APPROVED
by Moscow Exchange
Order No. МБ-П-2023-1597 of 20 June 2023

Basic Electronic Signature Rules for Moscow Exchange Clients

Moscow

2023

1. Terms and definitions

Rules - Basic Electronic Signature Rules for Moscow Exchange Clients, which define the procedure for the creation and use of a basic electronic signature by Moscow Exchange clients in the Negotiation System. The Rules are an integral part of the Information Technology Services Terms and Conditions of Moscow Exchange (the "ITS Terms and Conditions").

Operator - Moscow Exchange.

Basic Electronic Signature (BES) means an analogue of a handwritten signature, which, through the use of a basic electronic signature key in accordance with the Federal Law of the Russian Federation "On Electronic Signature", certifies the creation of an electronic signature by a particular person.

Client - a user of the Negotiation System who has entered into a pertinent agreement with the Operator.

Transaction - an over-the-counter transaction (purchase and sale of securities, repo, currency transaction, etc.) made by the Clients on the terms agreed in the Negotiation System.

Ticket - consolidated information on the material terms and conditions of a transaction agreed by the parties both in the Negotiation System and outside it, in other information systems.

The Negotiation System is an information system for exchange of legally significant electronic messages for the purpose of agreeing the terms and conditions of OTC transactions, recording the progress of negotiations and creating Tickets. Access to the Negotiation System is provided through the client part of MOEX Dealing software, through the Trade Radar information and trading terminal (if available) and other software solutions similar in functionality.

2. General provisions

2.1. The Negotiation System is operated by Moscow Exchange.

2.2. These Rules establish the procedure and conditions for the use of a basic electronic signature by Clients in the Negotiation System.

2.3. By signing the Application for ordering/changing/refusing access to the MOEX

Dealing System and the Trade Radar information and trading terminal (the "Application") under Technical Centre’s Information Technology Service Agreement of the Technical Centre (the "ITS Agreement"), the Customer accepts the terms and conditions of these Rules and agrees to use the MOEX Dealing System as a negotiation system, including for the use of a basic electronic signature when the Customers who have signed the Application to the ITS Agreement conduct negotiations for the purpose of agreeing the material terms of the Transactions and creating Tickets.

2.4. In order to fulfil the conditions of paragraph 2, Article 160 and paragraph 2, Article 184 of the Civil Code of the Russian Federation, each of the Customers, by acceding to these Rules and signing the Application to the ITS Agreement, authorises the Operator to reach an agreement with another Customer on the use of a basic electronic signature for exchanging electronic messages, conducting negotiations in order to agree on the material terms of the Transactions.

2.5. The Agreement specified in clause 2.4 of this Section is concluded in accordance with part 2, Article 6 of the Federal Law "On Electronic Signature", according to which an electronic document and/or electronic message signed with a basic electronic signature is recognised as equivalent to a paper document signed with a handwritten signature.

2.6. These Rules do not regulate the procedure for concluding Transactions.

3. Procedure of formation and verification of a basic electronic signature in MOEX Dealing

3.1. How a basic electronic signature is created and verified when accessing the Negotiation System using the client part of MOEX Dealing

3.1.1. The basic electronic signature key (the “BES Key”) used in the Negotiation System shall be formed and used in accordance with these Rules. When accessing the Negotiation System via the client part of MOEX Dealing, the login of the account of the Customer's representative in the Negotiation System and the password (a sequence of symbols known only to the user of the account login to ensure information security and confirm the account login user's authority) of the Customer's representative, whose full name is recorded in the Application to the ITS Agreement, are used as the BES Key.

The login of the Negotiation System account is assigned by the Operator.

3.1.2. In the Negotiation System, an electronic message and/or an electronic document shall be signed with a basic electronic signature if the Customer's representative correctly enters the BES Key when registering (logging in) to the Negotiation System.

3.1.3. The Negotiation System records the IP address from which the electronic document and/or electronic message was received, as well as the date and time it was created.

3.1.4. Identification and authentication of the Customer's representative is performed by recognising and verifying in the Negotiation System the information on the login and password of the Customer's representative, and IP address used to access to the Negotiation System and the second authentication factor used at login (if used). The Operator automatically verifies the authenticity of the basic electronic signature of the Customer's representative. In case of successful verification, the electronic document and/or electronic message is recognised as signed by the basic electronic signature of the person whose full name is specified in the Application to the ITS Agreement.

3.1.5. The password for the Negotiation System account is initially generated by the Operator in the Negotiation System using random number algorithms and is transmitted to the Customer's authorised representative in a way that prevents third parties from obtaining it via a secure communication channel. The Customer guarantees secure transfer of the password to its representative specified in the Application to the ITS Agreement. After the Customer's representative receives the password, it is recommended, using the Negotiation System, to change the password with the password generated directly by the representative specified in the Application to the ITS Agreement.

3.1.6. An authenticated representative of the Customer may change his/her password via MOEX Dealing provided that the minimum complexity requirements set in the Negotiation System are met and the history is tracked. The Negotiation System provides for temporary blocking of the login in case of repeated password entry errors to exclude brute force attack. The Negotiation System provides a limit on the maximum password lifetime between password changes, after which the password is locked.

3.1.7. In case of blocking or loss of the password by the user, the Operator shall, on the basis of a separate application of the Customer, form the password similarly to the initial procedure.

3.1.8. Access to the Negotiation System shall be carried out in the Operator's secured dedicated network (ConnectME, Universal Scheme, from the Moscow Exchange colocation area or via VPN).

3.1.9. The Operator shall ensure that access to the Negotiation System is restricted to specific representatives of the Customer only from the Customer's IP addresses specified by the Customer on the Operator's secure dedicated network.

3.2. How a basic electronic signature is created and verified when accessing the Negotiation System using Trade Radar Terminal

3.2.1. When accessing the Negotiation System using the Trade Radar terminal, the MOEX Passport login (email address of the Customer's representative registered in the User Authorisation and Registration System - MOEX Passport, https://passport.moex.com) and the password set by the Customer's representative for this login shall be used as a BES Key in the Negotiation System. The MOEX Passport login and password shall be entered by the Customer's representative each time he/she logs in to the Trade Radar terminal.

3.2.2. MOEX Passport login is specified by the Customer when requesting access to the Trade Radar terminal. The Customer guarantees that the MOEX Passport login belongs to the specified representative of the Customer. The Operator ensures an unambiguous correspondence between the MOEX Passport login specified by the Customer and the login of its representative in the Negotiation System.

3.2.3. Access of the Customer's representative to the Negotiation System using the Trade Radar terminal may be restricted, at the Customer's request, to the Operator's secured dedicated network (ConnectME, Universal Scheme, from the Moscow Exchange colocation area or via VPN).

3.2.4. The Operator shall ensure that access to the Negotiation System is restricted to specific representatives of the Customer only from the Customer's IP addresses specified by the Customer on the Operator's secure dedicated network.

3.2.5. Access to the Negotiation System using the Trade Radar terminal is protected by encryption of all transmitted information at the HTTPS protocol level.

3.2.6. In case of authorisation of access of the Customer's representative via the Internet at the Client's choice, the second authentication factor is used as an additional protection factor when the representative enters the Trade Radar terminal, which is an additional one-time password (OTP) sent to the Customer's representative by e-mail.

3.2.7. Identification and authentication of the Customer's representative is performed by recognising and verifying information about the MOEX Passport login, the password entered at each login of the Customer's representative to the Trade Radar terminal, information about the login to the Negotiation System, the IP address for access to the Negotiation System and the second authentication factor used at login (if used). The Operator automatically verifies the authenticity of the basic electronic signature of the Customer's representative. In case of successful verification, the electronic document and/or electronic message is recognised as signed by the basic electronic signature of the person whose full name is specified in the Application to the ITS Agreement.

4. Rights, obligations and guarantees of the Operator and Clients

4.1. The Customers undertake to keep logins, passwords and other identification data for access to the Negotiation System confidential, to ensure security of the equipment from which the Negotiation System is accessed, to minimise the use of public networks for access to the Internet, and to comply with other rules determined by the Operator.

4.2. In case of unauthorised access to login, password and other identification data, their loss or disclosure to third parties, as well as in case of detection of inappropriate information or errors in the Negotiation System, the Customer shall immediately notify the Operator at: infosecurity@moex.com.

4.3. The Operator has the right to suspend (block) access to the Negotiation System in case of detection of cases of compromise, detection of the fact of signing of electronic messages by third parties, as well as in order to prevent unauthorised access.

4.4. The Customer warrants that its representatives, whose full names are specified in the Application to the ITS Agreement, have the necessary authorisation to conduct negotiations in the Negotiation System.

4.5. The Customer warrants that it conducts negotiations in good faith.

4.6. The Clients have the right to record the results of electronic interaction via the Negotiation System, including for the purpose of using the received materials (printouts of negotiations and Tickets) as confirmation of the terms and conditions of the Transactions agreed by the Parties for the purposes of dispute resolution.

4.7. The Customer shall be entitled to request from the Operator a written confirmation of the existence of specific negotiations in the Negotiation System, one of the parties of which was the requesting entity, as well as the content and status of these negotiations, including technical details (time of significant actions, IP addresses of connections, other technical information), information on the compliance of identification data issued to the Customer with the data recorded by the Negotiation System. The Customer's right specified in this clause shall be valid both during the period during which access to the Negotiation System was provided and after the termination of the access.

4.8. The Operator shall ensure confidentiality of the information stored in the Negotiation Systems. In order to ensure invariability of all electronically signed electronic documents and/or electronic messages sent through the Negotiation System, the Operator's subdivision responsible for information security shall ensure availability and operation of the data storage protected against any alteration. Access to the storage shall be controlled exclusively by the head of the division responsible for the Operator's information security. Tickets and other information shall be stored for at least 5 (five) years.

4.9. The Operator does not check the Customers' ability to conclude Transactions (availability of a master agreement, availability of limits, etc.) on the terms agreed in the Negotiation System.

5. Effectiveness of the Rules, amendment

5.1. The Operator has the right to unilaterally amend these Rules at its own discretion, of which it notifies the Customer by publishing the text of the Rules as amended on the website www.moex.com at least 10 (ten) days before they come into force. These Rules shall be terminated on the basis of the Operator's decision.

5.2. Termination of these Rules shall not affect the legal force and validity of electronic documents and/or electronic messages signed with a basic electronic signature prior to the termination of these Rules.