|  |
| --- |
| APPROVEDby Minutes of the Board Meeting of JSC 'Belarusian Universal Commodity Exchange' dated 31.10.2019 No. 219 (as amended by Minutes of the Board Meetings dated 24.05.2021 No. 81, 26.08.2021 No. 158, 13.09.2021 No. 181, 10.06.2024 No. 131, 30.09.2024 No. 225) |

**REGULATIONS**

of JSC 'Belarusian Universal Commodity Exchange' on Distribution of Public Keys for Authentication of Digital Signatures for Participation in Exchange Trading

Minsk

TABLE OF CONTENTS

[CHAPTER 1. GENERAL PROVISIONS 3](#_Toc256000000)

[CHAPTER 2. STRUCTURE AND MAIN FUNCTIONS OF THE CERTIFICATION AND REGISTRATION AUTHORITIES OF THE EXCHANGE 4](#_Toc256000001)

[CHAPTER 3. TYPES OF ACTIVITIES 5](#_Toc256000002)

[CHAPTER 4. ISSUE OF PKCs FOR PARTICIPATION IN EXCHANGE TRADING 5](#_Toc256000003)

[CHAPTER 5. SUBSCRIBER PKC STATUS MANAGEMENT 7](#_Toc256000004)

[CHAPTER 6. AUTHENTICATION OF SUBSCRIBER PKCs ISSUED BY THE EXCHANGE 8](#_Toc256000005)

[CHAPTER 7. VALIDITY PERIODS OF THE KEY DOCUMENTS 9](#_Toc256000006)

[CHAPTER 8. EXCHANGE PRIVATE KEY COMPROMISE 9](#_Toc256000008)

[CHAPTER 9. SUBSCRIBER PRIVATE KEY COMPROMISE 9](#_Toc256000009)

[CHAPTER 10. RIGHTS AND OBLIGATIONS OF THE EXCHANGE 9](#_Toc256000010)

[CHAPTER 11. CHAPTER 11. RIGHTS AND OBLIGATIONS OF THE SUBSCRIBER 10](#_Toc256000011)

[CHAPTER 12. LIABILITY OF THE EXCHANGE AND THE SUBSCRIBERS 11](#_Toc256000012)

[CHAPTER 13. ARCHIVE STORAGE 11](#_Toc256000013)

# CHAPTER 1. GENERAL PROVISIONS

1.1. These Regulations are developed in accordance with the applicable legislation of the Republic of Belarus regulating operations in the area of protection of information, informatization, and electronic documents management, and provide procedures for the conduct by JSC 'Belarusian Universal Commodity Exchange' ('Exchange') of operations related to the distribution of public keys for authentication of digital signatures for participation in exchange trading.

The activities listed in paragraph 3 of these Regulations shall be carried out by the Exchange as part of provision to the exchange trading participants of exchange auctions organization and conduct services.

1.2. The Exchange shall distribute public keys for authentication of electronic digital signatures in accordance with the applicable legislation of the Republic of Belarus, and on the basis of License dated 15.10.2019 No. 01019/456 issued by Operations and Analysis Center under the President of the Republic of Belarus.

1.3. These Regulations shall be published on the official website of the Exchange at www.butb.by ('Exchange website').

The subscribers of the Exchange and other stakeholders shall be notified of amendments and additions to these Regulations, as well as of any other developments related to the distribution of public keys for authentication of electronic digital signatures for participation in exchange trading, by publication of the relevant information on the Exchange website.

1.4. The electronic digital signature devices received by the subscriber as a result of distribution by the Exchange of public keys for authentication of electronic digital signatures for participation in exchange trading, as well as the related private and public keys, shall be used with the information systems of JSC 'Belarusian Universal Commodity Exchange', and for other purposes as stipulated by the existing legislation of the Republic of Belarus, by-laws of the Exchange, and contracts on the use of electronic digital signature devices executed by the Exchange.

1.5. These Regulations shall use terms and their definitions as set out in the Law of the Republic of Belarus dated 28.12.2009 No. 113-Z 'On Electronic Documents and Electronic Digital Signatures', as well as the following terms and their definitions:

'subscriber' shall mean any legal entity or individual, including any individual entrepreneur, to which/whom a public key certificate is issued.

'generation of private and public keys' shall mean the process that involves implementation of the algorithm used to generate the private key and the corresponding public key;

'applicant' shall mean any legal entity or individual, including any individual entrepreneur, which/who approaches the Exchange for registration in the capacity of a subscriber;

'private key compromise' shall mean loss of trust in the private key;

'revocation of a public key certificate' shall mean the process that involves early termination of a public key certificate;

'suspension of a public key certificate' shall mean the process that involves modification of the public key certificate status to exclude the possibility of its use during the suspension period;

'registration of the subscriber' shall mean the process that involves verification of the documents provided by the subscriber and of correctness of completion of such documents, and entry of the relevant information in the electronic documents management system of the Exchange;

'registration authority' shall mean the functional unit of the Exchange authorized to register subscribers at the Exchange, and reliably confirm that any given public key is owned by a certain entity or individual;

'public key certificate (PKC)' shall mean an electronic document issued by the certification authority and containing information certifying that the public key specified in such certificate is owned by a certain entity or individual, as well as other information stipulated by the existing legislation of the Republic of Belarus;

'list of revoked certificates' shall mean the list of certificates terminated prior to the expiry of their validity periods, signed with the electronic digital signature;

'certificate validity period' shall mean the period of time during which the Exchange guarantees continuous certificate status information updates;

'certification authority' shall mean the functional unit of the Exchange responsible for the issue, distribution, and storage of public key certificates, attribute certificates ("ACs"), and lists of revoked certificates;

'authorized representative' shall mean the individual authorized to represent any legal entity or individual, including any individual entrepreneur, in its/his/her relations with the Exchange.

# CHAPTER 2. STRUCTURE AND MAIN FUNCTIONS OF THE CERTIFICATION AND REGISTRATION AUTHORITIES OF THE EXCHANGE

2.1. The following units shall be involved in the distribution of PKCs:

certification authority ('CA');

registration authorities ('RAs').

2.2. The CA shall be responsible for:

issue and life cycle support (storage, suspension, reactivation, revocation) of the root PKC of the Exchange;

issue and life cycle support of subscriber PKCs;

maintenance of the database of issued subscriber PKCs;

publication and storage of lists of revoked certificates.

2.3.The RAs shall be responsible for:

registration of the subscribers;

registration and storage of the documents provided by the subscribers;

reliable verification of ownership of a public key by a certain entity or individual;

remote installation and setup of the software required to use the electronic digital signature.

# CHAPTER 3. TYPES OF ACTIVITIES

3.1. The Exchange shall engage in the following activities related to the distribution of public keys:

registration of subscribers and issue of PKCs required for participation in exchange trading;

suspension, reactivation, revocation of subscriber PKCs;

authentication of issued subscriber PKCs;

remote installation and setup of the software required to use the electronic digital signature;

other activities as stipulated by the existing legislation of the Republic of Belarus and by-laws of the Exchange.

# CHAPTER 4. ISSUE OF PKCs FOR PARTICIPATION IN EXCHANGE TRADING

4.1. To proceed with the registration of the subscriber and issue of the PKC for participation in exchange trading, the applicant (authorized representative) shall provide, in electronic form, the following documents, thereby concurrently confirming its consent to the storage and use of the information contained in such documents, and retrieval and transfer of such information to third parties as stipulated by the existing legislation of the Republic of Belarus, and expressing its consent to the receipt from the Exchange of SMS notices on the status of review of such documents:

4.1.1. Legal entities and individual entrepreneurs – residents of the Republic of Belarus:

copy of the passport or other identity document containing the following information: personal (identification) number, series and number of the document, name (code) of the issuing authority, and date of issue;

power of attorney, drawn in the form presented in Attachment 2 to these Regulations, issued to the authorized representative (employee or another individual) (the power of attorney provided by the authorized representative of an individual entrepreneur shall be notarized);

other documents, as may be required by the Exchange.

*(subparagraph 4.1.1 as amended by Minutes of the Board Meetings dated 24.05.2021 No. 81, 26.08.2021 No. 158)*

4.1.2. Individuals not engaged in entrepreneurial activities:

copy of the passport or other identity document containing the following information: personal (identification) number, series and number of the document, name (code) of the issuing authority, and date of issue.

*(subparagraph 4.1.2 as amended by Minutes of the Board Meeting dated 26.08.2021 No. 158)*

4.1.3. Legal entities and individual entrepreneurs – non-residents of the Republic of Belarus:

legalized[[1]](#footnote-1) extract from the trade register of the country of registration of the applicant containing information on the registration, legal address, and scope of authority of the officers of the applicant, accompanied by its translation into the Belarusian or Russian language (the signature of the translator shall be notarially attested in the Belarusian or Russian language), such extract to have been issued not more than 1 (one) year prior to the date of its presentation;

copy of the passport or other identity document containing the following information: personal (identification) number, series and number of the document, name (code) of the issuing authority, and date of issue;

legalized\* power of attorney, accompanied by its translation into the Belarusian or Russian language (the signature of the translator shall be notarially attested in the Belarusian or Russian language; the entire document shall need to be translated, including all its details (stamps, seals)), drawn in the form presented in Attachment 2 to these Regulations.

The procedure for the registration of the subscriber and issue of the public key certificate for participation in exchange trading may be modified by resolutions of the Exchange with respect to legal entities and individual entrepreneurs – non-residents of the Republic of Belarus.

*(subparagraph 4.1.3 as amended by Minutes of the Board Meetings dated 26.08.2021 No. 158, 10.06.2024 No. 131)*

4.2. When filing a repeated application for the registration of the subscriber and issue of the PKC for participation in exchange trading, the applicant (authorized representative) shall submit to the registration authority the documents listed in paragraph 4.1 of these Regulations.

4.3. The provided documents shall have been reviewed by an employee of the Exchange within 3 business days following the date of their receipt. The decision to register the subscriber and issue the PKC for participation in exchange trading, or to decline the request for such registration, shall be made on the basis of the findings of such review.

If the Exchange needs any additional information, it shall request the applicant to provide such information by e-mail, or using any other method producing a confirmation of dispatch of such request.

4.4. Certain aspects of registration of representatives of the subscribers.

4.4.1.  The following individuals may be registered as representatives of the subscriber, provided that they have reached the age of 18 years:

for legal entities and individual entrepreneurs – individuals employed by them under labor or civil contracts;

for individuals not engaged in entrepreneurial activities – such individuals themselves.

4.4.2. One individual may be registered as a representative for only one subscriber of the Exchange for the purposes of participation in exchange trading.

4.5. The following shall operate as the grounds for refusal to register the subscriber and/or carry out other activities stipulated by these Regulations:

failure to provide the documents listed in paragraphs 4.1 and 4.2 and in the second part of paragraph 4.3 of these Regulations;

failure to comply with the provisions of paragraph 4.4 of these Regulations;

provision of documents which contain incomplete and/or inaccurate information or do not comply with the existing legislation of the Republic of Belarus or these Regulations.

4.6. The private and public keys of the subscriber shall be generated by the subscriber independently in accordance with the instructions published on the Exchange website.

4.7. The private key of the subscriber shall, following its generation, be stored in an encrypted form.

The password granting access to the private key shall have at least eight symbols. The password shall contain digits and/or Latin characters.

4.8. Upon completion of the registration of the subscriber and issue of the PKC, the subscriber (authorized representative) shall be furnished with:

required software;

Exchange PKC;

Subscriber PKC;

lists of revoked certificates;

other documents (as necessary).

The documents and software specified in the second to sixth indents of the first part of this paragraph may be furnished to the subscriber (authorized representative) by their publication on the Exchange website and/or in the personal account on the Exchange website, or in any other available way.

# CHAPTER 5. SUBSCRIBER PKC STATUS MANAGEMENT

5.1. Subscriber PKC status management shall involve the following activities of the Exchange:

revocation of subscriber PKCs;

suspension of subscriber PKCs;

reactivation of subscriber PKCs.

5.2. The Exchange shall revoke subscriber PKCs:

on the basis of a request filed by the subscriber, such request to be draw in the form presented in Attachment 1 to these Regulations;

if the Exchange private key is compromised;

if the subscriber private key is compromised;

in the event of breach of any requirements stipulated by these Regulations;

if the Exchange learns of liquidation of the legal entity, termination of operations of the individual entrepreneur (exclusion of the individual entrepreneur from the Uniform State Register of Legal Entities and Individual Entrepreneurs), death of the representative of the subscriber, or any change in the information on the subscriber contained in the subscriber PKC;

in other situations, stipulated by these Regulations.

*(subparagraph 5.2 as amended by Minutes of the Board Meeting dated 30.09.2024 No. 225)*

5.3. The Exchange shall suspend subscriber PKCs:

on the basis of a request filed by the subscriber, such request to be draw in the form presented in Attachment 1 to these Regulations;

if the subscriber fails to meet the terms for the provision of documents (fails to provide original documents), or provides inaccurate information;

in other situations, stipulated by these Regulations.

5.4. Subscriber PKCs shall be suspended for a period measured in calendar days.

5.5. Subscriber PKCs may be reactivated only during the period of time for which the relevant subscriber PKC was originally issued.

5.6. Revocation or suspension of subscriber PKCs and official notification of the subscribers of revocation of their PKCs shall be performed by the Exchange within two hours from the time of receipt from the subscriber of the request to suspend or revoke the relevant subscriber PKC.

5.7. To enable the subscribers to ascertain the validity of the subscriber PKCs issued by the Exchange, the Exchange PKC and the lists of revoked certificates shall be published on the Exchange website.

5.8. Publication of the list of revoked certificates on the Exchange website shall constitute official notification of revocation, suspension, or reactivation of subscriber PKCs.

The time of publication of the list of revoked certificates containing the information specified in the first part of this paragraph shall be regarded as the time of revocation, suspension, or reactivation of the relevant subscriber PKC.

# CHAPTER 6. AUTHENTICATION OF SUBSCRIBER PKCs ISSUED BY THE EXCHANGE

6.1. The need to authenticate a subscriber PKC issued by the Exchange may arise in the course of resolution of conflict situations involving participants of electronic documents exchange in the information system of the Exchange.

6.2. The Exchange shall authenticate the subscriber PKCs issued by it by checking the electronic digital signature of the Exchange in such PKCs.

6.3. The Exchange shall authenticate the subscriber PKCs issued by it on the basis of requests filed by the subscribers, such requests to be drawn in the form presented in Attachment 3 to these Regulations.

6.4. To authenticate the subscriber PKC issued by the Exchange, the Exchange shall use the PKC file provided by the subscriber and its hash value generated using the MD5 algorithm, which shall be compared against the PKC or AC stored in the certificates database of the Exchange and its hash value.

6.5. Authentication of the subscriber PKC shall be performed by the expert commission of the Exchange.

6.6. The results of authentication of the subscriber PKC shall be presented in the expert opinion drawn by the expert commission of the Exchange in the form presented in Attachment 4, such opinion to be prepared in four hard copies, with one such copy furnished to the subscriber.

6.7. The expert opinion on authentication of the subscriber PKC shall be delivered to the subscriber (authorized representative) against personal signature, or sent by registered mail with delivery confirmation.

# CHAPTER 7. VALIDITY PERIODS OF THE KEY DOCUMENTS

7.1. The key documents shall include the Exchange PKC, subscriber PKCs, subscriber ACs, and lists of revoked certificates.

7.2. The running of the validity period of the Exchange PKC shall start as of the date and time of issue of the Exchange PKC, and its duration shall not exceed fifteen years.

7.3. The validity period of the subscriber PKC shall be limited by the provided title documents, its running shall start as of the date and time of issue of the subscriber PKC, and its duration shall not exceed three years.

7.4. The running of the validity period of the list of revoked certificates shall start as of the time of their issue, and its duration shall not exceed 30 full days.

# CHAPTER 8. EXCHANGE PRIVATE KEY COMPROMISE

8.1. If the Exchange private key is compromised, the Exchange PKC shall be revoked. The subscribers shall be notified of the Exchange private key compromise by publication of the relevant notice on the Exchange website.

8.2. Following the PKC revocation, the Exchange shall perform unscheduled replacement of Exchange keys.

8.3. The Exchange shall revoke subscriber PKCs signed with the compromised Exchange private key, regardless of whether they were valid or suspended at the time of the Exchange private key compromise. All affected subscribers shall go through reregistration and reissue of PKCs for participation in exchange trading.

# CHAPTER 9. SUBSCRIBER PRIVATE KEY COMPROMISE

9.1. The following events shall result in the subscriber private key compromise:

loss of the subscriber private key;

third persons gaining unauthorized access to the subscriber private key password.

9.2. The determination as to whether its private key has been compromised shall be made by the subscriber independently.

If its private key is compromised, the subscriber shall file with the Exchange the subscriber PKC revocation request.

# CHAPTER 10. RIGHTS AND OBLIGATIONS OF THE EXCHANGE

10.1. The Exchange shall have the right to:

approve and modify these Regulations on Distribution of Public Keys for Authentication of Digital Signatures for Participation in Exchange Trading, and demand that the subscribers comply with the same;

decline the request of the subscriber to carry out any activities listed in paragraph 3 of these Regulations, if such subscriber fails to comply with these Regulations.

10.2. The Exchange shall have the obligation to:

carry out the activities listed in paragraph 3 of these Regulations;

notify the subscribers and other stakeholders of the procedures used by it to carry out the activities listed in paragraph 3 of these Regulations by publication of the relevant information on the Exchange website;

ensure that the serial numbers of the PKCs issued to the subscribers and the public key values in the PKCs issued to the subscribers are unique;

publish each new list of revoked certificates on the Exchange website within thirty minutes from the time of its issue;

revoke subscriber PKCs in the event of compromise of the Exchange private key with which the aforementioned subscriber PKCs are signed.

# CHAPTER 11. CHAPTER 11. RIGHTS AND OBLIGATIONS OF THE SUBSCRIBER

11. 1. The subscriber shall have the right to:

receive the PKC and use it in accordance with the requirements stipulated by these Regulations and by-laws of the Exchange;

receive information on the procedures used by the Exchange to carry out the activities listed in paragraph 3 of these Regulations, as published on the Exchange website;

receive information on the subscriber PKC status (in the form of the list of revoked certificates) for the purpose of checking such status;

request the Exchange to authenticate the subscriber PKC.

11.2. The subscriber shall have the obligation to:

comply with the requirements stipulated by these Regulations;

comply with the instructions provided by the Exchange;

independently fit out its computer equipment with system and applied software, electronic digital signature devices, hardware, and devices used to protect information from unauthorized access;

generate its electronic digital signature using only a valid private key;

keep the password granting access to its private key in secret, and take all steps reasonably required to prevent it from being compromised;

in the event of compromise of its private key, stop using such private key and request the Exchange to revoke the affected subscriber PKC and issue a new subscriber PKC;

file a subscriber PKC revocation request upon termination of the authority of the subscriber's representative who used the relevant private key;

in the event of any change in the information contained in the subscriber PKC, request the Exchange to issue a new subscriber PKC, such request to be filed not later than on the business day following the day on which such change occurred;

use the electronic digital signature device and the private and public keys only for the intended purposes, as stipulated by these Regulations;

if a subscriber PKC revocation or suspension request is filed with respect to the subscriber, refrain from using the relevant private key for the duration of the period from the time when such request is filed to the time when the subscriber is notified of revocation or suspension of such certificate.

# CHAPTER 12. LIABILITY OF THE EXCHANGE AND THE SUBSCRIBERS

12.1. The Exchange shall be liable for:

the consequences of its failure to promptly perform the revocation or suspension of the subscriber PKC;

the consequences of its failure to promptly publish the list of revoked certificates.

12.2. The Exchange shall not be liable for:

the consequences of provision of inaccurate information by the subscriber;

incorrect use of electronic digital signature devices;

failure to protect the private key file or the password granting access to the private key;

loss of the private key file by the subscriber, or incorrect modification by the subscriber of the password granting access to the private key;

deletion of the private key by the subscriber;

use of the public key by the subscriber other than for its intended purposes, and the consequences of such use.

12.3. The subscriber shall be liable for:

failure to comply with the requirements stipulated by these Regulations;

provision of inaccurate information, and the consequences of such actions;

incorrect use of electronic digital signature devices;

failure to protect the storage device containing the key information, the private key file, or the password granting access to the private key;

deletion of the private key by the subscriber;

use of the public key by the subscriber other than for its intended purposes, and the consequences of such use.

12.4. The type and scope of liability of the Exchange and the subscribers shall be determined in accordance with the existing legislation of the Republic of Belarus and these Regulations.

# CHAPTER 13. ARCHIVE STORAGE

The hard copies of the documents provided by the subscriber shall be stored by the Exchange in accordance with the procedure stipulated by the existing legislation of the Republic of Belarus on archives and archive operations.

1. The term is used in the meaning defined in paragraph 4 of the Rules of Exchange Trading at JSC 'Belarusian Universal Commodity Exchange' approved by Resolution of the Board of JSC 'Belarusian Universal Commodity Exchange' dated 22.11. 2005 No. 3. [↑](#footnote-ref-1)