APPROVED

by order of the Moscow Exchange

on 12 October 2026 (№ МБ-П-2026-4147)

ELECTRONIC DATA INTERCHANGE RULES

Section 1. GENERAL PROVISIONS

Article 1. Terms and definitions

EDI System Administrator means a person representing the EDI System Provider who is authorized to manage the ESVKC in the EDI System, certify the EDI system Provider's ESVKCs with the Moscow Exchange's electronic signatures and lists of revoked certificates with its electronic signature as well as ESVKCs and other documents in hard copy form related to the EDI System activity, with its handwritten signature.

Alternative Certification Authority (ACA) means an accredited certification authority (CA) other than the EDI System Provider's CA. The EDI System Provider or EDI Sub-system Provider may use Electronic Signature Verification Key Certificates created by the ACA in its electronic data interchange application systems, if technically possible. The EDI System Provider and/or EDI Sub-system Provider shall adopt the relevant internal documents establishing the procedure for using those certificates, if necessary.

Exchange Rules means documents approved by Moscow Exchange such as rules for regulated trading; rules for deposit and credit operations; rules for MOEX Board information system; rules and conditions related to the provision of technical access to Moscow Exchange's software and hardware suite and the provision of other information technology services, documents associated with the above-mentioned rules (including those establishing forms, formats and delivery process for information and reporting); and agreements regulating communications between Moscow Exchange and EDI Participants.

ESVKC Owner or Electronic Signature Verification Key Certificate Owner means a person that has obtained ESVKC in accordance with the established procedure.

Decompiling means the process aimed at deriving original text of loadable (executable) modules.

ED's Transference means a procedure of transference of ED from ED Sender to ED Recipient.

Secured (Secret) Encryption Key means an alternative name used herein for Encryption Key.

Secured (Secret) Electronic Signature Key means another name used herein for the Electronic Signature Key.

Applicant means an organization, a private entrepreneur, a natural person who is a representative of a legal entity applying for an unqualified electronic signature verification key certificate at the Certification Authority run by the EDI System Provider as a intended owner of such certificate.

Applicant authentication means efforts to identify and verify the Applicant's details which set out in Federal law No.63-FZ "On electronic signature" by using original documents and/or duly certified copies thereof and/or government and other information systems.

Qualified ESVKC means a complying Qualified Electronic Signature Verification Key Certificate created by an accredited certification authority, or by the federal executive authority responsible for monitoring the use of Electronic Signatures.

Electronic Signature Verification Key means a unique sequence of characters unambiguously related to the Electronic Signature Key and intended to verify the authenticity of the Electronic Signature (hereinafter the Electronic Signature Verification).

Electronic Signature Key means a unique sequence of characters intended to create an Electronic Signature.

Encryption key means a unique sequence of symbols intended for encrypting/decrypting electronic documents or electronic messages with the use of Cryptographic Tools.

Key Carrier means a removable physical storage media intended for Cryptographic Keys storing.

Key Compromise means stating by a person owning the Electronic Signature Key that circumstances arose in which the unauthorized use of such Key may happen.

Corporate Information System means the information system whose participants interacts electronically and compose a certain group of person.

Cryptographic Key means a general name for Electronic Signature and/or Encryption Keys.

EDI System Provider means Public Joint-Stock Company “Moscow Exchange MICEX-RTS” (Moscow Exchange).

EDI Sub-system Provider means a legal entity that has entered into an agreement on organizing the Electronic Data Interchange in the EDI Sub-system with the EDI System Provider.

Package of services means a set of ITS Services and the Services of the EDI System Provider, provided to the EDI Participant for a fixed fee of the EDI System Provider. The list of services is determined by the composition of the Package of services selected by the EDI Participant, according to the Procedure for providing the User with package offers for ITS Services and the Services of the EDI System Provider, posted on the Internet at **http://moex.com/a1819** (further - the Order). The Order is an integral part of the Conditions for Participation in the EDI System and the Agreement on participation in the EDI System.

Public Electronic Signature Key means an alternative name used herein for the Electronic Signature Verification Key.

Public Encryption Key means a unique sequence of symbols uniquely related to the encryption key by a special mathematical ratio. It is intended for encrypting/decrypting electronic documents or electronic messages with the use of Cryptographic Tools.

ED Sender means an individual, a legal entity or an individual entrepreneur, who sends an ED, or on whose behalf an ED is sent. This term does not apply to persons acting as information mediators with regard of a specific ED.

EDI Sub-system means the part of the EDI System being the combination of software, information and technical environment of the EDI Sub-system Provider and the EDI Participants.

ED Recipient means an individual, a legal entity or an individual entrepreneur, to which an ED is sent by, or on behalf of, the ED Sender. This term does not apply to persons acting as information mediators with regard of a specific ED.

EDI Sub-system Provider Rules means internal documents approved by an authorized body of the EDI Sub-system Provider and agreed with the EDI System Provider which stipulates special requirements for the EDI within a given EDI Sub-system. This term applied also to agreements stipulating an interaction between the EDI Sub-system Provider and EDI Participants.

Business day of EDI System Certification Authority means a time period from 9:00 am to 18:00 MSK on each day except for Saturdays, Sundays and public holidays in accordance with the law of the Russian Federation.

Electronic Signature Verification Key Certificate (ESVKC) means an ED or a hard copy document issued by a certification authority or by an agent of a certification authority which certifies that the Electronic Signature Verification Key belongs to the ESVKC Owner. EDI participants are entitled to use both qualified ESVKCs and non-qualified ESVKCs.

Electronic Data Interchange System (the EDI System) means an organizational and technical system operating the EDI and comprising software, dataware and hardware of the EDI System Provider, EDI Sub-systems Providers and EDI Participants.

The EDI System is a corporate information system in which the EDI System Provider manages ESVKCs if the Certification Authority of the EDI System is in place.

Cryptographic Tools means a combination of software and hardware tools that ensure that the following functions are available for execution: producing/verifying electronic signatures, encrypting/decrypting electronic documents and electronic messages, producing cryptographic keys. Cryptographic Tools may be used as either individual tools or as a part of application software.

In the EDI System both certified Cryptographic Tools providing encrypted reinforced qualified electronic signatures and non-certified Cryptographic Tools providing encrypted reinforced non-qualified electronic signatures may be used.

Electronic Signature Tools means encrypted tools being used to fulfill either electronic signature creation or electronic signature verification or electronic signature key creation or electronic signature key verification creation.

In the EDI System both certified Electronic Signature Tools providing encrypted reinforced qualified electronic signatures and non-certified Electronic Signature Tools providing encrypted reinforced non-qualified electronic signatures may be used.

Certification Authority (CA) means an individual, an individual entrepreneur, or a governmental or municipal authority that produces and delivers ESVKC and performs other functions stipulated by the law of the Russian Federation.

Certification Authority run by the EDI System Provider means a certification authority which is operated by the EDI System Provider.

Certification Authority run the EDI System Provider creates only ESVKC for the EDI Participant where along with the name of the Participant is specified an individual, acting on behalf of the legal entity on the basis of constituent documents of the legal entity or the power of attorney.

Cryptographic Keys Management means any activity of the EDI System Provider related to production (generation) of cryptographic keys and registration, safekeeping and distribution thereof.

ESVKC Management means any activities of the EDI System Provider related to production of ESVKC, record-keeping of ESVKC produced by the EDI System Provider, and revocation of ESVKC.

EDI Participant means a government agency, local authority, company and self-employed person, which has signed an EDI System participation agreement with the EDI System Provider.

Trading Member means an entity admitted to trading in one or several exchange markets of Moscow Exchange and/or Joint Stock Company National Mercantile Exchange.

Clearing Member means a Clearing Member of the CCP NCC or NSD (further - the clearing organization), who has signed the Clearing Agreement under which the clearing organization undertakes to provide clearing services according to Rules of clearing of Central Counterparty National Clearing Centre or Rules of clearing of National Settlement Depository.

Electronic Document Format means a structure of a substantial part of an electronic message being the basis of the electronic document. Availability of information on the electronic document format enables any person to convert this document into the form allowing its unequivocal interpretation.

Compression (archiving) of an electronic message using any software compatible with the WinZip software is allowed prior electronic signature procedure.

Encryption means a cryptographic processing of an electronic document or electronic message through applying private (secret) and public encryption keys which allows preventing access by unauthorized persons to the content of the encrypted ED or EM.

Electronic Document means an electronic message that complies with an established format, contains an electronic signature and may be transformed into the form allowing its unequivocal interpretation.

Electronic Data Interchange means an exchange of electronic documents in accordance with these Rules.

Electronic Signature means an electronic data that has been added to other electronic data (the data to be signed) or otherwise connected with such data and that serves for identifying the signatory.

Both the reinforced qualified electronic signature and reinforced non-qualified electronic signature as defined in the effective law of the Russian Federation may be used in the EDI System.

Electronic Message means a holistic set of structured data that is meaningful to participants of communications and encoded in such a manner that allows such data to be processed by a computer, transmitted via communication channels, and stored on a machine-readable medium.

Terms and definitions used herein (except for terms and definitions given in this clause) shall be construed as per their meanings specified in the laws and other regulatory acts of the Russian Federation.

Article 2. Subject of the Rules

1. These Rules as well as Appendices thereto establish general principles for conducting electronic document interchange between the EDI System Provider, EDI Sub-system Provider and other EDI Participants. Requirements for electronic documents content and completion, their formats and requisites, features for their processing, executing and safekeeping are set forth by the Exchange's rules, rules of the EDI sub-system Providers and other agreements executed between the EDI System Provider and EDI Sub-system Providers. Such requirements shall not contradict any principles stipulated herein.
2. Provisions of these Rules shall be applied unless otherwise stated by the legislative or other legal acts of the Russian Federation including regulatory acts of the Bank of Russia.
3. These Rules do not govern issues related to an exchange of electronic messages that are not electronic documents as per these Rules.
4. These Rules do not govern electronic document interchange conducted by using the simple electronic signature as defined in the effective law of the Russian Federation.
5. The EDI System Provider shall create non-qualified ESVKCs at the applicant's request. On the basis of clause 3 of Article 14 of the Federal Law "On Electronic Signature", in the case of issuing an electronic signature verification key certificate to a legal entity, both an individual acting on behalf of a legal entity without a power of attorney and an individual acting on behalf of a legal entity may be indicated as the owner of the electronic signature verification key certificate, along with the indication of the name of the legal entity persons by proxy. ESVKC, the owners of which are individuals acting on behalf of a legal entity under a power of attorney issued before the entry into force of this version of the Rules – 01.09.2023, are valid until the expiration of such ESVKC, and the keys of electronic signatures corresponding to such ESVKC – until the expiration of such keys.
6. In accordance with these Rules, it is unacceptable to recognize an electronic signature and (or) an electronic document signed by it as invalid only on the basis that such an electronic signature was not created with his own hand, but using electronic signature tools for automatic creation and (or) automatic verification of electronic signatures in an information system.

Article 3. Regulation of the electronic document interchange

1. The electronic document interchange in the EDI System and EDI Sub-system are governed by the following documents:
   - these Rules;
   - Exchange's rules;
   - Rules of the EDI Sub-system Providers;
   - agreements executed between the EDI System Provider and EDI Sub-system Providers.
2. The following items may be specified in the Exchange's rules, Rules of the EDI Sub-system Providers and agreements executed between the EDI System Provider and EDI Sub-system Providers:
   - scope and formats of electronic documents eligible for interchange, information interaction regulations, ED registration procedure, procedure for producing ED delivery confirmations, ED safekeeping procedure and other document interchange features related to services rendered to the EDI Participants;
   - procedure and features of the EDI System technical access arrangement.
3. Specific requirements for the following may be specified in the rules of the EDI Sub-system Providers:
   - Defining a list and formats of ED transferred by the EDI Participants within the relevant EDI Sub-system;

- Regulations of information interaction between EDI Participants within the relevant EDI Sub-system;
- ED registration procedure within the relevant EDI Sub-system;
- features of the procedure for producing ED delivery confirmations within the relevant EDI Sub-system;
- features of safekeeping of ED produced within the relevant EDI Sub-system;
- other features of the EDI related to EDI Sub-system Provider services rendered to EDI Participants.

The EDI Sub-system Provider's rules are subject to approval by the EDI System Provider.

4. The EDI Sub-system Provider is entitled to draw up its rules to include use of ACA's services in the provider's sub-system. In this case such ACA shall distribute Cryptographic Tools and Electronic Signature Tools, manage Cryptographic Keys and ESVKC within the relevant EDI Sub-system in accordance with ACA's internal documents. The EDI participants of the sub-system shall use ESVKC created by the ACA in accordance with these Rules and the Sub-system Provider's Rules.

5. EDI Participants shall have the right to have a qualified ESVKC created by an Alternative Certification Authority in accordance with the procedure approved by such certification authority for further use in accordance with these Rules, provided that the EDI System Provider has the technical capability to use such ESVKC. An unqualified ESVKCA may only be created by the Certification Authority operated by the EDI System Provider.

6. EDI Participants and EDI System Provider and/or EDI Subsystem Provider, subject to respective conditions in the Exchange Rules, are entitled to exchange electronic documents and use for their signing both the reinforced qualified signature, for which the respective ESVKC has been created by the Alternative Certification Authority, and the reinforced unqualified electronic signature, for which the EDI Provider has created the respective ESVKC, including, but not limited to:

   - when concluding, amending and terminating any agreements related to participation in organized trading, as well as when carrying out operations on the OTC market, agreements related to clearing and information technology services, listing services, as well as agreements in accordance with Appendix No. 3 to these Rules, both between the EDI Provider / EDI Subsystem Provider and EDI Participants, and EDI Participants with each other;
   - with regard to powers of attorney;
   - in respect of documents about the client which is the EDI Participant (files), including questionnaires, letters, notifications;
   - with regard to documents on securities, including issuance documents (hereinafter referred to as "Client documents").

7. EDI participants agree to use an electronic signature in accordance with these Rules to exchange electronic documents including signing Client's documents. To comply with clause 2, article 160 and clause 2, article 184 of the Russian Civil Code, each EDI participant authorises the EDI System Provider to obtain other EDI Participants' consent to use an electronic signature when they execute/amend/terminate agreements or exchange electronic documents. Such authorisation is to be valid for thirty (30) years. When an EDI participant adopts these Rules, the EDI System Provider executes its authority to agree to the use of electronic signatures between the EDI participant and existing/new EDI participants. These agreements are concluded in pursuance of part 2 of article 6 of the Federal law "On electronic signature" which stipulates that an electronic document signed with a simple electronic signature and/or reinforced unqualified electronic signature is deemed equivalent to a document in hard copy signed with a handwritten signature.

8. EDI participants acknowledge that agreements and other electronic forms signed between them or between them and the EDI System Provider/EDI Sub-system Provider with an enhanced encrypted certified digital signature or an enhanced encrypted uncertified digital signature have the same legal force as agreements in hard copy signed with a handwritten signature.

Article 4. Admission to the EDI System

An EDI Participant is to be admitted to the EDI System and EDI Sub-system(s) subject to fulfillment of the following:

1) Executing an EDI System Participation Agreement with the EDI System Provider;

2) Installing necessary hardware and software;

3) Receiving necessary passwords and IDs from the EDI System Provider or EDI Sub-system Provider to be able to access the EDI System;

4) Making cryptographic keys and ESVKC.

Article 5. Procedure for these Rules to come into effect and be amended

1. These Rules including all Appendices thereto are subject to approval by the EDI System Provider. Any amendments and supplements are introduced by the EDI System Provider unilaterally. The EDI System Provider is entitled to set a time frame and procedure for amendments and supplements to these Rules to come into effect.

2. These Rules becomes applicable to an EDI System Participant following its execution of the EDI System Participation Agreement with the EDI System Provider.

3. These Rules becomes applicable to an EDI Sub-system Provider following its execution of an agreement on arranging the electronic document interchange in the EDI sub-system.

4. The EDI Sub-system Provider draws up and approves the EDI regulations for the EDI sub-system on its own in accordance with the principles set forth in these Rules. If case of regulations' non-compliance with these Rules the provider must correct all inconsistencies.

Article 6. Amendment notifications

1. Unless otherwise decided by the EDI System Provider the EDI Participants and EDI Sub-system Providers shall be notified by the EDI System Provider on any amendments and supplements to these Rules and any Appendices thereto as well as decisions of the EDI System Provider on a time frame and procedure for such amendments and supplements to come into force by category V electronic documents. The stated notifications shall be provided at least 10 calendar days prior to the amendments and supplements effective date.

2. Electronic documents are to be send to addresses indicated by EDI Participants.

3. The EDI System Provider shall keep a hard copy of these Rules and all amendments and supplements thereto during 12 years after termination thereof.

4. An EDI Participant may request hard copies of these Rules and all amendments and supplements thereto. Such hard copies shall be provided within 15 calendar days after a relevant request was submitted by the participant.

Section 2. ELECTRONIC DOCUMENT

Article 7. Requirements for electronic document

1. Any electronic document produced via the EDI System shall be deemed legally enforceable and involving legal consequences stipulated in such document as per these Rules.

2. Any electronic document used in the EDI System shall be considered to be properly executed provided that it complies with the law of the Russian Federation and/or these Rules and/or Exchange rules and/or EDI Sub-system Providers rules and/or agreements executed between the EDI System Provider and EDI Sub-system Providers.

3. An electronic message shall be considered as a legal electronic document provided that it complies with these Rules and/or Exchange rules and/or EDI Sub-system Providers rules and/or agreements executed between the EDI System Provider and EDI Sub-system Providers.

4. Electronic documents shall be produced in one of formats specified in these Rules and/or Exchange rules and/or EDI Sub-system Providers rules and/or agreements executed between the EDI System Provider and EDI Sub-system Providers, and signed with the electronic signature.

5. Electronic documents produced in a format that does not comply with established rules shall not be considered as electronic documents under these Rules.

6. The visualization of an electronic signature is intended for ease of review and is not an electronic signature, which means that it does not give the document legal force. The legally significant original document is exclusively an electronic document signed by an electronic signature in accordance with the established procedure.

Article 8. Applying electronic signature and encryption when interchanging electronic data

1. Electronic documents shall be signed only with electronic signature keys for which the EDI System Provider or ACA has made ESVKC.
2. An electronic document shall be considered to be signed by an authorized person if it was signed with an electronic signature key for which the EDI System Provider or ACA made ESVKC intended for an authorized person of the EDI Participant.
3. Legal enforceability of an electronic document is not affected if it was signed with a private (secret) electronic signature key being valid as at the moment of signing.
4. Each EDI Participant shall have individual electronic signature keys to be used by such participant for signing EDs with its electronic signature.
5. Any ED containing confidential information shall be encrypted. The sender shall define by itself whether the ED is confidential or not.
6. When an encrypted ED is received it shall be decrypted in accordance with the established technology. Then the electronic signature of the ED is to be verified.
7. An ED is to have legal effect provided that its electronic signature was successfully verified.
8. To help reducing data volume transmitted with electronic documents specific algorithms for data compression may be applied. Compressed EDs may be encrypted if necessary.

Article 9. Use of electronic documents

1. All legal affairs processed by electronic documents in accordance herewith and other EDI System Provider's or EDI Sub-system Providers' documents shall be considered as executed in writing and shall not be disputed just because they were executed electronically.
2. An electronic document shall come into force as follows:
   - Category A electronic documents: from the moment of receiving the document "Confirmation" by the sender from the receiver. This document shall be signed with the receiver's electronic signature.
   - Category B electronic documents: from the moment of receiving a confirmation (receipt) by the sender from the receiver;
   - Category V electronic documents: from the moment of sending the electronic document by the sender;
   - Category G electronic documents: from the moment of receiving the electronic document by the receiver.
3. The electronic document's category stated in Clause 2 of this Article is defined in accordance with the Exchange rules, rules of the EDI Sub-systems Providers and agreements made by the EDI System Provider and EDI Sub-systems Providers. If the document category has not been identified, the document is given Category G by default.

Article 10. Electronic document originals

1. An electronic document may have an unlimited number of copies including those made on various types of machine-readable mediums. To produce one more copy of an existing electronic document a user shall reproduce content of such document with its electronic signature.
2. All copies of an electronic document shall be deemed as its originals.
3. An electronic document original does not exist if:
   - no copy of such electronic document registered by the EDI System Provider or the EDI Sub-systems Provider is available and restoration is not possible and/or;
   - the electronic signature used to sign the document cannot be identified.

Article 11. Copies of an electronic document

1. Electronic documents shall be issued from the electronic document repository in the form of electronic copies or hard copies.
2. Where it is necessary to certify copies of electronic documents, the electronic signature of the head of the organization or an officer authorized by the head shall be used or a hard copy of the document shall be certified in accordance with the established procedure (clauses 2.47, 5.14 of the Rules approved by Order No. 526 of the Ministry of Culture of Russia dated 31 March 2015).
3. As a general rule, a notation of certification of a copy shall be affixed under the "Signature" detail and shall include: the word "True"; the title of the person who certified the copy; his/her handwritten signature; the printed name (initials, family name); the date of certification of the copy (excerpt from the document). If the copy is issued for submission to another organization, the mark on certification of the copy is supplemented by an inscription on the place of storage of the document from which the copy was made ("The original document is kept with (name of the organization) in file No. _____") and certified by the seal of the organization. A stamp may be used to certify the copy (clause 5.26 of GOST R 7.0.97-2016, approved by Order No. 2004-st of Rosstandard dated 08 December 2016).
4. When certifying copies of electronic documents, the certification inscription shall be supplemented with an indication of the electronic form of the document and the name of the software by means of which the electronic document was accessed. For example: "The copy of the electronic document is correct. Copy reproduced using "Document" software. Title. Full name. Date".
5. Electronic document and its copies shall be authentic.
6. Software converting an ED for the purpose of its printing in hard copy is a part of the software used in the EDO Sub-systems.

Section 3. ELECTRONIC DOCUMENT INTERCHANGE ORGANIZATION

Article 12. Electronic Document Interchange

The Electronic Document Interchange provides for the following operations:

1) forming an electronic document;
2) sending and delivering electronic document;
3) verifying an electronic document;
4) confirming an electronic document delivery;
5) withdrawing an electronic document;
6) registration of incoming and outgoing electronic documents;
7) keeping electronic documents (keeping electronic documents archives);
8) producing extra copies of an electronic document;
9) producing copies of an electronic document.

Article 13. Forming electronic documents

An electronic document shall be formed as follows:

1) Forming an electronic document in a format established for such electronic documents of such type;
2) Signing of the electronic document with the electronic signature.

Article 14. Sending and delivering electronic documents

1. In sender-receiver relationships an ED shall be considered as being send by the sender if it was send by:
   - the sender itself, or
   - a person authorized to handle this document on behalf of the sender, or
   - an automatic information system used by the sender.

2. An ED shall not be considered as being send by the sender if:

   – the receiver knew or had to know including following the verification, that the ED was not send by the sender; or

   – the receiver knew or had to know including following the verification, that the corrupted ED was received.

3. Specifics of electronic documents sending, delivering and receiving shall be stipulated in these Rules, Exchange rules, rules of the EDI Sub-systems Providers, and agreements signed by the EDI System Provider and EDI Sub-systems Providers.

4. In order to exchange Client documents and other electronic documents provided for by the Moscow Exchange Rules, the EDI Participants and the EDI System Provider and/or the EDI Sub-system Providers have the right to use, at their discretion and choice, the following channels of information interaction:

   - e-mail services, access to which can be provided in accordance with the established procedure by both the EDI System Provider and other providers of e-mail services;

   - personal account of the participant (LKU);

   - issuer's personal account (LCE);

   - candidate's personal account (LCC);

   - universal file gateway (EDIgate);

   - other channels of information interaction provided for by the Exchange Rules, the rules of the EDI Sub-system Providers, contracts concluded between the EDI System Provider and the EDI Sub-system Providers (hereinafter referred to as internal documents).

   In case of contradictions between these Rules and internal documents regarding the names of information communication channels available for use by the EDI Participants and the EDI System Provider and/or the EDI Sub-system Providers, the internal documents adopted in the development of these Rules prevail.

Article 15. Proving the authenticity of electronic documents

1. The electronic documents verification procedure comprises of the following:

   – verification of ED compliance with a format set for such type of documents;

   – verification of authenticity of all electronic signatures contained in the electronic document.

2. Electronic Signature Tools used in the verification of the electronic signature provide the content of the electronic document signed with the electronic signature including the view of that signature as well as the number, owner and period of the Electronic Signature Verification Key Certificate, as well as they show if any changes were made to the electronic document.

3. If the ED verification process is successful this document shall be executed and processed. Otherwise, it shall be considered as not received and the receiver shall notify the sender thereof in accordance with the procedure which shall be set forth in these Rules, the Exchange rules, rules of the EDI System Provider, and agreements signed by the EDI System Provider and EDI Sub-systems Providers.

4. If an encrypted ED is received it shall be decrypted before being verified. If the decryption of such document is not available the receiver shall notify the sender in accordance with the procedure which shall be set forth in these Rules, the Exchange rules, rules of the EDI Sub-systems Providers, and agreements signed by the EDI System Provider and EDI Sub-systems Providers.

Article 16. Confirming electronic document delivery

1. Electronic document delivery shall be confirmed as follows:

   – For Category A documents: by sending the electronic document “Confirmation” to the sender;

   – For Category B documents: by sending the electronic message “Receipt” to the sender;

- For Category G documents: the sender finds out whether the document has been received, from the receiver.

2. No confirmations shall be required for Category V documents.
3. The electronic document “Confirmation” is the Category B document.
4. The format of the electronic document “Confirmation” is set by the Exchange rules, rules of the EDI System Provider, and agreements signed by the EDI System Provider and EDI Sub-systems Providers.
5. Unless otherwise stipulated in the Exchange rules, rules of the EDI System Provider, and agreements signed by the EDI System Provider and EDI Sub-systems Providers, Category A or Category B electronic documents (except for the electronic document “Confirmation”) shall not be considered as being received by the receiver until the sender gets relevant confirmation.
6. If a sender did not receive a confirmation within the established period of time it may notify the receiver thereof and indicate a time period during which such confirmation must be send.
7. If the confirmation was not received during the time period indicated by the sender, it is entitled to refrain from considering the ED as being sent. For cases where the confirmation is not received within the established time period the Exchange rules, rules of the EDI Sub-systems Providers and agreements signed by the EDI System Provider and EDI Sub-systems Providers may provide for an obligation of the sender to transfer information contained in the ED to the receiver by other communications means including telex, fax, etc.

Article 17. Electronic document withdrawal

1. An EDI Participant is entitled to withdraw an electronic document by sending the electronic document “Withdrawal Notification” to the receiver.
2. The “Withdrawal Notification” is of the same category as the document to be withdrawn.
3. The “Withdrawal Notification” shall contain a reason of the document withdrawal.
4. Any electronic document may only be withdrawn prior to its execution by the receiver.

Article 18. Record-keeping

1. Electronic documents are recorded in the electronic or paper registries. The electronic registries shall be fit for being fulfilled, administered (reviewed, searched and printed) and kept. Software and hardware used for keeping the electronic registrars shall be a part of the software and hardware used for arranging the EDI.
2. Specifics of electronic document record-keeping in the EDI System are set forth in the Exchange rules, rules of the EDI Sub-systems Providers and agreements signed by the EDI System Provider and EDI Sub-systems Providers.
3. When arranging the record-keeping for electronic documents in the EDI System the EDI System Provider and EDI Sub-systems Providers shall ensure registration of data that allows users being informed on all electronic document life cycle stages.
5. The EDI System Provider and EDI Sub-systems Providers shall ensure that any data recorded in the electronic registries is protected against an unauthorized access and unintended destruction and/or corruption. Records in the registries shall be kept for at least five years.

Article 19. Archiving of electronic documents

1. All electronic documents recorded in the EDI System shall be kept in the electronic archives within time periods set forth in the EDI System Provider’s or EDI Sub-Systems Providers’ internal documents, but not less than the periods of storage established by the legislation depending on the type of documents and the scope of regulation.
2. Unless otherwise stated in the Exchange rules, rules of the EDI Sub-systems Providers and agreements signed by the EDI System Provider and EDI Sub-systems Providers electronic documents shall be kept in a format in which they were formed, send or receiver.
3. Relevant electronic and paper registries, ESVKC and the software applied to those electronic registries and electronic signatures contained in documents kept shall be kept in addition to electronic documents. There shall be at least two copies of each electronic

document storage unit in the archive of EDI provider or EDI Subsystem Provider (main and working copies shall be on different physical devices).

4. Private (secret) encryptions keys shall be kept in electronic archives if any electronic documents encrypted with such keys are being kept.

5. Archived electronic documents shall be bound to relevant ESVKC in order for a dispute resolution procedure is available.

6. The EDI System Provider, EDI Sub-systems Providers and EDI Participants shall be responsible for keeping electronic documents.

7. The EDI Provider and the EDI Subsystem Providers shall appoint an official responsible for compliance with the requirements for the storage of electronic archive documents; shall ensure the delimitation and control of access to electronic archive documents; at least once every 5 years the technical control of the physical condition of carriers of electronic documents and reproducibility of electronic documents shall be performed; for quick access to electronic documents for reference and search purposes, an electronic documents fund shall be established within the archive.

8. Electronic archives and archives of electronic documents paper copies shall be protected against unauthorized access and unintended destruction and/or corruption.

9. Electronic files with expired storage period shall be marked for destruction on general grounds, after which they shall be physically destroyed or destroyed by software and hardware with a relevant note in the document destruction certificate.

Section 4. SETTLEMENT OF CONFLICTS AND DISPUTES ARISEN IN CONNECTION WITH THE EDI

Article 20. Potential conflicts related to the EDI

1. Any conflicts may arise in connection with forming, delivering, receiving, confirming delivery of electronic documents in the EDI System as well as applying the electronic signature to them. Such conflicts may arise, in particular, where:

   - a party has failed to prove the authenticity of electronic documents by the electronic signature tools of the receiving party;
   - the fact of electronic document formation is being disputed;
   - the fact that the ESVKC owner signing the document was identified is being disputed;
   - an EDI Participant has filed an application on electronic document corruption;
   - the fact that the electronic document was send and/or delivered is being disputed;
   - an electronic document sending and/or delivering time is being disputed;
   - the authenticity of copies of an electronic document and/or of its original and its hard copy is being disputed;
   - other conflicts related to the EDI.

2. Any conflicts may also arise where an EDI Participant, EDI System Provider or EDI Sub-system Provider:

   - distrusts content and formats of electronic documents kept in the local archive of the Participant's or EDI Sub-system Provider's terminal; or
   - distrusts terminal's software.

Article 21. Conflict notification

1. Where any conflict is expected the EDI Participant, EDI System Provider or EDI Sub-system Provider shall notify the EDI System Provider, or the EDI Sub-system Provider if the conflict has arisen within the EDI Sub-system, thereof promptly, or within three business days after the conflict appearance, or within a shorter period of time stipulated in the Exchange rules, rules of the EDI Sub-systems Providers, and agreements signed by the EDI System Provider and EDI Sub-systems Providers.

2. Any notification on an expected conflict shall contain information on the conflict essence and circumstances indicating the conflict as believed by the notification sender. Any notification shall contain all attributes of the electronic document stipulated herein regardless of its form (whether it electronic or written). In addition, it shall contain a full name, job title, phones, fax and e-mail of a person(s) authorized to negotiate on the conflict settlement.

   Conflict notifications shall be executed and sent as a Category A electronic document. In case the foregoing is unachievable, a conflict notification shall be written and shall be sent with a courier or otherwise provided that the delivery confirmation is to be available.

3. A party which has received a conflict notification shall check circumstances indicating the conflict promptly or no later than on the next business day (or within a shorter period of time stipulated in the Exchange rules, rules of the EDI Sub-systems Providers, and agreements signed by the EDI System Provider and EDI Sub-systems Providers) and inform the notification sender on the check results and measures taken to settle the conflict if necessary.

Article 22. Conflict resolution in the normal course of business

1. Any conflict shall be considered as being resolved in the normal course of business if the notification sender is satisfied with information received from the EDI Participant, EDI System Provider or EDI Sub-system Provider to which it had send the notification.

2. If the sender is not satisfied with information received from the EDI Participant, EDI System Provider or EDI Sub-system Provider to which it had send the notification the technical commission is to be established.

Article 23. Establishing the technical commission. Commission members.

1. The technical commission shall be formed no later than on the next business day after the decision on its formation was made or no later than on the sixth business day after the conflict notification was received provided that the conflict was not resolved in the normal course of business. Rules of an EDI Sub-system Provider may stipulate shorter time-frames for forming the commission.

2. Unless otherwise agreed by the EDI Participants involved in the conflict each conflict party shall provide at least one authorized representative to be a member of the commission. Number of such representatives from each conflict party shall be equal.

3. As a rule, the technical commission is composed of technical and information security specialists of the parties. Members of the commission shall have knowledge needed in creating cryptographic protection systems and operating computer information systems.

4. Regardless of agreements reached by the parties the commission shall include at least one representative of the EDI System Provider in addition to parties' representatives.

5. Each member of the commission shall act on behalf of relevant Party and EDI System Provider on the basis of the power of attorney to be valid during the commission period.

6. As may be initiated by any of the parties, independent experts that meet requirements set forth in Clause 3 of this Article may be involved in the technical expertise carried out by the commission members. The party getting involved independent experts shall pay for the expert services on its own.

Article 24. Scope of the technical commission competence and powers

1. When considering a conflict the technical commission shall establish availability or non-availability of actual technical evidences of facts that the electronic document was executed and/or send, it was authentic, signed with the specific electronic signature and that the document send and the document received are authentic.

2. The commission is entitled to consider any other technical issues that are needed, in commission's judgment, to clarify causes and consequences of the conflict.

3. The commission shall not estimate facts established by it from a legal or other point of view.

4. Special software stated as well as the Procedure stipulated in Appendices hereto shall be applied while carrying out necessary checks and documenting information used during the checking.

Article 25. Report on technical commission work

1. All actions undertaken by the technical commission in order to find out the actual evidences as well as its findings shall be written in the Report on the technical commission work.

   The Report on the technical commission work shall contain the following:

   - List of commission members and their qualifications;
   - Brief summary of the conflict;
   - activities undertaken by the commission in order to find out causes and consequences of the conflict. Date, time and venue of such activities;
   - findings of the commission;
   - signatures of all members.

2. If the opinion of the commission member(s) regarding the process, methods and objectives of commission activities does not coincide with the opinion of the majority of the membership a special record on that shall be made in the Report. Such record shall be signed by the member(s) having the alternative opinion.

3. The Report shall be produced in one original and hard copy which shall be kept with the EDI System Provider. Any party to the conflict or any member of the technical commission may require that a copy of the Report certified by the EDI System Provider is given to them. A copy of the Report certified by the EDI System Provider may be provided to the EDI Sub-system Provider, if necessary.

Article 26. The technical commission work statement

1. After the end of the technical commission work a statement with brief summary of commission findings shall be drawn up. Besides the findings that statement shall include the following:

   - members of the commission;
   - statement date and place;
   - dates, start and end times of the commission operation;
   - short list of activities undertaken by the commission;
   - signatures of the members;
   - reference to an alternative opinion of the commission member(s) if available.

2. The statement shall be made in a number of original copies. Each party to the conflict, EDI System Provider and the EDI Sub-system Provider, if necessary, shall receive one original copy of the statement. A member of the commission may require a copy of the statement certified by the EDI System Provider.

3. An alternative opinion of a member(s) of the commission that did not agree with the commission findings reported in the Statement may be enclosed. Such alternative opinion may be produced in no particular form. Number of the alternative opinion original copies shall coincide with the number of Statement original copies. The alternative opinion shall constitute and appendix to the Statement.

4. The technical commission work statement shall be sent to parties to the conflict by the EDI System Provider by special delivery or otherwise provided that delivery confirmation is to be available.

Article 27. Judicial conflict resolution

All disputes and disagreements not resolved via the procedure set forth in articles 20-26 hereof, are to be referred to the Moscow Arbitration Court.

Section 5. Miscellaneous

Article 28. Appendices

The following items shall be annexed hereto and shall constitute an integral part thereof:

Appendix No 1. EDI Participation Terms and Conditions.

Appendix No 2. Procedures of the Certification Authority run by the EDI System Provider.

Appendix No 3. Procedure for using electronic documents for executing, amending and terminating agreements and exchanging other non-formalized documents between EDI participants.

Article 29. Termination

1. There Rules shall be terminated with regard to all EDI Participants if relevant resolution of the EDI System Provider is available.
2. Termination of these Rules and Appendices thereto shall not affect a legal effect and validity of electronic documents that the EDI System Provider, EDI Sub-system Providers and EDI Participants interchanged prior to the termination.