



QUIK Server

Installation manual

Version 9.9



Contents

1. General statements	3
1.1 Components of QUIK system	3
1.2 Connection to trading systems	4
1.3 Technical requirements	6
1.4 License management on QUIK servers	6
2. Software installation	8
2.1 Delivery package	8
2.2 Manual installation of QUIK server	8
2.3 Installation and configuration of QUIK Administrator server part.....	24
2.4 Settings of authentication in QUIK Administrator by MP and OpenSSL cryptographic libraries	28
2.5 Registration of QUIK system users.....	30
2.6 Startup keys for QUIK server	30
2.7 QUIK Administrator account creation.....	32
2.8 QUIK workstation banner configuration	33
2.9 File transfer configuration	35
3. Appendix.....	36
3.1 Format of limits.....	36
3.2 Password encryption	38
3.3 Format of configuration file of encryption by means of OpenSSL library.....	39
3.4 Format of server part configuration file of encryption by means of MP library (MP_Pr_server.ini).....	40
3.5 Format of client part configuration file of encryption by means of MP library (MP_Pr_client.ini)	46

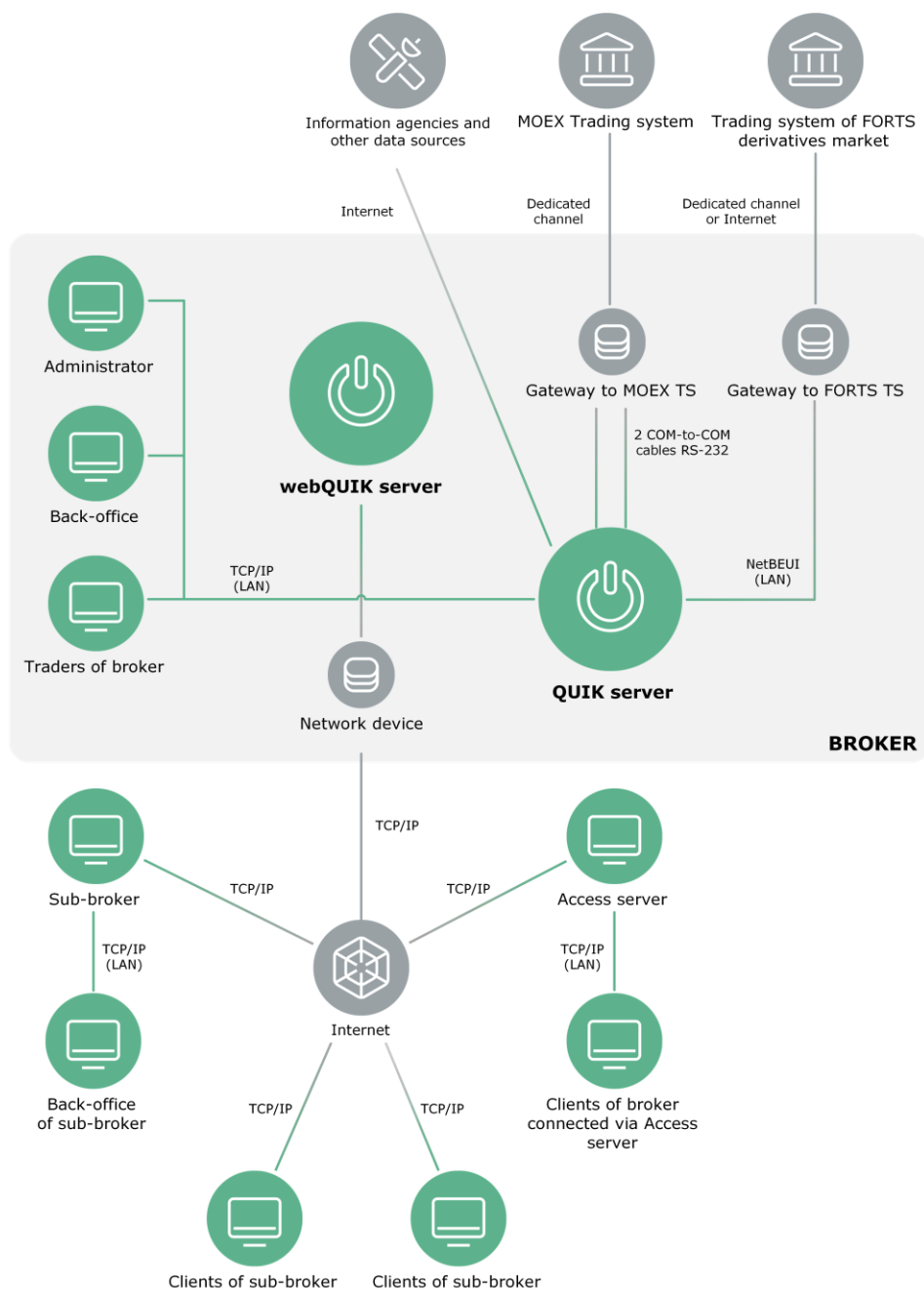
You may email your comments on this Manual to: quiksupport@argatech.com



1. General statements

1.1 Components of QUIK system

QUIK software is implemented on the basis of 'client-server' technology. Data exchange between the server and user terminals is carried by socket connection via protocol TCP / IP. The server provides the connection of information sources (trading systems, news flows and other) and processing of client orders. Client applications are designed for displaying the information and entering of customers' orders.



The central part of QUIK software is **QUIK Server** having the logical core and **interfaces** to connected elements (exchange gateways and other information sources, data storage). The modular concept of connection allows accumulating the system's capacities when necessary by equipping the basic configuration by new features.

The interaction with **database** is realized through a special interface to ease changing of the used type of **DBMS**. The database is used to store information with a storage period of more than one day - registration data of users and rights to work with the system, as well as logs of executed operations.

Current information received from the exchange trading systems is processed directly in RAM and not entered to the database. For a quick recovery in situation of failure the received data is cached on the disk in form of binary file. All work with the database is carried out through the dedicated database server.

Administration of the complex is carried out from the application **QUIK Administrator** unifying all the settings used by the logic core of server. Monitoring over the current state of the server and client connections is provided by terminal **QMonitor**.

1.2 Connection to trading systems

QUIK software is connected to the exchange trading system through soft-(hard) ware interfaces (so-called 'gateway'). Software of 'gateway' is not supplied within the 'QUIK-Broker' system and must be purchased separately.

1.2.1 Connection to trading system of the Moscow Exchange

Gateway to trading system of the Moscow Exchange is realized in form of two software components run on two separate computers working under operational system Windows NT, 2000, XP. One of the components is designed as an independent application connected to the trading system of the Moscow Exchange through dedicated communication channel between trading system of the Exchange and office of broker being a segment of MOEX individual network. The second component is designed in form of Windows DLL interacting with QUIK Server through the application programming interface (API). The components exchange information by using the serial interface (RS232) or Cisco PIX firewall.

Diagram of connection between QUIK Server and trading system of the Moscow Exchange with using the firewall Cisco PIX

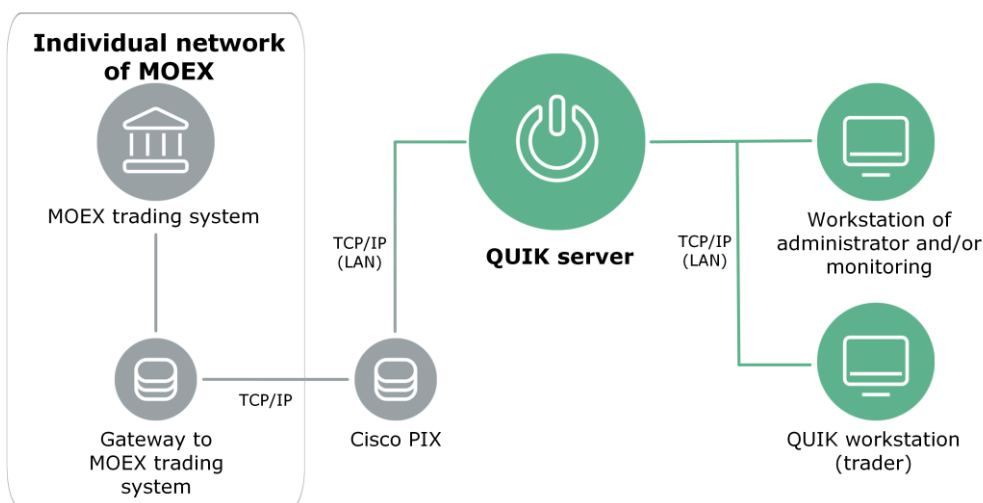
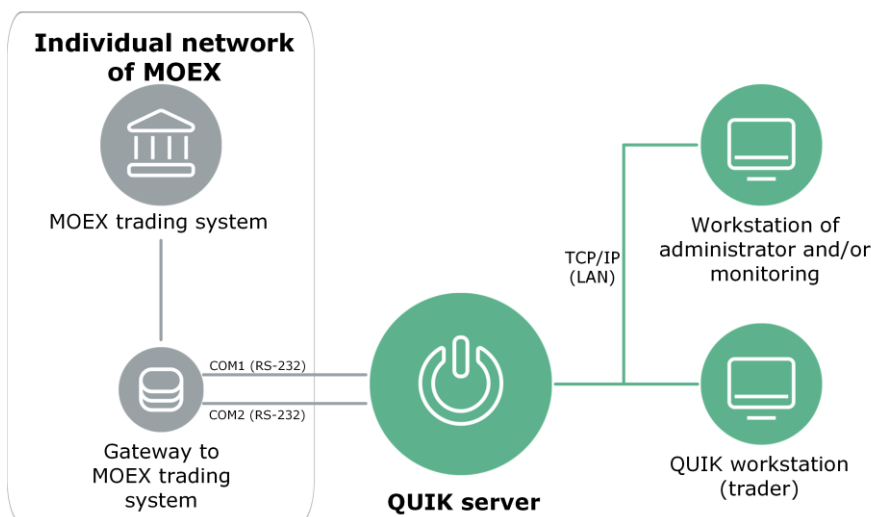


Diagram of connection between QUIK Server and trading system of the Moscow Exchange with using COM ports



MICEX Bridge gateway – software developed by the Moscow Exchange is used for connection to trading system of MOEX.

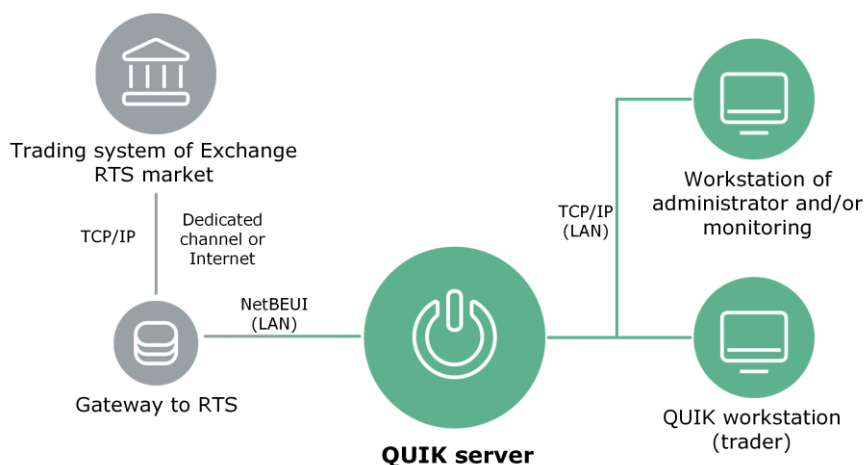
Gateway MICEX Bridge is presented in two software sets:

1. **TEServer** – for connection by COM ports.
2. **TEAP** – to work through PIX.

1.2.2 Connection to trading system of RTS

RTS Gateway is installed on a separate computer with two network cards. One card is used to connect to RTS trading system, the second one is used for interaction with QUIK Server. RTS Gateway is allowed to be installed on the same computer with FORTS Gateway.

Connection to RTS trading system can be established either through a dedicated channel (recommended) or Internet. Non-routable traffic NetBEUI is used to separate external networks and segment of broker's local network where the QUIK Server is installed. Software of RTS trading interface must be installed on the same computer as RTS Gateway.



1.2.3 Connection to trading systems of FORTS and RTS Standard

Connection of QUIK to FORTS trading system and RTS Standard market is established analogically to connection to RTS trading system. Software of gateway to FORTS trading system is allowed to be installed on the same computer where the gateway to RTS trading system is installed.

1.3 Technical requirements

For detailed system and software requirements for QUIK Server, Interface to MOEX trading system, Interface to RTS trading system, Interface to trading system of FORTS derivatives market, Workstation of the administrator QUIK Administrator and the monitoring workstation QMonitor, see [the official website of QUIK](#).

1.4 License management on QUIK servers

The licensing includes the right to connect one copy of the application (plugin, technologic or client module) to a QUIK server. Applications of one type are included in a license pool.

If the broker uses several QUIK servers, the total number of licenses within the license pool, which is distributed among them using the data synchronization service (the Replicator program), is controlled.

After the maximum number of available licenses is reached, a corresponding diagnostic is written to a server log file. If no licenses are available for the plugin, the message "Not enough licenses!" appears in a QUIK workstation.

The applications for which license management is supported:

- Q2Q adapter;

- FIX adapter program interface (accounts);
- FIX adapter program interface (transactions);
- FIX Drop Copy program interface;
- FIX Client Connector program interface;
- Market Data Export Module;
- Level 2 Quotes export module;
- QUIK workstation for mobile devices (PocketQUIK);
- CoLibri SM risk manager terminal module;
- CoLibri FM risk manager terminal module;
- CoLibri FX risk manager terminal module;
- Specialized multi-broker service workstation;
- FX Convertor;
- BasketTrading module;
- Option analytics module;
- Asset manager terminal module (TrustManager);
- webQUIK workstation;
- QORT2QUIK adapter;
- Position management program interface.



2. Software installation

2.1 Delivery package

Structure of catalogues in the delivered program package:

Server	
Addon	- additional modules of QUIK Server included to the configuration;
Gates	- interfaces to trading systems included to the configuration;
QUIK	
AstsGate	- interface to gateway of the Moscow Exchange trading system;
QuikAdministrator	- administration program of server QUIK Administrator;
CMAGat	- test copy of DF Server gate of CMA Company;
db	
Doc	- documentation;
Front	- QUIK Workstation;
KeyGen	- program of key management;
QUIKTools	- installation tools;
Server	- QUIK Server;
Install	
BDE5	- BDE distribution;
Utils	- different utilities.

2.2 Manual installation of QUIK server

2.2.1 DBMS configuration

1. Create a new database on **SQL** server to be used by QUIK server.

To obtain the actual scripts for creating database, contact QUIK technical support:
quiksupport@argatech.com, +7 (383) 219-16-06.

2. Open to edit **quik.ini** file in catalog QUIK\Server\ with settings of QUIK Server. In section [DB] of this file configure the following parameters instead of parameter 'file':



```
server=<name_of_SQL_server>
base=<DB_name_QUIK>
```

Example of the configured connection to SQL Server copy:

```
[DB]
server=Machine\Sq1ServerInstance,1234
base=QUIKDB
```

3. Configure the following parameters in section [DB]:

- **db_connect_timeout** – time of waiting for connection of QUIK Server to the DB server (in seconds). Range of valid values: from 1 to 600. Value by default: 60.
- **ANSI2OEM** – attribute of automatic conversion of all encoded character data transmitted to QUIK Server, from ANSI to OEM. Valid values:
 - 0 – data is sent in ANSI encoding;
 - 1 (by default) – data is encoded in OEM before being sent.
- **AuthMode** – used type of authentication on MS SQL server. Valid values:
 - login (by default) – use login and password specified in 'user' and 'password' parameters (the password can be [encrypted](#));
 - domain – use domain authentication.

When using the domain authentication, the 'user' and 'password' in section [DB] are ignored and may be not specified.

- **Driver** – name of driver which is used to connect to the QUIK server's database. Valid values:
 - ODBC Driver 13 for SQL Server – this value should be selected when operating with MS SQL Server 2014, 2016 or a newer DBMS (from the list of supported ones);
 - "" (empty) (by default) – this value should be selected when operating with MS SQL Server 2012 or an older DBMS (from the list of supported ones).
- **Provider** – name of provider which is used to connect to the QUIK server's database. Valid values:
 - SQLOLEDB – this value should be selected when operating with MS SQL Server 2014, 2016 or a newer DBMS (from the list of supported ones);
 - SQLNCLI10 (by default) – this value should be selected when operating with MS SQL Server 2012 or an older DBMS (from the list of supported ones).

Example of using driver and provider by default:



```
Driver=
Provider=SQLNCLI10
```

Example of using ODBC driver:

```
Driver=ODBC Driver 13 for SQL Server
Provider=SQLOLEDB
```

For the correct functioning ODBC Driver 13 for SQL Server must be installed.

- **AdditionalParameters** – additional parameters of the database connection. Value by default: "" (empty).

4. In section [DB], configure the possibility of receiving unread messages of the previous trading days:

- **messages_delivery_period** – number of days for which messages are loaded. Value by default: 0 (load only messages for the current trading day).

5. In section [db_module], configure the database provider being used:

- **driver** — the name of the executable file of the database provider. Value by default for MS SQL: quik_db_ms.exe. Value for PostgreSQL: driver=quik_db_pg.exe.

Example of sections after making changes:

```
[DB]
server=MSSQL_SRV
base=QUIK_DB
user=sa
password=password
db_connect_timeout=30
ANSI2OEM=1
AuthMode=login
Driver=ODBC Driver 13 for SQL Server
Provider=SQLOLEDB
AdditionalParameters=MultiSubnetFailover=False;ApplicationIntent=ReadWrite

[db_module]
module=dstubrc.dll
driver=quik_db_ms.exe
```



2.2.2 Copying files

1. Create the catalog for installation of QUIK system (hereinafter <quik_dir>).
2. Copy there AstsGate, QuikAdministrator, Front, KeyGen, QUIKTools, Server catalogs from <inst_dir>. If CD-ROM drive was a source, clear the 'Read only' checkbox in attributes of all copied files.

2.2.3 Creating a key for Server

Using the **KeyGen** program create public and secret keys that will be later used by QUIK server (see KeyGen.pdf – User's manual for KeyGen.exe).

1. To configure the parameter 'Name of key holder' type the name of organization in format 'Name (identifier)', for example:

```
Test-Invest (testinvest)
```

2. The identifier in parentheses will be then used to configure the system, call it <name_of_QUIK_server>.
3. Remember the password provided to protect the key. Call it <password_of_server_key>.
4. Copy the secret key of server (program KeyGen.exe saves file a:\secreg.tsk by default) to catalog <quik_dir>\Server. For convenience in further work rename it to secrserv.tsk.
5. Copy the public key of server (program KeyGen.exe creates file a:\pubreg.tsk by default) to catalog <quik_dir>\KeyGen. For convenience in further work rename it to <name_of_QUIK_server>.tsk. This key will be used by all users of the server with the software package KeyGen.
6. Open to edit file <quik_dir>\KeyGen\qcrypto.cfg and specify identifier of organization as value of parameter IMPORT:

```
IMPORT=<name_of_QUIK Server>
```

7. Using the **KeyGen** program create public and secret keys for manager of QUIK server (see KeyGen.pdf – User's manual for KeyGen.exe). In step 3, the program prompts you to select file with public key of the system – select <name_of_QUIK_server>.tsk file. Select the public key of the server in the list of keys (in the example that is 'Test Invest (testinvest)'). Select the checkbox 'Record and use skipping this step' to allow your users to avoid unnecessary operations subsequently when forming keys.

2.2.4 Registration in Windows services

1. Install the QUIK Server and the gateway to trading system of the Moscow Exchange as services of WindowsNT. To do this, type the following in the command line:



```
<quik_dir>\Server\quik.exe -install
<quik_dir>\AstsGate\AstsGate.exe -install
```

2. Verify the successful installation of these programs. Open **ControlPanel\Services** and verify the presence of records identifying services of QUIK Server and gateway to trading system of the Moscow Exchange. These are services with identifiers 'Quik Update Information Kit' and 'Quik Transaction Gate'.
3. Create a user and groups WindowsNT that are necessary to work in QUIK system. Groups to be created:

Name	Group description
Quik	Users of this group have access to start the QUIK server (<quik_dir>\Server\quik.exe)
Quik_source	Users of this group have access to start gateway to the system of the Moscow Exchange (<quik_dir>\AstsGate\AstsGate.exe)
Quik_ctl	Users of this group can manage the QUIK server
Quik_stat	Users of this group can receive statistics on the QUIK server operation

4. Create a user-administrator giving him a name (for example <quikserv>) and password (for example <passwd>). Add this user to the groups created previously. Administrator of WindowsNT server on which the QUIK Server will work is also recommended to be added to these groups.
5. Configure services with identifiers 'Quik Update Information Kit' and 'Quik Transaction Gate' specifying name and password to work in WindowsNT in startup parameters of these services. For this select 'Log on as:' and enter the administrator credentials of QUIK system – name <quikserv> and password <passwd>.
6. To use the domain authentication on MS SQL server, specify name of the domain user and password in startup parameters of the services. Assign the user by right 'Lock pages in memory'. For this do the following:
 - Open the Windows menu item **Start / Settings / Control Panel / Administrative Tools / Local Security Policy**;
 - Open section **Local Policies / User Rights Assignment**. In settings of attribute 'Lock pages in memory' press button 'Add user or group' and add complete the list by user with rights under which the services function.

2.2.5 Currency and cross rates configuration

1. Run QUIK Administrator, select **QUIK server / Security classes** and add a class to the dictionary:



Parameter	Description
Currency cross rates	
Code	CROSSRATE
Description rus. / eng.	Currency cross rates
Ter расчётов	
Class type	Currency cross rates

Only listed attributes should be enabled. Other attributes should be disabled.

- On the computer where the QUIK server is installed, open the **quik.ini** file in the **QUIK\Server** directory and edit it as follows:

- add a string (if not present) to [natural_level_section] section:

```
module=cur_module
```

- add strings in the end of the **quik.ini** file:

```
[cur_module]
module=dwcurg.dll
class_cfg=crossrate.ini
```

- Open the **crossrate.ini** file in the **QUIK\Server** directory and edit it as follows:

- specify for each currency code in [crossrate] section:
 - currency full name;
 - currency short name;
 - accuracy of cross rate value;
 - accuracy of cash position parameter values. Possible values are in the range [0, 8]. If the value is not specified, it is equal to 2 by default.

Example:

```
[crossrate]
...
RUR=Rouble,Rouble,2
SUR=Rouble,Rouble,2
```



```
JPY=Japanese yen,Yen,6,0
```

IMPORTANT!

If the accuracy of cash position parameter values for a currency differs from 2, all the interfaces, which are connected to the server, that transmit:

- _ this currency;
- _ instruments that are traded in this currency;
- _ currency pairs containing this currency;
- _ any monetary values expressed in this currency;

must support the transmission of monetary values with an accuracy that differs from 2, and an accuracy of a corresponding currency must be the same as se on the QUIK server. Otherwise, correct function of the system cannot be guaranteed.

For information about the transmission of monetary values with an accuracy that differs from 2 by a specific interface, contact QUIK technical support: quiksupport@argatech.com.

- _ specify each currency conversion rate in [crossrate_rate] section. As a rate value a free number can be used with the number of decimal places which does not exceed the **accuracy of cross rate value**, specified in the [crossrate] section (see as above).

For example:

```
[crossrate_rate]
RUR=1
SUR=1.00
JPY=0.627686
```

If you use cross rate for currencies, which are not specified in the [crossrate_rate] section, the QUIK server will diagnose a calculation error.

- _ specify in [main_currency] section:
 - _ currency code. Value by default: RUR;
 - _ currency symbol code in Unicode standard. Value by default: 0.

Currency codes are available by link:

https://www.unicode.org/charts/nameslist/n_20A0.html



- string with HTML code of a currency symbol in the format <Unicode-currency code>. If the code is specified in the 16-ary system, then add symbol 'x' before it. Value by default: "" (empty).

Example:

```
[main_currency]
MAIN=RUR,20BD,8381
```

2.2.6 QUIK Server parameters configuration

Open **crypto.cfg** file in catalog <quik_dir>\Server\ and edit it as follows:

1. In [CryptoProviders] section specify the encrypting methods that are used (0 – disabled, 1 – enabled), for example:

```
[CryptoProviders]
openssl=1
```

2. In section, which corresponds to the encrypting method, selected on the previous step, specify full or relative paths to the executable and configuration files, for example:

```
[openssl]
Module=OpenSSL_Pr.dll
IniFile=OpenSSL_Pr.ini
```

3. Specify the following settings in the [auth] section:

```
[auth]
sign=secprov.dll
sign_provider=openssl ; encryption method that is used for digital signature
```

Open **quik.ini** file in catalog <quik_dir>\Server\ and edit it as follows:

1. In section [dealer-library], configure the following parameters:

```
<code_of_your_firm_in_system_of_Moscow_Exchange>=DealLib.dll
```

2. In section [db], configure the following parameters:

```
server=QDB1 ; name of DB server
base=QUIK_DB ; name of QUIK DB, by default QUIK_DB
```



```
user=sa          ; user name of DB administrator
password=secret   ; password of DB administrator. A password must not begin with $
and #
```

Stop orders of users partially or completely blocked in QUIK Administrator (authorization is expired, the attribute 'Blocked' is selected, authorization for markets is expired) can be also loaded from the QUIK server database at startup. Checking for blocked users and setting a period are managed by the quik.ini file settings:

- **stoporders.load_when_expired_la** – indicates of loading of stop orders for users with a general authorization expired as well as expired authorization for markets. Valid values:
 - 0 (by default) – stop orders of the users with expired authorization are not loaded;
 - 1 – stop orders of the users with expired authorization are loaded.
- **stoporders.mark_expired_as_foreign** – indicates of marking stop orders of the users with expired authorization by the "Foreign" attribute. The setting is used if stoporders.load_when_expired_la=1. Valid values;
 - 0 – stop orders of the users with expired authorization are not marked by the "Foreign" attribute;
 - 1 (by default) – stop orders of the users with expired authorization are marked by the "Foreign" attribute.
- **stoporders.expired_la_period** – number of days for loading stop orders of blocked users. Value by default: 14.

3. In section [Files], configure the following parameters:

- **EventsLogFileName *** – path and name of the main log file. Value by default: events.log.
- **ErrorsLogFileName *** – path and name of the errors log file. Value by default: errors.log.
- **DeallibLogFileName *** – path and name of the Limits calculation library log file. Value by default: Deallib.log.
- **DataFilesFolderName** – path to data files (*ik files). Value by default: .\.
- **LogFilesFolderName** – path to log files (events.log, errors.log, DB provider, deallib.log). Value by default: .\.

(*) If the parameter contains only log file name, the path specified in the LogFilesFolderName parameter is used.

4. In section [usend_module], configure the following parameters:



```

module=dwsend.dll
sysname=Information and Trading System QUIK 'TestInvest' ; name of system displayed
in the informational window when connecting to server
name=testinvest ; server key
password=secret ; password to access the server key
port=15100 ; port number for user terminals connection
crypto_provider_ini_file=OpenSSL_Pr.ini; full or relative path to the encryption
settings file
connection_acceptance_tmo_ms ; timeout in milliseconds to wait for a new
connection. Valid values: from 0 to 60000. Value by default: 500

```

5. In section [ctl_module], configure the following parameters:

```

module=dwwqctl.dll
port=15120 ; port number for QMonitor connection
name=testinvest ; server key
password=secret ; password to access the server key

```

6. In section [time-set], specify the **hourshift parameter if the server time is different from the gateway time:**

```

hourshift=3 ; difference between the QUIK server time and the time of data
transmitted by the gateway, in hours

```

7. In section [mail], configure the following parameters of access to SMTP server:

```

Server=smtp.quik.ru ; Name or IP address of SMTP server
Port=25000 ; Port of SMTP server. Value by default: 25
User=test_user ; User name for authentication on SMTP server
Password=secret ; Password for authentication on SMTP server. A password must not
begin with $ and #. A password can be encrypted
FromAddress ; Sender address of emails related to two-factor authentication (and
password recovery)

```

8. In section [limits_module], configure the following parameters:

— for mail distribution:

```

loadlimits_FromAddress=test@post.ru ; Address of message sender
loadlimits_mail_to=test1@post.ru ; Addresses of message receivers separated by commas

```



```
sign_settings_file=.\\qloadlimitx.ini    ; Path to the QLoadLimitsX program settings
file for setting up clients' positions that QUIK server uses to load the limits file
signed by Bicrypt electronic digital signature
```

- **calclimit_old_stoporders** – attribute of blocking funds under stop orders of previous days. Valid values:
 - 0 (by default) – do not block funds;
 - 1 – block funds.

For example:

```
calclimit_old_stoporders=0
```

The setting must not be used simultaneously with the Do not reserve actives for stop-orders on all of classes setting of Limits calculation library (for the setting description, see the Administrator's manual of Limits calculation library settings).

9. In section [trans_module], configure the parameters:

- **Change_wrong_single_clientcode** – the algorithm of client code change. The parameter is responsible for algorithm of substitution if the user has the only active client code. Valid values:
 - 0 – transaction is rejected with diagnostics 'Incorrect client code' if the client code does not match the user rights (Client specified the only code that does not match the rights. Or the client has two codes, one of them has an authorization expired and the client code in the submitted transaction does not match rights);
 - 1 (by default) – transaction is not rejected.

Example:

```
change_wrong_single_clientcode=1
```

- **trans_handling_privileged_users** – the list of users whose transactions are processed by the server regardless of the processing stage of these users' previous transactions.

The setting is applied after saving the configuration file, the server reboot is not required.

Format:

```
trans_handling_privileged_users=<list of UIDs, separated by commas>
```



Example:

```
trans_handling_privileged_users=100,200,300
```

10.In [data_module] section, configure the parameter.

- **inactive_stops_lifetime** – maximum possible time in days from the last activation of stop order after which the stop order is cancelled. Values in range 1 to 13 are rounded to the minimum possible value – 14 days.
 - 0 – the setting is disabled;
 - 14 (by default) – minimum possible number of days (setting enabled).

Example:

```
inactive_stops_lifetime=14
```

If the replacement settings are enabled in the section (`firm_substitute = 1`, `client_codes_substitute = 1`), and the `codes.ini` or `firms.ini` files are empty or missing, the server crashes with an error:

Error reason	Diagnostics
codes.ini replacement file is missing	Configuration file "path-to-codes.ini" not found
firms.ini replacement file is missing	Configuration file "path-to-firms.ini" not found
codes.ini replacement file is empty	Configuration file "path-to-codes.ini" is empty
firms.ini replacement file is empty	Configuration file "path-to-firms.ini" is empty

11.In section [Position], configure correspondence between alias of FORTS gateway firm and firm code on QUIK server with the unified cash position. The setting is relevant if the firm code of the gateway and unified cash position firm does not coincide. Alias is set by FORTS gateway when transmitting data on futures restrictions and positions of unified cash position firm. Using the alias defines a type of account the data from FORTS gateway is intended for.

Format:

```
<alias firm with the unified cash position of FORTS gate>=<code of firm with the unified cash position on QUIK server>
```

Example:

```
UNIFIED_FIRM=NC0038900000
```



Additional alias configuration is also required in section [Position] of FORTS gateway. Alias length must not exceed 12 characters.

12.In the [trade_date] section set up the parameter:

```
ClearingTime=085000 ; trade session change date in format <HHMMSS>. Value by default:  
000000
```

13.Two-factor authentication with sending PIN code at the moment of connection to QUIK server is available to be configured for mobile devices. Operation system of mobile terminals must be specified in **System** setting of section [mobile_terminals] of **quik.ini** file. Value by default: Android,iPhone.

Example:

```
system=Android,iPhone
```

When receiving the parameter value that includes one of strings of the setting, server identifies the mobile terminal and requests PIN only after whole checking the terminal's right to work.

14.In the [data_pipe_module] section, configure the inbound / outbound replication of the date / time of the last login using the following settings:

- _ **disable_last_login_replication_in** – accept / not receive information about the date / time of the last login from the replicator. Default value is 0 (accept).
- _ **disable_last_login_replication_out** — send / not send information about the date / time of the last login to the replicator. Default value is 0 (send).

15.In the [quik_auth] section set the permission/prohibition of password recovery if the user (login) has a temporary lock using the **RetrievePasswordOnLockedUsers** setting.

Example when a prohibition is used (default):

```
RetrievePasswordOnLockedUsers=0
```

Other parameters can be configured by means of **QUIK Administrator**.

2.2.7 Configuration of the user distribution

Catalogs <quik_dir>\Front and <quik_dir>\KeyGen are intended for distribution to customers, so they are recommended to be copied to a separate place.



Catalog <quik_dir>\Front contains the files of QUIK Workstation configured for working with the specified server. Catalog <quik_dir>\KeyGen is a software package for working with access keys.

The directory of the QUIK Workstation installation kit can be changed in the quik.ini file in the [areas] in the frontend parameter. The default setting value is areas\frontend.

A pair of access keys – public and secret ones must be generated for each new user registered in the system via the **KeyGen** program. Public key is registered via **QUIK Administrator**.

2.2.8 Configuration of block encryption

Open to edit the file in catalog <quik_dir>\Server\quik.ini and configure the following parameters in section [usend_module]:

- **enable_block_crypt** – indicates of block encryption. Valid values:
 - _ 0 (by default) – block encryption is not used;
 - _ 1 – block encryption is used.
- **block_crypt_size** – size of encryption block. Valid values: from 100 to 8192 (inclusively). Value by default: 1024.

2.2.9 Setting of asynchronous Limits calculation library usage

Parallel pre-trade and post trade control of operations with different orders can be set up. Firms to which asynchronous Limits calculation library usage is applied should be listed in <quik_directory>\Server\quik.ini in section [dealer-library-async]. For example:

```
[dealer-library-async]
NC0038900000
SPBFUT389
```

In section [behavior] set up the following parameters:

- **numberofexecutors** – full number of queues of parallel processing of Limits calculation library algorithms for all the firms which use Limits calculation library asynchronously.
- **deallib.temppath** – file path to the directory for temporary storage of DLL copies for Limits calculation library.

For example:

```
[behavior]
deallib.temppath=.\Temp
numberofexecutors=3
```



2.2.10 Exclusions for antivirus software

This section contains files and folders of the QUIK server that must be excluded from checking by antivirus software, as they are used during the server operation.

Files and folders to be excluded:

1. Folder with the QUIK server.

2. Folders and files specified in the server settings in quik.ini:

- paths to log files and ik files that are specified in the [Files] section in the **LogFilesFolderName** and **DataFilesFolderName** parameters, for example:

```
LogFilesFolderName=.\Logs  
DataFilesFolderName=.\Data
```

- paths to the files of substitutions that are specified in the [data_module] section in the **firm_substitute_file** and **client_codes_substitute_file** parameters, for example:

```
firm_substitute_file=.\firms.ini  
client_codes_substitute_file=.\codes.ini
```

- paths to the archives that are specified in the [archive_module] section in the **ttp_dir** and **minutes_dir** parameters, for example:

```
ttp_dir=.\archive\minutes_ttp  
minutes_dir=.\archive\minutes
```

- path to the cross-rate settings that is specified in the [cur_module] section in the **class_cfg** parameter, for example:

```
class_cfg=crossrate.ini
```

- path to the crypto provider settings that is specified in the [usend_module] section in the **crypto_provider_ini_file** parameter, for example:

```
crypto_provider_ini_file=.\MP_Pr.ini
```

- paths to the templates that are specified in the [quik_auth] section in the **TemplateRuRetrievingNotSupportedFileName** and **TemplateRuUnknownErrorFileName** parameters, for example:



```
TemplateRuRetrievingNotSupportedFileName=Templates\ru\RetrievingNotSupported
TemplateRuUnknownErrorFileName=Templates\ru\UnknownError
```

3. Folders with the settings of crypto providers in the `crypto.cfg` file that are specified in the **IniFile** parameter, for example:

```
IniFile=MP_pr.ini
```

Besides that, net ports that are specified in the settings of server and access servers in the `quik.ini` file in the port parameter must be added to the exclusions.

2.2.11 Configuration of message text about termination of attorney power

The text of the message that is displayed when connecting with the keys of a user whose power of attorney to use the system has expired can be changed.

By default, the following text is displayed: Your authorization to use the system has expired.

To change the message text, open the **Server/quik.ini** file, in the `[usend_module]` section add the **licence_expired_text_25** key and set the message text as its value, for example:

```
[usend_module]
module=dwsend.dll
licence_expired_text_25=Истек срок действия доверенности
```

Russian text must be in DOS encoding.

2.2.12 Rolling positions

The QUIK server can be launched in the mode of rolling clients' positions by money and instruments (stock market).

Before configuring position rolling, contact QUIK technical support for additional instructions: quiksupport@argatech.com.

To roll positions, do the configuration:

1. In the **quik.ini** file in the `<quik_дир>\Server\` directory configure the following parameters:
 - `[data_module]` section:



- **rolling.rotation_depth** — rotation depth of files with positions located in the Backup directory. The server stores no more than the number of files specified in the setting for each type of position by money and by instrument. When the maximum value of the setting is reached, old files are deleted. Default value: 7.
- [limits_module] section:

```
UnifiedLeverageOnClient=1
```

2. Start the server with the -rolling key (/ro) (see [2.6.12](#)).
3. Connect the interface that will activate the positions after rolling.

The information of the transferred positions is updated only after the interfaces (trade interfaces or the Holiday Information interface) are connected.

2.3 Installation and configuration of QUIK Administrator server part

1. Copy all files from catalog <inst_dir>\QUIKAdministrator\Server to an arbitrary directory. The given catalog provides **QAdminSrv.ini** file including the program settings.
2. Catalog <inst_dir>\QUIKAdministrator\Client\ provides client application of the program.
3. To install the program log into the system as user having rights of administrator.
4. Assign name to the service in **QAdminSrv.ini** file. For that in section [Service] set the appropriate values in parameters name, displayname.
5. Install the server by executing the following command from the command line:

```
QAdminSrv.exe -install
```

6. Configure the following settings in the **QAdminSrv.ini** file:

- In section [Instances], specify configuration files of database connections in format:

```
<Port used for the given DB>=<Name of configuration file>
```

Example:

```
[Instances]
15301=cfg_broker1.ini
15302=cfg_broker2.ini
```



Parameters of connection with every database are described in a separate file.

- In section [Files], in the **Logs** parameter set the name of file for logging, if necessary.
- In section [General], edit the following settings, if necessary:
 - **MaxDeallibSize** – the maximum file size of the Limits calculation library settings to be saved to the Audit log. Value by default: 10485760 (it is 10 MB).
 - **MaxDeallibSize_<Instance>** – the maximum file size of the Limits calculation library settings to be saved to the Audit log for the specified port (<Instance>). The value of the **MaxDeallibSize** setting is used as default.
 - **PathRelease** – path to the directory with update files of the QUIK Administrator client part. The path may be absolute or relative. Value by default: frontend\release\ (relative path from the QUIK Administrator server part directory).
 - **InactiveUserDisconnectTimeout** – indicates that a connection between the server and client parts of the QUIK Administrator program breaks when the user inactivity period in seconds, which is set in this setting, expires or, regardless of this period, when a session is blocked or a remote session is disconnected. If the value is 0, the setting is disabled. Default value: 900.

7. Configure the following settings in <Name of configuration file>.ini server configuration file:

- In section [DB] configure the parameters of access to the database:
 - **Server** – name of server;
 - **Base** – name of database;
 - **User** – login to work with database;
 - **Password** – password to work with database. The password can be [encrypted](#).
 - **UsePersonalLogin** – to use personal logins for connection to the database specify the value "1".
 - **Type** – database type to which the connection is made. Default value: MSSQL.
 - **Driver** – name of ODBC driver which is used to connect to the QUIK server's database. Valid values:
 - ODBC Driver 13 for SQL Server – used when operating with MS SQL Server 2014, 2016 or a newer DBMS (from the list of supported ones);
 - "" (empty) (by default) – used when operating with MS SQL Server 2012 or an older DBMS (from the list of supported ones).
 - **Provider** – name of OLEDB provider which is used to connect to the QUIK server's database. Valid values:
 - SQLOLEDB (by default) – used when operating with MS SQL Server 2014, 2016 or a newer DBMS (from the list of supported ones);
 - MSOLEDBSQL – used when operating with MS SQL Server 2014, 2016 or a newer DBMS (from the list of supported ones);



- SQLNCLI10 – used when operating with MS SQL Server 2012 or an older DBMS (from the list of supported ones);
- SQLNCLI11 – used when operating with MS SQL Server 2012 or an older DBMS (from the list of supported ones).

Example of using driver and provider by default:

```
Driver=
Provider=SQLOLEDB
```

Example of using ODBC driver:

```
Driver=ODBC Driver 13 for SQL Server
Provider=SQLOLEDB
```

For the correct functioning ODBC Driver 13 for SQL Server must be installed.

- **AdditionalParameters** – additional parameters of the database connection. Value by default: "" (empty).

Example:

```
[DB]
Server=QSERV
Base=QBROKER
User=login
Password=secret
UsePersonalLogin=1
Driver=ODBC Driver 13 for SQL Server
Provider=SQLOLEDB
AdditionalParameters=MultiSubnetFailover=False;ApplicationIntent=ReadWrite
```

- Set personal logins in section of [DataBaseLogin_<random text>] view if parameter **UsePersonalLogin**=1. Any number of sections may be specified.
 - **User** – login to work with database;
 - **Password** – password to work with database. A password must not begin with \$ and #. A password can be [encrypted](#);
 - **Users** – list of identifiers of users who can use the login. To establish a connection with server part of QUIK Administrator identifier must be also set in the configuration file of subbroker access.
- In section [Connect] configure the parameters of authorization:



- _ **Name** – key identifier;
- _ **Password** – password for the key. A password must not begin with \$ and #.
A password can be [encrypted](#);
- _ **check_tmo** – the parameters allows keeping active network connection to the server.

Example:

```
[Connect]
Name=KEY
Password=secret
Check_tmo=150
```

- _ In section [QuikOptions] specify the following parameters:
 - _ **RSakeysInTransReport** – the mode of displaying RSA keys of user in report on transactions. Valid values:
 - _ 0 – RSA keys of user are not displayed in report on transactions;
 - _ 1 – all RSA keys of user are displayed in report on transactions;
 - _ 2 – only RSA keys not revoked for the moment of transaction registration are displayed in report on transactions.
 - _ **ClientCodeDelimiter** – delimiter used when setting up the “Code on the dealer’s side” list in the rights by classes in the user editing dialog. Value by default: “,” (comma).
 - _ **FirmId** – list of firms (separated by commas) available for selection in the Firm code field in the rights by classes in the user editing dialog.
 - _ **UserExpireCheckDays** – number of days before the user’s authorization expires, when the notification starts. Value by default: 5.
 - _ **ServiceUserExpireCheckDays** – number of days before the expiration of service user’s authorization, when the system notification starts. Value by default: current value of **UserExpireCheckDays**.
 - _ **Title** – additional title of the QUIK Administrator program. Displayed after User UID.
 - _ **PINCodesInTransReport** – feature of displaying PIN codes used for the Quik two-factor authentication type in the transaction report. Valid values:
 - _ 0 (by default) – PIN codes are not displayed in the transaction report;
 - _ 1 – PIN codes are displayed in the transaction report.
 - _ **EnableMultiple2FaLogins** – attribute of using the same login for multiple users for the Active Directory two-factor authentication type. Logins are set in the Logins for another authorization system dictionary in QUIK Administrator. Valid values:
 - _ 0 (by default) – a login can only be used by one user;



- _ 1 – the same login can be used for multiple users.
- _ **UsersCountThreshold** – the number of entries in the Users dictionary of the QUIK Administrator program at which the dictionary is split into pages containing the number of entries set in the **PageSize** parameter. Value by default: 10000.
- _ **PageSize** – the number of entries on a page in the Users dictionary of the QUIK Administrator program. This parameter is used, if the number of dictionary entries set in the **UsersCountThreshold** parameter is reached. Value by default: 100.

8. Configure the following settings of **crypto.cfg** file in first who strings without the section title:

- _ **PUBRING** – value: quik.dwq;
- _ **SECRING** – path to file with secret key.

Example:

```
PUBRING=quik.dwq
SECRING=secring.txk
```

9. To create a QUIK Administrator new account and assign a user with administrator's permissions, run QUIK Administrator server part using the key **-set-admin-right**. For details, see [2.7](#).

2.4 Settings of authentication in QUIK Administrator by MP and OpenSSL cryptographic libraries

1. In **QAdmin.ini** (for client) and **QAdminSrv.ini** (for server) specify settings of crypto providers to be used for authentication by login/password or for authentication in ActiveDirectory domain:

- _ In the [CryptoProviders] section specify available providers:
 - _ **openssl** – indicates that OpenSSL provider is used. Valid values:
 - _ 0 – provider is disabled;
 - _ 1 – provider is enabled;
 - _ **mp** – indicates that MP provider is used. Valid values:
 - _ 0 – provider is disabled;
 - _ 1 – provider is enabled.
- _ In the [CryptoProvidersSettings] section in the **CipherCryptoProvider** setting specify the default provider. Valid values:
 - _ **openssl** – default provider – OpenSSL;
 - _ **mp** – default provider – MP_Pr.

If the key is absent the Crypto32 provider is used by default.



- _ When the OpenSSL provider is used specify its settings in the [openssl] section:
 - _ **Module** – path to the provider’s module. Value by default: OpenSSL_Pr.dll.
 - _ **IniFile** – path to the provider’s settings file. Value by default: OpenSSL_Pr.ini.
 - _ When the MP provider is used specify its settings in the [mp] section:
 - _ **Module** – path to the provider’s module. Value by default: MP_Pr.dll.
 - _ **IniFile** – path to the provider’s settings file. Value by default: MP_Pr.ini.
2. Specify the setting of provider for client in OpenSSL_pr.ini or MP_Pr.ini depending on provider in use: in the [TLS Connection Settings] section in the **UsedHandShakeScheme** parameter set up the authentication scheme number. Valid values:
- _ 2 – authentication scheme by domain login and password through the Domain Controller;
 - _ 4 – authentication scheme by login and password;
 - _ 7 (by default) — all modes are supported, except for 8 (password recovery);
 - _ 8 — password recovery.

When multiple authentication modes are supported, the setting value is set as a sum of values corresponding to the supported modes.

If you use OpenSSL the scheme specified for client must be the same as specified for server.

3. Specify the settings of provider for server:
- _ If you use OpenSSL in the OpenSSL_pr.ini file in the [TLS Connection Settings] section in the **UsedHandShakeScheme** parameter set up the authentication scheme number. To select both schemes at once (2 and 4), specify 6.
 - _ If you use MP specify its settings in the MP_pr.ini file:
 - _ In the [Certificate Stores] section set up certificate storage. For details see [3.4.2](#).
 - _ In the [TLS Connection Settings] section set up the following settings:
 - _ **UsedHandShakeScheme** – authentication scheme number in correspondence with the rules of authentication schemes compatibility at server and client;
 - _ **CSPUseLocalMachineStore=0** – the key is located in the current user’s storage;
 - _ **CheckRevocation=0** – the certificate check for revocation is not performed;
 - _ **CSPCertHash** – hash of the server’s certificate.

For details about the settings see [3.4.3](#).

4. In QUIK Administrator specify administrator’s login:
- _ For authentication by login and password in domain – specify administrator’s login in the **Logins for another authorization system** dictionary;



To sign in login can be specified with domain or without it. If domain is specified full correspondence of domain and login is checked. If domain is not specified login is checked for the default domain.

- For authentication by login and password – specify administrator's login in user editing dialog box on the **Security** tab.

2.5 Registration of QUIK system users

1. Run QUIK Administrator.
2. Select the menu item **QUIK server/Organizations**. Add your organization to the dictionary, please fill in all fields.
3. Select the menu item **Users / Users (full)**. Add the account of QUIK system administrator to user's dictionary.

For that select name of your organization in the dictionary, enter initials of the manager and establish authorization's validity period.

List of classes contains names of security classes specified in settings. Choose sequentially each of them and press the **Manager** button to set rights to work with the class.

4. Specify the identifier of the trading participant in MOEX trading system in field **Identifier in TS**. Field **Client code on the dealer's side** may remain blank.
5. Register the user's public key generated during installation of QUIK Server (see [2.2.3](#), item 6), by pressing button **RSA keys**. In the opened window select the key file by pressing button **RSA file**. Load from these the key by pressing button **Add** and then close the window.
6. Similarly, add other users of your system installing the necessary parameters of access to the system using templates rights. Complete the field **Client code on the dealer's side** by the symbolic code that will be subsequently used by manager for setting limits and authentication of users when working with the system.

Detailed description of **QUIK Administrator** work is presented in the Administrator's manual.

QUIK system is ready to work!

Run the QUIK Workstation using the access keys and credentials of your first user.

2.6 Startup keys for QUIK server

If the configuration file of Limits calculation library is empty or is not available the Server start is interrupted with conclusion of the relevant diagnostic to log file.

2.6.1 -new (/n)

Run QUIK Server in the loading mode with new data and cleaning all files with .ik extension except the news file (news.ik), file of server QPILE portfolios (cstructp.ik), file of cash limits (mlimit.ik) and file of limits for securities (dlimit.ik).



2.6.2 -clean (/c)

Run QUIK Server in the loading mode with full cleaning of data as well as cleaning all files with .ik extension.

2.6.3 -old (/o)

Run QUIK Server in mode of loading with old data without cleaning storages.

2.6.4 -holiday (/h)

Redefining a business day as a holiday. The key overrides the default settings and those specified in quik.ini file.

2.6.5 -workday (/w)

Redefining a holiday as a business day. The key overrides the default settings and those specified in quik.ini file.

2.6.6 -loadlimits (/l)

Start server with loading limits from a file. Name of file with limits and its path must be typed in the command line after the key. Field formats of limits to be loaded are given in Appendix (see [3.1](#)). The information of the limits loaded from the file is updated only after connecting the interfaces (trading interfaces or the Holiday Information interface).

2.6.7 -install (/i)

Install QUIK Server as a service of Windows.

2.6.8 -remove (/r)

Delete QUIK Server as a service of Windows.

2.6.9 -removestops (/rs)

Run in mode of deleting stop orders from the current QUIK Server.

After that, users must make stop orders own on any other server so that these orders could trigger.

Key -removestops can be used together with keys -new and -clean.

2.6.10-text (/t)

Exporting data of a particular type to a text file.

Format:

```
quik.exe -text [-ansi] [<FILE>] [<TYPE>] [tsv]
```



where:

- -ansi – key to convert data from OEM encoding (CP866) to ANSI encoding (Windows-1251);
- <FILE> – exported file with orders and trades.
- <TYPE> – data type. Valid values:
 - _ orders – export orders from file (order.ik);
 - _ trades – export trades from file (trade.ik).

If names of files with orders and trades are different from order.ik and trade.ik, <TYPE> parameter is required.

- tsv – convert file to tsv format.

For example:

```
quik_02.exe -text -ansi trade.ik trades tsv > trade.txt
```

2.6.11-removelimits (/rl)

Start the server with cleaning data on client cash and securities positions, and restrictions of accounts at derivatives market. Other data (e.g., orders, trades, data from the Quotes table, etc.) are not deleted. The key can be used with the -loadlimits key.

2.6.12-rolling (/ro)

Launch the server with rolling positions. The information of the transferred positions is updated only after the interfaces (trade interfaces or the Holiday Information interface) are connected.

2.7 QUIK Administrator account creation

To create a QUIK Administrator new account and assign a user with administrator's permissions, run QUIK Administrator server part using the key **-set-admin-right**.

The format:

```
QAdminSrv.exe -set-admin-right -instance=[<instance>] -UID=[<UID>] -QUIK-key-  
filename=[<QUIK-key-filename>]
```

where:

- <instance> – database identifier. The database identifiers are listed in [Instances] section of the QAdminSrv.ini file. If the QUIK server uses a single DB, then the parameter is not required.



- <UID> – identifier of a user to assign an RSA key. If the parameter is not specified, a new user will be created.
- <QUIK-key-filename> – path and name of the file containing a public key RSA. The relative or absolute path can be specified. If the name and / or path contains spaces, then the value is quoted, for example, C:\Path\some file.txk. If the file contains more than one public key RSA, then the first key in the file is used. If the <UID> parameter is specified and there is an RSA key for a user, then this parameter is not required.

For example:

```
QAdminSrv.exe -set-admin-right -UID=350 -QUIK-key-filename="C:\Path\some file.txk"
```

2.8 QUIK workstation banner configuration

In QUIK workstation, on the toolbar there is a banner, which by clicking on it opens a website (for example, a broker's website).

2.8.1 Configuration of banner

To configure banner, follow the steps below:

1. Copy a banner image file to the directory **QUIK\Server\Areas\Banners**. The file requirements are:
 - _ file format – .bmp;
 - _ file extension – any. Recommended: 468*60 pixels:
 - _ color depth – 8 bit.
2. In the directory **QUIK\Server\Areas\Banners**, in the **banners.ini** file configure the settings in section [url_set]:
 - _ **url** – URL address.
 - _ **image** – name of the banner image file.

Example:

```
[url_set]
url=http://www.broker-website-example.ru
image=broker.bmp
```

3. On the computer where a QUIK server is run, in the file **QUIK\Server\quik.ini** configure the following settings:

```
[natural_level_section]
```



```
module=banner_module
[banner_module]
module=dwbanner.dll
```

The banner settings for the server and the access server are the same

2.8.2 Deactivation of banner

To disable receiving banners from the access server, do the following:

1. Make sure that the following line is present in the [natural_level_section] section in the quik.ini access server settings file:

```
module=banner_module
```

2. Make sure quik.ini file of access server has the following section:

```
[banner_module]
module=dwbanner.dll
```

3. Add the following key to [banner_module] section of quik.ini file of access server:

```
ignore_up_dwell=1
```

```
[banner_module]
module=dwbanner.dll
ignore_up_dwell=1
```

4. Make sure the dwbanner.dll module is present and then start the access server.

After applying such settings, the banner won't be sent from the server to the access server and users of the access server won't see it.

2.8.3 Replacement of banner

To replace the banner, configure the scheme as follows:

1. The .\Areas\Banners\ directory has to contain the .ini file with the settings as following:

```
[url_set]
```



```
url=c:\  
image=test.bmp
```

where:

- _ Value of the url key — url, that opens in QUIK Workstation;
 - _ image — name of the file in .\Areas\Banners\ directory.
2. Change the old file to new one with the name that differs from the current banner name (for example test2.bmp) in .\Areas\Banners\ directory.
 3. Change the value of the image key to a new one in .ini file — test2.bmp.

URL can be changed without changing the image.

Also, without changing image and url, you can add another .ini file with a different url and image. In this case, the banner from the new .ini file is used.

2.9 File transfer configuration

In the QUIK system, you can transfer files from the server to QUIK workstations (via personal file areas to the QUIK server). This makes possible to organize sending of reports to customers, also reports can be signed with digital signature.

To send files to clients that are not intended for updating the QUIK workstation, the files must be placed in the specified directory:

- Server\Areas\private\ — for sending to specific users.
- Server\Areas\public\ — for sending to all users.

After that, you need to use the **System / Receiving files** dialog box:



3. Appendix

3.1 Format of limits

Parameters obligatory for configuration are ticked by '*'.

Format of security limit:

Parameter	Description	Size, exactness (expressed in symbols)
* DEPO:	Title of line with expressed security position	
* FIRM_ID	Identifier if trading participant	12
* SECCODE	Instrument code	12
* TRDACCID	Trading account	12
* CLIENT_CODE	Client code	12
* OPEN_LIMIT	Opening limit	30
* OPEN_BALANCE	Client position	30
CURRENT_LIMIT	Current limit	30

Parameter	Description	Size, exactness (expressed in symbols)
WA_POSITION_PRICE	Purchase price	30, 6
LIMIT_KIND	Limit kind. Valid values: – 0 – for current limits; – <N> – for limits on positions with T+<N>; – value less than zero – for technological limits	32, 0

Format of cash limit:

Parameter	Description	Size, exactness (expressed in symbols)
* MONEY:	Title of line with expressed cash position	
* FIRM_ID	Identifier if trading participant	12
* CURR_CODE	Currency code	4
* TAG	Settlement tag	4
* CLIENT_CODE	Client code	12
OPEN_LIMIT	Opening limit	30, 2
* OPEN_BALANCE	Client position	30, 2
CURRENT_LIMIT	Current limit	30, 2
LIMIT_KIND	Limit kind. Valid values: – 0 – for current limits; – <N> – for limits on positions with T+<N>; – value less than zero – for technological limits	32, 0
* LEVERAGE	Leverage	30, 2

Leverage for cash limit:

Parameter	Description	Size, exactness (expressed in symbols)
* MONEY:	Title of line with expressed cash position	



Parameter	Description	Size, exactness (expressed in symbols)
* FIRM_ID	Identifier of trading participant	12
* CURR_CODE	Currency code	4
* TAG	Settlement tag	4
* CLIENT_CODE	Client code	12
*	Client position	30, 2
OPEN_BALANCE		
CURRENT_LIMIT	Current limit	30, 2
LIMIT_KIND	Limit kind. Valid values: – 0 – for current limits; – <N> – for limits on positions with T+<N>; – value less than zero – for technological limits	32, 0
* LEVERAGE	Leverage	30, 2

Example of records in limits file:

```
MONEY: FIRM_ID = NC0038900000; TAG = EQTS; CURR_CODE = SUR ; CLIENT_CODE = 004;
OPEN_BALANCE = -46.52; OPEN_LIMIT = 0.00;
MONEY: FIRM_ID = NC0038900000; TAG = EQTS; CURR_CODE = SUR ; CLIENT_CODE = 004;
OPEN_BALANCE = -46.52; LEVERAGE = -1;
MONEY: FIRM_ID = NC0038900000; TAG = EQTV; CURR_CODE = SUR ; CLIENT_CODE = 004;
OPEN_BALANCE = 1048.51; OPEN_LIMIT = 450000.00; LIMIT_KIND = 1;
DEPO: FIRM_ID = NC0038900000; SECCODE = HYDR; CLIENT_CODE =10004/10004; OPEN_BALANCE
= 113955; OPEN_LIMIT = 0; TRDACCID = L01-00000F00;
DEPO: FIRM_ID = NC0038900000; SECCODE = IRAO-004D; CLIENT_CODE =10006/10006;
OPEN_BALANCE = 738467; OPEN_LIMIT = 0; TRDACCID = L01-00000F00; LIMIT_KIND = 1;
```

3.2 Password encryption

Passwords specified in the Module settings can be encrypted. The password must not begin with "\$" and "#" symbols. If you use a password that begins with any of the above symbols, change the first symbol.

To activate password encrypting functionality, add '\$' before the password in the configuration file.



For example:

```
Password=$secret
```

When trying to use a password, the server encrypts the password and saves it to the configuration file in an encrypted form. The encrypted password is marked by '#' symbol at the start of a string.

When transferring the program to another computer or reinstalling the operational system, the encrypted passwords get unavailable for unencrypting. In this case, the appropriate passwords must be reset.

3.3 Format of configuration file of encryption by means of OpenSSL library

The current section describes settings of encryption by means of OpenSSL cryptographic library (www.openssl.org). OpenSSL application does not require saving certificates in OS register on the platform with the QUIK server. It makes certificate installation and servicing easier.

3.3.1 [General] section

- **CertStoreFile** – certificate storage file name. Value by default: certs\store.pem.
- **ServerCertificateKey** – password of server's certificate key. The password must be encrypted (for details see [3.2](#)).
- **NewServerCertHash** – new server's certificate hash.
- **NewServerCertDomainName** – new server's certificate domain.

NewServerCertHash and NewServerCertDomainName settings specify the parameters of a new certificate when planned certificate replacing at the server. After certificate replacement the values of NewServerCertHash and NewServerCertDomainName settings are recorded to ServerCertHash and ServerCertDomainName parameters of OpenSSL_Pr.ini file in the QUIK Workstation.

- **ClientCertificatesDir** – path to the directory that contains certificates for checking digital signature. Value by default: certs\client.

3.3.2 [TLS Connection Settings] section

The following connection parameters are specified in the section:

- **ServerHandShakeScheme** – the supported authentication scheme. Possible values:



- _ 1 – authentication by certificate;
- _ 2 – authentication in domain;
- _ 4 – authentication by login and password;
- _ 8 – password recovery;
- _ 7 (by default) – all the schemes are supported besides 8 (password recovery).

When a few authentication schemes are supported, the specified value of the field is the sum of values, corresponding to the supported schemes.

- **UsedHandShakeSchemePrefer** – the preferred authentication scheme. It must be selected if a client had chosen scheme 0 (is defined by server). Possible values:
 - _ 1 – authentication by certificate;
 - _ 2 – authentication in domain;
 - _ 4 (by default) – authentication by login and password.
- **SSLProtocols** – the list of TLS protocol versions available for connection, separated by a comma. Possible values:
 - _ TLSv1.0;
 - _ TLSv1.1;
 - _ TLSv1.2.
- **CA** – path to the directory that contains root certificates. Value by default: certs\CA.
- **CRL** – path to the directory that contains certificate revocation lists. Value by default: certs\CRL.

3.4 Format of server part configuration file of encryption by means of MP library (MP_Pr_server.ini)

3.4.1 [Crypto Provider Settings] section

The section contains description of the cryptographic provider settings required for check of a digital signature.

To use the digital signature, specify a key container using any of the following methods:

1. Specify parameters of the container:

- _ **CSPName** – name of a Cryptographic Service Provider (CSP) used by the certificate.
- _ **CSPContainerName** – name of the key container.
- _ **CSPTYPE** – CSP provider type.



If CSPName parameter is not specified, the system provides a CSP provider, assigned by default for a specified type of cryptographic provider.

2. Specify a file of the certificate linked to the key container:

- _ **CSPCertFileName** – path to the certificate file.

3. Specify a hash of the certificate linked to the key container:

- _ **CSPCertHash** – hash of the installed certificate.

To get a certificate hash:

- _ Open the certificate file;
- _ Switch to the **Details** tab;
- _ Copy the value of the **Thumbprint** field and remove the spaces.

Additional parameters to set up the digital signature (optional):

- **CSPUseInService** – indicates that cryptographic provider works in 'silent' mode. Possible values:
 - _ 0 – cryptographic provider works online;
 - _ 1 – cryptographic provider works in 'silent' mode.

The cryptographic provider doesn't interact with the user in 'silent' mode. An error appears upon the occurrence of an event that requires interactive communication (for example, entry of the password to access the container).

- **CachKeyAndCertificates** – indicates that keys and certificates are cached for quick access to them. Possible values:
 - _ 0 – do not cache;
 - _ 1 – cache.
- **CSPUseLocalMachineStore** – private key location. Possible values:
 - _ 1 – the key is located in the local computer store;
 - _ 0 (by default) – the key is located in the current user's storage.
- **CheckRevocation** – indicates that the certificate is checked for revocation. Possible values:
 - _ 0 – the check is not performed;
 - _ 1 – the check is performed.



3.4.2 [Certificate Stores] section

The section contains description of the certificates store, where the certificates are searched to set up the encryption modes and digital signature:

At least one certificate store should be specified to ensure correct work of the cryptographic provider.

- **MY** – standard personal store of the user certificates. Possible values:
 - _ 0 – not used;
 - _ 1 – used.
- **CA** – standard store of the Certification Authorities' certificates. Possible values:
 - _ 0 – not used;
 - _ 1 – used.
- **ROOT** – standard root store. Possible values:
 - _ 0 – not used;
 - _ 1 – used.
- **SPC** – standard store of the software vendors' certificates. Possible values:
 - _ 0 – not used;
 - _ 1 – used.
- **CUSTOM_STORE** – third-party external store. Possible values:
 - _ 0 – not used;
 - _ 1 – used.

Each store is described by the following parameters:

- **HOST** – host where the store is located. Value: "." (full stop).
- **LOCATION** – physical store location.
- **TYPE** – store type. Possible values:
 - _ 1 – system store;
 - _ 2 – external store located in a specific file.
- **UPDATABLE** – feature of an updatable store. Possible values:
 - _ 0 – not allowed to be updated;
 - _ 1 – allowed to be updated.
- **PRIORITY** – priority. Value: 1.

For example:



```
[CUSTOM_STORE]
HOST=.
LOCATION=D:\QUIK\Server\CPStorage\usercerts.sto
TYPE=2
UPDATABLE=1
PRIORITY=1
```

3.4.3 [TLS Connection Settings] section

The section is used to configure a TLS connection.

- **SSLProtocols** – list of the protocols used (separated by spaces (" ") or commas (",")).

Possible values:

- _ SSLv2;
- _ SSLv3;
- _ TLSv1;
- _ TLSv1.1;
- _ TLSv1.2.

If the parameter is not specified, SSPI automatically selects the latest version of the protocol supported by the server and client. The parameter is not specified by default.

To work in encryption mode, specify a private key. To do this, specify a certificate linked to a private key by using one of the following methods:

1. Specify parameters of the container:

- _ **CSPName** – name of a Cryptographic Service Provider (CSP) used by the certificate;
- _ **CSPContainerName** – name of the key container;
- _ **CSPTYPE** – CSP provider type.

If CSPName parameter is not specified, the system provides a CSP provider, assigned by default for a specified type of cryptographic provider.

2. Specify a file of the certificate:

- _ **CSPCertFileName** – path and name of the certificate file.

3. Specify a hash of the certificate linked to the key container:

- _ **CSPCertHash** – hash of the certificate.

Authentication parameters:

- **UsedHandShakeScheme** – authentication scheme used. Possible values:



- 1 – authentication scheme by certificate, i.e. the client is checked by certificate that he provided establishing an SSL/TLS connection;
- 2 – authentication scheme by domain login and password through the Domain Controller;

IMPORTANT! The authentication scheme cannot be used, if in the QUIK Administrator's server configuration file in the [QuikOptions] section the EnableMultiple2FaLogins setting contains '1'.

- 4 – authentication scheme by login and password;

Server's and client's authentication schemes compatibility:

If the first authentication scheme is configured on the server, the client can use the first and fourth schemes.

If the second authentication scheme is configured on the server, the client can use the second and fourth schemes.

If the fourth authentication scheme is configured on the server, the client can use only the fourth scheme.

- 7 (by default) — all modes are supported, except for 8 (password recovery);
- 8 — password recovery.

When multiple authentication modes are supported, the setting value is set as a sum of values corresponding to the supported modes.

- **DomainController** – address of the Domain Controller being referenced when authenticating a client. This parameter is used if the second authentication scheme is applied.

If the DomainController setting is not specified, the current Domain Controller is used.

- **DomainLogin** ^{*} – user's domain login for the access server authentication. Value by default: "" (empty).
- **DomainPasswd** ^{*} – user's domain password for the access server authentication. Value by default: "" (empty).

(^{*}): These parameters are used only when connected via the access server where the second authentication scheme is configured.

Additional parameters to set up the encryption mode (optional):



- **CSPUseInService** – indicates that cryptographic provider works in 'silent' mode. Possible values:
 - _ 0 – cryptographic provider works online;
 - _ 1 – cryptographic provider works in 'silent' mode.

The cryptographic provider doesn't interact with the user in 'silent' mode. An error appears upon the occurrence of an event that requires interactive communication (for example, entry of the password to access the container).

- **CSPUseLocalMachineStore** – private key location. Possible values:
 - _ 0 (by default) – the key is located in the current user store;
 - _ 1 – the key is located in the local computer store.
- **CheckRevocation** – indicates that the certificate is checked on the revoked certificates list by the cryptographic provider. Possible values:
 - _ 0 – the check is not performed;
 - _ 1 – the check is performed.
- **IOBufferMaxSize** – buffer size (in bites) for input/output data in TLS connection handshake. Value by default: 65536.
- **CheckClientCert** – indicates that the client's certificate is verified using the additional tools of Windows operating system.
- **HashCalcCount** – number of iterations of the password hash function calculation on the server. Possible values: from 1 to 10037. Value by default: 4999.

3.4.4 [TLS Extra Parameters] section

The section contains the settings (optional) for the planned change of server's certificates.

IMPORTANT! The settings of the planned change of certificate should be specified before the expiration date of the current certificate. The settings are deleted after the certificate change.

- **NewServerCertHash** – possible values:
 - _ Hash of a new server's certificate – after the certificate change, this value is written to the **ServerCertHash** setting of the client's .ini file (**MP_Pr_client.ini**), and then the value of the **NewServerCertHash** setting is deleted.
 - _ DELETE – cancellation of the certificate change procedure.

Value by default: "" (empty).

- **NewServerCertDomainName** – possible values:



- Domain name of a new certificate – after the certificate change, this value is written to the **ServerCertDomainName** setting of the client's .ini file (**MP_Pr_client.ini**), and then the value of the **NewServerCertDomainName** setting is deleted.
- DELETE – cancellation of the certificate change procedure.

Value by default: "" (empty).

3.5 Format of client part configuration file of encryption by means of MP library (MP_Pr_client.ini)

In the file broker can set up parameters, which will be used by the MP provider for creation of private key and user certificate (cryptographic provider, algorithm, size and purpose of the key, etc.). Besides that, format and content of certificate issue claim, which user can print after key creation, are set up in the file.

3.5.1 [SubjectFieldList] section

The section contains the list of fields to be added to the Subject section of certificate request in format:

```
<ParamName>=<0,1>
```

Where

- <ParamName> – user-defined field name. For each field a section of [fieldDesc_<ParamName>] view must be created in the configuration;
- Value 0 (by default) – field is disabled, and is not displayed in the dialog box;
- Value 1 – field is displayed in the dialog box (if the **Visible** attribute in the field description does not have another value).

3.5.2 [AlternateFieldList] section

The section contains the list of fields to be added to the Subject Alternative Name section of certificate request. The section format is the same as the format of the [\[SubjectFieldList\]](#) section.

3.5.3 [fieldDesc_<ParamName>] section

The section contains the description of <ParamName> field, which is added to the certificate request dialog box.

When the value of the described field is processed, spaces on the right and on the left of the string are discarded. If a string consists of spaces only, it is meant to be empty.



- **Name** – field name. If the parameter is absent, the corresponding field is not displayed on the dialog box. After the field name symbol `:` is added on the dialog box.
- **OID** – identifier of field in the certificate request. If the parameter is absent, the corresponding field is not displayed on the dialog box.
- **Type** – field type. Valid values:
 - _ 0 (by default) – text;
 - _ 1 – figure;
 - _ 2 – non-editable enumerated;
 - _ 3 – editable enumerated.

Enumerated fields depend on the EnumList and EnumFile attributes. If the attribute value is not specified, the list is empty. If both attributes are specified, the lists are joined. If enumerated list is used in the parameter entry dialog box, then quick search by context value is available.

- **Banner** – text of tip to the field, which is displayed when the field has no value specified.
- **LengthMax** – maximum field size in symbols. Value by default: 64.
- **LengthMin** – minimum field size in symbols. Value by default: 1.
- **Required** – indicates that the field is required to be filled. Valid values:
 - _ 0 – field is not required to be filled;
 - _ 1 – field is required to be filled. The field has `\*` in the parameter entry dialog box.
- **Visible** – indicates that the field is displayed in the parameter entry dialog box.
 - _ 0 – field is not displayed. At this field value is equal to the default value if it is specified. If the PrintTag attribute is specified, then the hidden field value is transmitted to the print template. If the default value is not specified, then no value is transmitted to the template;
 - _ 1 (by default) – field is not displayed.
- **PrintTag** – token to link the print field. Token value is a set of symbols excluding spaces and separators. Tokens in square brackets (`[]`) are linked to the field value in the print template.
- **RemoveEmpty** – attribute, which indicates that empty fields must be deleted. If the field is not required to be filled (Required=0), and its value is not specified, then the corresponding field is not added to the request, and the string corresponding to the PrintTag is deleted from the print template. Valid values:
 - _ 0 – do not delete;
 - _ 1 (by default) – delete.
- **EnumList** – list of enumerated field values separated by `|`.
- **EnumFile** – file with the list of enumerated field values. Values in the file are specified each in a new string.



- **EnumSort** – sorting order of enumerated field values. Valid values:
 - _ 0 (by default) – lexicographical with sorting by values;
 - _ 1 – lexicographical with sorting by keys;
 - _ 2 – as listed.
- **DefaultValue** – default value of the field. For enumerated list must contain a value from the list. If it contains a value not from the list or a field value is not specified, the first value in the list is selected. For editable list the specified value is always selected.

3.5.4 [Generation Settings] section

- **DialogName** – the heading of the dialog box for key creation and entering values for certificate request. If the value is not specified, then the dialog box heading is "Creating key pair and request for certificate".
- **CertReqFileName** – certificate request file name. Value by default: certrequest.pem.
- **UseCSPPParameters** – mode of using the key creation predefined parameters. Valid values:
 - _ 0 (by default) – mode is disabled;
 - _ 1 – mode is enabled. Fields of cryptographic provider and key settings selection are blocked, values correspond to provider's settings.
- **CSPTType** – type of cryptographic provider.
- **CSPName** – name of cryptographic provider.
- **KeyAlgorithm** – key algorithm. If the value is not specified, then the default algorithm is selected.
- **CSPContainerName** – key container name. If the value is not specified, then it is generated automatically based on the time stamp.
- **KeyLength** – key length. If the value is not specified, then the default value for the selected algorithm is used.
- **KeyUsage** – key usage. Bit mask of values specified in decimal format. Value by default: 0xF0 (Digital signature + Immutability + Key encryption + Data encryption).
- **KeyExtension** – key extensions. Text values of extension identifiers separated by comma. Value by default: 1.3.6.1.5.5.7.3.2 (Client Authentication).
- **PrintTemplate** – template file name. If the value is specified, then after a key and certificate request are created the template will be used for claim printing. Value by default: "" (empty).
- **OutputFile** – file with claim created by the template.

3.5.5 Example of configuration file intended to customize the dialog box for certificate request

```
[SubjectFieldList]
CN=1
O=1
L=1
S=1
```



```
[AlternateFieldList]
INN=1
OGRN=1

[fieldDesc_CN]
Name=User name
OID=2.5.4.3

[fieldDesc_O]
Name=Firm name
OID=2.5.4.10

[fieldDesc_L]
Name=User location
OID=2.5.4.7

[fieldDesc_S]
Name=Region
OID=2.5.4.8

[fieldDesc_INN]
Name=INN
Type=1
LengthMin=13
LengthMax=14
OID=1.2.643.3.131.1.1

[fieldDesc_OGRN]
Name=OGRN
Type=1
LengthMin=12
LengthMax=12
OID=1.2.643.100.1
```

For the above example the values entry dialog box will have the following view:



Generate key pair and certificate request

Keypair creation params

Crypto provider: Microsoft Strong Cryptographic Provider

Key algorithm: RSA

Key length (bit): 2048

Key usage: ☒ Digital sign ☒ Data encryption

Certificate owner

User name: John Smith

Firm name: United company

User location: London

Region:

INN: 95000003450001

OGRN: 099927321117

OK Cancel

