PROCEDURES OF THE CERTIFICATION AUTHORITY RUN BY THE EDI SYSTEM PROVIDER (PROCEDURES OF EDI CA)

1. GENERAL PROVISIONS

1.1. SUBJECT MATTER

Procedures of certification authority run by the EDI System Provider ("EDI CA") are developed in accordance with the current laws of the Russian Federation and the Electronic Data Interchange Rules approved by the authorized body of Moscow Exchange (the "EDI Rules").

These Procedures determine the manner and conditions of services rendering by EDI CA including the basic organizational and technical measures focused on support of work of EDI CA, using enhanced electronic signature in EDI System and electronic signature verification key certificates, those including qualified electronic signature verification key certificates (hereinafter "ESVKC").

Amendments to these Procedures shall be unilaterally made by the EDI System Provider. The EDI Participants shall be notified of making amendments to the Procedures by the EDI System Provider in accordance with the EDI Rules.

1.2. INFORMATION ABOUT THE CERTIFICATION AUTHORITY

The CA is located at Bolshoy Kislovsky pereulok 13 Moscow Russia. There are no branches.

The CA provides services to the EDI Participants during its business hours.

1.3. INFORMATION ABOUT THE SERVICES RENDERED BY THE CA

Information about the services provided by the CA is available on the Moscow Exchange's website at http://moex.com/s1425, and on request from EDI participants by email stated below.

Contacts: telephone number +7 495 363 32 32, email: pki@moex.com, http://moex.com.

1.4. COST OF SERVICES

The CA's services as to the creation of ESVKCs, provision of cryptographic tools and their maintenance, and other services related to the administration of the electronic document interchange process under the EDI Rules are rendered for a fee, unless otherwise provided for by the Tariffs. The prices (tariffs) for the services shall be approved by the authorized body of the EDI System Provider. Information of the prices (tariffs) shall be published on the EDI System Provider's website at http://www.moex.com/s1425.

The payment procedure and periods are set forth in the Terms and Conditions for participation in the EDI System (Appendix 1 for EDI Rules).

2. SCOPE OF FUNCTIONS PERFORMED BY THE CA

2.1. EDI CA shall perform the following functions and render the following services to the EDI Participants:

2.1.1. Creation and issuance of the ESVKC subject to: the applicant authentication; receiving the confirmation of the authority for the person acting on behalf of the applicant which is the legal entity to apply for the qualified certificate;

2.1.1.1. Confirmation of an electronic signature key holder receiving an ESVKS;

2.1.1.2. determination of ESVKC validity period;

2.1.2. cancellation of ESVKC issued by the EDI CA;

2.1.3. provision of electronic signature tools for the creation of the electronic signature key and the electronic signature verificaiton key by an applicant;

2.1.4. maintenance of ESVKC issued and cancelled by EDI CA (hereinafter the "Register of Certificates"), among others including the data contained in ESVKC issued by EDI CA, and the data of ESVKC expiration or cancellation with reasons specified; assurance of access to these registers via information and telecom networks, also via Internet;

2.1.5. issue of ESVKC in electronic form from the Register of Certificates upon request;

2.1.6. confirmation of verification keys uniqueness in the Register of Certicates;

2.1.7. confirmation of an electronic signature at the request of an EDI Participant, as well as for the purpose of technical examination when settling conflict situations related to the electronic data interchange;

2.1.8. confirmation of authenticity of the electronic signature of EDI CA at request, as well as for the purpose of technical examination when settling conflict situations related to the electronic data interchange;

2.1.9. provision and technical maintenance of Cryptographic Tools, inclusive of appropriate software;

2.1.10. arrangement for maintenance services provided to trading and/or clearing members who are EDI Participants in the course of electronic data interchange with the use of electronic signature;

2.1.11. other services related to the use of electronic signature.

2.2. Employees of EDI CA may be engaged as experts for settlement of disputable issues related to using of ESVKC produced by EDI CA.

2.3. Procedures for keeping the Register of Certificates and accessing the Register of Certificates are identical for both the qualified and non-qualified certificates.

3. RIGHTS AND OBLIGATIONS OF THE CA

3.1. **The CA is entitled to:**

3.1.1. Request documents to confirm information given in the certificate application;

3.1.2. Request and receive information necessary to prove the authenticity of documents and details submitted by an EDI Participant from operators of major government databases by using the infrastructure facilitating data and technical interoperability of data systems used to provide government and municipal services and perform relevant functions in the electronic form;

3.1.3. Request and receive the following forms from government data bases:
- An extract from the unified state register of legal entities regarding corporate applicants;
- An extract from the unified state register of individual entrepreneurs regarding applicants who are individual entrepreneurs;
- An extract from the unified state register of taxpayers regarding foreign corporate applicants;

3.1.4. Request that an EDI participant provide further documents proving the authenticity of details submitted if the CA has identified any discrepancies between information submitted by such EDI Participant and information received by the CA as per section 2.2, article 18 of the Federal Law "On electronic signature";

3.1.5. Reject documents submitted by an EDI Participant if they do not meet requirements set forth in Russian regulatory acts currently in effect;

3.1.6. Refuse to issue an ESVKC for an EDI Participant if the participant fails to perform obligations set forth in section 2, article 18 of the Federal Law "On electronic signature" and regulatory acts issued under the law;

3.1.7. Refuse to cancel an ESVKC if it has already been annulled or terminated for other reasons;

3.1.8. Without a request from the holder, cancel an ESVKC in case the CA is aware of actual compromise of the holder's electronic signature key; the holder fails to fulfil obligations set forth in Russian law in the area of electronic signature; the CA has true information on falsification of documents submitted by the EDI Participants in order to receive the ESVKC and/or unauthenticity of such documents with regard to data included into the ESVKC; or services to create and issue the ESVKC have not been paid in due course.

3.2. The CA must:

3.2.1. Inform EDI participants in writing of terms and procedures for using electronic signatures and electronic signature tools, of risks associated with the use of electronic signatures and measures to ensure security of electronic signatures and verification process;

3.2.2. Insert only accurate and updated information proved by appropriate documents into ESVKCs;

3.2.3. Keep information updated in the Register of Certificates and ensure its protection from unauthorised access, destruction, modification, blocking and other unlawful actions;

3.2.4. Ensure 24 hours access to the Register of Certificates in Internet excluding periods of scheduled and unscheduled maintenance;

3.2.5. Keep confidential electronic signature keys created by the CA;

3.2.6. According to section 5, article 18 of the Federal Law "On electronic signature", send information on the issued qualified certificate;

3.2.7. Refuse creating an ESVKC if ownership by the EDI Participant regarding the electronic signature key specified by the participant in the certificate application;

3.2.8. Refuse creating an ESVKC if the uniqueness check of the electronic signature verification key stated by the EDI Participant in the ESVKC application fails in the

Register of Certificates.

4. PROCEDURES AND TIME FRAMES

4.1. Creation of electronic signatures keys

4.1.1. An applicant creates electronic signature keys (cryptographic keys) by himself by using software provided by the CA and sends the electronic request to the CA to issue the ESVKC via email or user account on the EDI Provider's website at https://cabinet.moex.com/about?show_login_popup=1. The first production of Cryptographic Keys by the ESVKC owner is performed during the owner registration process. In case of scheduled of off-scheduled change of the Cryptographic Keys the owner of the ESVKC uses his existing cryptographic keys to interact with the CA.

4.1.2. When creating and subsequently using his/her cryptographic keys, the ESVKC owner shall follow information security requirements set forth in the documentation and the cryptographic tools form, as well as security precautions set forth herein with regard to electronic signature, electronic signature facilities and cryptographic tools (See Appendix No. 7 to this Procedure).

4.1.3. Validity period of the CA's Electronic Signature Keys is three (3) years. In the event of planned CA's Electronic Signature Keys substitution, the new Electronic Signature Keys of EDI CA shall be generated. The CA shall provide the EDI Participants with an option to renew CA's ESVKC at the place of working of the ESVKC owner during the period remaining until expiry of the keys. Scheduled changes of Electronic Signature Keys are announced on the Moscow Exchange's website at http://moex.com/s1270 with new CA's ESVKCs posted on the website at the same time as an update signed with the old CA's electronic signature key.

4.1.4. The CA's ESVKCs in hard copy are provided to EDI Participants on request.

4.1.5. Unscheduled changes of the electronic signature key from the CA is made upon its actual or threatened compromise. All ESVKCs signed with an electronic signature key to be changed are terminated simultaneously with the key change with details on such ESVKCs entered into the Register of Certificates. Where an unscheduled change of the electronic signature key from the CA is made, the CA creates free of charge ESVKCs for all owners whose ESVKC is terminated due to the change.

4.1.6. Either electronic signature keys of ESVKC owners may be changed upon the application to create the ESVKC (see the application form in Appendix 1 hereto) or a request to issue the ESVKC delivered in the form of the electronic document signed with the electronic signature key of the ESVKC owner.

4.1.7. If an electronic signature key of an ESVKC owner is changed due to its actual or threatened compromise, the CA cancels the ESVKC upon application from the owner or the EDI Participant (see the application form in Appendix 4 hereto) and create a new ESVKC upon relevant application. Electronic signature keys are also changed if the application to create the ESVKC is submitted with violation of some applicable requirements.

4.1.8. New ESVKCs in the form of the electronic document are sent to applicants via email or their user accounts on the Moscow Exchange's website at https://cabinet.moex.com/about?show_login_popup=1. New ESVKCs are recorded in the CA's Register of Certificates.

4.1.9. The EDI System Administrator prints out a new ESVKC in hard copy in two copies, certifies them with handwritten signature and the CA's seal and then delivers to the owner with a written acknowledgment of the owner's acceptance of the certificate.

4.1.10. The CA delivers ESVKCs subject to article 18 of the Federal Law "On electronic

signature".

4.1.11. The requirement for the scope of ESVKCs, i.e. the area of relations in which the EDI Participant's ESVKC may be used continues to be in force for ESVKCs created before 1 July 2020; this requirement does not apply to ESVKCs created after 1 July 2020.

4.1.12. The list of areas in which ESVKCs are used:

- Electronic data interchange across the Money Market;
- Electronic data interchange across the Equity & Bond Market;
- Electronic data interchange of the FX and Precious Metals Markets;
- NSD electronic settlement system;
- Electronic data interchange across NSD;
- Access to trading via ASTSBridge and WEB2L;
- Electronic data interchange across CCP NCC;
- Electronic data interchange NME;
- Corporate electronic data interchange;
- ESVKS application areas are not required.

4.2. Creation and delivery of certificates

4.2.1. Procedure for registration of ESVKC owners

4.2.1.1. Only legal entities or individual entrepreneurs having obtained the status of an EDI Participant are eligible to ne registered as the ESVKC owner by EDI CA.

4.2.1.2. A new ESVKC owner shall be registered only upon submission by the EDI Participant of the following documents:
- Application for production (generation) of ESVKC (form of the application is furnished in Appendix No. 1 hereto);
- Power of attorney for the ESVKC owner (form of the Power of Attorney is furnished in Appendix No. 2 hereto);
- The power of attorney for a person authorised to represent the corporate applicant to the Certification Authority (the form of the power of attorney is given in Appendix 3 hereto).

The application to create the ESVKC may be furnished as an electronic document signed by the owner or the authorised person of the EDI Participant.

Documents in foreign languages must be enclosed with their translations certified by a notary or the consulate.

If any data to be included into a certificate needs to be proved with a document for which the effective legislation provides for the established form, the applicant should furnish the CA with the document in such form.

As agreed with the EDI Provider, the EDI Participant shall provide documents listed in Appendix 5 (for RF residents), or Appendix 6 (for non-residents) hereto, in addition to the documents listed in this clause.

EDI CA shall be entitled to request the EDI Participant to provide other documents in order to settle any disputes arising in connection with confirmation of EDI Participant's legal capacity and EDI Participant's representative's authority, also of the person authorized to act on behalf of EDI Participant without a power of attorney.

The documents listed above or their duly certified copies shall be submitted only in case they were not submitted before.

In case of change of earlier provided data, the EDI Participant has the right to provide the documents (according to Appendices 5 and 6) confirming such changes, in electronic form with electronic signature of the EDI Participant.

4.2.1.3. According to the procedure set out in clauses 1 and 2 of Article 18, Federal Law "On electronic signature", the CA proves the identity of the ESVKC owner applying for the ESVKC or other applicant acting on behalf of the legal entity to verify its authority to apply for the certificate.

4.2.1.4. EDI CA shall verify the correctness of execution of the documents submitted.

4.2.1.5. The EDI Participant shall pay for the services of EDI CA in accordance with the procedure stipulated by the relevant agreement on participation in Electronic Data Interchange System.

4.2.1.6. The ESVKC owner makes his/her cryptographic keys on his/her own by using software provided by the EDI CA, and then send a request to the EDI CA for the ESVKC initial production via user account on the EDI System Provider's website at https://cabinet.moex.com/about?show_login_popup=1.

4.2.1.7. The owner prints off the request, signs it by hand, stamps with the EDI Participant's seal (if any) and sends to the EDI CA.

4.2.1.8. The EDI System Administrator matches the electronic and paper requests. If the requests match, the Administrator creates an ESVKC based on information stated in the ESVKC production application and the request.

4.2.1.9. As the ESVKC has been produced under the above-mentioned procedure, the ESVKC owner is considered to be registered.

4.2.1.10. The ESVKC is passed to the user via the electronic communication channels (email or the Participant's personal account on the EDI Administrator official website at https://cabinet.moex.com/about?show_login_popup=1) and added to the certificate register of the EDI Administrator.

4.2.1.11. When giving a qualified certificate, the CA ensures that the applicant reads and understands information contained in the qualified certificate. The applicant shall confirm that it has read information in the qualified certificate by using the qualified electronic signature if any valid qualified certificate is available, or by using the basic electronic signature of the individual applicant with the key received in person while applying for government or local government services in electronic form set out by the Russian government, provided that the citizen was identified using information technologies without his/her personal attendance by deriving data from the unified identification and authentication system and unified biometric system. This confirmation as signed with the electronic signature including the simple electronic signature is recognized as the electronic document with the same force and effect as the document in hard copy signed manually by the individual.

4.2.2. Production of ESVKC

4.2.2.1. When producing (generating) ESVKC, it is added by the information submitted by the EDI Participant at the time of contract conclusion with the EDI System Provider, which ensures participation in the Electronic Data

Interchange System, as well as the data specified in the application for production (generation) of ESVKC at the time of the ESVKC owner registration. In case of change of the specified information, the ESVKC owner shall submit to EDI CA a new application for ESVKC production (generation).

4.2.2.2. The validity period of Electronic Signature and Secured (Secret) Encryption Keys of the ESVKC owner shall be established when generating ESVKC and is equal to one (1) year, the validity period of ESVKC shall be equal to ten (10) years. For the legal entities, belonging to Moscow Exchange Group, the EDI System Provider, if necessary, has the right on its own initiative and in coordination with such legal entity to set a different validity period of Electronic Signature and Secured (Secret) Encryption Keys when forming ESVKC. The Parties undertake to record the new validity period in the relevant Agreement providing participation in Electronic Data Interchange System.

4.2.2.3. EDI Participants with electronic signature keys expired before 1 August 2020, may obtain ESVKC with the content similar to the expired qualified certificates and the period of validity of one year and three months starting from the termination date for the qualified certificate. This ESVKC is given on the basis of the application (certificate request). In this case, the service fee charged by the CA remain unchanged.

4.2.3. ESVKC creation and delivery times

4.2.3.1. ESVKCs are created and delivered within three (3) business days after the relevant application has been received by the CA provided that the CA receives a request to issue the ESVKC in the form of the electronic document serving as the basis for the certificate creation.

4.2.4. Fees for ESVKC creation and delivery

4.2.4.1. Fees for creation and delivery of ESVKCs are set in accordance with section 1.4 hereof.

4.3. **Validity confirmation for electronic signature having been used to sign electronic documents**

4.3.1. EDI CA shall render to the EDI Participants the services of examination works related to proving of authenticity of the electronic signature in the electronic document, as well as participate in the technical examination in case of settlement of the conflict situations related to the Electronic Data Interchange.

4.3.2. Authenticity of the electronic signature in the electronic document shall be proved upon the application of the EDI Participant which it files to EDI CA in the form of a paper document. The application shall contain the following information:
- date and time of the application filing;
- identification data of the ESVKC owner, authenticity of the electronic signature of which shall be proved in the electronic document;
- time and date of generation of the electronic signature of the electronic document;
- time and date as of which the electronic signature authenticity shall be established.

4.3.3. The obligatory enclosure to the application for proving of authenticity of the

electronic signature in the electronic document shall be the electronic data storage carrier containing:

- ESVKC using which authenticity of the electronic signature in the electronic document shall be proved;
- electronic document — in the form of one file containing the data and the electronic signature indicator for these data (the electronic signature in the associated format), or two files one of which contains the data and the second — the electronic signature indicator for these data.

4.3.4. The works of proving of authenticity of the electronic signature in the electronic document shall be performed by the commission formed of the number of employees of EDI CA. The result of the commission works shall be the conclusion of EDI CA.

4.3.5. The conclusion shall contain:
- the result of verification of electronic signature of the electronic document (true/untrue);
- report on the verification performed.

4.3.6. The report on the verification performed shall contain:
- time and place of the verification;
- membership of the commission performing the verification;
- grounds for verification;
- data the commission is provided with for the purpose of the verification;
- content and results of the verification;
- explanation of the verification results.

4.3.7. Conclusion of EDI CA on the verification performed shall be executed in free form in two copies, signed by all the commission members and certified by the seal of EDI CA. One of the verification conclusion copies shall be provided to the applicant.

4.3.8. Proving of authenticity of the electronic signature in one electronic document and writing the conclusion on the verification performed shall take no more than three (3) business days from the date of the application receipt by EDI CA.

4.3.9. When authenticity of an electronic signature having been used to sign electronic documents is confirmed, all validity of ESVKCs in the chain of verification for a given ESVKC to the CA's ESVKC issued by the principal certification authority.

4.3.10. A fee for confirmation of validity of an electronic signature having been used to sign electronic documents is already included in the service fee for trading and/or clearing members for electronic data interchange with the aid of digital signatures which is set in accordance with section 1.4 hereof.

4.4. Procedures to terminate and revoke certificates

4.4.1. ESVKC shall be terminated in the following cases:
- in case of these Procedures termination in respect of an EDI Participant (termination of the contract providing participation in the Electronic Data Interchange System);
- in case of termination of the Power of Attorney for the ESVKC owner, which establishes the limitation of powers when using the ESVKC
- at request of ESVKC owner or the EDI Participant (form of the application is

furnished in Appendix 4 hereto);

- upon expiry of ESVKC;
- compromise of the Electronic Signature Key of EDI CA;
- the CA ceases its business activities without its business functions being transferred to third parties;
- in other cases provided for in the EDI Rules.

4.4.2. EDI CA shall cancel ESVKC in the following cases:

- if it is not affirmed that the ESVKC owner holds the Electronic Signature Key that matches the Electronic Signature Verification Key specified in such ESVKC;
- in case it is affirmed that the Electronic Signature Verification Key in ESVKC is already present in ESVKC generated earlier;
- in case the court decision affirming inaccurate information in ESVKC becoming effective.

4.4.3. The record on ESVKC termination shall be made by EDI CA in the Register of Certificates within 12 hours once the circumstances listed in sections 4.4.1 and 4.4.2 herein arise, or once EDI CA became or should have become aware of such circumstance. ESVKC shall terminate once the record thereof has been made in the Register of Certificates.

4.4.4. The official notice of EDI CA of the ESVKC cancellation shall be publishing of the first (the earliest) revoked certificates list containing the information of the revoked ESVKC and issued not earlier than the specified event takes place. The time of the ESVKC revocation shall be deemed the time of issue of the specified revoked certificates list kept in the field "thisUpdate" of the revoked certificates list. The information on the revoked certificates list publishing shall be entered to the issued ESVKC of EDI CA in the name suffix "ESVKC CRL Distribution Point".

4.4.5. In case of the ESVKC cancellation upon its expiry, the time of the ESVKC cancellation shall be deemed the time saved in the field "notAfter" of the field "ESVKC Validity". In this case the information on the cancelled ESVKC shall not be included in the revoked certificates list. In case of EDI CA Electronic Signature Key compromise the time of cancellation the ESVKC of the ESVKC owner shall be deemed the time of EDI CA Electronic Signature Key compromise fixed in the register of EDI CA.

4.4.6. In case of EDI CA Electronic Signature Key compromise, the information of the ESVKC of ESVKC owner shall not be entered in the revoked certificates list.

4.4.7. The application for cancellation of ESVKC shall be sent by the ESVKC owner to EDI CA by postal or courier service.

4.4.8. The specified application for cancellation of ESVKC shall be accepted during the operating hours of EDI CA.

4.4.9. In case of refusal to cancel the ESVKC, EDI CA shall notify the relevant EDI Participant.

4.5. **Procedure to handle the compromise of electronic signature key**

4.5.1. The ESVKC owner or the EDI Participant shall independently take the decision on the

fact of compromise threat of their Electronic Signature Key.

4.5.2. The events on the basis of which the ESVKC owner holding the Electronic Signature Key or the EDI Participant takes the decision on Electronic Signature Key compromise shall include without limitation the following:

- loss of the key carriers, including with their finding afterwards;
- dismissal of the ESVKC owner having access to the key carriers;
- revelation by the ESVKC owner of the EDI Participant of the facts and events of unauthorized using of the key carrier by the third parties;
- violation of the rules of key carriers storage.

4.5.3. In case that the ESVKC owner or the EDI Participant reveals the fact of Electronic Signature Key compromise, it shall contact EDI CA and take the actions for cancellation of the ESVKC thereof in accordance herewith.

4.5.4. The ESVKC owner shall perform the off-scheduled change of the compromised Cryptographic Keys in accordance herewith.

4.6. **Procedure for keeping the Register of Certificates**

4.6.1. The CA's Register of Certificates has been implemented in the form of a network directory of certificates with access via LDAP.

4.6.2. The network directory with the register of qualified certificates is available at ldap://simple/vcert.pki.moex.com:50001/c=RU. The network directory with the register of unqualified certificates is available at ldap://simple/vcert.pki.moex.com:50003/c=RU.

4.6.3. Entries on the certificate cancellation or revocation are made into the register of certificates in accordance with section 4.4.3 hereof.

4.7. **Procedure for scheduled and unscheduled maintenance of the register of certificates**

4.7.1. The register maintenance lasts for no more than 24 hours.

4.7.2. The register maintenance is announced on the CA's website at http://moex.com/s1270.

5. PROCEDURE FOR THE CERTIFICATION AUTHORITY TO FULFILL ITS OBLIGATIONS

5.1. Notices to applicants on terms and procedures of using electronic signatures, risks and security measures

The CA notifies applicants of terms and procedures of using electronic signatures and electronic signatures tools, risks associated with the use of electronic signatures and security measures applied to electronic signatures and the verification process thereof by publishing from time to time these Procedures on the Moscow Exchange's official website at http://fs.moex.com/files/8905, as well as by proving applicants with documents and forms applicable to certified cryptographic tools.

5.2. Updates to the register of certificates and its protection

The CA keeps information in the register of certificates updated. The CA protects such information from unauthorised access, destruction, modification, blocking and other unlawful actions. Updated versions of the register are published in Internet according to the procedure and within the time frames determined by the CA. The CA does not guarantee that such information is free from errors, full and blocked from unauthorised access; it will not be held responsible for occurrence of such violations if it takes all reasonable and sufficient security measures.
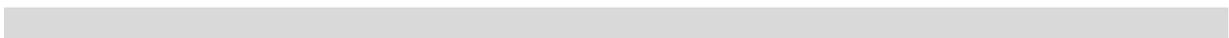
5.3. Access to the register of certificates

The CA ensures 24 hours access to the register of certificates in Internet excluding periods of scheduled and unscheduled maintenance;

5.4. Confidentiality of electronic signature keys

The CA ensures confidentiality of electronic signature keys produced by itself. The CA takes necessary security measures to ensure confidentiality of such keys throughout their life cycle. Confidentiality procedures and security measures with regard to electronic signature keys are determined by the CA.

5.5. The CA registers qualified ESVKCs in the unified identification and authentication system pursuant to part 5, article 18 of the Federal Law "On electronic signature".

5.6. The CA gives free access to the network directory with information in the register of certificates including revocations of ESVKCs, for any person.

Appendix No. 1 to Procedures of EDI CA

(ESVKC for a legal entity or individual entrepreneur with specification in ESVKC of the information on the individual acting on behalf of the legal entity or individual entrepreneur)

On the letterhead of the organization/individual entrepreneur

For the attention of EDI
System Administrator

Application
for Generation of the Electronic Signature Verification Key Certificate

1. For the purpose of using in the Electronic Data Interchange System the organizer of which is Moscow Exchange

_____
(full name of the organization including the form of incorporation or full name of the individual entrepreneur)

Represented by _____
(full name of the applicant acting on behalf of the legal entity – owner of the ESVKC or other applicant)

Acting on the basis of _____

hereby requests to produce ESVKC in accordance with the data specified in this application:

1.1.attributes of the subject name (DN) for the ESVKC to be produced:

INN*	*INN (Taxpayer Identification Number) of the organization/individual entrepreneur*
OGRN/OGRNIP**	*OGRN (Primary State Registration Number) of the organization/OGRNIP of the individual entrepreneur*
SNILS***	*Insurance Number of Individual Personal Account (SNILS) of the ESVKC owner*
title (T)	*Position of the ESVKC owner*
commonName (CN)	*First name, patronymic and last name of the ESVKC owner*
organizationUnitName (OU)	*Division of the organization (shall not populate the field for the individual entrepreneur)*
organizationName (O)	*Organization/individual entrepreneur name*
localityName (L)	*Settlement name*
stateOrProvinceName (ST)	*Name of the territorial subject (for example, 77 Moscow)*

* for EDI Participants registered with the Russian tax authorities;
** for EDI Participants registered in the Russian Federation;
*** for ESVKC holders who are citizens of the Russian Federation

2. Applicant authentication:

☐ in person;

☐ not in person, but using the qualified electronic signature.

3. The Owner of the ESVKC being produced shall act on the basis of:

☐ foundation documents (Articles of Association) ☐ Power of Attorney ☐ Is an individual entrepreneur

4. The EDI Participant uses Cryptographic Tools:

☐ in the Russian Federation   ☐ in other countries

5. ESVKC type to be produced for the EDI Participant:

☐ qualified ESVKC (certified Cryptographic Tools shall be applied)

☐ non-qualified ESVKC (non-certified Cryptographic Tools shall be applied)

6. Contracts from the EDI Participant:

Name and surname: ....

Telephone number: ....

Email: ....

7. I, _____
<div align="center">(full name of the ESVKC owner)</div>

_____
<div align="center">(series and number of the passport, name of the issuing authority and the date of issue)</div>

in accordance with the Federal Law No. 152-FZ dated July 27, 2006 On personal Data for the purpose of registration and servicing with the Electronic Data Interchange System the organizer of which is Moscow Exchange (Russian Federation, 125009, Moscow, Bolshoy Kislovsky per, 13), do hereby interested and agree for Moscow Exchange to process (including collection, arrangement, accumulation, storage, clarification, renewal, amendment, using, distribution (including transfer), depersonalization, blocking, destruction) my personal data with or without the automated means, including: name, patronymic, last name, residence address, details of the principal identity document (series, number, name of the issuing authority and the date of issue), place of work, position, contact telephone number, insurance number of individual personal account and other information required for the purposes of the Electronic Data Interchange Rules approved by the Authorized body of Moscow Exchange.

I agree to include my first name, patronymic and last name, place of work, e-mail, insurance number of individual personal account in public sources of personal data that are Electronic Signature Verification Key Certificate and Register of Electronic Signature Verification Key Certificate.

This Agreement shall enter into force upon signature, acts before the specified by regulatory enactments expiration of the terms of storage relevant information or documents are used in the processing of my electronic signature. This Agreement may be revoked any time upon the written application of the ESVKC owner (person acting on behalf of the EDI Participant) with simultaneous cancellation (revocation) of the issued ESVKC as established by the Electronic Data Interchange Rules.

ESVKC owner (a person acting
on behalf of the EDI Participant based   _____   _____
on the power of attorney   (signature)   (initials, last name)
No _____ dated ____)

_____ 20 (date)

On the letterhead of the organization/individual entrepreneur

Power of Attorney No. _____

_____   _____
(place of issue)   (date of issue)

_____,
(full name of the organization including the form of incorporation, or full name of individual entrepreneur, OGRNIP)

hereinafter — the "EDI Participant" represented by

_____
(position)*

_____
(full name)*

acting on the basis of the Articles of Association*, does hereby authorize

_____
(full name)

_____
(series and number of the passport, name of the issuing authority and the date of issue)

in accordance with the Electronic Data Interchange Rules approved by the Authorized Body of Moscow Exchange to represent the interests of the EDI Participant as the owner of the Electronic Signature Verification Key Certificate, namely:

- to sign by handwritten signature the application for production or for cancellation of the Electronic Signature Verification Key Certificate the owner of which is the specified authorized person, Electronic Signature Verification Key Certificates and requests for initial production of the Electronic Signature Verification Key Certificates in the form of a paper documents;

- to sign by its Secured (Secret) Electronic Signature Key the requests in the form of electronic documents for production of the Electronic Signature Verification Key Certificates the owner of which is the specified authorized person, for future use of these certificates and the Cryptographic Keys corresponding thereto during the validity periods specified in these certificates, on behalf of the EDI Participant upon its instruction and due to participation in the Electronic Data Interchange within the framework of the Electronic Data Interchange System the organizer of which is Moscow Exchange;

- to obtain Cryptographic Tools software and software tools to deal with the Electronic Signature Verification Key Certificates at the EDI Participant's client workplace.

This Power of Attorney shall expire on _____, 20___ .

Position and full name of the Head Officer of the EDI Participant Organization/Full name of individual entrepreneur

Signature of the Head Officer of the EDI Participant Organization/individual entrepreneur

* Is filling in case of issue of the power of attorney on behalf of the legal entity.

(Form of the Power of Attorney for a person who has the authority to represent the CA on behalf of the applicant-legal entity)

On the letterhead of the organization/individual entrepreneur

Power of Attorney No. _____

_____   _____
     (place of issue)   (date of issue)

_____,
    (full name of the organization including the form of incorporation or full name of individual entrepreneur, OGRNIP)

hereinafter — the "EDI Participant" represented by

_____
    (position)*

_____
    (full name)*

acting on the basis of the Articles of Association*, does hereby authorize

_____
    (full name)

_____
    (series and number of the passport, name of the issuing authority and the date of issue)

for taking of the following actions within the framework of the Electronic Data Interchange System the organizer of which is Moscow Exchange:

- to sign by handwritten signature the application for production or for cancellation of the Electronic Signature Verification Key Certificate the owner of which is the specified authorized person, Electronic Signature Verification Key Certificates and requests for initial production of the Electronic Signature Verification Key Certificates in the form of a paper documents;

- to submit and certify the correctness of the copies of documents necessary to obtain the services of the Certification Authority;

- to obtain Cryptographic Tools software and software tools to deal with the Electronic Signature Verification Key Certificates at the EDI Participant's client workplace.

This Power of Attorney shall expire on _____, 20___ .

Position and full name of the Head Officer of the EDI Participant Organization/Full name of individual entrepreneur

Signature of the Head Officer of the EDI Participant Organization/individual entrepreneur

* Is filling in case of issue of the power of attorney on behalf of the legal entity.

On the letterhead of the organization/ individual entrepreneur

For the attention of EDI
System Administrator

Application
for Cancellation of the Electronic Signature Verification Key Certificate

_____
(full name of the organization including the form of incorporation or full name of individual entrepreneur, OGRNIP)

represented by

_____
(position of the Head Officer of the EDI Participant Organization)*
_____
(full name of the Head Officer of the EDI Participant Organization)*

due to _____
(reason for cancellation (revocation) of ESVKC)

requests to cancel (revoke) the ESVKC containing the following data:

serialNumber	*ESVKC serial number*
ESVKC issuer name (DN)	*INN=007702077840,OGRN=1027739387411,CN=MOEX CA,O=Moscow Exchange,L=Moscow,ST=RU Moscow,C=RU*

used by the ESVKC owner

_____
(Full name of the ESVKC owner)

in accordance with the Electronic Data Interchange Rules approved by the Authorized Body of Moscow Exchange.

You are requested to cancel this ESVKC on _____, 20___.

Position* and full name of the EDI Participant's representative
Signature of the EDI Participant's representative

_____ 20__ (date)

L.S.

* to be specified in case of issue of the power of attorney on behalf of the legal entity.

POOL OF DOCUMENTS
to be provided by a new RF resident participant for getting connection to the EDI system

1. **Legal entities:**

- A copy of the passport of the ESVKC owner acting in behalf of the EDI Participant or other applicant acting on behalf of the EDI Participant. Such copy must be signed by an authorised representative.

- Copy of Individual Personal Account (SNILS) of a person acting in behalf of the applicant.

- The power of attorney (either original document, or copy certified by the notary) issued to the ESVKC owner(in case of signing contracts, other documents, document certification, other legally significant actions are executed by the authorized representative).

- Original document of the content for personal data processing from the persons the delivered documents have been issued to (in the case of additional documents containing personal data and not provided for in this Appendix).

- Signed by the authorized person and certified by the seal of the organization (if available) Application for access to information support "Personal account of the Participant" (hereinafter – PAP). Details on the procedure for providing access to the PAP - on the website of Moscow Exchange at: http://moex.com/a1676.

- The power of attorney authorising the holder to apply for an ESVKC on behalf of a person who is not the owner of the ESVKC and is acting on behalf of the corporate applicant;

- The document authorizing the applicant to act on behalf of the legal entity without the power of attorney, or to act on behalf of a government agency or local government agency.

2. **Individual entrepreneurs:**

- A copy of the passport of the ESVKC owner or other applicant acting in behalf of the EDI Participant. Such copy must be signed by an authorised representative.

- Insurance Number of Individual Personal Account (SNILS) of a person acting in behalf of the applicant.

- A copy of the individual entrepreneur registration certificate. Such copy must be signed by the individual entrepreneur.

- A copy of the certificate confirming the individual entrepreneur's registration for tax purposes. Such copy must be signed by an authorised representative.

- The power of attorney (either original document, or copy certified by the notary) issued to the ESVKC owner(in case of signing contracts, other documents, document certification, other legally significant actions are executed by the authorized representative).

- Original contents for the processing of personal data from persons specified in the documents to be furnished.

- Signed by the authorized person and certified by the seal of the individual entrepreneur (if available) Application for access to information support "Personal account of the Participant" (hereinafter – PAP). Details on the procedure for providing access to the PAP - on the website of Moscow Exchange at: http://moex.com/a1676.

POOL OF DOCUMENTS
to be provided by a new non-resident participant for getting connection to the EDI system
(all the documents, except for those listed in item 4, should be certified with apostille or otherwise in accordance with established procedures and should be translated into Russian with the translation certified by a notary)

- A copy of the main proof of identity of the ESVKC owner acting on behalf of the EDI Participant. Such copy must be signed by the authorised representative.

- A proof of state registration of the entity.

- A proof of registration with the RF tax authority (a copy of documents certified by a notary or the legal entity).

- Abstract of trade register (if available).

- A proof of legal entity senior officer's authorities, or a power of attorney issued to the authorized persons (in case of signing contracts, other documents, document certification, other legally significant actions are executed by the authorized representative).

- The power of attorney authorising the holder to apply for an ESVKC on behalf of a person who is not the owner of the ESVKC and is acting on behalf of the corporate applicant.

GUIDELINES
for Ensuring Safe Usage of Electronic Signature
and Electronic Signature Tools

1. General Provisions

These Guidelines regulate security precaution issues with regard to reinforced qualified electronic signature, reinforced non-qualified electronic signature, and related reinforced qualified and non-qualified electronic signature tools.

Foremost, the Guidelines' provisions shall apply to reinforced qualified electronic signature and reinforced qualified electronic signature tools. These Guidelines also may apply to reinforced non-qualified electronic signature and reinforced non-qualified electronic signature tools to their fullest extent, except for requirements which are not applicable since the options named in these Guidelines are not implemented in reinforced non-qualified electronic signature tools (such as the option use of key carriers).

With regard to reinforced qualified electronic signature and reinforced qualified electronic signature tools, these Guidelines shall, according to the Federal Law "On electronic signature" dated 6 April 2011, serve as an instrument to officially notify EDI Participants on terms and conditions, risks and procedures for using reinforced qualified electronic signature and reinforced qualified electronic signature tools, and security precautions when using reinforced qualified electronic signature.

For unification purposes, generalized terms *electronic signature* and *electronic signature tools* are used throughout the text of these Guidelines.

In addition to these Guidelines, when ensuring safe usage of electronic signature and electronic signature tools the EDI Participant should be guided by operational documentation requirements and electronic signature facility forms (if any), as well as requirements of the federal executive authority responsible for monitoring the use of Cryptographic Tools.

2. Space requirements

When locating computer equipment with electronic signature tools installed, security precautions must be taken to prevent any unauthorized access by outside parties to the premises where electronic signature tools are located. If unauthorized persons need be present in the premises, their actions should be monitored to avoid them negatively affecting electronic signature tools, cryptographic tools, and provided information.

The internal layout premises, location and equipment of workstations should ensure safe keeping of confidential documents and data, including key information, provided to contractors.

3. Requirements to electronic signature tools, general-system and special software installation

3.1. When using electronic signature tools, the following security precautions should be taken to prevent unauthorized access to data:

3.1.1. Password setting and resetting policy should be developed and used (to access OS, BIOS etc), enforcing the following password complexity requirements:

- the password has a minimum length of 6 characters;

- the password contains uppercase and lowercase characters, digits and special symbols (@, #, $, &, *, % and etc.);

- the password may not be a simple combination of letters and digits (may not contain names, surnames, common abbreviations, user's account name, postal address, dictionary entries, slang, dialect or jargon words);

- the password can't have more than two repeated characters;

- if you are changing or resetting your password, your new password should be at least four positions different from your last password;

- the password should be reset when logging in the AWS for the first time and then changed on a regular basis (once a quarter).

3.1.2. When using the Electronic Signature Keys, computer equipment configuration should meet the following requirements:

- non-standard, modified or debug OS versions may not be used;

- OS other than those required for normal operation may not be downloaded and used;

- OS and OS settings may not be controlled, administered or modified remotely;

- all unused resources should be disabled (protocols, services ets);

- security modes in OS should be set to a maximum level;

- all users and groups registered in OS should be assigned minimum possible authorizations required for normal operation;

- measures should be taken to limit access to:

- system registry;

- files and catalogs;

- temporary files;

- system logs;

- swap files;

- cached data (passwords etc);

- debug information.

3.1.3. For AWS used:

- efforts shall be taken to prevent in AWS any software that enable OS errors be used to extend granted privileges;

- OS security update packs (Service Packs, Hot fix etc) shall be regularly installed, anti-virus databases shall be regularly updated.

3.1.4. When hardware with installed electronic signature tools is connected to public data networks, it is necessary to take all efforts to exclude any possibility of opening and executing files and script objects received from public data networks if not scanned for software bugs and viruses

3.1.5. The following should be arranged and applied:

- audit system and regular audit findings analysis;

- set of anti-virus measures.

3.2. The following is prohibited:

- unauthorized copying of data from key carriers;

- disclosing contents of key carriers or provide key carriers to parties which are not authorized to access to such contents, displaying or printing out key information, or outputting it to any other display devices;

- using key carriers in modes other than normal modes of using key carriers;

- modifying electronic signature tools software in any manner;

- recording any outside information to key carriers;

- leaving computer equipment with installed electronic signature tools unattended after key information has been entered;

- deleting key information from key carriers before ESVKC expires or is cancelled.

4. Security precaution requirements when handling key information and key carriers with electronic signature keys

4.1. Protecting Electronic Signature Keys.

When you create Electronic Signature Keys, they shall be written to pre-initialized (formatted) key carriers of valid types according to technical and operational documentation.

Should it be technically possible, Electronic Signature Keys written to key carriers shall be password (PIN-code) protected. The password (PIN-code) shall be created by a person who generates keys according to the operational documentation for the electronic signature key tools used.

The Electronic Signature Key's owner shall be responsible for keeping passwords (PIN-codes) secure.

Should it be technically possible, passwords (PIN-codes) shall meet complexity requirements listed in Section 3 herein.

4.2. Handling key information and key carries.

It is not allowed to e-mail files with key information (except for public keys) via both Internet and intranet mail services.

Storing key information in local or network drives, or in built-in memories of hardware with electronic signature tools contributes to the commission of fraudulent actions.

The Electronic Signature Key's owner shall keep Electronic Signature Keys secret and confidential, not disclose them to other parties and shall make every effort to prevent them from compromising.

Key carriers shall be used by their owners only and kept out of reach of third parties (lockers, sealed boxes, metal cases etc).

Key carriers shall be kept inserted in the reading device only for the period while electronic signature tools are generating and verifying electronic signature keys, or encrypting and decrypting. Keeping key information inserted in the reading device for a long time significantly increases the risk of unauthorized access to key information.

Storing any other information (including work or personal files) on key carries is not allowed.

5. Security precautions for AWS with installed electronic signature tools.

To control outgoing and incoming traffic, hardware with installed electronic signature tools shall be protected with firewalling software or hardware.

Hardware with installed electronic signature tools shall meet the following requirements:

- passwords used for OS user accounts meet complexity requirements listed in Section 3 herein;

- only licensed software is installed;

- licensed anti-virus software with regular virus database updates is installed, anti-virus software operates continuously in automatic mode;

- all unused services and processes of the operating system should be disabled (including remote administration and control, shared access to network, system drives, etc.);

- software development and debug tools may not be used with hardware;

- OS updates are regularly installed;

- efforts are taken to prevent unauthorized access (physically and/or remotely) to hardware with electronic signature tools and cryptographic tools;

- information security event log is activated;

- auto screen lock is enabled after the user leaves his/her workstation.

Should hardware with installed electronic signature tools be transferred (written off, submitted for repairs) to any third party, all the information which if used by authorized parties might cause harm to the EDI Participants, should be guaranteed to be deleted, including electronic signature tools, EDI system logs etc.