APPROVED BY PRESIDENT OF
AO “MIZUHO BANK (MOSCOW)”
Internal order No.84/22 of 14.12.2022

THE RULES

for provision of service in the Remote Banking System (RB System)
of
AO Mizuho Bank (Moscow)

Moscow

December, 2022/ Edition 10

Contents

1. General Provisions

1.1. These Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow) (henceforth – "the Rules") are an integral part of the Contract for rendering services related to remote banking system (henceforth – "the Contract") by AO Mizuho Bank (Moscow) (henceforth – "the Bank") and govern the procedure and conditions of:

- access and provision of remote banking system services (henceforth – "RB System") to corporate customers (expect for credit institutions);
- electronic document flow within RB System;
- consideration of dispute situations related to authenticity of electronic documents.
- ensuring information security within RB System

1.2. The Bank performs services rendering within RB System in accordance with the Contract and the Rules in effect at the moment of rendering a service.

1.3. Information traffic within RB System is performed through open channel communication with the help of Internet.

1.4. For the access to the Bank's RB System the Customer should arrange a workstation and prepare a personal computer in accordance with Requirements to soft hardware of the customer's automatic workstation (Appendix 1 hereto).

1.5. In the course of RB System operation, the Parties themselves take necessary measures ensuring functioning of their automatic workstations, communication channels and protection of electronic signatures' keys, passwords and automatic workstations resources from unauthorized access, at their sites.

1.6. Communication between the Bank and the Customer is performed through transfer and receipt of electronic documents to and from the Bank.

- Each electronic document transferred to the Bank should be signed by electronic signatures of persons which have the authorities for such actions commitment.
- Each electronic document transferred from the Bank signed by electronic signature of the Bank.
- Control of the rights of subscribers who signed an electronic document with their electronic signature is performed automatically by RB System in the course of processing of this document in the Bank.
- The list of electronic documents used within RB System is presented in Appendix 2 hereto.

1.7. An electronic document gives rise to rights and responsibilities of the Parties under this Contract, Bank Account Contracts, other Contracts which regulate cooperation with the use of remote banking system if an electronic document is duly prepared by the Transferring Party, verified by correct electronic signatures of persons which have the authorities for such actions commitment and transferred through remote banking system, and received by the Accepting Party.

1.8. Any attachments in electronic documents (including scanned copies of documents) are considered as the exchanging of documents, and representatives of the Parties, which used ES keys while sending electronic documents, confirm the identity of the scanned copies to

their originals and are responsible for consequences of using such documents by the other Party if such electronic documents have been signed by an electronic signature.

1.9. The validity period of electronic signature keys for RB System subscribers is set equal to13 (thirteen) months but not exceeding the validity period of the Subscriber's authorities. The subscribers are obliged to perform the planned electronic signature keys change in accordance with the procedure set forth in section 4 hereof.

1.10. The Bank carries out the processing of personal data of the Customer's authorized persons with the purposes of provision services to the Customer in the system of remote banking as well as provides their protection in accordance with the current legislation. The Customer guarantees the consent of the Customer's authorized persons to their personal data processing and transfer to the Bank.

2. Terms and definitions

2.1. **RB System Subscriber** is the Customer's authorized person registered in RB System having ES keys the certificates of which had been registered in the register of the Bank's Certification Authority and having authorities to perform some or all of the listed actions with the electronic documents: creation, signing, acceptance and transfer.

2.2. **Automated Work Station (AWS) of RB System** is a personal computer (or laptop) with RB system software installed on it, which is designed for preparation, acceptance/transfer and subsequent processing of electronic documents in RB system, and also cryptographic security system software for the use of electronic signature and data encryption for transferred electronic documents.

2.3. **RB System Administrator** is the Bank's authorized officer responsible for RB System functioning and working capacity.

2.4. **ES Public Key Certificate Request (certificate request)** is an electronic file with RB System subscriber ES Public key, this subscriber details and additional data which is the basis for an ES Public key certificate prepared by the Bank.

2.5. **A notice of Receipt** is an electronic document prepared by an Accepting Party and containing information about the status of processing of an electronic document being accepted.

2.6. **The customer** - the customer of the Bank, which concluded an Agreement with the Bank for provision of the services in the Remote Banking System of AO Mizuho Bank (Moscow)

2.7. **A key of an electronic signature (ES key)** is a unique sequence of symbols, which intended for creation an electronic signature in electronic documents with the use of electronic signature facilities.

2.8. **Check key of an electronic signature (ES check key)** is a unique sequence of symbols absolutely connected with an electronic signature key and intended for authentication check of an electronic signature (hereinafter referred to as "electronic signature check").

2.9. **An ES key compromise** is an event resulting in the possibility to use an electronic signature key by an unauthorized person. The events resulting in an electronic key compromise include but are not limited to the following ones:

2.9.1. key details carrier loss;

2.9.2. key details carrier loss (including theft) with the consequent detection of their location;

2.9.3. transfer of a Private ES key through a communication line in open form;

2.9.4. violation of rules for storing key details carriers;

2.9.5. suspicion of unauthorized information propagation or its misrepresentation within the RB System;

2.9.6. negative result of an ES check;

2.9.7. violation of the integrity of key *carriers'* package;

2.9.8. unauthorized copying of key details carriers;

2.9.9. other events determined by the Customer as familiarization with ES keys by an authorized person (persons).

The events listed in cl. 2.9.1 – 2.9.4 should be interpreted as a definitive compromise of the valid keys. The events listed in cl. 2.9.5– 2.9.9 could not be interpreted as a definitive compromise of the key and in each separate case require special investigation.

2.10. **An Electronic Document (ED) Copy** is an electronic document resulting from copying of an original (copied) electronic document with the help of integral RB System means and identical to an original electronic document in contents but having a different from an original electronic document, unique ID within RB System.

2.11. **An invalid electronic document (ED)** is an electronic document which received a negative result after the check (did not pass the check) in accordance with one or more of the following procedures:

- decryption.
- ES authenticity confirmation.
- document fields correct filling-in check

2.12. **key information carrier (key carrier)** is a data carrier which contain an electronic signature key as well as an electronic signature check key.

2.13. **ES authenticity validation in an electronic document** is the positive result of ES ownership by an RB System subscriber check through Cryptographic Information Protection Means (CIPS) with the help of ES key certificate.

2.14. **Certificate of an electronic signature check key (ES Public key certificate, ES Certificate)** is an electronic or a paper document issued by the Bank's Certification Authority and verifying the accessory of an ES check key to the owner of the certificate of an ES check key .

2.15. **Cryptographic Information Protection System (CIPS) within the RB System** is the specialized software used within the Bank's RB System for ES creating, ES authenticity checking, encryption and decryption of electronic documents transferred through the system.

2.16. **Electronic signature facilities** are encryption (cryptographic) tools which used for realization at least of one of the following functions: creation of an electronic signature, check of an electronic signature, creation of an electronic signature key and an electronic signature check key.

2.17. **The Bank's Certification Authority –** is an organizational unit of the Bank that performs the functions of creating and issuing certificates of electronic signature verification

keys, maintaining a register of certificates for electronic signature verification keys and other functions provided for by Federal Law 63 “On Electronic Signatures”.

2.18. **An Electronic Document (ED)** is a document in which information is presented in electronic digital form.

2.19. **An Electronic Signature (ES)** is information in an electronic form which is attached to an electronic document or connected in another way with an electronic document and which is used for identification of a person who’s signing the information. According of these Rules an electronic signature is an enhanced encrypted non-certified electronic signature in terms of Federal Law as of 06.04.2011 No63-FZ “On digital signature”. An electronic signature is formed as a result of a cryptographic transformation of information by using an electronic signature key; an electronic signature helps to identify a person signing the document; an electronic signature allows to find out a fact of making amendments into an electronic document after its signing and is created by means of electronic signature facilities.

2.20. **Encryption** is a way of conversion of non-restricted information into restricted and vice versa. It is applied for storing important information in unreliable sources and its transfer through unprotected communication channels. Encryption is divided into encryption and decryption processes.

3. The procedure of access to the RB System

3.1. Upon the Customer’s request the Bank prepares and delivers to the customer the Contract for rendering services related to remote banking system by AO Mizuho Bank (Moscow) (henceforth – the Contract) for signature.

3.2. The Customer signs an agreement and sends it to the Bank.

3.3. The Customer fills in an Application for a Subscriber’s registration to RB system (Appendix 3 to the current Rules) for each authorized person and sends it to the bank. The right to sign electronic documents available to the Subscriber in accordance with the submission to the Bank the validity signature cards and seal and other documents which certified the powers of the Subscribers

3.4. Within 3 working days after the receipt of the signed Application for a subscriber’s registration to RB-system, the Bank performs all operations necessary for the Customer’s registration in the RB System and preparation of all system access means necessary for the Customer’s Subscribers.

3.5. the Customer’s authorized representative acting under the duly prepared power of attorney (a sample of the power of attorney is indicated in Appendix 4 to these Rules) or the Director of the Customer’s company arrives in the Bank for the receipt of the RB System access facilities

3.6. A representative of the Bank passes RB System access to a representative of the Customer in accordance with Certificate of RBS access facilities handover (Appendix 5 to these Rules). Certificate of RBS access facilities handover is composed in 2 (two) original copies: one copy for each Party.

3.7. In the exceptional cases determined by the Bank, the means of access to the RB system may be delivered to the Client's subscribers using the following alternative channels:

3.7.1. By the courier service, subject to measures that exclude uncontrolled access during delivery. For shipment, access kits, as well as documents to be signed by the Client, are placed in a strong package (safe package). The packages are sealed in such a way that it is impossible to extract the contents from them without violating the packages and seal. The return of documents signed by the Client is carried out by courier delivery or by registered mail.

3.7.2. If the Client has at least one RBS Subscriber with access to the RBS system, the Bank has the right to transfer the access identifiers and passwords of the Subscribers of this Client, inside encrypted files protected by passwords, attached to the free format document of the RBS system.

When transferring access identifiers and passwords of Subscribers via RBS, a separate file is generated for each RBS subscriber. Also, the Client is provided with an electronic version of the Certificate of acceptance and transfer of means of access to the RBS system (Appendix 5 to these Rules)

3.7.3. If there are no active RBS Subscribers, the Bank has the right to transfer the passwords of the Subscribers of this Client inside encrypted files protected by passwords using e-mail to the address officially provided by the client in the application for registration of the RBS Subscriber. In this case, the Subscriber's access identifier is not transmitted by e-mail.

When sending Subscribers' passwords to the e-mail address, a separate file is generated for each RBS subscriber. The Client is also provided with an electronic version of the Certificate of acceptance and transfer of means of access to the RB system (Appendix 5 to these Rules).

When using electronic information transfer channels in accordance with clauses 3.7.2 and 3.7.3, the transfer of the RB Subscriber's access identifier and/or the password from the file is made to the RB Subscriber personally by the phone number specified by this Subscriber in the Application for Registration of the RB Subscriber. At the same time, before transferring the password from the encrypted file, the Bank's Representative is obliged to additionally identify this Subscriber by requesting information known only to this Subscriber. The password is communicated to the Subscriber only if correct answers to the requested information are received.

After receiving the means of access to the RB system, the Client is obliged to print out in 2 copies the Certificate of acceptance and transfer of means of access to the RB system, sign by an authorized employee of the Client, stamp the Client's organization and send the Certificates to the Bank by courier delivery or registered mail.

To speed up the process of obtaining access to the system, a scanned copy of the Act can be sent by the Client to the e-mail address of the RB system support service.

3.8. The signature of the Acceptance and delivery act for the RB System access means confirms the fact of rendering a service of the Customer registration within the RB System and comprises the grounds for the Customer to pay a consideration for the Customer's registration in the RB System in accordance with the Tariffs.

3.9. After receipt of access means the Customer’s Subscribers by themselves initiate the generation process of their own working ES keys as well as ES check keys , certificate requests to the Bank mailing, certificates receipt and procession.

3.10. The process of initial access to the RB System and actions required for generation and registration of own working keys of an electronic signature are described in the Customer’s AWS installation, setting-up and update manual available at the bank’s web-site; please follow the link: http://www.mizuhobank.com/russia/ru/service/remotebanking.html.l.

3.11. In case of the need to have technical support the Customer addresses the RB System Support Service via the Bank telephone numbers and/or by email: support@mhcb.ru.

3.12. After receiving a request for a certificate of the RB subscriber's ES verification key, an authorized employee of the Bank's Certification Center checks the compliance of the information in the RB System Subscriber Registration Application with the information contained in the certificate request. If the verification result is positive, it creates a certificate of the ES verification key (Appendix 6 to these Rules) and prints it in 2 copies.

3.13. The issuance of the certificate of the ES verification key to the owner - subscriber of the RB System is carried out in the Bank, with the personal presence of the subscriber of the RB System. When issuing a certificate, an authorized employee of the Bank is obliged to identify the RBS System Subscriber, based on the data of the RBS System Subscriber's identity document, or its notarized copy.

3.14. The Bank has the right to authorize the handover of certificates of ES verification keys to the RBS System Subscribers to the Client's Chief executive officer for RBS System Subscribers related to this Client, based on a Power of Attorney issued by the Bank to the Chief executive officer of the Client.

When performing the actions entrusted by the Bank, the Chief executive officer of the Client is obliged to identify the owner of the ES verification key certificate in his personal presence. In this case, the signing of the Certificate of the ES verification key by the Chief executive officer of the Client is an unconditional confirmation of the identification of the owner of the certificate.

3.15. Not later than the next business day after receiving a copy of the ES verification certificate signed by the Client, the RB System Administrator enters the Client's Subscriber's ES key certificate into operation. In this case, both copies of the certificate must also be signed by the Administrator of the RB System, certified by the signature of an authorized employee and the seal of the Bank. One copy of the certificate signed by the Bank is returned to the Client's Subscriber, the second remains for storage in the Bank.

3.16. Until the ES verification key certificate is put into operation, the Subscriber - the owner of this certificate - is not provided with access to the RB System

3.17. A connection of a new Customer’s subscribers is performed according to the order stipulated in items 3.3-3.15 of these Rules.

3.18. It is only possible to change the list of the Customer’s Subscribers with the right to sign electronic documents after the delivery to the Bank of a new duly prepared sample signature and seal card as well as other documents verifying Subscribers’ authorities.

3.19. In case of change of an operating zone for registered Subscribers’ ES keys, the Customer prepares and submits to the Bank an Application for a change of an operating zone

for an electronic signature key of the RB system subscriber by using a form of Appendix 9 of these Rules.

4. The procedure for the planned change (regeneration) of an ES key

4.1. The period of validity for an ES key within the RB System is set equal to 13 (thirteen) months.

4.2. 30 (thirty) calendar days before the termination of the validity period for an ES key of the Customer's subscriber the RB System offers a subscriber to make a planned change (regeneration) of an ES key at every booting-up. If the Customer's subscriber agrees to make the change the RB System performs generation of a new electronic signature key, formation of a request for a certificate and its sending it to the Bank through the RB System.

4.3. If the request for a certificate is signed with the correct ES of the Customer's subscriber, the Bank's Certification Authority generates the certificate of a new working key of ES of the Client's subscriber. If the customer did not make a timely planned change of its ES keys, then he does not have the opportunity of using ES keys to sign electronic documents. In case of the necessity of providing the right to the Client's subscriber to sign electronic documents using the ES keys the customer has to repeat the steps to register the Subscriber according to items 3.3 -3.16 of the current Rules.

4.4. The period of storage of an ES key certificate in the form of an electronic document in the Bank as well as the period of archive storage is determined in accordance with the laws of the Russian Federation.

5. The procedure in case of an ES key compromise

5.1. If one of the Parties discovers any signs of unauthorized use of an ES key by unauthorized persons (including unauthorized writing-off or an attempt to write off any funds from an account), the Party, which discovered any signs of unauthorized use of an ES key by unauthorized persons, should immediately inform the other Party about this fact.

5.2. Actions taken in case of ES key compromise belonging to the Customer's subscriber.

5.2.1. The resolution about an ES key compromise can be taken by the Customer's Subscriber in favor of which the ES key was issued, or by the Customer's manager.

5.2.2. The work with the compromised ES key should be suspended immediately after the fact of the ES key compromise is discovered.

5.2.3. In case the resolution on an ES key compromise is taken, the Customer should immediately notify the Bank by telephone about the fact of its compromise. The Bank is entitled to require additional information for the Customer's Subscriber identification.

5.2.4. Having received a preliminary notification by telephone of an ES key compromise the Bank immediately suspends processing of electronic documents signed with the compromised ES key until the receipt of a notification of the ES key compromise in the form of a paper document or via the RB System.

5.2.5. Within 1 (one) working day following the day of a preliminary telephone notification of an ES key compromise, the Customer should deliver to the Bank a Notification of an ES key compromise in accordance with the form of Appendix 7 hereto (henceforth – Notification of Compromise). Such Notification of Compromise can be delivered to the Bank:

- in paper form, signed by the manager or a person acting under the duly prepared power of attorney within the scope of powers granted to him and certified by the Customer's seal;
- via the RB System by sending the Notification of Compromise as an attachment to an electronic document ("an arbitrary document" in terms of the RB System) indicating "Notification of ES keys compromise" in the "Title" field. The Notification is sent with the use of valid (uncompromised) keys, if any.

5.2.6. After the receipt of a message about ES keys compromise the RBS System Administrator should lock the corresponding certificate in the RB System

5.2.7. If necessary, in accordance with section 3 hereof, the Parties perform the procedure of creation and certification of a new ES key for the Customer's subscriber whose ES key was compromised.

5.2.8. The Bank starts acceptance and processing of electronic documents signed with the new working ES key of the Customer's subscriber no later than a working day following the day of receipt from the Customer of a duly prepared Registration Form for an ES key certificate of the Customer's subscriber.

5.2.9. Upon receipt of information concerning a possible compromise of the Customer's subscriber key not from the Customer, the RB System Administrator gets in touch with the Customer's subscriber by the telephone number indicated in the Application for generation of certificate for an electronic signature key in order to confirm the fact of a compromise immediately after the receipt of such information. If it is impossible to get in touch with the Customer's subscriber during 15 (fifteen) minutes, the Bank has the right to take an independent decision about blocking of a corresponding certificate to prevent possible falsification of an electronic messages.

5.3 . Unlocking of a Customer Subscriber's key.

5.3.1. The unlocking if the Customer subscriber's key is possible only in case of the key blocking in accordance with circumstances which cannot be categorically treated as an absolute key compromise. If in the course of an investigation carried out according to item 2.10 a key compromise has not been confirmed, the key of the Customer's subscriber can be unlocked upon the Customer's application.

5.3.2. The Customer prepares an application for the key unlocking in any form; it should be signed by the Customer's subscriber and sent to the bank on paper or in a form of an attachment by RB system by using valid (uncompromised) keys. In case of absence of a technical possibility to use RB System the Customer can send an application to the bank by fax or by e-mail but then on a mandatory basis send a paper-based application to the bank not later than 1 (one) working day. After sending the application to the bank, the Customer's subscriber gets in touch with the support team of the bank by telephone and informs about the sending of the application for unlocking.

5.3.3. In order to unlock the key of the Customer's subscriber, the bank employee gets in touch with the Customer's subscriber by the telephone number indicated in the application for generation of a certificate of an electronic key within 2 (two) working hours after the call of the Customer's subscriber and receipt of a relevant application from the Customer sent in accordance with item 5.3.2, and confirms the validity of the Customer's decision about the key unlocking. Besides, the Customer's subscriber must say the Customer's full name and serial number of the public key certificate. The Bank can request to provide additional information for identification of the Customer's subscriber.

5.3.4. Unlocking the key is carried out within 2 (two) hours after receiving the Application for the key unlocking on paper, or confirmation of the customer solutions for unblocking key in case of a declaration on the RBS system, as well as by fax or e-mail.

6. The procedure for electronic document flow within the RB System

6.1. The transfer of electronic documents different from those listed in the "List of electronic documents used in the RB System by AO Mizuho Bank (Moscow)" (Appendix 2 hereto) within the RB System does not involve any obligations of the Parties except for the cases which are specifically stated by the Parties in additional Contracts to the Contract.

6.2. Each electronic document is prepared by a Transferring Party in accordance with the requirements of the current legislation of the Russian Federation and of regulatory acts if the Bank of Russia. The sender is responsible for the correct preparation of an electronic document.

6.3. An electronic document can be generated directly within the RB System or prepared and imported from any external system. The information about compatibility of the Bank RB System with the Customer's external system can be specified in the support service for the Bank RB System.

6.4. Each electronic document within the RB System has a unique ID allocated to it by the system at the moment of document generation. The Parties agree that electronic documents of the same type and content signed with the same ES' are deemed different in case their unique ID's differ.

6.5. An electronic document gives rise to the obligations of the Parties only if it meets the following requirements:

- It is prepared in accordance with cl. 6.2 hereof;
- It passed all necessary kinds of control;
- It is certified by valid ES' of its sender and ES details' authenticity is acknowledged;
- It is delivered to the recipient.

6.6. The Customer is obliged to check for the presence of Receipts from the Bank and the status of processing of all electronic documents transferred by him in due time. The Customer has the right to request the Bank for additional explanation in case of refuse to process an electronic document transferred by him.

6.7. The Customer has the right to present to the Bank documents specified in Appendix 2 hereto ("The list of electronic documents...") prepared in paper form in accordance with the

requirements of the current legislation of the Russian federation and regulatory acts of the Bank of Russia. In this case the Customer is not obliged to duplicate them within the RB System.

6.8. The Customer has the right to present an application to the Bank to limit the implementation of transactions on the account in the RB System, including limiting the maximum amount of one transaction and (or) transactions for a certain period. For submission, the Customer has to send a written application to the Bank in the form of Appendix 10.

6.9. The Bank is not responsible for timeliness of an electronic document transfer by the Customer to the Bank. The Customer is obliged to perform timely transfer and receipt of electronic documents by himself.

6.10. Preparation and sending of electronic documents to the Bank is performed in accordance with the following procedure:

6.10.1. The Customer's Subscriber prepares an ED under the guidance of the rules specified in clauses 6.3 and 6.10 of these Rules and saves any prepared ED's in the RB System database. Such prepared and saved ED's receive "New" status .

6.10.2. Any officials – Customer's subscribers having the right of a single, the first or second signature sign a Customer's ED with the help of ES keys in their possession. Moreover, the RB System automatically checks the authenticity of each ES. If an ES is incorrect or the subscriber does not have the corresponding powers such ES is not saved and the ED is deemed not signed.

6.10.3. If an ED is signed with the necessary number of correct ES, the document received "Signed" status.

6.10.4. The Customer's Subscriber chooses ED's subject to be sent from the general documents list and transfers them to the Bank for processing.

6.10.5. The RB System sequentially and automatically checks the authenticity of ES' and the details of each ED. An ED which passed the check on the Bank's part successfully receives "Accepted" status.

6.10.6. Any ED's which have incorrect ES' and/or errors in details are not accepted by the Bank for procession and remain with the same status. The Customer's AWS shows a message with the details of errors.

6.10.7. The time when an ED received "Accepted" status is deemed the time of the document delivery to the Bank.

6.10.8. The allocation of "Accepted" status to the document does not imply that the Bank has assumed an obligation to execute the ED because by that moment the document has not passed through all kinds of bank control.

6.11. The Customer's electronic document processing by the Bank:

6.11.1. "Not Accepted" or "Refused by ABS" status is allocated to an ED if the Bank does not confirm writing-off of funds from the Customer's account under this document The reason for rejection of the Customer's document execution is indicated by the bank in the field "Information from the Bank" of an electronic document or in a form of a free-format document (free-format document from the bank).

6.11.2. "Implemented" status is allocated to a document if the Bank confirmed writing-off of funds from the Customer's account (the document is executed from the Customer's account).

6.11.3. The Bank delivers to the Customer a corresponding Receipt for any changes of an ED listed in this section.

6.12. Receipt of the account statement:

6.12.1. The Bank on a daily basis before 11 o'clock Moscow time generates for the Customer account statements in the form of electronic documents for all accounts operated within the RB System. Such account statement reflects all operations executed with the Customer's account during the previous Bank's transaction day.

6.12.2. The Customer can request an account statement by delivering to the Bank the corresponding electronic document and automatically receive a generated account statement from the Bank.

7. The procedure for considering disputed situations

7.1. General Provisions.

7.1.1. This section describes the procedure for settlement of disputed situations between the Customer and the Bank related to the authenticity of electronic documents. It considers disputed situations of two types:

- a Party rejects an electronic document (a Party argues that its subscriber did not sign an electronic document accepted by the other Party while the other Party argues the opposite);
- a Party denies the fact of receipt of an electronic document (a Party argues that an electronic document sent by it was accepted by the other Party while the other Party denies the fact).

7.1.2. A Party initiating consideration of a dispute (henceforth – "the Originator") should prepare and send to the other Party (henceforth – "the Respondent") a document (application) signed by an authorized officer describing the circumstances of a case. Before such application is filed the Applicant is recommended to ensure the permanence of the ES used and make sure that no unauthorized actions were taken by the personnel. The application should indicate:

- company name;
- date, number and type of the electronic document under dispute;
- type and nature of a claim.

7.1.3. Basing on the application, the Respondent within 5 (five) working days considers it and either satisfies the Applicant's claim or delivers to the Applicant a written rejection to satisfy the claim with the rationale of the cause of rejection.

7.1.4. In case the Originator disagrees with the rejection, he sends to the Respondent a written application stating his disagreement and requiring convocation an expert committee for consideration of the disputed situation.

7.1.5. Basing on this application, no later than 15 (fifteen) calendar days after the day of its receipt, the joint decision of the Parties convenes the expert committee for consideration of the emerged disputed situation. The representatives of the Originator and the Respondent can be persons being the employees either of those companies (equal

number from each of the Parties) or of other appropriate institutions. In the latter case their powers are determined through the powers of attorney. The list of committee members is coordinated by the Parties and approved by a bilateral act.

7.1.6. It is recommended that the expert committee includes the following members:

- subscribers who participated in the exchange of electronic documents on the parts of both Originator and Respondent;
- representatives of security and technical departments of the Originator and the Respondent.

Besides, independent experts and technical specialists can be invited, if necessary, from other appropriate institutions, including companies manufacturing the software being in use.

7.1.7. Within 5 (five) working days from the moment of convocation of the expert committee the Parties present to it the following materials:

- the application from the Originator with the claim summary;
- the Respondent's written rejection to satisfy the Originator's claim;
- the disputed electronic documents signed with the ES and the receipt for those documents;
- certified Registration Forms for ES keys certificates of the Parties' subscribers and the certificates which were used to generate the ES of the disputed document and the ES of a receipt thereof in electronic form on flexible disks or other data carriers;

7.1.8. Besides, the Bank presents to the expert committee:

- a benchmark personal computer (a personal computer free from viruses and software bugs) for the automatic work station for the settlement of a disputed situation;
- benchmark SW installation package received from ES means manufacturer intended for ES check of the disputed electronic document;
- other materials related to the nature of the considered claim.

7.1.9. The Parties should assist the expert committee in its work and present all required materials.

7.1.10. The expert committee considers a disputed situation within the Bank's territory. the check of ES authenticity on the disputed electronic documents is performed in accordance with the following procedure:

7.1.10.1. in front of the expert committee members, the RB System Administrator installs the benchmark SW from the installation package delivered to the expert committee at the automatic work station for consideration of a disputed situation (benchmark PC);

7.1.10.2. the expert committee makes sure that the benchmark SW operates as required;

7.1.10.3. the expert committee with the help of the benchmark SW checks the authenticity of the ES which the disputed electronic document is signed with;

7.1.10.4. no later than 10 (ten) working days after the receipt of all materials specified in clause 7.1.7 hereof, the expert committee by a majority members vote makes a resolution on the guilt of one of the Parties and prepares it in the form of an act executed in paper form and signed by all members of the expert committee.

7.1.11. The act executed by the expert committee is final and not subject to revision. The actions imposed by the act are binding for the Parties.

7.1.12. The expert committee act constitutes the ground for raising claims against persons guilty of the dispute.

7.1.13. In case the expert committee cannot make a resolution or if one of the Parties does not agree with the resolution made by the expert committee, avoids convocation of the expert committee, prevents the other Party from participation in the expert committee work, then the Parties have the right to refer the dispute to the Arbitrary Court of Moscow for consideration.

7.2. The procedure for settling a dispute related to a Party's denial of the fact of sending/signing an electronic document.

7.2.1. This section describes the procedure for settling a dispute caused by the rejection of one of the Parties of an electronic document: the Originator argues that its subscriber did not sign an electronic document accepted and executed by the Respondent while the respondent argues the opposite.

7.2.2. A disputed electronic document is required from the Respondent. In case the Respondent refuses to present the disputed electronic document the dispute is settled in favor of the Originator.

7.2.3. The consistency of the subscriber's ES for the presented electronic document is checked in accordance with clause 7.4 hereof. If the ES is deemed incorrect the dispute is settled in favor of the Originator.

7.2.4. In all other cases the dispute is settled in favor of the Respondent.

7.3. The procedure for settling a dispute related to a Party's denial of the fact of an electronic document receipt.

7.3.1. This section describes the procedure for settling a dispute caused by the denial by one of the Parties of the fact of an electronic document receipt: the Originator argues that an electronic document generated by him with correct ES' in accordance with the RB System operating rules was transferred to the Respondent and accepted by the latter while the Respondent denies the fact of acceptance of such electronic document.

7.3.2. The Originator is required to provide the disputed electronic document and its delivery receipt corresponding to it. In case the Originator refuses to present the disputed electronic document or its acceptance receipt, the dispute is settled in favor of the Respondent.

7.3.3. The consistency of the Originator's subscriber ES for the electronic document is checked in accordance with clause 7.4 hereof. If the ES is incorrect the dispute is settled in favor of the Respondent.

7.3.4. The consistency of the Respondent's subscriber ES for the acceptance receipt is checked in accordance with clause 7.4 hereof. If the ES is incorrect the dispute is settled in favor of the Respondent.

7.3.5. The compliance of the receipt with the electronic document is checked. In case the receipt does not comply with the electronic document the dispute is settled in favor of the Respondent.

7.3.6. In all other cases the dispute is settled in favor of the Originator.

7.4. The procedure for checking the authenticity of an electronic signature on an electronic document.

7.4.1. This section describes the procedure for checking the authenticity of a subscriber's ES for an electronic document. This procedure is used when settling a dispute on the authenticity of electronic documents or receipts thereof.

7.4.2. A Party which sent an electronic document is required to present an ES key certificate which was used to generate the ES for a disputed electronic document and/or a receipt. The ES of a disputed electronic document is checked at the automatic work station for settling dispute situations in accordance with the RB System user documentation. If the program does not consider the ES correct at the moment of its generation the resolution on the electronic document ES incorrectness is taken.

7.4.3. If one of the Parties expresses doubts on ownership of an ES key certificate by a subscriber then the procedure is performed to check the ownership of such certificate in accordance with clause 7.5 hereof.

7.4.4. In case when a certificate is deemed not belonging to the subscriber the ED ES is considered incorrect.

7.4.5. In all other cases the resolution is made on the correctness of a subscriber's ES for the electronic document.

7.5. The procedure for checking certificate ownership by a subscriber.

7.5.1. This section describes the procedure for checking ES key certificate ownership by a subscriber.

7.5.2. To check certificate ownership by a subscriber the Bank is required to present a certified copy of the Registration Form for the ES key certificate for this Subscriber.

7.5.3. The subscriber's ES key certificate compliance with the data of the Registration Form is checked. According to the results of the check the resolution is made whether the Subscriber owns this certificate or not.

8. Information security assurance in the RB System

8.1. General Provisions

8.1.1. The Parties are obliged to take appropriate measures to protect confidential information within the RB System.

8.1.2. The Parties acknowledge it obligatory to use an additional authentication means in the RB System with the help of dynamic passwords for the Customer's Subscribers with the right of a signature.

8.1.3. Compliance with information security requirements while arranging electronic documents exchange ensures:

- information confidentiality (only authorized persons can have access to the information);
- the integrity of the information transferred (guarantee that the data are transferred unaltered and the possibility of information substitution is eliminated);
- authentication (the information transferred can only be received by its addressee and its sender is a person on whose behalf it is sent).

8.1.4. Information security requirements for electronic documents exchange are regulated by the law of the Russian Federation, regulatory documents of the Bank of Russia and FSB of Russia; they are realized with the application of software and hardware tools and organizational measures.

8.1.5. Software and hardware tools include the following:

- the RB System software;
- password and ID's system restricting users' and operators' access to hardware and software of the RB System;
- cryptographic information protection means;
- software and hardware means of protection from unauthorized access;
- computer viruses protection means;
- computer systems attacks protection means.

8.1.6. Organizational measures include the following:

- hardware installation in the rooms with controlled access;
- administrative restrictions of the access to those means;
- arrangements for the use of passwords and ID's by users and operators;
- only specially trained and authorized persons have access to electronic documents exchange;
- maintenance works for software and hardware;
- software and hardware means backup;
- service personnel training;
- protection of hardware from damaging exposures (fire, water exposure, etc.).

8.2. CIPS and key carriers' protection assurance

8.2.1. Any CIPS, operation and technical documents thereto, licenses, key data carriers are subject to single copy record keeping in special logs intended for those purposes.

8.2.2. Only a system-maintained external disconnectable carrier (such as USB-key RU Token ЭЦП, USB flash drive etc.) should be used as a key data carrier. For the purposes of protection of key data from unauthorized access, the Bank recommends to use devices specially intended for those purposes, i.e. devices with cryptographic algorithms contained directly on a key carrier (USB-key RU Token ЭЦП).

8.2.3. CIPS installation media on data carriers, operation and technical documents for CIPS, and key carriers should be stored in individual lockers (safes, storages) in circumstances where uncontrolled access thereto, as well as their unintentional destruction are impossible.

8.2.4. It is allowed to store key data carriers in a storage which is used by other employees as well; but then they should be stored in individual packages (containers) sealed with the personal seal of an owner of such key data carrier, excluding the possibility of secret access of unauthorized persons thereto.

8.2.5. In case of failures or faults in CIPS or key carriers operation a Subscriber should notify of the fact to the RS system support center.

8.2.6. A Subscriber is PROHIBITED from:

- making unauthorized copies of cryptographic keys;
- leaving (even for minimum time) key carriers inserted into a computer if a Subscriber does not use them, or on open access (e.g. on a table);
- using key carriers for encryption and signing electronic documents not related to work within the Bank's RB System;
- disclosure of the contents of key data carriers or pass the carriers to the persons without access thereto, call up the ES key to a display and/or for printing;
- insert cryptographic key carriers into any readout devices in the modes not envisaged for CIPS standard operating procedures as well as into readout devices of personal computers not intended for work with the Bank's RB System;
- save any outside data on the cryptographic key carriers;
- make any changes to CIPS software.

8.3. The RB System access means security assurance

8.3.1. The RB System subscribers are recommended:

- Not to allow using simple passwords (123456, qwerty, etc.) – please use various complex combinations of letters (including those in different cases) and figures which are not located "in succession" on a keyboard.
- Perform regular (at least once per month) change of the passwords used within the RB System.
- Not to use a password used for any other systems and services for the access to the RB System.
- To change password and regenerate ES keys (via the corresponding features of the RB System) or address the Bank for the receipt of new access means immediately in the following cases:
  - After dismissal of an employee who had access to ES keys;
  - In case any suspicions emerge of ES keys and/or access means compromise.
  - In case of detection of any malware on a computer used for work in the RB System.

8.3.2. The RB System Subscribers are strictly prohibited from telling their access ID's (logins) or passwords used in the RB System to anybody including any service technicians for system operation checks, Bank interaction setup, etc. In case of the need

for such checks an access means owner must insert his/her login and password personally.

8.4. The RB System AWS security assurance

8.4.1. The Customer operating an AWS should take measures necessary to exclude making unauthorized changes to the AWS hardware and software, to their contents, emergence of computer viruses and software intended for destruction or alteration of the RB System software, electronic documents or for password, ES keys and other confidential information search attacks at an AWS and in the RB System.

8.4.2. It is recommended to equip the RB System AWS with data mining control means.

8.4.3. An AWS should be equipped with a set of measures and means of protection from the threats of Internet public network ensuring data protection from unauthorized access through the network. The Customer operating an AWS should constantly use anti-virus software and timely update it.

8.4.4. It is recommended to use specialized security software packages: Firewalls, Anti-Spyware software and other specialized software for ensuring IT-security.

8.4.5. The Customer should ensure timely download and installation of updates of an AWS system as well as regular update of other system and application software as their new versions appear.

8.4.6. It is recommended to create trustworthy environment at an AWS of the RB System:

- Do not install software from questionable sources.
- Do not download software from any file hosting web sites.
- It is strongly recommended not to use an AWS for regular web browsing or entertainment as viruses and malware are most frequently spread through entertainment web sites.
- If possible, completely prohibit all (in and out) connections with Internet and only allow access to necessary resources (in particular, to those used by the RB System).
- Perform anti-virus check of any files and programs downloaded from Internet or received by email or on external media (flexible disks, flash data carriers, CD/DVD, etc.).
- Disable “Automatic Execution” function for external devices: flash data carriers, compact disks. Lots of viruses access the system through autoexec from a flash data carrier or compact disk.
- Restrict computer access for personnel not related to working with the RB System.
- Do not allow working with Windows Administrator Account; instead, it is necessary to use a low-rights account in Windows operating system installed on a PC.
- Do not allow using “empty” or simple passwords (123456, qwerty, etc.) for all accounts with the right to enter Windows; perform regular passwords change (the recommended frequency is once a month).

- Monitor all actions of the employees (including service technicians) during all the time when they perform any actions on the PC's used for work in the RB System.

8.4.7. As an additional means of protection from external attacks in the RB System the Customer's Subscribers query filtering can be applied:

- for internal and external IP-addresses of the Customer's AWS;
- for physical (MAC) addresses of network interface cards of the Customer's AWS'.

A list of IP and MAC addresses allowed to connect to the RB System can be set up for each Customer's Subscriber.

8.4.8. To enable Customer's Subscribers query filtering according to IP and/or MAC addresses the Customer shall:

- Set constant (static) IP addresses for the Customer's AWS'
- Send to the Bank an Application for enabling access filtering for the RB System in paper form and in accordance with the form of Appendix 8 hereto.

8.5. Requirements for premises used for the RB System AWS placement and key carriers storage

8.5.1. Placement, special equipment, supervision and access mode arrangement in the premises with the RB System AWS installed or key carriers stored (henceforth – data rooms) should provide the preservation thereof.

8.5.2. Data rooms are allocated in accordance with the space of controlled areas regulated by CIPS operation and technical documentation. The rooms should have strong entrance doors with locks to guarantee safe closure of the rooms for non-working hours. Windows of the rooms located on the first or last floor of buildings as well as windows located near fire ladders and other places which can allow access of unauthorized persons to the data rooms should be equipped with metal grates or shutters, or security alarm, or other means preventing uncontrolled penetration into the data rooms.

8.5.3. The inner arrangement, special equipment, supervision and access mode organization in the rooms should exclude the possibility of uncontrolled penetration or presence of unauthorized persons therein, as well as the possibility of unauthorized persons watching any works performed therein.

8.5.4. The rooms supervision mode, including access rules for employees and visitors during working and non-working hours should envisage regular control over technical supervision means (if any) condition.

8.5.5. The doors of the data rooms should be constantly locked and can be opened only for authorized access of employees and visitors.

8.5.6. The cryptographic keys, operation and technical documents, CIPS installation media should be stored in the necessary number of safe metal containers equipped with inner locks with two sets of keys and digital security locks or devices for sealing key holes. One set of key from the container should be with a person responsible for an AWS operation. Container keys copy should be stored in a special safe of the Customer's company manager.

8.5.7. At the end of a working day, a data room and any containers located therein should be locked and the containers should be sealed. The seals for containers sealing should be with the employees responsible for the corresponding containers.

8.6. ES keys destruction

8.6.1. Unused or disabled ES keys are subject to destruction.

8.6.2. The destruction of ES keys on key carriers is performed by a Subscriber owning those keys.

8.6.3. ES keys are destroyed by way of their deletion (destruction) according to the procedure approved for multiple use key carriers . The Customer's Subscriber, if necessary, can address the RB System technical support service to consult on any issues regarding ES keys destruction.

9. Suspension or stoppage of RB System use

9.1. The Customer can be disconnected from the RB System by submission of a free format paper base Application for the Agreement's cancellation.

9.2. The Bank can suspend or stop the Customer's use of RB System at its own discretion in case the latter violates the procedure of RB System use and also in cases stipulated by the Agreement and the legislation of the Russian Federation.

9.3. When the Bank detects the operations meeting the criteria of fraud operations made without the Customer's consent, the Bank suspends a use of RB System by the Customer's Subscriber who signed the payment order and acts in accordance to AO Mizuho Bank (Moscow) General Provisions of Customer Accounts Opening and Maintenance for legal entities and individual entrepreneurs. The Bank renews the payment order execution and use of the electronic means of payment by the Subscriber upon receiving of the Customer's confirmation in accordance with the General provisions. When not getting of the Customer's confirmation the Bank renews the payment order execution and use of the electronic means of payment by the Subscriber after two business days following the day of its actions in accordance to the General provisions.

10. The procedure for amending the Rules

10.1. Any amendments and additions hereto and Appendices hereto, as well as the terms and the procedure for their entry into force are published at the Bank's official web site in Internet at the following link: http://www.mizuhobank.com/russia/ru/service/remotebanking.html and Customers are deemed notified of them starting from the date of such publishing.

10.2. The wordings of these Rules and all amendments and additions thereto should be stored by the Bank in paper form during 3 (three) years after their lapse.

10.3. The Customer has a right to request copies of the wordings of these Rules and all amendments and additions thereto in paper form. The documents specified in this clause

should be delivered to the Customer by the Bank within 15 working days after receipt of the corresponding written request from the Customer.

Appendices

Appendix 1 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

TECHNICAL REQUIREMENTS TO CUSTOMER'S AWS (PC) FOR RBS

Personal computer with the following characteristics:

- Microsoft operational system: Windows 10, Windows 11. **(**English or Russian versions);
- Web-browser: Microsoft Internet Explorer 11, Google Chrome, Mozilla FireFox
- Existence of an access to the Internet.
- Existence of a free USB-port.

Appendix 2 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

THE LIST OF ELECTRONIC DOCUMENTS USED IN THE RB SYSTEM

Payment documents:
(signed by persons from the signature card)
- Payable order
- Currency transfer
- Foreign currency purchase order
- Foreign currency selling order
- Currency conversion order
- Order for writing off of amounts from transit currency account

Documents of currency control:
(signed by persons from the signature card or persons authorized by the Power of attorney)
- Currency control form
- Supporting documents certificate
- Contract transaction passport
- Credit Contract transaction passport
- Application for closing/transfer of transaction passports

Documents for transaction conclusion:
(signed by persons in accordance with the terms of the Agreement)
- KL: credit tranche issue
- KL: credit tranche issue with a floating rate
- KL: credit tranche prolongation
- KL: early repayment of the credit tranche
- KL: consolidation of credit tranches
- MLA: loan issue
- MLA: loan issue with a floating rate
- MLA: loan prolongation
- MLA: early repayment of the loan
- MLA: consolidation of loans
- MGA: Bank's guarantee issue
- MGA: FC Bank's guarantee issue
- MGA: Bank's guarantee amendment
- DEP: deposit opening
- DEP: deposit placement without account
- DEP: early repayment of a deposit
- DEP: early repayment of a deposit without account

Other documents used in the RB system:
(signed by persons from the signature card)
- Free-format document (text information message and/or attachment to an electronic document)

Appendix 3 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

A P P L I C A T I O N
FOR A SUBSCRIBER'S REGISTRATION TO THE RB SYSTEM

" _____" _____ 20__

_____
(company full name)

for the purposes of use within the RB System of AO Mizuho Bank (Moscow) applies for registration of a Subscriber:

Position . . . . . .
Last name . . . . . .
Name . . . . . .
Patronymic (if any) . . . . . .
ID document details . . . . . .
Registered at the address . . . . . .
Tel. . . . . .
e-mail . . . . . .

Operating zone of an electronic signature key:
(***in accordance with the rules stipulated in the Appendix 2 to the Rules***)

☐ Signing of electronic payment documents and currency control documents
☐ Signing of documents for transactions conclusion
☐ Access to RB system without the right of signing of electronic documents

Key carrier:
☐ New USB-key Ru Token
☐ Previously issued USB-key Ru Token (serial number_____)**
☐ Own key carrier (USB-flash)

Notes:……
……

Subscriber of RB system _____ / _____ /
(Signature) (Name)

Company Manager _____ / _____ /
(Signature) (Name)

Stamp Here

** All fields of the application are subject to filling-in*
*** Possible only when replacing the Customer's authorized Subscriber*

The Bank's notes:

Appendix 4 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

THE FORM FOR THE POWER OF ATTORNEY FOR THE RECEIPT OF ACCESS MEANS TO THE RB SYSTEM

POWER OF ATTORNEY NO. _____

_____ _____

Name of locality Date, month, year

_____

(name of a company)

Represented by _____, acting on the basis_____

(position, full name)

by this power of attorney authorizes_____

(position, full name)

Born on _____, passport series _____No_____

(date of birth)

Issued by _____

(who and when was issued by)

To receive in AO Mizuho Bank (Moscow) access facilities to the system of remote banking, for this purpose to sign acceptance-transfer certificates of access facilities to RB system as well as to perform other actions related to the fulfillment of this task.

Signature of a person received the power of attorney _____ is certified.

This power of attorney is issued for a period of 30 (thirty) days without the right to delegate powers hereunder.

_____ _____ _____

(the manager's position) *(signature)* *(last name and initials)*

Stamp Here

Appendix 5 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

CERTIFICATE OF RBS ACCESS FACILITIES HANDOVER

Moscow "____" _____20___
(to filled in by the Bank)

This Certificate is prepared to certify that Joint-Stock Company Mizuho Bank (Moscow) (henceforth – "the Bank") represented by _____, acting under _____ , has transferred ,
and _____
(Company full name)

(henceforth – "the Customer") represented by _____
(position, name).

acting under _____
(document name)

in accordance with the conditions of the Contract for rendering services related to remote banking system by AO Mizuho Bank (Moscow) dated ___.____._____ No. _____ has accepted the access facilities to the Bank's RB System comprised of:

Item No.	Title	Quantity
1.	USB-key eToken (regeneration)	
2.	Autonomic one-time passwords generator eToken PASS	
3.	USB -key eToken	
4.	Personal identifier and a password for RB system access	
5.	The printout of the Bank's EDS key certificate	

BANK

_____
(position)

_____
(last name and initials)

_____
(signature)

"____"_____ 20__

Stamp Here

CUSTOMER

_____
(position)

_____
(last name and initials)

_____
(signature)

Stamp Here

BANK'S MARKS: **Received by Operation division** "____" _____20___		

Appendix 6 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

CERTIFICATE OF THE ELECTRONIC SIGNATURE VERIFICATION KEY.

Moscow "___"_____20___

Company name: _____

Key data:

Algorithm: _____
Valid from date: _____
Valid until date: _____
ES check key unique (serial) number: _____
Owner's full name: _____
ES tool and standards: _____

ES Check key:

This Certificate of an ES check key is issued and registered by the Certification Authority of AO Mizuho Bank (Moscow)

RS System Administrator

_____ / /

Owner of the certificate of an ES check key

_____ / /

BANK

_____
(position)

_____
(last name and initials)

_____
(signature)

"____"_____ 20__

Stamp Here

CUSTOMER

_____
(position)

_____
(last name and initials)

_____
(signature)

"____"_____ 20__

Stamp Here

Appendix 7 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

[PREPARED ON THE COMPANY'S BLANK SHEET]

NOTIFICATION ABOUT ELECTRONIC SIGNATURE COMPROMATION

"___" _____20__

_____ hereby

(company's full name)

notifies about the compromise of electronic signature keys owned by the following subscribers:

Item No.	Last name, first name, patronymic (in full)	ES key certificate serial number	Compromise cause
1			
2			
…			

Contact person: _____

(position, name, telephone, E-Mail)

_____ _____ _____

(M*anager's position)* *(signature)* *(last name and initials)*

Stamp Here

Bank's Marks:

The Notification about an ES key compromise was received by the Bank, the data presented by the Customers are verified, the Manager's signature is valid:

_____ _____ _____

(position of a bank employee) *(signature)* *(last name and initials)*

"___" _____ 20___

Appendix 8 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

APPLICATION
FOR ENABLING ACCESS FILTERING TO THE RB SYSTEM

"___" _____20__

_____ hereby

(company full name)

Applies for enabling access filtering for the RB System for the following subscribers:

Item No.	Last name, first name, patronymic (in full)	Allowed IP and/or MAC addresses
1		
2		
…		

Contact person: _____

(position, name, telephone, E-Mail)

_____ _____ _____

(*Manager's position)* *(signature)* *(last name and initials)*

Stamp Here

Bank's Notes:

Application is received

_____ _____ _____

(position of a bank employee) *(signature)* *(last name and initials)*

"____" _____20__

Appendix 9 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

APPLICATION
FOR A CHANGE OF AN OPERATING ZONE FOR AN ELECTRONIC SIGNATURE KEY OF THE RB SYSTEM SUBSCRIBER

" _____ " _____ 20__

_____
(Name of the company)

For a Subscriber:

Last Name .....

First Name.....

Patronymic (if any) .....

Contact information:

Tel. .....

e-mail .....

To assign an operating zone of an electronic signature key:
(***in accordance with the rules stipulated in the Appendix 2 to the Rules***)

☐ Signing of electronic payment documents and currency control documents
☐ Signing of documents for transactions conclusion
☐ Access to RB system without the right of signing of electronic documents

Notes: .....

.....

Manager of the company

_____ _____
(signature) *(last name and initials)*

Stamp here

Bank's notes:

Appendix 10 to the Rules of rendering services related to remote banking system by AO Mizuho Bank (Moscow)

APPLICATION
FOR LIMITATION OF TRANSACTIONS

" _____ " _____ 20__

Hereby

_____
(Name of the company)

Requests to introduce the following restrictions on operations on accounts in the RBS system:

Account number	Maximum amount per document (in account currency)	Maximum amount per period (in account currency)	Time period in days

Notes: .....
.....

Manager of the company

_____ _____
(signature) *(last name and initials)*

Stamp here

Bank's notes: