APPROVED
Internal Order of AO Mizuho Bank (Moscow)
dated 01.04.2026 No 45/26
President A.I Malyshev

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 40601D00C99450EB8BEAF69867AF066C
Владелец: МАЛЫШЕВ АЛЕКСАНДР ИЛЬИЧ
Действителен: с 14.02.2025 до 14.12.2037

AO Mizuho Bank (Moscow)

REMOTE BANKING RULES FOR CUSTOMERS – LEGAL ENTITIES

01.04.2026 / Version 1

Contents

Document Information			
Business Process:		**A4.10.1 Remote banking** **Legal Entities**	
Business Process Owner		**Head of Operations**	
Approval date	**Version**	**Author**	**Comments**
01.04.2026	1	Operations Department L.D. Osipenko	Establishment

Remote Banking Rules for Customers – Legal Entities (except for credit institutions) of AO Mizuho Bank (Moscow) define the terms and rules for interaction on remote banking service issues, establish the general principles of electronic document management using the remote banking service system and are an integral part of the Agreement on remote banking service (hereinafter **- RBS Agreement**).

Terms and Definitions

Subscriber number is a number that uniquely identifies the subscriber equipment connected to the mobile communication network and SIM card installed on it.

Authorization is a process of successful comparison of the Login entered by the Subscriber and registered Login existing in the database of the RBS by software of the RBS as well as checking the ownership of the entered Login (by checking the entered Password), after which the RBS Subscriber is considered Authorized in the RBS.

Certificate Acceptance Document - Certificate Acceptance Document for Electronic Signature Verification Key (Appendix No. 3 to the RBS Rules).

Authentication is a procedure for checking compliance of the Login and Password entered by the Subscriber of the RBS as well as login using the Certificate of the electronic signature key to the Login and Password in the database of the RBS certification of eligibility to contact the Bank, obtaining information on Accounts with the Bank in the manner stipulated by the RBS Rules.

Bank - AO Mizuho Bank (Moscow)

RBS Subscriber (Subscriber) is an individual who is the Customer's authorized representative to whom the Bank, being an agent of the Certification Center, a Certificate of the PE verification key is issued (or is in the process of issuing on the basis of the Application provided by the Customer) and who owns the existing PE Key that allows creating PEs in the Electronic Document (sign the Electronic Document), or to whom the Login is issued in the System for Identification.

Temporary password is a digital code sent as an E-mail message to the e-mail specified by the Customer in the Application for connection of subscribers to the RBS/SMS to the mobile phone number specified by the Customer in the Application for connection of subscribers to the RBS. Used at the first login to the RBS, and if the RBS Subscriber has forgotten his/her Password. The E-mail/SMS message contains, in addition to the temporary password, its validity period, during which the Subscriber must independently log into the RBS and change the Temporary Password to a permanent one.

The electronic signature private (secret) key is a key (sequence of bytes) independently generated by the Subscriber using the means of RBS designed to form an Electronic Signature in Electronic Documents.

Application on RBS Rules Accession (Application) – is an Application on Remote Banking Rules Accession (Annex No. 1 to RBS Rules),

Application for connection of Subscribers to the RBS (Application) – is an application for registration for further connection of Subscribers to the RBS (Appendix No. 2 to the RBS Rules).

Application for blocking/unlocking access to RBS/issuing of password login/issuing password/login (Application) is an Application for blocking/unlocking access to remote banking system/issuing password/login (Appendix No. 5 to RBS Rules). Within the framework of restricted access, only viewing account information is provided, without the right to sign Electronic documents in the RBS.

Identification is the process of confirming the Subscriber's rights to perform certain actions in the RBS according to the list of rights established in the RBS and granting the rights to perform these actions in the manner provided by the RBS Rules.

Samples Card is a card with samples of signatures and the company's seal.

The Customer is a legal entity (other than credit institutions) having an Account(s) with the Bank and having entered an RBS Agreement with the Bank.

The key medium is the material medium of the Private (Secret) key.

Electronic Signature Key is a unique sequence of characters known to the Subscriber – owner of the Electronic Signature Verification Key Certificate designed to be created for Electronic documents Signature.

Electronic Signature Key Compromise is an event determined by the Party (Subscriber - owner of Electronic Signature Key Certificate) as familiarization of the unauthorized person () with its Private Key.

Correct Electronic Signature is a confirmation of the authenticity of the Electronic Signature in the Electronic Document is a positive result of verification of the corresponding Electronic Signature in the Electronic Document to the RBS Subscriber the lack of distortions in the Electronic Document signed by this Electronic Signature.

Login is a unique set of letters, numbers and symbols, which is used by the RBS Subscriber to enter the RBS. Used in conjunction with Password.

Operating day is the period of time established by the Bank during which the Bank receives settlement (payment) documents other than documents from the Customer and executes them by the current date. The duration (beginning and end) of the Operating Day shall be fixed by regulatory documents of the Bank.

Electronic signature public key (Verification Key) is a key (sequence of bytes) of electronic signature, depending on electronic signature key, independently generated by the RBS Subscriber using the RBS means intended for Identification of the person who signed the information in electronic form.

Password is a combination of numbers and/or letters, which allows to Authenticate to the RBS Subscriber when login to the RBS.

Password requirements for RBS Subscribers:

- Use a unique and complex password:

- password length - at least eight characters (from 8 to 20);

- a reliable password must contain all types of characters: capital letters, numbers, symbols;

- the password must not contain a sequence of identical characters and groups of characters, personal information (for example, name, date of birth, phone numbers), popular (known) passwords (for example, Passw0rd, Qwerty123);

- password should not match previous (previously used) passwords;

- the password must not match the passwords used in another system (e-mail, personal account, social networks, etc.);

- Mandatory periodic password change shall be carried out at least once every three months;

Remote Banking Rules (RBS Rules) - these Rules for Remote Banking of Customers - legal entities (except credit institutions) of AO Mizuho Bank (Moscow), which determine the procedure for operation of the Remote Banking System for legal entities (except credit institutions), as well as the procedure for interaction between the Bank and the Customer within the framework of this RBS.

Rules of the Service "Faktura.ru" - rules published on the Internet on the website https://bank.faktura.ru/rules, which determine the procedure for the operation of the Service "Faktura.ru," conditions for use by participants of the Service "Faktura.ru," as well as the procedure for joining participants to the Rules of the Service "Faktura.ru."

"BeSafe" System Rules - rules of electronic document flow of the corporate information system "BeSafe," a local regulatory act published on the Internet on the www.besafe.ruestablishes general principles, procedure and conditions for information interaction and electronic document flow when using the System "BeSafe."

Certification Center Operation rules are a local regulatory act published on the Internet on the https://info.authority.ru/Home/License website, and establishes the general principles, procedure and conditions of operation of the Certification Center "AUTHORITY," as well as determines the procedure and conditions for creating and issuing Certificates by the Certification Center, the terms of validity of Certificates, the procedure for updating the Certificate and terminating their validity.

Simple Electronic Signature is an electronic signature which by using one-time SMS passwords sent to the Subscriber's mobile phone number of the Subscriber of the RBS/E-mail, to the e-mail message specified by the Customer in the Application for connection of subscribers to the RBS and confirms the formation of the Electronic Signature by the Subscriber - the owner of the Simple Electronic Signature.

One-time SMS/E-mail-password is a unique character set used for Subscriber Authentication purposes when logging into the RBS. A one-time SMS/E-mail-password is provided to the Subscriber of the RBS for the mobile phone number/e-mail provided by the Customer for connection of subscribers to the RBS or other forms of Applications, in a form of SMS/E-mail-message, has a limited validity period. Actions in the

RBS confirmed by a one-time SMS/E-mail-password are considered to be performed by the RBS Subscriber personally.

The Bank's website is Bank's official Internet-site, located at https://www.mizuhogroup.com/ru/emea/russia, contains information about Bank's banking products and services, as well as other information necessary to the Customer.

Faktura.ru service is an information technology service that allows participants to organize the exchange of electronic documents, SMS messages, PUSH/E-mail messages or other information.

Electronic signature verification key certificate (Certificate) is an electronic document with the electronic signature of the Certification Center, the agent of which is the Bank. Includes Electronic signature Verification Key of the Subscriber – owner of electronic signature Verification Key Certificate is issued by System participant to confirm the authenticity of the electronic signature identification of the Subscriber - owner of Electronic Signature Verification Key Certificate. Used each time you log in to the RBS, send and sign Electronic Documents.

"BeSafe" System is a corporate information system "BeSafe," which is a set of software, information and hardware that implements electronic document management in accordance with the Rules of the "BeSafe" System. Organized by Center of Digital Certificates Closed joint stock company INN 5407187087, PSRN 1025403189602 for providing contractual and technological conditions of formation and development of financial and information electronic service. It is a common system for a number of services whose users can carry out legally significant electronic document management using an electronic signature.

The Internet-Bank Remote Banking System (RBS) is a corporate remote banking information system which is a set of software, information and hardware that implements electronic document management through telecommunication channels between the Parties for the Customer to conduct transactions on Bank accounts using electronic documents and transfer other information related to the Customer's banking services. The RBS is implemented on the basis of "Faktura.ru" Service which provides information and technological interaction between the Customer and the Bank. Instructions of the user "Internet Bank Faktura.ru" for Customers are posted on the Internet on the website www.Faktura.ru.

Parties are jointly mentioned Bank and Customer.

Account is the Customer's bank account opened in the Bank on the basis of the Bank Account Agreement concluded between the Parties in relation to which Electronic Documents are exchanged through the RBS.

Bank's tariffs (Tariffs) are the Bank's tariffs for settlement and cash service of Customers - legal entities.

Enhanced Unqualified Electronic Signature is an electronic signature that is obtained as a result of cryptographic conversion of information using an electronic signature key; allows to identify the person who signed the Electronic Document and to detect the fact of making changes to the Electronic Document after the moment of its signing; is created using electronic signature tools.

SMS/E-mail-authentication is a service that is a method of additional security verification:

- upon entering RBS by sending a one-time SMS password to the Subscriber's phone number and its subsequent input to the RBS by the RBS Subscriber. Login to RBS will be allowed if one-time SMS password entered within the required period coincides the one-time SMS password sent to the Subscriber number specified in Application for Accession to the RBS Rules;

Device for working with the RBS (Smart Key) is a personal device for Authentication and secure data storage which stores the generated Subscriber Certificate.

Electronic signature – is an information in electronic form that is attached to other information in electronic form (signed information) or otherwise related to such information that is used to identify the person signing the information (Electronic document). Types of electronic signatures in accordance with the Federal Law of 06.04.2011. No. 63-FZ On electronic signature are a simple electronic signature and an enhanced electronic signature. Enhanced unqualified electronic signature and enhanced qualified electronic signature differ.

E-mail is the electronic address of the Subscriber/Customer used to send the second authentication factor of the RBS Subscriber, as well as other information for operation in the RBS.

Requirements for electronic addresses for operation of the RBS:

- Postal addresses must be bound to the Customer's corporate domain;
- To send the second authentication factor, addresses registered on public e-mail services are not allowed (for example, @ yandex.ru, @ gmail.com)

Electronic Document is a collection of bytes containing a document, an order to perform an Account transaction or an information message generated using RBS presented in electronic digital form and certified by the electronic signature to the Subscriber.

An e-mail message is a message generated within the framework of the RFC 2822 standard, used to transmit information in networks operating over TCP/IP.

An SMS message is a short message used to transmit information in cellular networks using a mobile phone, up to 160 characters in 7-bit GSM encoding in accordance with the GSM 03.38/3 GPP 23.038 specification or up to 70 characters in a different encoding.

1. General conditions

1.1. These RBS Rules define the provisions of the RBS Agreement between the Bank and the Customer common to all Customers.

1.2. Current versions of the RBS Rules and Applications for Accession to the RBS Rules (Appendix No. 1 to the RBS Rules) are posted on the Internet information and telecommunication network on the Bank's Website.

1.3. These RBS Rules are established in accordance with the legislation of the Russian Federation and national standards of the Russian Federation in terms of ensuring information security and information protection, the requirements of the Bank of Russia, the requirements of federal executive authorities authorized in information security, communications, information technology and mass communications.

1.4. The obligatory condition for the conclusion of the RBS Agreement is the Customer's opened Bank account operations on which are planned to be carried out using RBS.

1.5. The RBS Agreement shall be concluded by the Customer submitting to the Bank a signed Application for Accession to the RBS Rules (Offer), including one signed and sent using the BSS remote banking service (Banks Soft Systems), accepted by the Bank through the transfer of the Smart Key/or the issuance of the Certificate of the electronic signature verification key/or sending a login to the RBS in accordance with the RBS Rules.

1.6. Based on the Application for Accession to the RBS Rules, the RBS Subscriber shall be granted access to all Accounts opened with the Bank at the time of submission of the Application. All Accounts opened by the Customer are connected to the RBS without additional statements of the Customer.

1.7. The RBS Rules define the conditions and the procedure for Parties to exchange Electronic Documents using RBS.

1.8. The RBS Rules are developed considering the provisions of the "Faktura.ru" Rules, Certification Center Rules and the “BeSafe” Information System Rules and apply by the Parties to the extent applicable to the relations of the Parties and not contrary to the provisions of these rules.

1.9. Servicing the Customer under the RBS shall be performed by the Bank in accordance with the current legislation of the Russian Federation, regulations of the Bank of Russia established in accordance with them by banking rules, customs used and international practice by international rules, as well as the terms of the RBS Rules. In case of changes in the legislation of the Russian Federation, regulations of the Bank of Russia, RBS Rules until the moment of their change by the Bank, shall be applied in part that does not contradict the requirements in the legislation of the Russian Federation and the regulations of the Bank of Russia.

1.10. The Customer, by submitting the Application for Accession to the RBS Rules, confirms that it is familiar with and agrees with the RBS Rules, Rules of Service "Faktura.ru," Rules of operation of Certification Center "AUTHORITY" and Rules of corporate information system "BeSafe," current versions of which are posted on official websites on the Internet, and is aware and agrees that these rules may be unilaterally modified by their owners, therefore, undertakes to monitor these changes and comply with the above rules.

1.11. The terminology used in the RBS Rules which begins with capital letters, shall be used in the meaning specified in the "Faktura.ru" Service Rules, the "AUTHORITY" Certification Center Rules and the “BeSafe” Information System Rules, unless otherwise expressly provided by the RBS Rules.

2. “Internet Bank” Service

2.1. The Parties using the Internet Bank Service, shall exchange and sign Electronic Documents[1] (subject to the authority of the person who sent and signed the document) related to:

2.1.1. Operations:

- cashless money transfers (payment order);
- foreign currency transactions (application for foreign currency transfer, order for the purchase of foreign currency, order for the sale of foreign currency, order for the conversion transaction, order for the transit currency account, notification of the crediting of foreign currency, notification of the crediting of the currency of the Russian Federation, as well as other documents provided for by the currency legislation of the Russian Federation);
- other transactions established by the Bank.

2.1.2. Sending messages/letters/other documents to the Bank. The methods of determining the person who signed the above documents are established by Section 3 of the RBS Rules.
The Parties shall also exchange other Electronic Documents necessary for the Parties to perform the obligations established by the RBS Agreement, the legislation of the Russian Federation, as well as in the framework of other service agreements with the Bank providing for this exchange.

2.2. operation conditions of the RBS are specified in Section 3 of the RBS Rules.

3. RBS connection and operation conditions

3.1. Connection to the RBS is made if the Subscriber has the access that meets the RBS requirements.

3.2. Before connecting to the RBS the Customer shall specify one of the ways of Subscriber’s connection (if technically available):

- by Login and Password and additional SMS/E-mail-authentication;
- by Certificate using Smart Key and additional SMS/E-mail authentication.

3.3. When connecting the Subscriber to the RBS using the Smart Key:

3.3.1. The Bank within 3 (Three) working days from the moment of submission of the Application to Accession to the RBS Rules and the Application for Connection of Subscribers to the RBS:

- provides the Subscriber with the RBS software and documentation on the RBS operation procedure; additionally, the instructional material is posted on the Bank's Website, as well as at the following address https://business.faktura.ru/f2b/faq;
- provides a Key Medium (Smart Key) with means of producing Display Keys (Private (Secret) and Display Verification Keys (Public Keys)).

3.3.2. The electronic signature keys (smart keys) in the Bank's office or otherwise shall be transmitted by the Bank's representative to the Customer's representative or Subscriber under the Smart Key Acceptance Certificate (Appendix No. 6 to these Rules). The Smart Key Act shall be drawn up in two (2) copies, one for each of the Parties.

3.3.3. In exceptional cases determined by the Bank, the means of access to the RBS can be delivered to the Customer Subscribers by courier service, subject to measures that exclude uncontrolled access during delivery. Access kits, as well as documents to be signed by the Customer, shall be placed in a strong package (safe package) for forwarding. Packages are sealed in such a way that the contents cannot be removed from them without disturbing packages and printing. Documents signed by the Customer shall be returned by courier delivery or by mail by registered mail.

3.3.4. Creation of Private (Secret) and Public keys, PIN-codes and secret passwords is carried out in accordance with the RBS requirements.

3.3.5. Connection to the RBS is confirmed by the Certificate, the fact of which is confirmed by RBS Subscriber by the Certificate of Acceptance (Appendix No. 3 to the RBS Rules).

[1] The list of documents is not closed and applies in part that does not contradict at the time of transfer of information to the legislation of the Russian Federation.

3.3.6. Operations in the RBS shall be carried out by the RBS Subscriber from the moment of signing of Acceptance Certificate and passing it to the Bank. The Certificate transmitted by the Bank to the Subscriber of the RBS is formed on the basis of the Application for issuance of the Certificate of the electronic signature verification key in the form of Appendix No. 4 to the RBS Rules, taking into account the requirements established by the current legislation.

3.3.7. The Certificate is valid for 365 calendar days from the date and time of its generation (manufacture). Renewal of the Certificate validity period is executed by issuing a new Certificate with the mandatory key change until the Certificate validity period expires. At the same time:

- in case of change of persons having the right to sign Electronic Documents, change of data identifying the Customer, change of electronic signature keys, in other cases terminating the Certificate, the Certificate shall be replaced in the manner provided for its execution when connected to the RBS;
- change of electronic signature keys shall be made immediately in case of threat of unauthorized access to Accounts, software and hardware of the RBS Subscriber or suspicion of copying the Keys by third parties, changes in the composition of persons having access to the RBS (having the right to use the Private (Secret) Key).

3.3.8. The Customer recognizes the electronic signature method functioning in accordance with GOST R 34.10-2018 (and previously GOST R 34.10-2012) and used in the RBS when transferring Electronic Documents from the Subscriber to the Bank, as well as the fact that:

- when selecting a method of login (Identification and Authentication) to the RBS using the RBS Subscriber electronic signature recorded on the Smart Key, the RBS Subscriber (within the current session) uses the RBS Subscriber electronic signature recorded on the Smart Key to sign all Electronic Documents sent to the Bank;
- if the Electronic Document is arbitrarily modified after transmission, the electronic signature and the amended document shall be invalidated;
- knowledge of information transmitted between the Parties via the System communication channel does not lead to compromise of the Parties' Closed (Secret) signature keys;
- forgery of the RBS Subscriber electronic signature, i.e. creation of the correct Electronic Document electronic signature on behalf of the Customer, is impossible without knowledge of the RBS Subscriber electronic signature Key (Private (Secret) electronic signature key);
- created in a single instance of the Private (Secret) Key of the RBS Subscriber electronic signature is unique, the creation of a duplicate of the Private Key is possible only by the RBS Subscriber or if the RBS Subscriber violates the conditions of storage and/or use of the Private Key;
- is responsible for keeping secret of his electronic signature Keys, PIN-codes, Passwords, for correctness of filling in and execution of Electronic Documents and for actions of his personnel when working with the RBS;
- The Public Key of the RBS Subscriber electronic signature specified in the Certificate certified by the signature (s) of the authorized person (s) and print (if any) of the Customer is owned by the RBS Subscriber.

3.3.9. The bank on the basis of the Declaration of accession signed by the CustomerRBS Rules and Applications for connection of subscribers to the RBS (Appendix No. 1 or Appendix No. 2 to RBS Rules) / applications is a free form for shutdown of the RBS / Application for a blocking/unblocking of access to the RBS/issue of the login of the password (Appendix No. 5 to RBS Rules) (further - the Statement):

- generation of the Login and, if necessary, sending it to the electronic mail of the RBS Subscriber specified in the Application;
- sending the Temporary Password for entering the RBS to the e-mail or Subscriber's mobile phone number of the RBS Subscriber specified in the Application (at the same time, the RBS Subscriber is obliged to change it during initial Authorization in the RBS).

3.3.10. When you select the login method (Identification and Authentication) for the RBS (Internet Bank) by Login and Password, the Subscriber of the RBS (the current session) uses the electronic signature in form of Login/Password/One-time SMS/E-mail-password to log into the RBS. At the same time, the Subscriber of the RBS with the login method and the Password has the right to create documents, save them in the RBS, view statements and other information.

3.4. Electronic documents, the forms of which are provided in the RBS, as well as other documents, RBS and issued by the Subscriber and sent to the Bank, outside the approved forms, including references, inquiries, letters, addresses, statements, applications, documents, provided as part of the Customer information update, other documents provided by the Customer at the Bank's request, certified by the RBS Subscriber's electronic signature are recognized as legally equivalent to the relevant documents on paper signed by the authorized person by the Customer's person (s) and certified seal (if paper documents are to be certified by the Customer's seal), provided that the Customer's Private (Secret) Key, electronic signature and Certificate are created in accordance with the "BeSafe" System Rules, "Faktura.ru" Service Rules.

3.4.1. The Parties acknowledge that questionnaires and other documents executed by the Customer and sent to the Bank, outside the approved forms, including references, inquiries, letters, appeals, statements, applications, documents provided within updating of information about the Customer other documents provided by the Customer at the Bank's request, except for the Card and other documents, accepted only in paper form according to the annexes to the General Conditions for Opening and Maintaining Accounts of Legal Entities and Individual Entrepreneurs - Customers of AO Mizuho Bank (Moscow), "may be transmitted via the RBS as in a scanned copy of the document on paper with the signature of the authorized representative of the Customer and the seal of the Customer (if available) on a document as files (in jpeg, pdf, tiff, rtf formats) as part of the Appendix to the Electronic Document signed by RBS Subscriber's electronic signature and have legal force.

3.4.2. contracts/agreements between the Bankthe Customer provide for signing of the Electronic Document of electronic signature/several persons, the electronic documents shall be recognized as such only if all necessary signatures are available.

3.4.3. When creating the Electronic Signature of the RBS Subscriber:

- the person making the EP shall be shown the content of the information signed;
- EP is created only after confirmation by the person signing the electronic documents;
- displays the fact that the display is created.

3.4.4. When verifying the Electronic Signature:

- shows the contents of the electronic documents signed by the electronic signature, including visualization of this electronic signature, containing information that the document is signed by the electronic signature, as well as the number, Subscriber and period of validity of the electronic signature Verification Key Certificate;
- making changes to the signed electronic document is displayed.
- Specify the person whose electronic signature Key is signed the electronic document.

3.4.5. The Bank reserves the right, after carrying out control procedures provided by the current legislation of the Russian Federation and regulations of the Bank of Russia, in relation to documents received by the Bank from the Customer in case of non-conformity/contradictions, as well as in case of doubts about their reliability, to request original documents to establish their compliance by the Bank's employee.

3.5. Electronic documents containing statements of the Customer's Accounts and attachments to them, currency control documents, notifications, messages and requests from the Bank, including requests for supporting documents, other documents sent to the Customer using the RBS, are legally equivalent to the relevant documents on paper signed in accordance with the established legislation of the Russian Federation and banking rules. Copies of documents requested by the Bank and transmitted using the RBS are legally equivalent to copies on paper, if this method of submission meets the annexes to the General Conditions for Opening and Maintaining Accounts of Legal Entities and Individual Entrepreneurs - Customers of AO Mizuho Bank (Moscow) or the Bank in the request indicated the possibility of submitting such documents through the RBS.

3.6. As part of connection to the RBS as well as during operation it the RBS Subscriber creates a Password for entering RBS if necessary and can change the previously created Password.

3.6.1. Creation (issuance) of Password for login to the RBS can be performed in the following ways:

- by sending by the Subscriber of the RBS an Application for blocking/unlocking access to the RBS/issuing a password login/issuing password/ login (Appendix No. 5) by e-mail to the technical support of the Bank of support@mhcb.ru;
- by personal contact of the RBS Subscriber to the Bank, providing the Application for blocking/unlocking access to the RBS/issuing the password login/issuing password/ login (Appendix No. 5).

3.6.2. Password change service is provided by the Bank and free of charge.

3.6.3. The password is sent to the RBS Subscriber to the mobile phone specified in the Application. Upon first login, the Subscriber changes the temporary password sent by the Bank to a permanent one[2].

3.6.4. Remote Password Change Service is provided by epy Bank in case of no technical restrictions for its implementation.

3.6.5. part of the Remote Password Change Service:

3.6.5.1. The Bank may:

- block access to the RBS if there are reasonable suspicions of compromising the Subscriber key of the RBS and/or other circumstances that may lead to financial and other costs of the Customer and/or the Bank;
- contact the Customer by trusted telephone to confirm the request by e-mail to obtain a remote Password change service;
- at its discretion or by the decision of the Service OPERATOR "Faktura.ru" as part of measures to manage information and financial risks in cases where failure to take measures may lead to a threat to the regular operation of the RBS and/or the Faktura.ru Service or the occurrence of risks (property, reputation, operating, other) for the Customer, the Bank and other participants of the "Faktura.ru," due to disruption of communication channels, power outages and others, technical faults beyond the Bank's control that make it impossible to exchange Electronic Documents, has the right to restrict the functionality of the RBS and/or Service "Faktura.ru" or to completely disable the functionality of the RBS and/or Service "Faktura.ru," that subsequently may not be the basis for any claim by the Customer of the Bank, including in terms of compensation for losses incurred in this regard.

3.6.5.2. The Subscriber may:

- make in Bank on the RBS an inquiry on change of the Password personally or by e-mail of technical support of support@mhcb.ru; E-mail shall be addressed from a mail address bound to the Customer's corporate domain.

3.6.5.3. The Subscriber and the Customer shall:

- immediately, not later than 24 hours, contact the Bank through the official communication channels during the Bank's working hours (telephone +7 (495) 212-03-33, +7 (495) 212-03-40, technical support phone support@mhcb.ru) and act according to the instructions of the Bank's employee if there are reasonable suspicions that the data of the electronic signature/entry key of the RBS Subscriber became known by third parties. The Bank bears no financial, legal and other responsibility for the costs incurred by the Customer in case of compromising the electronic signature key.

3.6.5.4. The Customer shall:

- Agree/ensure prior consent of the Subscriber to receive newsletters via the mobile radiotelephone network and other information technology materials (including SMS-MESSAGES, PUSH-MESSAGES, E-MAIL-MESSAGES) from the Bank and other third parties, participating in information and technological maintenance of the Customer within the RBS, including receiving SMS messages, the INDIVIDUAL TEXT NUMBER or from the text number "Faktura.ru" on all phone numbers, e-mail addresses and other contact data provided to the Bank for the purposes of servicing the Customer in the RBS, and subsequent submission of this information on the consent of the Bank and the Bank to third parties, as well as compensation by the Customer for losses of the Bank due to failure to perform or improper performance of this obligation;
- agree and ensure that the Bank may transfer to the OPERATOR the "Faktura.ru" Service and the TECHNOLOGY PARTNERS any information for the purposes of service under the RBS in accordance with the Bank's documents and procedures;
- To ensure the consent of the Subscriber (and other personal data subjects) to the processing of personal data transferred to the Bank for the purposes of ensuring the exchange of information and the provision of services within the framework of the RBS, the conclusion and execution of the RBS Agreement, with the right to further instruct the Personal Data Processing Bank to the Faktura.ru Service Operator and TECHNOLOGY PARTNERS.

3.7. Remote renewal of the Certificate is carried out by the Customer in accordance with the User's Instruction "Internet Bank Faktura.ru" F. Business "Remote renewal and receipt of the certificate," posted on the Internet at www. Faktura.ru.

[2] Password requirements are specified in Terms and Definitions, Password

3.7.1. The Bank shall notify the RBS Subscriber of the need to renew the Certificate 30 (thirty) calendar days before the Certificate expires.
3.7.2. If the RBS Subscriber has not updated the Certificate before its expiration, the Customer Certificate is automatically blocked in the RBS.
3.7.3. The Certificate is also blocked due to compromising/suspicion of compromising, in case of change of the name or form of the Customer/change of the person performing the functions of the sole executive body of the Customer (sole executive body), at the end of the sole executive body term of office, as well as in case of change of other information required for identification of the Customer, provided by the current legislation and regulations of the Bank of Russia.
3.7.4. To renew the Certificate, the Subscriber in the RBS goes to the page of the Certification Center, when passing through which the Subscriber completes the Request for a technological certificate.
3.7.5. Upon receipt of the Bank's electronic Request for Technological Certificate, the Bank shall send in response to the Subscriber a link to download the updated Certificate, after which the Subscriber shall save the updated Certificate.
3.7.6. The Bank shall, not later than the working day following the day of receipt from the Subscriber of the electronic Application issuing the Certificate and the Certificate of Acceptance and Transfer, ensure that the Subscriber can use the electronic signature in RBS certified by the new Certificate. At the same time, the Subscriber ceases to use in the RBS the electronic signature certified by the Certificate previously issued to him, if the use of the specified electronic signature is not terminated due to the expiration of the Certificate.

4. Customer Service Procedure

4.1. The Bank carries out operations on the basis of Electronic Documents provided that they comply with the requirements of the legislation of the Russian Federation, the Bank Account Agreement, the formats established by the RBS, if there is a Correct electronic signature, if there are funds in the Customer's Accounts for the transaction.
4.2. In case of non-compliance of the Electronic Document with the requirements specified in Clause 4.1. of the RBS Rules as well as the provisions of the agreements concluded by the Parties in the event of a threat of unauthorized access to Accounts and hardware, the receipt of damaged documents, if the Customer's Accounts do not have sufficient funds to carry out the transaction, the Bank refuses the accept of documents, notifying the Customer about this.
4.3. Electronic Documents shall be accepted by the Bank during the Operating Day. An electronic document received after the end of the Business Day shall be deemed to be accepted on the next Business Day.
4.4. Acceptance of Electronic Documents is confirmed by the Bank's electronic notification via RBS. The Customer confirms that the time of the documents receipt is the current time for the system of Bank's hardware.
4.5. For each Operating Day the Subscriber in the RBS has a cash flow statement for the Account.
4.6. Connection, modification or disconnection of services related to operation of System as well as functional set of RBS itself is performed:

- Upon Application on Accession to the RBS Rules (Appendix No. 1 to the RBS Rules) at the same time as accession to the RBS Rules, Application for Connection of Subscribers to the RBS (or Appendix No. 2 to the RBS Rules) and initial installation of the RBS;
- upon application in free form for shutdown of the RBS during use of the RBS;
- Upon application for blocking/unlocking of access to the System (Appendix No. 5 to the RBS Rules) in the process of using the RBS.

4.7. If no confirmation of the order is received from the Customer in accordance with Clause 4.1. RBS Rules and/or information requested in accordance with item 4.2. The RBS Rules, the Customer's order shall be deemed to be non-enforceable.

5. Settlement Terms

5.1. The costs for services for RBS connection and its usage, the procedure and term of their payment are determined by the Bank's Tariffs.

5.2. Payment of the cost of services under the RBS Agreement is made by debiting without additional order (acceptance) of the Customer the funds from the Customer's Account with the Bank in the manner established by the General Conditions for Opening and Maintaining Accounts of Legal Entities and Individual Entrepreneurs - Customers of AO Mizuho Bank (Moscow).

5.3. In accordance with paragraph 1 of Article 450 of the Civil Code of the Russian Federation, the Parties agreed that the Bank has the right to amend the RBS Rules and the Bank's Tariffs. The Customer shall be informed about the changes in the RBS Rules and Tariffs not less than 10 (Ten) working days before the effective date of such changes, by notifying the Customer, including through the RBS and/or by placing information on stands in the Bank's offices or on the Bank's Website.

5.4. Absence of the Customer's refusal of Internet-Bank remote banking services (termination of the RBS Agreement), as well as the Customer's first (from the date specified in the Bank's information on changing the RBS/Tariff Rules) operation by means of the RBS, are the Customer's consent to the new RBS Rules (taking into account the annexes thereto) and the application of the Bank's new Tariffs.

5.5. In case of disagreement with changes and/or additions made to the RBS Rules and/or Bank Tariffs, the Customer shall have the right to apply to the Bank for termination of the RBS Agreement before such changes or additions come into force.

5.6. In case of payment according to the Bank's Tariffs the Bank has the right to temporarily disconnect from the RBS in the manner specified in Clause 6.1.5 until the Customer pays the debt fully.

6. The Bank’s rights and obligations

6.1. **The Bank may:**

6.1.1. After a preliminary warning to the Customer, suspend or terminate the use of the RBS by the Customer in the following cases:

- based on the relevant Application received from the Customer;
- non-payment of monthly fee for use of the RBS according to the Bank's Tariffs within 10 (working days) from the day following the date of non-payment (last working day of the month)
- other cases established by the General Conditions for Opening and Maintaining Accounts of Customers-Legal Entities and Individual Entrepreneurs of AO Mizuho Bank (Moscow), internal regulatory documents of the Bank and regulatory acts of the Russian Federation.

The resumption of services is carried out after the reasons for the suspension of the service have been eliminated.

6.1.2. Temporarily disconnect the Customer from the RBS without prior notice in the following cases:

- refusal of the Customer from timely submission of the Application for blocking/unlocking of access to the RBS/issuance of the password login in connection with change of officials - until the corresponding Application is submitted and executed.
- compromise of the electronic signature Key, or other violations of the protection mechanisms when the Customer provides the Application for blocking/unlocking access to the RBS/issuing the password login in connection with the compromise - before the submission and execution of the corresponding Application.

6.1.3. Change the forms of documents to the RBS Rules, the procedure for providing remote banking services as well as changes and additions to RBS Rules, Bank Tariffs in cases and in order established by the legislation and the RBS Rules.

The Customer shall be informed of the changes not less than 10 (Ten) working days before the date of such changes, by notifying the Customer, including by means of the RBS and/or by placing information on stands in the Bank's offices or on the Bank's website.

6.1.4. Refuse to conclude the RBS Agreement.

6.1.5. After a preliminary warning, suspend the provision to the Customer of the RBS, including the right to refuse the Customer to accept orders from him in electronic form for the transaction of Accounts signed by the Electronic Signature, without explanation.

6.1.6. case of refusal to accept the document for execution, send to the Customer the information on cancellation of the document indicating the reason why the document will not be executed by the Bank.

6.1.7. Charge the Customer for service in the RBS and other services in the framework of the RBS Agreement a commission in accordance with the Bank's Tariffs by debiting without additional order (acceptance) of the Customer funds from the Customer's Account with the Bank in accordance with the procedure established by the RBS Rules.

6.1.8. Suspend the operation of the RBS for routine, preventive and other work, as well as if it is necessary to apply measures to manage information, financial and other risks, when failure to take, these measures may lead to a threat to the safety of the RBS.

6.1.9. framework of the risk management system implemented by the Bank and in accordance with the RBS Rules, suspend the Customer's use of the RBS for the period of finding information related to such Customer and (or) its RBS, in the database of cases and attempts to make money transfers without the voluntary consent of the Customer if the Bank received information from the Bank of Russia contained in the database of cases and attempts to make money transfers without the voluntary consent of the Customer, which contains information related to the Customer and/or its RBS.

6.2. **The Bank shall:**

6.2.1. Accept for execution the Electronic documents received under the RBS, executed and signed in accordance with the requirements of the RBS Rules.

6.2.2. Stop receiving Electronic Documents at the moment of receipt of notification from the Customer on Application for blocking/unlocking of access to the RBS/issuing of password login.

6.2.3. Perform the procedure of Identification, Authentication, Authorization of persons working in the RBS.

6.2.4. If it is impossible to provide services in the RBS for technical or other reasons, place the information in one of the following ways: in the RBS send the information to the Subscriber/Customer by e-mail, notify by phone, by posting on the Bank's Website.

7. The Customer’s obligations

7.1. **The Customer may:**

7.1.1. After registration of the Keys, the Electronic Documents shall be sent to the Bank by means of the RBS in accordance with the procedure established by the RBS Rules.

7.1.2. Contact the Bank by telephone for free consultations related to Customer service as well as operation of the RBS. In order to obtain information about operation in the RBS (except for information constituting bank secrecy), the Customer shall give the name of the Customer’s first name and patronymic of the Subscriber when the Bank remotely by telephone.
The Bank's unlimited number of Customers has the right to receive telephone information related to service issues in RBS, and Customer's employees have the right to receive:

- a person who is the executive body of the Customer (in relation to legal entities);
- another person of the Customer holding a valid Certificate and/or Login and Password for working in RBS (Subscriber).

7.1.3. At any time stop the transfer of Electronic Documents by issuing an application in free form for disconnection of the RBS.

7.2. **The Customer shall:**

7.2.1. Implement basic recommendations for information protection during operation in the RBS posted on the Bank's Website (https://www.mizuhogroup.com/ru/emea/russia/service?tab=remote-banking).

7.2.2. Inform the Bank about the detection of unauthorized access to the RBS.

7.2.3. Ensure availability of maintenance of protection of RBS software installed. Follow recommendations to ensure information security when working in the RBS located at the following address https://business.faktura.ru/f2b/faq.

7.2.4. Timely pay for connection to the RBS, maintenance and other services of the Bank related to the use of the RBS in accordance with the procedure and conditions established by the Bank's Tariffs.

7.2.5. Ensure regular familiarization with the information published on the Bank's Website sent by the RBS by e-mail of the Subscriber specified in the Application.

8. Joint obligations and responsibilities of the Parties

8.1. The Parties shall be responsible for the reliability of the information provided to each other within the framework of the use of the RBS.

8.2. The Parties shall be liable for non-fulfillment or improper performance of their obligations under the RBS Agreement in accordance with the current legislation of the Russian Federation.

8.3. The Bank shall not be liable for damage caused to the Customer as a result of the use of the EP Key by third parties who are not entitled to work with the RBS and give orders on the Customer's Account, as well as for the consequences of malware, including in connection with violation and/or improper fulfillment of the Customer's requirements for the protection of technical means (computer, laptop, tablet, mobile phone, etc.). The Customer understands the increased risk of unauthorized use of the RBS, including Compromise of the electronic signature Key/Certificate, Login, Password, one-time SMS/E-mail password and unauthorized remote management of the software and hardware used by the Subscriber to work in the RBS, if the Customer does not comply with security measures.

8.4. The Parties shall not be responsible for the operation of the Internet, its programs and protocols, as well as other telecommunication channels and communication systems, including wired and mobile telephone communications. Losses incurred by one of the Parties in case of their full or partial inoperability shall not be compensated by the other Party. No claims regarding the Internet, its programs and protocols, other telecommunication channels and communication systems shall be accepted or considered by the Parties.

8.5. The Bank shall not be liable for losses arising as a result of Subscriber's execution of Electronic Documents, disruptions, interference of the operation of the communication line used by the Subscriber, leading to the impossibility of documents transfer to the Bank to fulfill the obligations stipulated by the RBS Rules by the Customer.

8.6. The Bank shall not be liable for losses arising the refusal to accept or fail to comply with Customer's orders and cases stipulated by the current legislation of the Russian Federation and RBS Rules.

8.7. The initiator of communication with the Bank is always the Customer. The absence of the Customer's initiative in establishing communication sessions with the Bank does not entail the Bank's responsibility for failure to fulfill its obligations (including upon notification of the Customer about the Account transaction).

8.8. The Parties determined that the Bank may temporarily suspend the operation of RBS for no more than 2 (Two) hours a day, as well as in other stipulated by the RBS Rules. The temporary suspension by the Bank of the operation of the RBS shall not be the basis for claims by the Customer to the Bank, including in terms of compensation for losses incurred in connection.

8.9. The Parties undertake to ensure confidentiality of information about RBS technology.

8.10. Each Party shall, at its own expense, maintain its own software and hardware used in working with the RBS.

8.11. The Customer assumes the risks associated with the faulty operational condition of the hardware (computer, laptop, tablet) providing the possibility of receiving notifications from the Bank about the Account transactions with the use of the RBS.

8.12. In case of failure of RBS hardware or software or its elements, in other cases it is impossible to perform operations on the basis of Electronic Documents, as well as case of restoration of the System operability the Parties shall notify each other about this fact within 2 (Two) hours by any available method.

8.13. The Parties undertake to form and maintain archives for at least 5 (Five) years (case of disputes - until their resolution):
all public keys,
all incoming Electronic Documents in accepted form with electronic signature,
all outgoing ones - in initial form with electronic signature,
electronic form with electronic signature) on receipt of Electronic Documents,
free format messages signed by electronic signature.

electronic protocols of information exchange sessions,
are responsible for their integrity and credibility.

8.14. In case of conflict situations between the Customer and the Bank when using the RBS the Parties shall participate in the consideration of conflicts in accordance with Section 10 of the RBS Rules to comply with the requirements of this Section and be responsible according to the conclusions of the conflict situation.

8.15. The Parties shall participate in resolving economic and other disputes that may arise connection and use of RBS, provide writing their assessments, evidence and conclusions at the request of the interested party.

8.16. The Parties shall be exempt from liability for non-performance or improper performance of obligations taken upon signing of Application on accession to the Customer's RBS Rules in case of force majeure, which include natural disasters, fires, accidents, power outage, damage of communication lines, mass riots, strikes, military actions, unlawful actions of third parties, entry into force of legislative acts, acts of bodies of federal or local acts of the Bank of Russia binding on one of the Parties, directly or indirectly prohibiting the activities specified in RBS Rules or preventing the Parties from fulfilling their obligations in accordance with RBS Rules under the Bank Account Agreement, if the Party affected by their influence shall inform the other Party about the new incident as soon as possible after the occurrence of these circumstances.

8.17. The Bank shall not be liable if the Customer has not been familiarized with the information on the change of the terms of the RBS Agreement published in the manner and within the time limits established by these RBS Rules.

9. SMS/E-mail Authentication Service

9.1. The use of SMS/E-mail-authentication service is mandatory for the Customer when working with the RBS according to the Login and Password, as well as according to the electronic signature Key Certificate.

9.2. The SMS authentication service is provided to owners of cellular phones with technical capability.

9.3. E-mail authentication service is provided for Subscribers with corporate e-mail in case of technical capability.[3]

9.4. Regardless of the state phone of the Subscriber of the RBS the phone is off, the phone is range of the cellular operator's network phone is disconnected and non-payment of the cellular operator phone buffer is full etc., One-time SMS-password is considered delivered to the Subscriber of the RBS from the moment of its sending by the Bank.

9.5. Regardless of the state of Subscriber's email of the RBS: e-mail is full, the letter is sent for quarantine, blocked, etc., the one-time password is considered delivered to the Subscriber of the RBS from the moment of its sending by the Bank.

9.6. The Customer will not be reimbursed with the cost of incoming one-time SMS passwords (according to rates of the cellular operator) sent by the Bank as part of the SMS/E-mail authentication service.

9.7. The Parties agree that by the Customer (in relation to the legal entity - represented by its sole executive body or authorized person[4]) of the Subscriber of the cellular telephone at the moment of accession to RBS Rules, upon completion and signing of the Application, is sufficient confirmation that this number is the Subscriber's telephone number.

9.8. The Bank shall proceed to provide the Customer with SMS/E-mail authentication service no later than the day following after the day of receipt from the Customer duly executed paper Application signed by the Customer at the Bank's office (for new and existing Bank Customers).

9.9. **The Bank may:**

9.9.1. Unilaterally change the format of the one-time SMS/E-mail-password, the terms of sending of the RBS a one-time SMS/E-mail-password such changes to the Customer.

[3] Requirements for Subscriber's e-mail are specified in Terms and Definitions, E-mail

[4] When applying to the Bank of an Authorized Person who is not the sole executive body, the Client shall be obliged to provide documents confirming the authority of such person in accordance with the requirements of the Bank and the legislation.

9.9.2. Temporarily block SMS/E-mail authentication service without prior notification of the Subscriber, if in the opinion of the Bank such a measure is necessary to ensure the security of the RBS including the security of settlements in RBS.

9.10. **The Bank shall:**

9.10.1. Provide the authentication service to the Customer in accordance with the RBS Rules.

9.10.2. Terminate the SMS/E-mail authentication service in its entirety or the part specified by the Customer no later than the day following the day of receipt from the Customer the Application on change of parameters/disconnection of the RBS.

9.10.3. Suspend the provision of SMS/E-mail authentication service in the event of receipt a written statement an arbitrary form from individual whose Subscriber's cellular phone number was indicated by the Customer the Application that such individual does not agree to further receipt of information to Subscriber'sphone number of that person. The Bank shall notify the Customerreceipt of such written application of an individual.

9.11. **The Customer may:**

9.11.1. To instruct the Bank to send information in the form of one-time SMS/E-mail passwords to Subscriber numbers specified by the Customer.

9.11.2. any time one or more Subscriber Numbers to which information is sent in the form of one-time SMS/E-mail passwords by submitting an Application to the Bank for changing parameters/disconnecting the RBS.

9.12. **The Customer shall:**

9.12.1. case of change of Subscriber number, termination of authority of Customer's representative whose Subscriber number is indicated by Customer in the Application, loss or theft of Customer's cellular phone (Customer's representative), occurrence of other circumstances, as a result of which information transmitted by Bank may become available to unauthorized persons, immediately notify about it.

9.13. The Bank shall not be responsible for disclosing information constituting bank secrecy, including personal data contained n the documents submitted to the Bank as a result of the Bank's provision of SMS/E-mail authentication in cases when such information became available to unauthorized persons not through the Bank's fault in particular, but not limited in following cases:

- indication by the Customer of the incorrect Subscriber Number in the Application submitted to the Bank;
- theft or loss of the Customer's cellular phone (Customer's representative), the Subscriber number of which is indicated by the Customer in the Application submitted to the Bank;
- transfer by the Customer (representative of the Customer) of the cellular telephone to an unauthorized person;
- transmission by the Customer (representative of the Customer) of the received information to unauthorized persons;
- due to the fault of the telecom operator;
- Failure or delay in performance by the Customer of the obligations stipulated in Clause 9.11. of this Section.

9.14. The telecom operator shall be responsible for delivery or transfer rate of one-time SMS passwords and keeping secret of one-time SMS passwords in accordance with legislation of the Russian Federation.

9.15. The Bank shall not be liable for non-receipt/late receipt by the Customer (representative of the Customer) of one-time SMS/E-mail passwords not due to the Bank's fault as well as for possible losses or other adverse consequences for the Customer, in particular, but not limited to following cases:

- the Customer's cellular telephone (Customer's representative) does not support SMS (delivery, reception, etc.) functions or is technically faulty; SMS transmission (delivery, receipt, etc.) is not included in the list of services,
- failures/technical faults in communication networks and services of providers, service interruptions of telecom operators and providers, technical faults of equipment of telecom operators, other similar cases;
- Failure/improper fulfillment by the Customer of obligations to the telecom operator servicing it, in particular, in case of delay in payment of the telecom operator's services/availability of debts to the telecom operator, other similar;

- indication by the Customer of the incorrect Subscriber number of the Customer's cellular phone (Customer's representative) in the Application submitted to the Bank;
- theft or loss of the Customer's cellular phone (Customer's representative);
- transfer by the Customer (representative of the Customer) of the cellular telephone to an unauthorized person;
- disconnection of the Customer's telephone set (Customer's representative) or its location outside the communication network.

9.16. The Customer confirms that they have received written consent to subscribers - individuals to provide information about their Subscriber Numbers, E-mail, the Bank telecom operators subscribers - individuals have given written consent to send them information in accordance with the RBS Rules as well as process their personal data by the Bank in purpose of providing SMS/E-mail authentication service in accordance with the RBS Rules.

10. Procedure for resolution of disputes related to acceptance (non-acceptance) and/or execution (non-fulfillment) of Electronic Document in RBS

10.1. Any disputes (including disputes regarding and/or authenticity of a document transmitted using RBS signed by the Customer's Private (Secret) electronic signature Key for verification the electronic signature Verification Key Certificate registered in RBS shall be resolved between the Parties through negotiations. At the same time, on disputes regarding authorship and/or authenticity of the document transmitted to the RBS the Customer sends to the Bank a Statement signed and certified by printing (if any) according to the Card, in free forma description of the situation/claim.

10.2. Resolution of disputes related to work in the RBS for Customers using PES shall be carried out into account the conditions (requirements) specified in Sections 3 and 9 of the RBS Rules. At the time of resolution of the disputed situation, the Bank has the right to immediately suspend the acceptance/sending of EDs unilaterally. In this case, the Bank shall notify the Customer of the suspension of its work in the RBS according to the RBS or otherwise defined by the General Conditions for Opening and Maintaining Accounts of Legal Entities and Individual Entrepreneurs - Customers of AO Mizuho Bank (Moscow).

10.3. If it is impossible to resolve the dispute regarding and/or authenticity of the document signed by the Customer's Private (Secret) Key the participants shall have the right to use the procedure for resolving conflict situations and disputes **of the** "BeSafe» Rules.

10.4. If as result of the negotiations, the Parties have not reached an agreement, such a dispute will be submitted to the Moscow Arbitration Court in the manner established by the current legislation of the Russian Federation.

11. Final provisions

11.1. The RBS Agreement shall be deemed concluded and shall enter into force upon acceptance by the Bank the Application for Accession to the RBS Rules. The RBS Agreement is considered concluded in the city of Moscow for an indefinite period.

11.2. The closure of the Account shall terminate RBS Agreement in respect of the Account (the RBS Agreement shall continue to apply to remaining Accounts). The RBS Agreement shall be deemed terminated closing day the last of the Accounts providing for the use of the RBS.

11.3. The RBS Agreement may be terminated unilaterally out of court at the request of either Party:
on the Bank's initiative on any grounds, including if the Customer violates the requirements of the RBS Rules. In this case, the Bank shall notify the Customer not later than 10 (Ten) business days before the date of the proposed termination of the RBS Agreement by sending the relevant notification, including through RBS. The Bank's obligations to accept and execute Electronic Documents using the RBS shall be deemed terminated from the date specified in the notification.
on the Customer's initiative - in case of termination of the RBS Agreement, the Customer is obliged to contact the Bank and sign a free application to disconnect the RBS. The exchange of Electronic Documents between the Bank and the Customer shall cease date specified by the Customer in the

application for disconnection of the RBS. The RBS Agreement shall be deemed terminated as soon as the Parties have duly fulfilled all obligations assumed.

12.Applications

Appendix No. 1

Application for accession to the Remote Banking Rules

Appendix No. 2
Application for Subscribers connection to the RBS

Appendix No. 3

Certificate of acceptance/transfer of Electronic Signature Verification Key Certificate

Appendix No. 4
Application for Electronic Signature Verification Key Certificate

Appendix No. 5

Application for blocking/unlocking of access to the RBS/issuing of password login

Appendix No. 6

Smart Key Act

Appendix No. 7

Power of attorney