицами, в том числе возникшие в результате исполнения Электронных документов, подписанных корректной ЭП.

9.2 Банк и Клиент самостоятельно несут ответственность за любые действия их уполномоченных лиц, совершенные посредством Системы, в том числе за действия их уполномоченных лиц, являющихся Владельцами Сертификатов, и соблюдение Владельцами Сертификатов положений настоящих Правил.

9.3 Банк и Клиент взаимно не несут ответственности за неправильное заполнение форм Электронных документов противоположным Участником Системы.

9.4 Банк и Клиент освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств в случае, если такое неисполнение или ненадлежащее исполнение вызвано обстоятельствами непреодолимой силы, включая, но не ограничиваясь стихийными бедствиями, забастовками, авариями, пожарами, массовыми беспорядками, военными действиями, если Участник Системы, пострадавший от влияния обстоятельств непреодолимой силы, предпримет все усилия для своевременного уведомления другой стороны и ликвидации последствий обстоятельств непреодолимой силы.

9.5 Банк не несет ответственности за обеспечение надлежащего уровня Интернет-соединения, в том числе, за возникновение технических сбоев в работе Системы, связанное со сбоями или перерывами в работе оборудования и каналов связи третьих лиц. Банк не несет ответственности за

9. Liability of System Participants

9.1 The Bank and the Customer shall be held solely liable for losses due to the disclosure or transfer of ES Keys to third parties and any other instances of ES compromise. The Bank shall not be liable for the Customer's losses arising due to the unauthorized use of an ES Key by unauthorized persons, including those arising as a result of the execution of Electronic Documents signed with a valid ES.

9.2 The Bank and the Customer shall be held solely liable for any actions taken by their authorized representatives via the System, including for actions of their authorized representatives that are Certificate Holders, and for Certificate Holders' compliance with the provisions of these Rules.

9.3 The Bank and the Customer shall not have cross liability for the improper completion of Electronic Document forms by the opposing System Participant.

9.4 The Bank and the Customer shall be exempt from liability for default on or improper performance of their assumed obligations in the event that such default or improper performance is due to force majeure, including without limitation natural disasters, strikes, accidents, fires, mass disturbances, and hostilities, provided that the System Participant that is affected by the force majeure makes every effort to give timely notification to the other party and to remedy the consequences of the force majeure.

9.5 The Bank shall not be held liable for the provision of an adequate internet connection, including for the occurrence of malfunctions in the System's operation relating to failures or interruptions in the operation of third-party equipment and communications links. The Bank shall not be held liable for the operability of the

работоспособность программного обеспечения группы компаний «Сигнал-КОМ» и за совместимость программного обеспечения Системы с другим программным обеспечением Клиента.

9.6. Участник Системы не несет ответственности за упущенную выгоду другого Участника Системы в связи с заключением и исполнением Договора, а также соблюдением настоящих Правил.

9.7. Банк не несет ответственность за неисполнение и/или ненадлежащее исполнение Клиентом обязанности установить и контролировать в Системе (включая но, не ограничиваясь, CitiDirect BE, Системе CitiConnect, Системе) лимиты для Уполномоченных лиц Клиента на совершение определенных видов действий (включая, но, не ограничиваясь, перевод денежных средств, размещение депозитов, совершение конверсионных операций, и т.п.). Банк не возмещает ущерб и/или упущенную выгоду Клиента, причиненные Клиенту превышением таких лимитов Уполномоченными лицами Клиента.

10. Разрешение споров

10.1 В случае возникновения спорной ситуации в связи с формированием, доставкой, получением, подтверждением получения электронных документов, подпись под которыми была воспринята Банком как подлинная ЭП Клиента, данная спорная ситуация разрешается в следующем порядке. Клиент не позднее чем в течение 3 (трех) рабочих дней после возникновения спорной ситуации, должен направить Банку претензию (в виде электронного документа либо на бумажном носителе способом, согласованным между сторонами) с изложением сути претензии и детальным описанием спорной операции. К претензии также должны быть приложены материалы, имеющие отношение к предмету спора.

Банк проверяет наличие обстоятельств, свидетельствующих о возникновении спорной ситуации, в том числе, с помощью специальных программных средств. Полученное заключение Банк доводит до сведения Клиента вместе с принятым решением об удовлетворении претензии Клиента либо о необоснованности таких

software from the Signal-COM group and for the compatibility of the System software with other software of the Customer.

9.6. A System Participant shall not be liable for the lost profits of another System Participant in connection with the conclusion and performance of the Agreement, as well as with compliance with these Rules.

9.7. The Bank is not liable for non-fulfillment and / or improper fulfillment by the Customer of the obligation to establish and control in the System (including but not limited to CitiDirect BE, CitiConnect System, CitiManager System) the limits for the Customer's Authorized Persons on performing certain types of actions (including but, without being limited to, funds transfers, deposit placement, conversion operations, etc.). The Bank does not reimburse the damage and / or lost profit of the Customer caused to the Customer by such Customer's Authorized Persons by exceeding such limits.

10. Dispute resolution

10.1 In case of a disputed situation in connection with the generation, delivery, receipt, or confirmation of receipt of electronic documents on which the signature was accepted by the Bank as the genuine ES of the Customer, the given disputed situation shall be resolved as follows.

Not later than three (3) business days after the disputed situation occurs, the Customer must send the Bank a complaint (in the form of an electronic document or in hard copy by the means agreed between the parties) stating the essence of the complaint and providing a detailed description of the disputed transaction. The complaint must also be accompanied by the materials that are relevant to the subject matter of the dispute.

The Bank shall verify the facts attesting to the occurrence of the disputed situation, including with the use of special software. The Bank shall notify the resulting opinion to the Customer together with the adopted decision to satisfy the Customer's complaint or on the illegitimacy of such claims and the reasoned refusal of the Customer's complaint.

требований и о мотивированном отказе в удовлетворении претензии Клиента.

В случае несогласия с ответом Банка об отказе Клиент направляет уведомление о несогласии с требованием о формировании согласительной комиссии (далее – «Комиссия») для рассмотрения спорной ситуации.

В состав Комиссии входит равное количество, но не менее чем по одному уполномоченному представителю от Банка и Клиента, а также эксперт – представитель группы компаний «Сигнал-КОМ» или Внешнего Удостоверяющего Центра.

Право представлять в Комиссии соответствующую Сторону, а также группу компаний «Сигнал-КОМ» или Внешний Удостоверяющий Центр, должно подтверждаться доверенностью, выданной каждому представителю на срок работы Комиссии.

Комиссии передаются все материалы и документы, относящиеся к предмету спора. Комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению Комиссии, для выяснения причин и последствий возникновения спорной ситуации, а также использовать необходимые технические средства для установления фактов и исследования организационных и технических обстоятельств, связанных с возникновением спорной ситуации. Комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.

Комиссия формирует свое заключение в течение 5 (пяти) рабочих дней с момента начала работы. Финальный вариант заключения подписывается всеми участниками Комиссии и представляется для изучения Банку и Клиенту.

10.2 В случае возникновения иных спорных ситуаций, Участники Системы формируют согласительную комиссию в порядке, предусмотренном в пункте 10.1 настоящих Правил за исключением положений о привлечении эксперта. Решение о необходимости привлечения эксперта из независимой организации принимается совместно Банком и Клиентом, при этом независимая организация утверждается совместно Банком и Клиентом из числа представленных ими кандидатур.

If it disagrees with a refusal received from the Bank, the Customer shall forward a notice of disagreement requesting the formation of a conciliation commission (hereinafter – “Commission”) to examine the disputed situation.

The Commission shall be made up of an equal number, but at least one authorized representative each from the Bank and the Customer, as well as an expert representing the Signal-COM group or the Third-Party Certification Authority.

The right to represent on the Commission the relevant Party, as well as the Signal-COM group or the Third-Party Certification Authority, must be confirmed by a power of attorney issued to each representative for the working duration of the Commission.

The Commission shall be provided with all materials and documents relating to the subject matter of the dispute. The Commission shall have the right to consider any other technical issues as necessary, in the Commission’s opinion, in order to determine the causes and consequences of the disputed situation, as well as to use the necessary technical equipment to ascertain the facts and to investigate the organizational and technical circumstances related to the occurrence of the disputed situation. The Commission shall not have the right to give a legal or any other appraisal of the facts ascertained by it.

The Commission shall produce its report within five (5) business days after the start of work. The final version of the report shall be signed by all Commission participants and shall be provided for review by the Bank and the Customer.

10.2 In case of other disputed situations, the System Participants shall form a conciliation commission in the manner provided in clause 10.1 of these Rules, apart from the provisions on retaining an expert. A decision on the need to retain an expert from an independent organization shall be made jointly by the Bank and the Customer, with the independent organization being jointly approved by the Bank and the Customer from among the candidates proposed by them.

10.3 Если по результатам работы Комиссии стороны не достигли договоренности, дальнейшее разбирательство спора продолжается в установленном действующим законодательством порядке в Арбитражном суде г. Москвы.

10.3 If as a result of the Commission's work the parties have failed to come to an agreement, further proceedings in the dispute shall continue in the manner prescribed by applicable laws at the Moscow City Arbitration Court.

Приложения:

Приложение 1. Справка о группе компаний «Сигнал-КОМ», программно-аппаратном комплексе «Notary-PRO» и других продуктах группы компаний «Сигнал-КОМ».

Приложение 2. Заявление о присоединении к Регламенту удостоверяющего центра.

Приложение 3. Запрос на сертификат ключа проверки электронной подписи.

Приложение 4. Доверенность, выданная ЗАО «Сигнал-КОМ» на имя АО КБ «Ситибанк».

Приложение 5. Действия, совершаемые Администратором Системы CitiDirect BE.

Приложение 6. Перечень электронных документов, подлежащих подписанию ЭП в рамках настоящих Правил.

Приложение 7. Процедуры безопасности.

Приложение 8. Инструкция о порядке взаимодействия по осуществлению обмена Электронными документами.

Приложение 9. Порядок регистрации, права и ответственность пользователей в Системе CitiManager.

Приложение 10. Заявление на присоединение Держателя Карты к Правилам.

Приложение 12. Основания ограничения доступа Клиента в Системы в соответствии с пунктами 3.1 и 3.2 Правил.

Annexes:

Annex 1. Fact sheet on the Signal-COM group, the Notary-PRO hardware and software system, and other products from the Signal-COM group.

Annex 2. Application for Accession to the Regulations of the certification authority

Annex 3. Request for an Electronic Signature Verification Key Certificate.

Annex 4. Power of attorney issued by ZAO Signal-COM in favor of AO Citibank.

Annex 5. Actions taken by the CitiDirect BE System Administrator.

Annex 6. The list of electronic documents to be signed by Electronic Signature under these Rules.

Annex 7. Security Procedures

Annex 8. Instructions on the procedure for Electronic Documents Exchange.

Annex 9. Registration procedure, rights and responsibilities of the users in CitiManager System.

Annex 10. Cardholder Application for Accession to the Rules.

Annex 12. Grounds for restricting the Client's access to the Systems in accordance with clauses 3.1 and 3.2 of the Rules.