KAZAKHSTAN STOCK EXCHANGE

A p p r o v e d

by Kazakhstan Stock Exchange
Board of Directors decision

(minutes No. 15 of November 6, 2002)

Effective

from November 7, 2002

N O T I C E

Rules have been translated into English by employees of Kazakhstan Stock Exchange for information purposes only. In case of any incompliance of this translation with the original version of Rules in Russian, the Russian version shall always prevail.

RULES

on Use of Programming-Cryptographic Information Security Devices at Operation of the Trading System in the Remote Access Mode

Almaty

2002

L I S T O F A M E N D M E N T S

1. Changes No. 1:

– approved by Kazakhstan Stock Exchange Board of Directors decision (minutes No. 6 (3) of March 25, 2003);

– effective from March 25, 2003.

2. Changes No. 2:

– approved by Kazakhstan Stock Exchange Board of Directors decision (minutes No. 14 of March 28, 2014);

– effective from May 6, 2014.

These rules determine the procedures on use of programming-cryptographic information security devices at operation of the trading system of Kazakhstan Stock Exchange (hereinafter referred to as the Exchange) in the remote access mode for purposes of *(this paragraph was changed by the Exchange Council decision of January 15, 2004)*:

1) authentication of the Exchange Trading server (hereinafter referred to as – the Trading server) and users;

2) encryption of traffic – maintaining of confidentiality and integrity of information transmitted from users to the Trading server and vice versa;

3) interchange of electronic documents between the Exchange and its members.

Chapter 1. GENERAL PROVISIONS

Article 1. Concepts

1. The concepts used herein mean the following:

1) **"authentication"** – an unambiguous automated determination of the Trading server and the user at the stage of registration of the user for operation in the Exchange trading system (hereinafter referred to as the Trading system) in the remote access mode;

2) **"electronic data"** – information, presented by means of computer techniques and other electronic devices of generation, processing, storage, transmission and receipt of information;

3) **"floppy–token with key information"** or **"floppy–token"** – a floppy, or a chip electronic data media (a so-called "token"), or other external media of such data, whereon the user key information and the open key certificates of the user and the Exchange are stored;

4) **"privacy key"** – a unique sequence of symbols, introduced in the form of the electronic data, known to its author only (the owner of the public key certificate, corresponding to this sequence) and intended for generation of an electronic signature, and authentication and encryption of traffic;

5) **"key"** – a privacy or public key;

6) **"key information"** – data in the electronic form, containing information on public and privacy keys in a certain format;

7) **"key information compromise"** – deliberate or reckless acts, or failure to act on the side of the user, who owns key information, or any other person, having an authorized access to a floppy–token with this key information, in violation of the requirements on the key information safety ensuring set hereby, which caused a loss, physical damage or erasure of the floppy-token, or created prerequisites to copying, unsanctioned modification, erasure of this key information or its cognizance by the persons, who are not the indicated user, or gave any handle to suspect a possibility of the unsanctioned use of this key information;

8) **"information confidentiality"** – protection of information against unsanctioned reading;

9) **"Exchange administrator"** – an employee of the Exchange, exercising functions on organization and holding of trades in financial instruments;

10) **"public key"** – a publicly accessible unique sequence of symbols, introduced in the form of electronic data, and intended for check of the electronic digital signature, and authentication and encryption of traffic;

11) **"electronic document originality"** – a feature of an electronic document in regard of its compliance with the following conditions:

an electronic document was examined (by way of electronic digital signature) for absence of changes and amendments, made therein after signing of the electronic document by electronic digital signatures[1]; and

the public keys, used for examination of electronic digital signatures in the electronic document, are effective as on the moment of signing of the electronic document by these electronic signatures, and belong to the persons, mentioned in the electronic document as the authors (senders) of the information contained therein (registered on these persons);

12) **"electronic document signing"** – implementation of an electronic digital signature into an electronic document;

13) **"user"** – a natural person, authorized for execution of certain actions in the trading system on behalf of the Exchange or the Participant, or other natural person – a client (client employee) of the Participant, using the trading system for transmission of directions (client orders, requests) to the Participant via the Internet or other communications channels for execution of deals in the trading system by the latter at the expense and in the interests of the person;

14) **"public key certificate"** or **"certificate"** – the aggregate of a public key and additional data in the electronic form, represented in a certain format and used for purposes of an unambiguous binding of the public key to the Trading server or a certain user, and also for purposes of the public key validity interval determination;

15) **"trading system"** – a programming technical complex, internal documents of the Exchange and other necessary assets and procedures, by means of which deals in the serial securities and other financial instruments between Exchange members *(this sub-item is changed by the Exchange Board of Directors decision of march 28, 2014)*;

16) **"reader"** – a device reading the information, contained on the floppy-token;

17) **"Participant"** – other, except for the Exchange, organization, using programming-cryptographic information security devices at operation of the trading system;

18) **"information integrity"** – protection of information against its unsanctioned modification (changes in and/or additions to);

19) **"certification Center"** – a legal entity, which subject to the agreement with the Exchange, executes functions on:

storage of the applications on receipt of public keys certificates received from users;

public keys certificates issue;

public keys effect registration, storage and termination;

storage and registration of the terminated public keys and, if needed, announcement (disclosure) of information on such keys;

other functions, specified by the legislation of the Republic of Kazakhstan;

20) **"electronic digital signature"** – mandatory and inherent requisites of an electronic document; data in the electronic form, received by use of the privacy key as a result of cryptographic transformation of the information, which is contained in this electronic document, used for originality check of this electronic document;

[1] Programming-cryptographic information security devices allow for the possibility of endorsement of an electronic document either by one electronic digital signature or by several electronic digital signatures.

21) **"electronic document"** – data in the electronic form, containing information of any type and electronic digital signatures of authors (senders) of the information.

2. Other concepts, used herein, are identical to the concepts, defined by other internal documents of the Exchange.

3. The concepts, used herein, are also used in the Exchange explanatory instruction materials regarding use of programming-cryptographic information security devices at operation of the trading system in the remote access mode (hereinafter referred to as – the user manuals).

Article 2. Area of Application of the Rules

1. Programming-cryptographic information security devices at operation of the trading system in the remote access mode may be used only by the natural persons, who are employees or clients (clients' employees) of the organizations (the Exchange members and other organizations, having the right to use the trading system), that submitted the applications according to the form of Appendix 1 hereto.

2. These Rules have the force of a deed of adherence. Submission of the application, specified in item 1 of this article, means conclusion of an agreement on the whole in compliance with specified hereby.

Article 3. Legal Force and the Application Field of an Electronic Document

1. The electronic document, complying with the electronic document originality conditions set hereby, is equivalent to the document containing identical information on the paper or other similar in meaning media, that is signed by the persons, indicated in this electronic document as the authors (senders) of the information contained in this electronic document (if a legal entity is indicated as the author (sender) of the information contained in this electronic document – to be signed by a natural person that is authorized for signing of the corresponding documents on behalf of this legal entity), and has a legal force equivalent to such document.

2. An electronic document is considered to be signed by the authors (senders) of the information contained therein in case the public keys, used for check of electronic digital signatures in this electronic document, belong to the persons (registered on the persons), indicated in the electronic document as the authors (senders) of the information.

   The electronic documents, formed, signed and sent on behalf of the Exchange by the Trading server, are considered to be signed by the person that is an authorized signer of the respective documents on behalf of the Exchange.

3. Public keys substitution has no effect on the legal force of the electronic document, provided it complies with the conditions of an electronic document originality set hereby.

4. These Rules govern only the electronic documents that are subject to signing on behalf of the Exchange, or the Participants, by the persons duly authorized:

   1) exchange certificates;

   2) the reports provided by the Exchange to its members (statements) in respect to the deals concluded thereby (on their behalf);

   3) the Exchange invoices for payment of membership fees and commissions;

   4) other electronic documents subject to the Exchange Board decision.

Article 4. Electronic Document Paper Copy or Analogous Media Copy

1. Software, necessary for production of duplicate (print-out) of an electronic document on the paper or other analogous in its meaning media (hereinafter referred to as – the electronic document paper copy), are a part of the trading system composition.
2. An electronic document paper duplicate stands in equal legal force with this document subject to the following conditions:
   1) it has a note "Electronic document copy" thereon;
   2) the information contained therein is completely identical to the information, contained in the electronic document;
   3) it is signed by the natural persons that are registered for the public keys, used for check of electronic digital signatures in the electronic document (in case a public key is registered for the Trading server – it is signed by the natural person, authorized for signing of the corresponding documents on behalf of the Exchange).

Article 5. Tariffs

The Exchange tariffs for the operations, related to the use of programming-cryptographic information security devices at operation of the trading system in the remote access mode, are determined by the Exchange Board.

Chapter 2. USE OF PROGRAMMING-CRYPTOGRAPHIC INFORMATION SECURITY DEVICES AT OPERATION OF THE TRADING SYSTEM IN THE REMOTE ACCESS MODE

Article 6. Bases of Programming-Cryptographic Information Security Devices

1. The Exchange software, used for purposes of programming-cryptographic information security devices at operation of the trading system in the remote access mode is based on:
   1) standard SSL (Secure Sockets Layer) – in relation to authentication of the Trading server and users;
   2) algorithm DES (Data Encryption Standard) with 56 bit key length – in relation of traffic encryption;
   3) algorithm RSA (Rivest–Shamir–Adleman) with 1,024 bit key length – in relation to electronic digital signature.
2. The pairs composed of public and privacy keys, generated separately for the Trading server and every user are used for purposes of programming-cryptographic protection of information at operation of the trading system in the remote access mode. At that, every public key complies with only one privacy key and vice versa; it is possible to get a public key from a privacy key, but it is impossible to get a privacy key from a public key. The pairs of such keys, represented in the form of the key information, are stored on floppy-tokens.

   Except for the primary key information, the users' key information is independently generated thereby.

   The primary key information for the users that are employees of the Participants is generated by the Exchange and is used by such users only once for generation of their own keys, change of the trading system access passwords and receipt of certificates from the Certification Center. The order of execution of the indicated actions is determined by the user manuals.

   Primary key information for the users that are clients (employees of clients) of the Participant is generated by this Participant and used by such users only once for generation of one's own keys, change of the trading system access

passwords and receipt of certificates from the Certification Center. The execution order of the indicated actions is determined by the user manuals.

Article 7. Primary Key Information

1. The users, that are employees of the Participant, are given primary key information on floppy-tokens and primary trading system access passwords against the signature directly at the Exchange (in the envelopes glued downed with the Exchange stamp print) after receipt of the application from this Participant subject to item 1 of article 2 hereof *(this item was changed by the Exchange Board of Directors decision of March 25, 2003)*.
2. It is allowed to receive floppy-tokens with primary key information and the trading system initial access passwords on the basis of duly formalized proxies of the users in respect of whom the primary key information and the trading system initial access passwords were generated, or the Participants whose employees are users of the Rules *(this item was changed by the Exchange Board of Directors decision of March 25, 2003)*.
3. The norms prescribed by items 1 and 2 of this article do not cover the users who are the Exchange employees, in respect of whom a streamlined proceeding for granting of primary key information and the trading system initial access passwords is applied (without envelope, against signature).
4. The Exchange maintains records of the users that received floppy-tokens with the primary key information and trading system initial access passwords.
5. The liability for safety control of floppy-tokens with primary key information during the transportation from the place of receipt (from the Exchange) to the user terminal is incurred by the Participant, whose employee is this user. With that the security of a floppy-token means:
    1) its protection against a possibility of loss, physical damage or destruction;
    2) protection of the primary key information contained therein against the possibility of its copying, modification or erasure;
    3) prevention of its receipt and/or disclosure of the primary key information contained therein to the persons that are not the users in whose respect the primary key information recorded on this floppy-token was generated, including other employees of the Participant.
6. The order of delivery of primary key information and trading system initial access passwords to the clients (clients' employees) of the Participant is determined by the Participant.

Article 8. Logging in. Authentication. Close of Business in the Trading System

1. Logging in to the trading system using a floppy-token with key information is possible, provided the user has a valid certificate of a public key and a trading system access password.
2. The Trading server and user are authenticated by the trading system automatically at logging therein, using a floppy-token with the key information. With that, the trading system automatically checks the user certificate validity.
3. At operation in the trading system with use of the floppy-token containing key information, the traffic is automatically encrypted by the trading system with the aid of the session keys generated for the trading system operation session period on the basis of the key information of the Trading server and user.
4. All user actions executed in the trading system with use of the floppy-token containing key information are considered to be proper, if the user was authenticated at logging in to the trading system, and the traffic between the user and the Trading server was encrypted with the aid of session keys.

5. On close of business in the trading system with use of the floppy-token containing key information this floppy-token must be obligatory removed from the reader.

Article 9. Key Information Security

1. The Participants, and the clients thereof, using programming-cryptographic information security devices at operation of the trading system, must take all necessary and sufficient measures for safety control of the floppy-tokens containing key information (the floppy-tokens containing primary key information received from the Exchange or the Participants, and the floppy-tokens with own key information of users), including, but not limited to (in respect of every floppy-token):

   1) grant of access to this floppy-token only to the person, who owns the key information recorded on this floppy-token (by way of the floppy-token storage in the place inaccessible to unauthorized persons, restriction of access to unauthorized persons to the room, where this floppy-token is stored, and by other possible ways);

   2) the floppy-token protection against loss, physical damage or destruction;

   3) protection of the key information contained on this floppy-token against copying, unsanctioned modification (including generation of new keys by the persons that are not the users who own the key information recorded on this floppy-token) or destruction, including protection against the computer viruses and programs, reading out the information contained on floppy-token in the off-line mode while located in the reader, or defining the text being typed on a computer keyboard and others;

   4) protection of the key information contained on this floppy-token against familiarization therewith by the persons that are not the users who own the key information recorded on this floppy-token;

   5) control of the floppy-token removal from a reader on close of business in the trading system;

   6) dispensation of the floppy-token (sending to the Exchange a message on invalidation of the key information recorded on this floppy-token) in case, the person, who owned the key information recorded on this floppy-token, lost the right to use the trading system due to resignation, change of job or other possible reason.

2. The liability for violation of conditions of item 1 of this article is incurred by the Participants.

3. In case of the key information compromise, the user, who owns this key information, must immediately personally or via the other person address the Exchange administrator with an application (including in the verbal form or by phone) on necessity of blocking of access to the trading system on the basis of this key information. Responsibility for the consequences resulted from the application submission delay, is incurred by the Participant, whose employee or client (client employee) is this user.

   Upon receipt of the application the Exchange administrator must immediately block the access to the trading system on the basis of the compromised key information and, if necessary, inform other users of the key information compromise. The responsibility for the consequences resulting from the trading system access blockage delay on the basis of the indicated application is incurred by the Exchange.

   After blocking of the trading system access on the basis of the compromised key information, the issuer is provided with the floppy-token with new primary key information. The order of receipt of such floppy-token is similar to the order

specified by article 7 hereof. With that, the Exchange issues such floppy-token to the user who is an employee of the Participant, only upon receipt of the free form statement from the Participant signed by the persons that have the rights of first and second signatures on behalf of the Participant in compliance with the retained at the Exchange notarially certified signatures and stamp print specimen form of this Participant and verified by the stamp print thereof.

Article 10. Change of Keys and Access Passwords

1. Keys have life-spans. As the life-spans thereof expire, the users must timely generate new keys and receive certificates of public keys. The indicated actions execution order is determined by the user manuals.

   Responsibility for the consequences resulted from new keys generation delay by the user and untimely receipt of a public key certificate thereby is incurred by the Participant, whose employee or client (client employee) is the user.

2. The user, may in any moment, on the basis of his valid key information change his trading system access password jointly with his keys on receipt of a new public key certificate. The order of this change is determined by the user manuals.

3. Regardless of the key life-spans and the change frequency thereof, the Certification Center keeps the public keys, in respect of which they were issued the certificates, within the whole term of storage of the electronic documents, for the check of which these public keys are required.

Article 11. Formation and Signing, Sending and Originality Check of an Electronic Document

1. Formation, signing and sending of an electronic document on behalf of the Exchange is made by the Trading server.

   Formation, signing and sending of an electronic document on behalf of the Participant is made by the trading system terminal upon the request of the user – an employee or a client (a client employee) of this Participant using the privacy key belonging to this user. The order of formation, signing and sending of electronic documents on behalf of the Participants is determined by the user regulations.

2. An electronic document may be signed only by the electronic digital signature, the public key for the check of which is registered in the Certification Center, and is valid on the moment of signing of this electronic document.

3. The electronic document originality check is made by the Trading server or the trading system terminal automatically, and upon request of the user. The order of actions execution for purposes of the electronic document originality check is determined by the user manuals.

   At signing of an electronic document by several users its originality check is made jointly with checks of all electronic digital signatures used for endorsement of the electronic document.

   Originality check of all archive electronic documents (the electronic documents, whose checking public keys have already expired) is made by the Certification Center.

4. The electronic documents sent and received are registered by the trading system by way of maintaining electronic registration logs both on the Trading server, and on the users' terminals. The order of maintaining of such registration logs on users' terminals is determined by the user manuals.

Chapter 3. CONTROVERSIAL SITUATIONS, CONCERNED WITH ELECTRONIC DOCUMENTS

Article 12. Procedures for Settlement of Controversial Situations

1. On occurrence of the controversial situation, related to electronic documents (hereinafter referred to as – the controversial situation), the attacker claim (of the Exchange or the Participant) must be presented to the other party in controversy within thirty days from the day of occurrence of such situation.
2. Controversial situations are considered by the Conciliatory Commission composed of equal number of representatives of each party in controversy, a Certification Center representative, a representative (representatives) of the third, disinterested, party, that is (are) to be defined on accordance of the parties in controversy. For these purposes, the attacking party may include the third party candidate (candidates) proposed thereby into the pretension text specified in item 1 of this article, for his (their) inclusion into the Conciliatory Commission composition.
3. The Conciliatory Commission must be formed within five working days from the day of receipt of the claim specified in item 1 of this article.
4. A controversial situation must be considered by the Conciliatory Commission within ten working days from the day of its foundation.

Article 13. Resolution Order of "Electronic Document Sending Negation" Situation Type

A controversial situation of "electronic document sending negation" type (when one party in controversy claims, not to have sent an electronic document, and the other party in controversy claims that this electronic document, formed by the first of the controversy parties, was received thereby) is subject to resolution in the following way:

1) this electronic document is to be presented by its receiver;
2) the originality of this electronic document is checked;
3) in case, this electronic document is original, the controversial situation is settled in favor of the receiver;
4) in case, this electronic document is not original, the controversial situation is resolved in favor of the other party in controversy.

Article 14. Resolution Order of "Electronic Document Sent does not Correspond with that Received" Situation Type

A controversial situation of "electronic document sent does not correspond with that received" type (when one party in controversy claims that an electronic document formed and sent thereby to the other party in controversy does not correspond with the electronic document received by the second party in controversy, and the other party in controversy claims that the electronic document received thereby correspond with the electronic document formed and sent by the first of the two parties in controversy) is subject to resolution in the manner as follows:

1) this electronic document is presented by its receiver;
2) the originality of the document is checked;
3) if the document is original, the controversy is resolved in favor of its receiver;
4) if the document is not original, the controversy is resolved in favor of the other party.

President A. Joldasbekov

Appendix 1

to the Rules on Use
of Programming-Cryptographic
Information Security Devices
at Operation of the Trading
System in the Remote Access
Mode

(This appendix was changed by the Exchange Board of Directors decision of January 15, 2004).

[on a letterhead]

Kazakhstan Stock Exchange

APPLICATION

Herewith, we express the intent to use programming-cryptographic information security devices at operation of your trading system in the remote access mode.

We state that we have familiarized ourselves with the Rules on use of programming-cryptographic information security devices at operation of the trading system in the remote access mode; we agree therewith and undertake to comply with the requirements thereof. The obligation undertaken by us includes also the obligation to comply with the conditions of subsequent changes and additions thereto, provided such changes and additions were brought to our notice, or we were duly notified on necessity of receipt of such changes and additions, but failed to appear to receive those.

In addition, at work with programming-cryptographic information security devices at operation of your trading system, we also undertake to follow your explanatory and instructional materials regarding the usage of the named programming-cryptographic devices. The obligation, undertaken by us, also includes the obligation to follow subsequent changes and additions in the materials referred to, or their new versions (editions) provided that such changes and additions or new versions (editions) were brought to our notice, or we were duly notified on the necessity to receive such changes and additions, or new versions (editions), but failed to appear to receive those.

We assume the responsibility for violation of the obligations, contained in this application. This responsibility includes also responsibility for actions (inaction) of our employees and clients (client employees), working on our behalf with your trading system in the remote access mode with the usage of programming-cryptographic information security devices in defiance of (non-compliance with) the norms of the aforementioned Rules and explanatory-instructional materials and for the consequences of such actions (inaction).

[position] [signature] [surname, initials] [2]

[position] [signature] [surname, initials][3]

[2] Position title, signature, surname and initials of the person having the right of first signature subject to the signatures and stamp print specimen form of the Exchange member provided to the Exchange.

[3] Position title, signature, surname and initials of the person having the right of second signature subject to the signatures and stamp print specimen form of the Exchange member provided to the Exchange.