Chapter 1. Before Starting

1.1 General information 2
1.2 System requirements 3
1.3 Program installation 3
1.4 Adding and selecting cryptographic provider in QUIK workstation settings 5
1.5 Configuration of encryption carried out by means of qrypto32 library 8
1.6 Configuration of QUIK workstation to operate with SSLAndMessagePro cryptographic provider 9
1.7 Configuration of encryption and digital signature carried out by means of MP library 18
1.8 Configuration of encryption and digital signature carried out by means of OpenSSL library 23
1.9 Running keys of the QUIK workstation 27
1.10 Configure connection 28
1.11 Connecting to the QUIK Server 35
1.12 Monitoring the connection status 38
1.13 Versions of components and plugins 42
1.14 Program updates 43
1.15 Receiving files 43
Appendix 1. Error messages 46
Appendix 2. Example of certificate retrieval via web interface of Certification Authority 50

> **This User's manual describes the operation rules, basic functions and installation / setup procedure for the software. Before carrying out your first trade, please read this manual carefully to avoid errors.**

1.1 General information

QUIK workstation is the main user application of the software package that provides access to trading and market information in real time (internet trading).

1.1.1 Basic functions

Obtaining information

One of the main features of the program is display of the exchange information in a near real-time. QUIK workstation allows monitoring current state of the market, including Level II Quotes, and the log of executed transactions. It also provides a means for receiving news from news agencies, and exchanging messages with the broker.

Charts and indicators

The trading behavior is represented on charts. Charts in QUIK can be plotted for any market parameter using technical analysis tools, and displaying history of trade operations. The program features over 30 technical analysis indicators, Fibonacci lines, angles and arcs, and allows for plotting trend, horizontal and vertical lines, graphic and text labels.

Executing transactions

QUIK workstation allows the client to view the status of his own assets, create buy/sell orders for instruments and submit them to the broker's server. Orders can be entered from software by means of integrated programming languages as well as from a chart.

Standard functions of QUIK workstation makes it possible to configure so called scalper's level II quotes (quotes window view) allowing to quickly submit orders by using buttons on the toolbar or with drag-and-drop technologies.

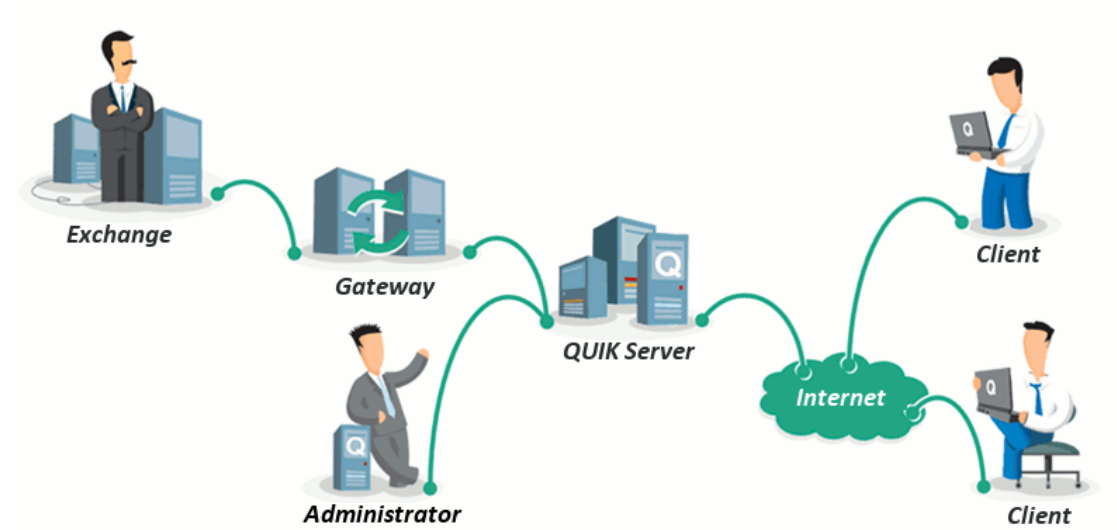
Export and import of data

Integrated export mechanisms allow you to use the obtained data in other programs such as user’s own databases, and systems of technical analysis. Data on trades and any parameters of the trading session can be exported. Data can be exported both as ticks (i.e. for each transaction) and as candles (for a time interval). Data from most tables, including Level II Quotes table, can be exported into MS Excel or a database via DDE or ODBC.

Import of transactions is a possibility of connecting external programs for automation of creation and submission of orders to the trading system. Import is implemented by means of exchanging data via text files or API.

1.1.2 Internet trading structure

QUIK Server is the core unit of the system. The server is connected to trading systems of various exchanges through special gateways that transfer information about trading and broker's assets on the exchange to the server and receive orders to sell or buy. The server collects information from trading systems and transmits it to all active (connected) clients with the least possible delay.



The system administrator is authorized to register users, grant them the rights to use information, and determine limits within which the client can transact.
The system user can receive information on exchange trading and available funds and can independently participate in trading by sending orders to the trading system directly from the QUIK workstation.
The client terminal connects to the QUIK server through the internet using the TCP / IP protocol. All information transmitted between the server and the client is encrypted. To prevent unauthorized use, a password is used.

1.2 System requirements

For detailed system and software requirements, see the official website of QUIK.

1.3 Program installation

1. Get the QUIK workstation installation kit. Usually, it contains settings to work with a particular QUIK Server, so it must be obtained directly from the organization maintaining the server (Broker or Exchange).
2. Start the executable installation file and follow the installation program's instructions. After the installation process is over, the **QUIK** submenu will be created in the **Start / Programs** Windows menu.
3. Cryptographic data protection is used for secure mutual authentication of QUIK software server part and user's client part, and to protect information transmitted over the communication channels. Additionally, digital signature can be used for transactions, as well

as two-factor authentication mechanism. The security tools are configured in the QUIK workstation by a user.

If your broker provided you with a manual on how to set up authentication and digital signature, follow it. If you have no such a manual, request from your broker the information on authentication and digital signature configuration in the QUIK workstation.
This information must include answers to the following questions:

- Which way of authentication at the QUIK server will be used, by means of which cryptographic provider;
- Whether the digital signature will be used, and which cryptographic provider will be employed.

4. Specify the settings of authentication and cryptographic data protection. For this install or select from the list of preset cryptographic providers the one, which is used by your broker, and configure it. The following cryptographic providers are supported in the QUIK workstation:

   - grypto32 – the default authentication mechanism based on the Public / Private key technology. For description of access key generation procedure, see User's manual for Program of keys creation and management (KeyGen). The program comes as part of the distribution kit.
   - MP – for description, see Configuration of QUIK workstation to operate with SSLAndMessagePro cryptographic provider.
   - OpenSSL – for description, see Configuration of encryption and digital signature carried out by means of OpenSSL library.

The way of cryptographic provider selection in QUIK workstation for encryption and digital signature is described in the QUIK workstation settings.

To run the QUIK workstation, use the shortcut **QUIK Information & Trading System** (info.exe).

1.3.1 Language settings

If the user has the QUIK workstation installed in Russian, and a language other than Russian is selected in the computer locale (**Control Panel** / **Clock and Region** / **Region**, **Administrative** tab, **Language for non-Unicode programs** section), then unreadable characters may appear in the QUIK workstation.

To fix unreadable characters, follow these steps:

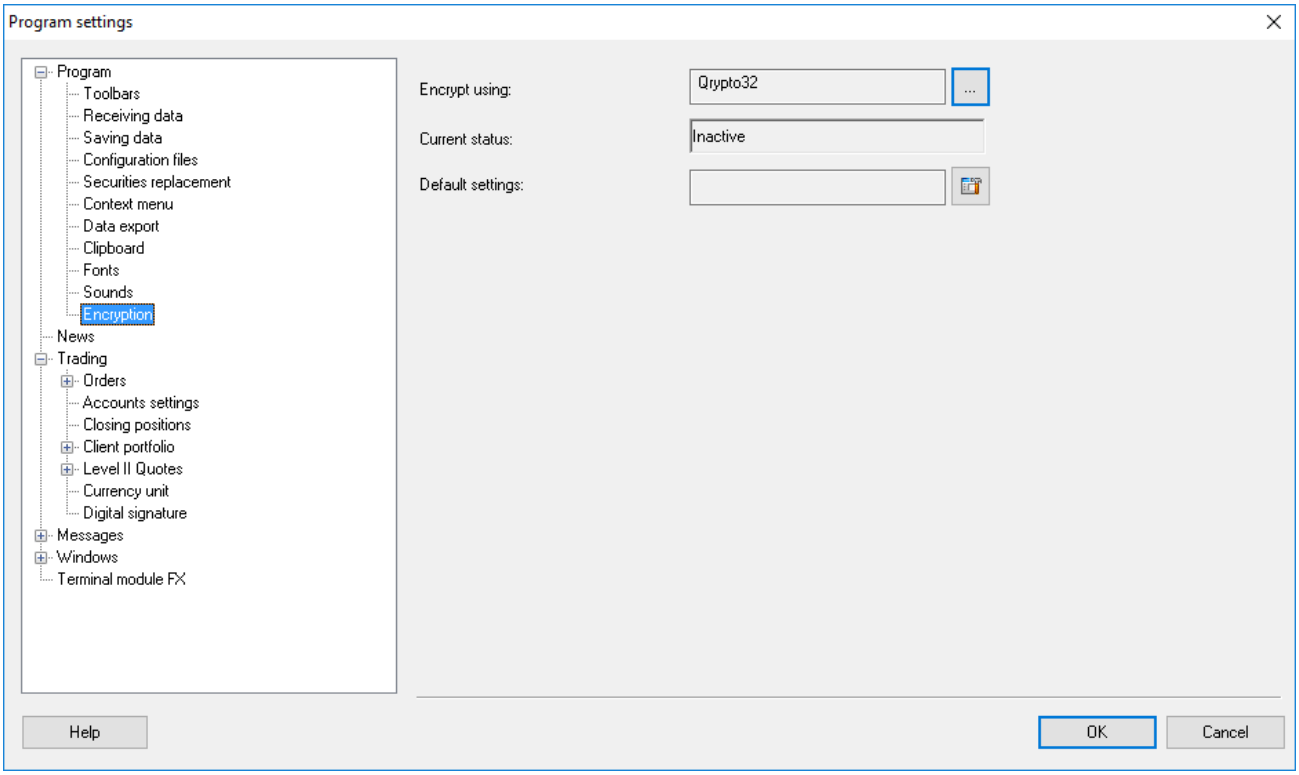
1. Close the QUIK workstation.
2. In the computer settings, go to the **Control Panel** / **Clock and Region** / **Region** section, **Administrative** tab, in the **Language for non-Unicode programs** section, click the **Change system locale** button and select Russian language.
3. After making all changes, recreate all open tables and reorder the data (**System / Data request / Reorder data...** menu item) for correct displaying.

1.4 Adding and selecting cryptographic provider in QUIK workstation settings

1.4.1 Encryption mode

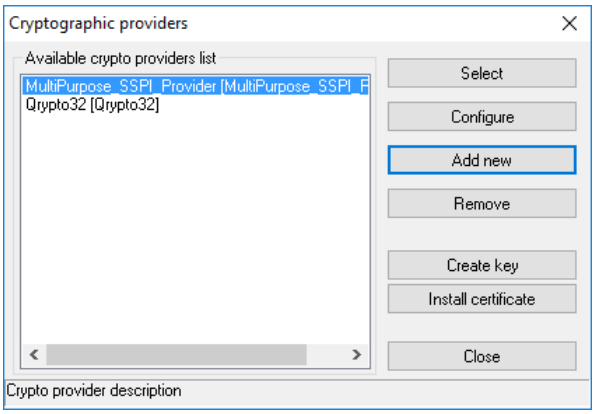
This mode is used for operation via secured client-server connection.

1. Launch the QUIK workstation. In the main menu select **System / Settings / General settings...** menu items.
2. In the opened window select **Program / Encryption** section.

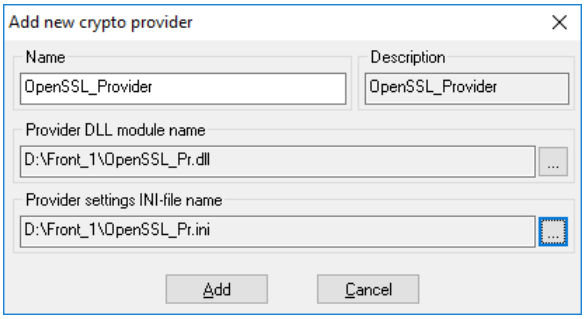


Click ... button in **Encrypt using** box.

Cryptographic providers dialog box will be opened. The dialog box contains the list of added cryptographic providers and the set of buttons for their managing:



3. To add a new cryptographic provider click **Add new**. On clicking the button, the dialog box of the following view is opened:

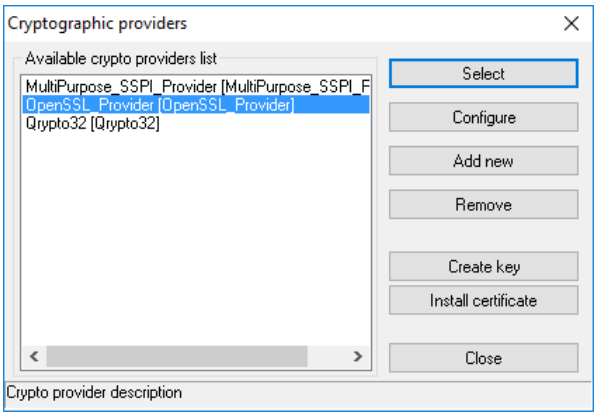


Fill in the following fields in the **Add new crypto provider** dialog box:

- **Provider DLL module name** – path to the supplied encryption library file. If the file is valid, the **Name** and **Description** fields will be filled in automatically.
- **Provider settings INI-file name** – path to the encryption configuration file.

To save the settings click the **Add** button. To close the dialog box without saving settings click **Cancel**.

4. Newly added cryptographic provider appears in the list of available cryptographic providers:

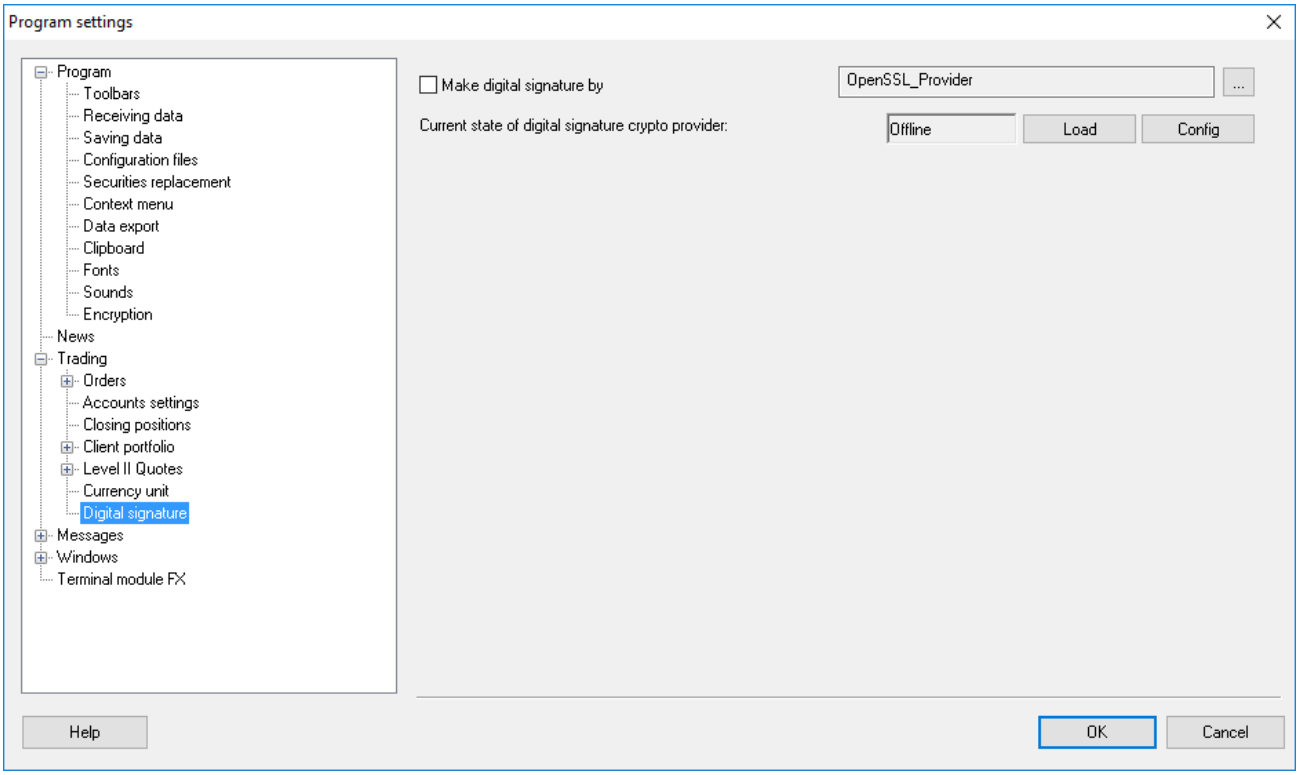


5. Select the required cryptographic provider and click the **Select** button.

1.4.2 Digital signature mode

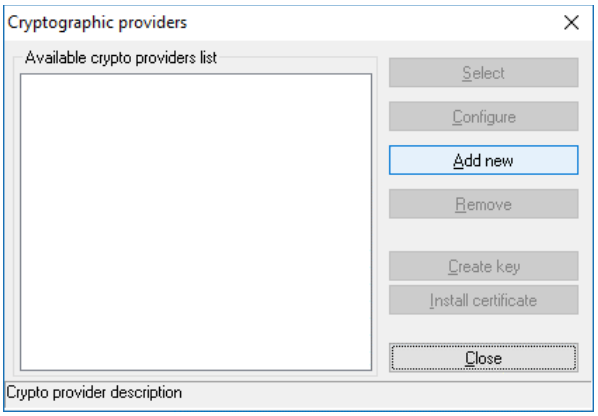
This mode is used for operations with the usage of digital signature.

1. Launch the QUIK workstation. In the main menu select **System / Settings / General settings...** menu items.
2. In the opened window select **Trading / Digital signature** tab.

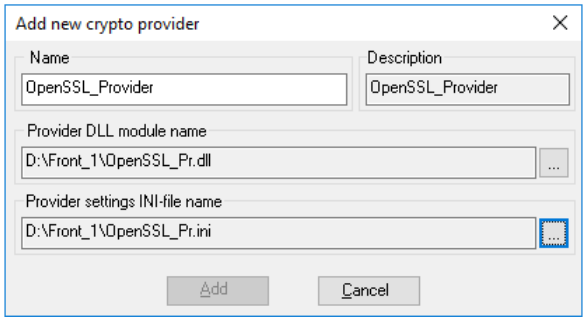


Click ... button in **Make digital signature by** box.

Cryptographic providers dialog box will be opened. The dialog box contains the list of added cryptographic providers and the set of buttons for their managing:



3. To add a new cryptographic provider, click the **Add new** button. On clicking the button, the dialog box of the following view is opened:

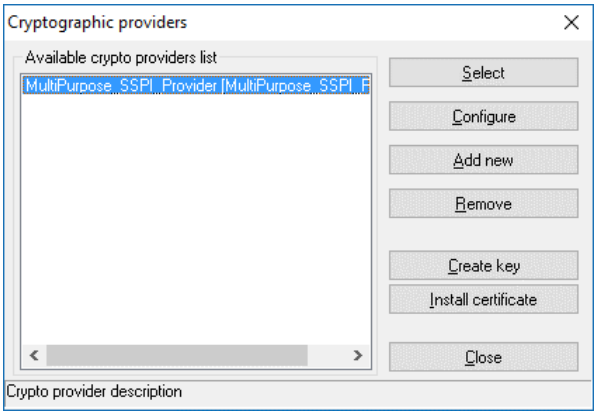


Fill in the following fields in the **Add new crypto provider** dialog box:

- **Provider DLL module name** – path to the supplied encryption library file. If the path and name are specified correctly, the **Name** and **Description** fields will be filled in automatically.
- **Provider settings INI-file name** – path to the encryption configuration file.

To save the settings click the **Add** button. To close the dialog box without saving settings click **Cancel**.

4. Newly added cryptographic provider appears in the list of available cryptographic providers:

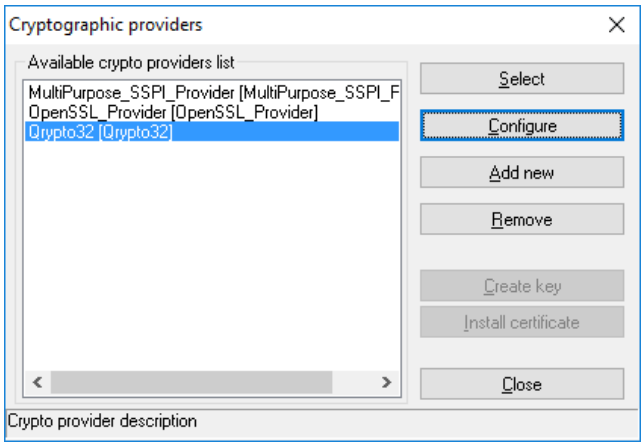


5. Select the required cryptographic provider and click the **Select** button.

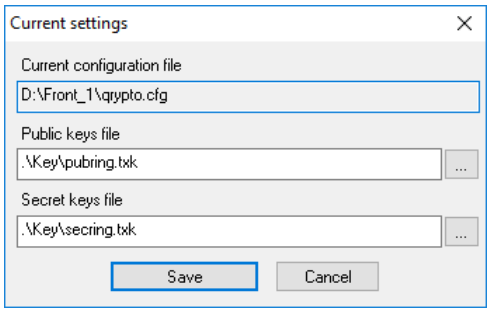
1.5 Configuration of encryption carried out by means of qrypto32 library

After generation of public and private keys according to the instructions, described in the User's manual for Program of keys creation and management (KeyGen), receive the confirmation of public key registration from your broker and set up the cryptographic provider in the QUIK workstation in the following way.

In the **Cryptographic providers** dialog box select Qrypto32 provider and click **Configure**.



In the opened dialog box select the file paths to the public and private keys:



The current configuration file will be selected automatically.

Click **Save** to complete the setting.

1.6 Configuration of QUIK workstation to operate with SSLAndMessagePro cryptographic provider

1.6.1 Purpose

The **SSLAndMessagePro** cryptographic provider provides the ability to work with two cryptographic libraries Message-Pro and SSL-Pro.

1.6.2 Program configuration

Copy the files necessary for the program to work to the working directory:

- **sslpro.dll** – SSL-Pro library, provided by Signal-COM;

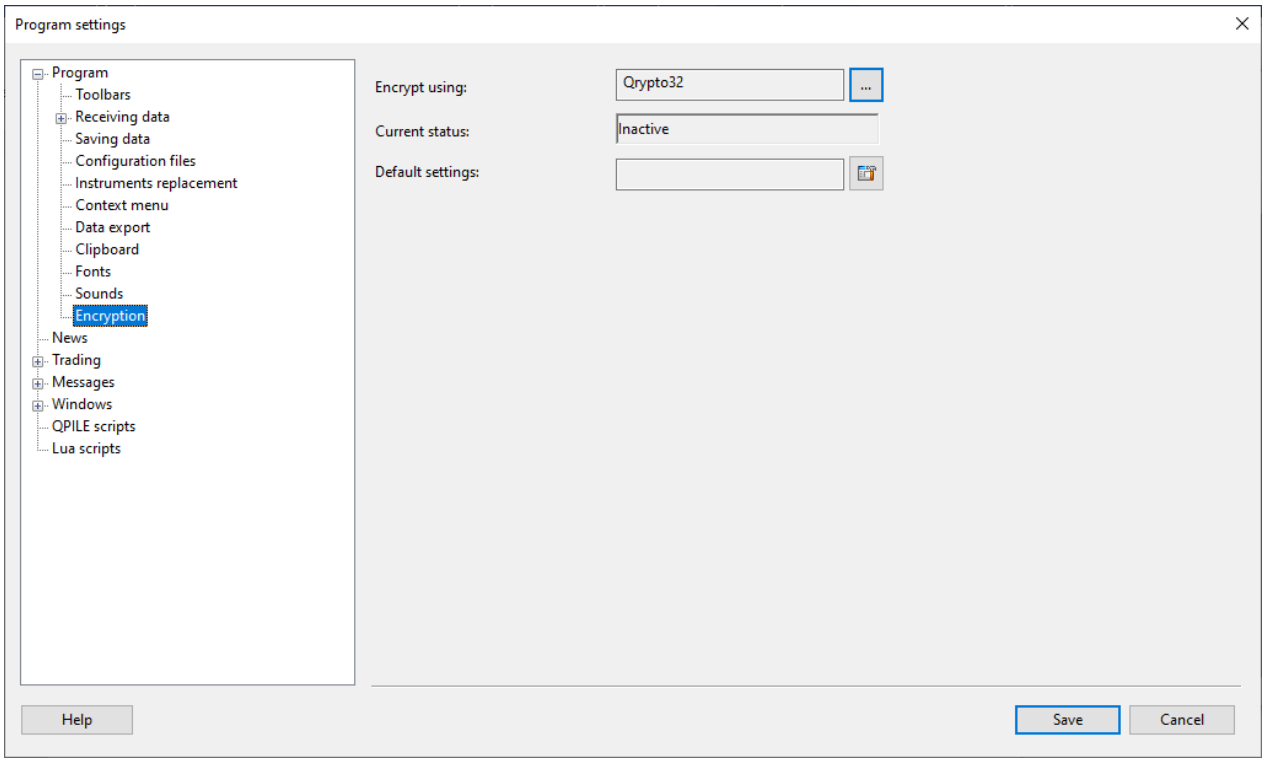
> **The version of the SSL-Pro library must match the version of the library of the same name installed on the QUIK server.**

- **mespro.dll** – Message-Pro library, provided by Signal-COM;
- **SignalCom_Pr.dll**;
- **SignalCom_Pr.ini**.

If the user has already configured encryption providers and digital signature, then only the provided files need to be replaced. In this case, the encryption settings are automatically copied from the **SSLPro.ini** file to the **SignalCom_pr.ini** file.

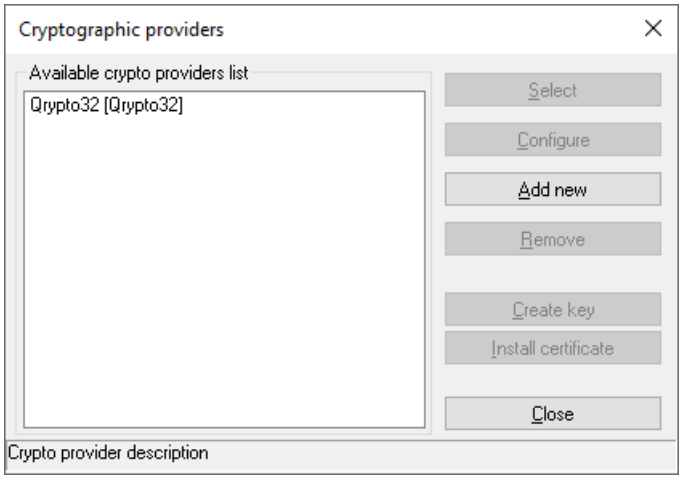
Encryption support with SSL-Pro library

Run the QUIK workstation. In the main menu, select the **System / Settings / General settings...** menu item, and in the opened window, select the **Program / Encryption** tab.



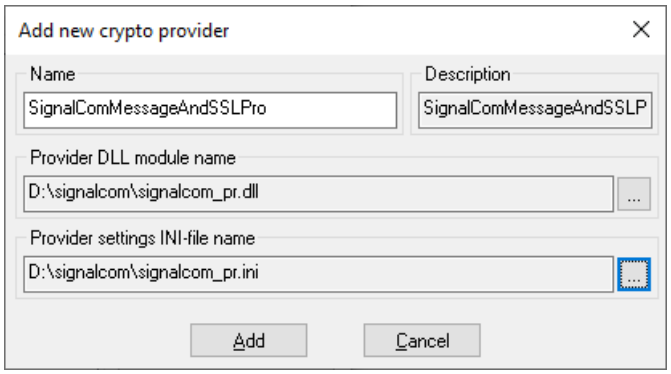
The following settings are available on the tab:

1. **Encrypt using** – select a cryptographic information protection system used for encryption. When clicking on the ... button, the **Cryptographic providers** window appears on the screen:



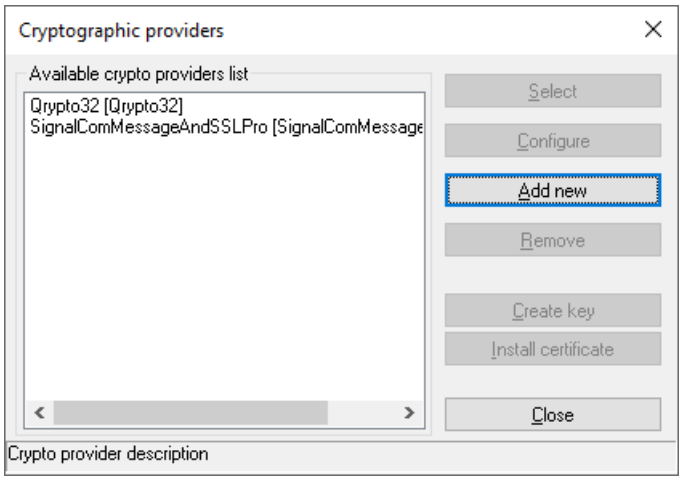
   To add a new cryptographic provider, click on the **Add new** button.

In the opened window, fill in the fields as follows:



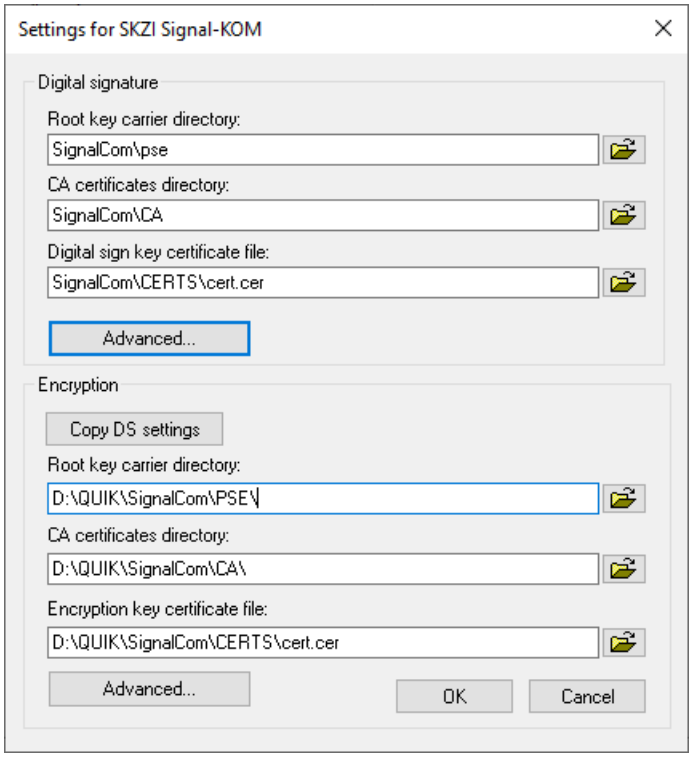
- **Provider DLL module name** – path to the **SignalCom_Pr.dll** file from the distribution set. If the file is specified correctly, the **Name** and **Description** fields are filled automatically.
- **Provider settings INI-file name** – path to the **SignalCom_Pr.ini** file.

The configuration is completed by clicking the **Add** button. The added cryptographic provider appears in the list of installed cryptographic providers:

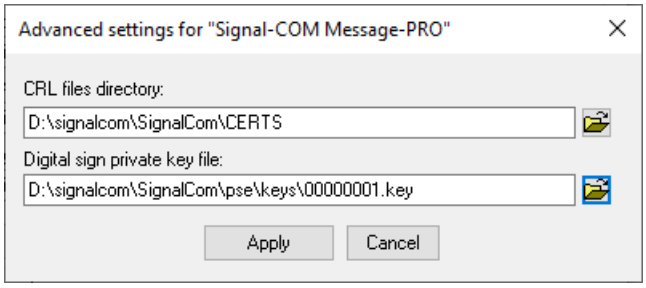


Select the required cryptographic provider with the left mouse button and click the **Select** button.

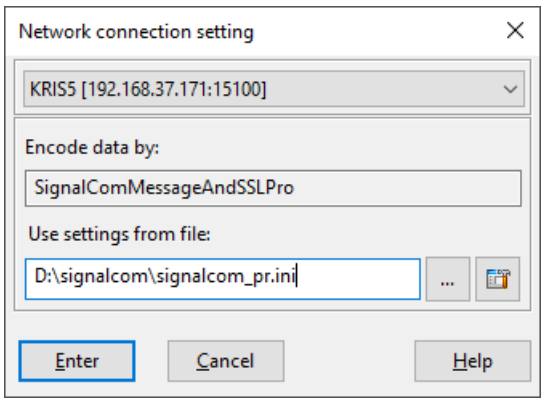
2. **Current status** – the field is not editable.
3. **Default settings** – path to the file with cryptographic provider settings. File name by default is **SignalCom_Pr.ini**, located in the same directory as the program executable file. When clicking the  button, a window opens for viewing and editing the settings specified in the **SignalCom_Pr.ini** file:



In the dialog box for additional settings of the cryptographic information protection system (**Advanced** button), the directory with certificates of intermediate certification authorities, the directory with files of revoked certificates lists and the file of the secret signature key are specified:

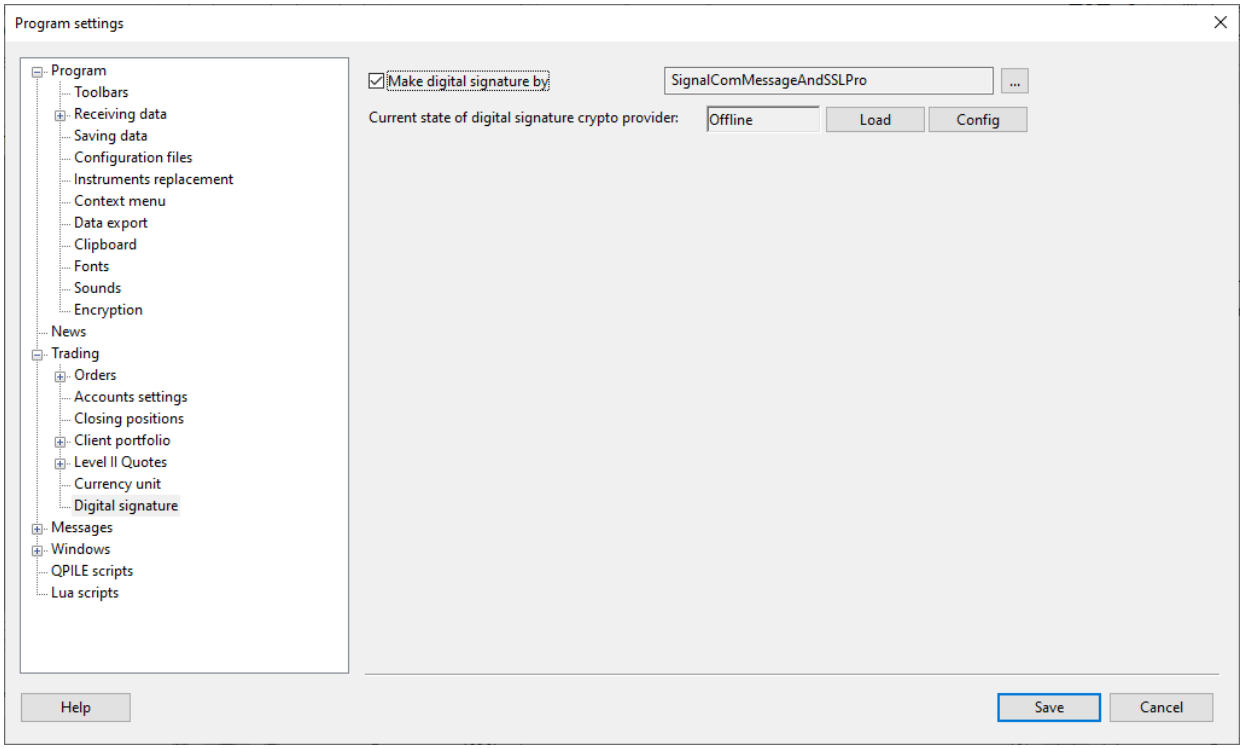


The encryption setup is completed by clicking the **OK** button. Now the user works with the server through a channel protected by the SSL-Pro provider, and the network connection establishment dialog on the workstation looks like this:



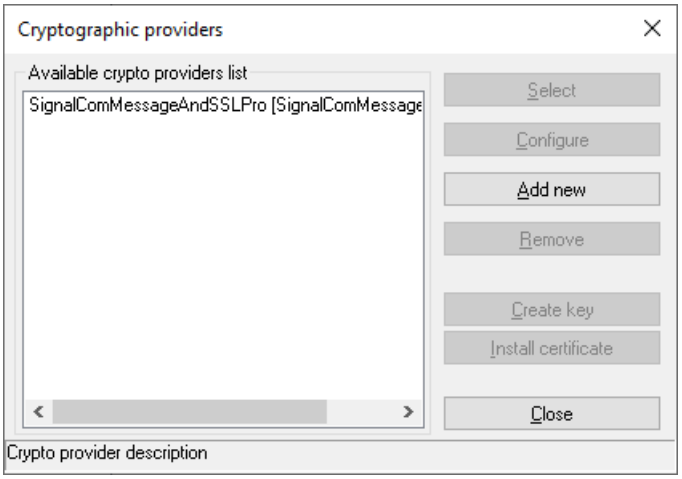
Digital signature support with Message-Pro library

Run the QUIK workstation. In the main menu, select the **System / Settings / General settings...** menu item, and in the opened window, select the **Trading / Digital signature** tab.



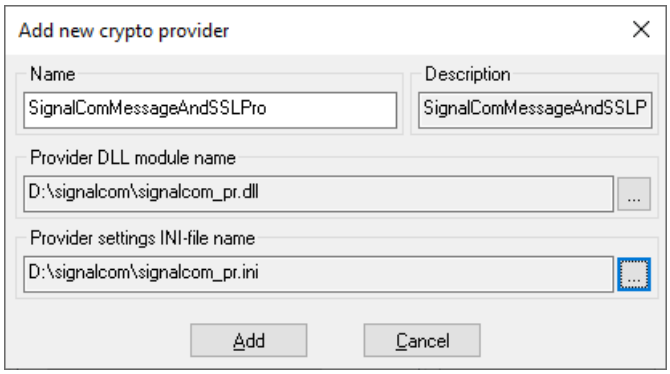
The following settings are available on the tab:

1. **Make digital signature by** – activates the digital signature function of all active operations selected from the list by the cryptographic information protection system. When clicking the ... button, the **Cryptographic providers** window appears on the screen:



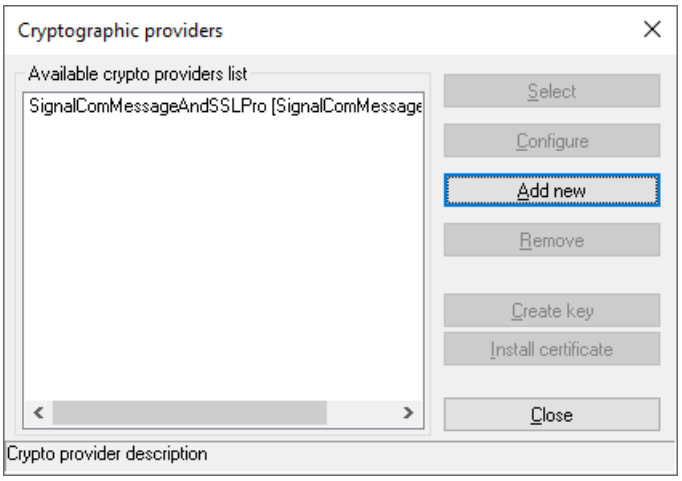
   To add a new cryptographic provider, click on the **Add new** button.

In the opened window, fill in the fields as follows:



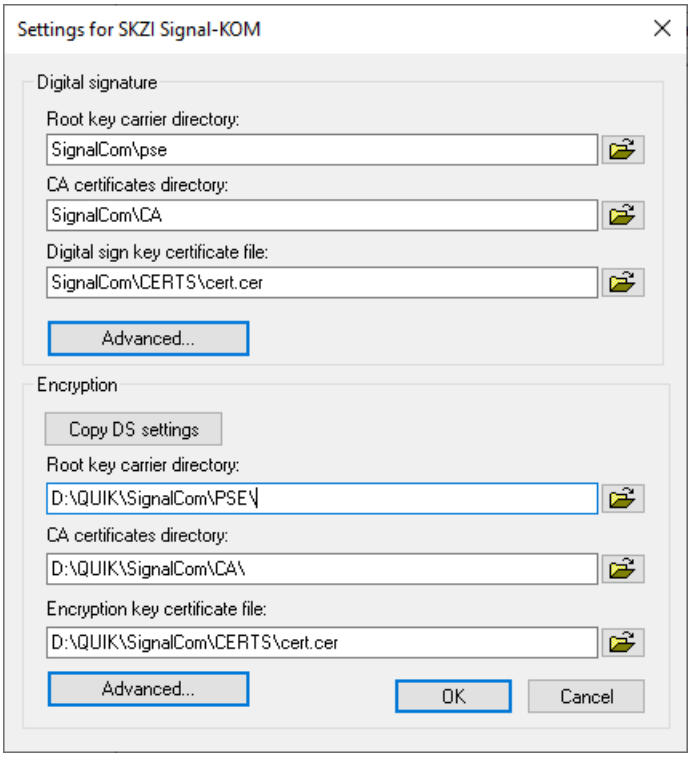
- **Provided DLL module name** – specify path to the **SignalCom_Pr.dll** file from the distribution set. If the file is specified correctly, the **Name** and **Description** fields are filled automatically.
- **Provider settings INI-file name** – specify path to the **SignalCom_Pr.ini** file.

The configuration is completed by clicking the **Add** button. The added cryptographic provider appears in the list of installed cryptographic providers.

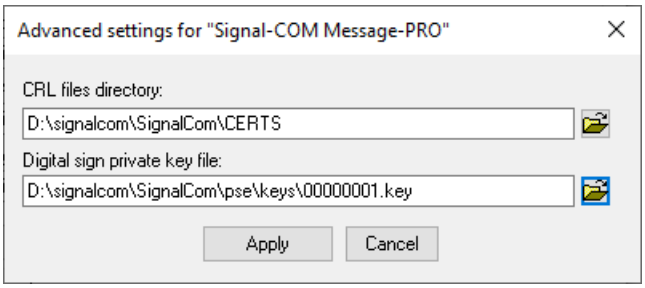


Select the required cryptographic provider with the cursor and click the **Select** button.

2. **Current state of digital signature crypto provider** – the field is not editable.
3. Clicking the **Load** button switches the selected cryptographic information protection system into operation mode; in the **Current state of digital signature crypto provider**, the **Online** appears.
4. When clicking the **Config** button, a window opens for viewing and editing the settings specified in the **SignalCom_Pr.ini** file:



In the dialog box for additional settings of the cryptographic information protection system (**Advanced** button), the directory with files of revoked certificates lists and the file of the secret signature key are specified:



The encryption setup is completed by clicking the **OK** button. Now the user sends transactions to the server using the digital signature using the Message-Pro library.

1.6.3 Configuration file format

> **To avoid errors, it is required to edit the file using the QUIK workstation settings (System/Settings/General settings...).**

The settings for the SSLAndMessagePro cryptographic provider are stored in the **SignalCom_Pr.ini** file located in the directory with the QUIK workstation files.

Configuration file structure:

1. The [SIGNAL_COM_SSL_PRO_COMMON_SETTINGS] section contains the description of the global cryptographic provider settings.

2. The [SIGNAL_COM_SSL_PRO_CIPHER_SETTINGS] section contains the description of cryptographic provider settings required to correctly create an encryption context:

   - **PSE_PATH** – path to the root directory cryptographic information protection system key carrier. Required parameter.
   - **TRUSTED_CA_CERTS_DIR** – path to the root CA (certification authority) certificate directory. Required parameter if the path to the file with the root CA certificate is not specified in the TRUSTED_CA_CERT_FILE_NAME parameter.
   - **TRUSTED_CA_CERT_FILE_NAME** – path to the root CA file. Required parameter if the path to the directory with the root CA certificate is not specified in the TRUSTED_CA_CERTS_DIR parameter.
   - **UNTRUSTED_CA_CERTS_DIR** – path to the directory of intermediate CA certificates. Optional parameter.
   - **UNTRUSTED_CA_CERT_FILE_NAME** – path to the file with the intermediate CA certificate. Optional parameter.
   - **CRL_FILES_DIR** – path to the directory with the list of revoked certificates. Optional parameter.
   - **CRL_FILE_NAME** – path to file with list of revoked certificates. Optional parameter.
   - **CIPHER_CERT_FILE_NAME** – name of the file containing the certificate corresponding to the secret key used to encrypt data during a communication session. Required parameter.
   - **CIPHER_KEY_FILE_NAME** – name of the file containing the secret key, which is used to encrypt data during a communication session. Optional parameter.

3. The [SignalComCommonSettings] section:

   - **DefaultNewKeyAlgorithm** – asymmetric key data encryption algorithm. Value by default: ECR3410.

> **To generate keys in accordance with state standard, specify "GOST3410-2012-512-A-ParamSet" as the value of the DefaultNewKeyAlgorithm setting.**

4. The [signal_com_message_pro_common_settings] section contains the description of a global cryptographic provider settings:

   - **certificates_path** – path to user certificate directory. Required parameter. Value by default: A:\certs.
   - **CRLs_path** – path to the directory of the revoked certificates lists. Optional parameter. Value by default: A:\crl.
   - **CAs_path** – path to the directory of CA certificates. Required parameter, if the file with the CA certificate is not specified using the **CA_cert_file_name** parameter in the [signal_com_message_pro_sign_settings] section. Value by default: A:\ca.
   - **output_data_format** – output data format. In a standard configuration, it is not configurable by the user. (the default value is used). Valid values:
     - **FORMAT_ASN**;

- **FORMAT_PEM** (by default).

5. The [signal_com_message_pro_sign_settings] section contains the description of the cryptographic provider settings required to generate a digital signature:

   - **sign_cert_file_name** – path and name of the file with the user certificate, with which the digital signature is carried out. Required parameter. Value by default: A:\certs\cert.pem.
   - **CA_cert_file_name** – path and name of the file with the CA certificate. Required parameter if the certificate directory is not specified using the **CAs_path** parameter in the [signal_com_message_pro_common_settings] section. Value by default: A:\cacert.cer.
   - **CRL_file_name** – path and name of the file with the list of revoked certificates. Optional parameter. Value by default: A:\Curr_crl.crl.
   - **pse_path** – path to the root key storage directory. Required parameter. Value by default: A:\.
   - **sign_key_file_name** – path and file name of the private key corresponding to the specified user certificate. Optional parameter. If the parameter is not specified, the file name is determined automatically based on the specified directory of the root key carrier.

1.6.4 Restrictions working under WINE

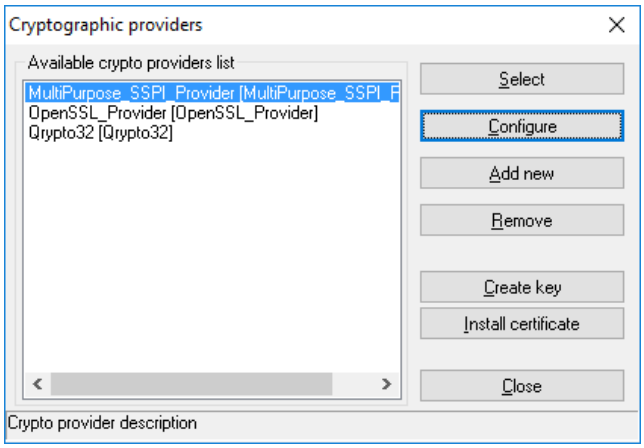
The **Signal-COM** company libraries use key storages with non-extractable keys such as eToken, Rutoken, MS_Key, and other tokens compliant with interface with the PKCS#11 standard. For more information, see the **Signal-COM** developer company website: https://www.signal-com.ru/products.

However, the specified tokens do not work under the WINE at the moment. Instead, a file-based storage is used, where keys are protected with password encryption or remain unprotected.

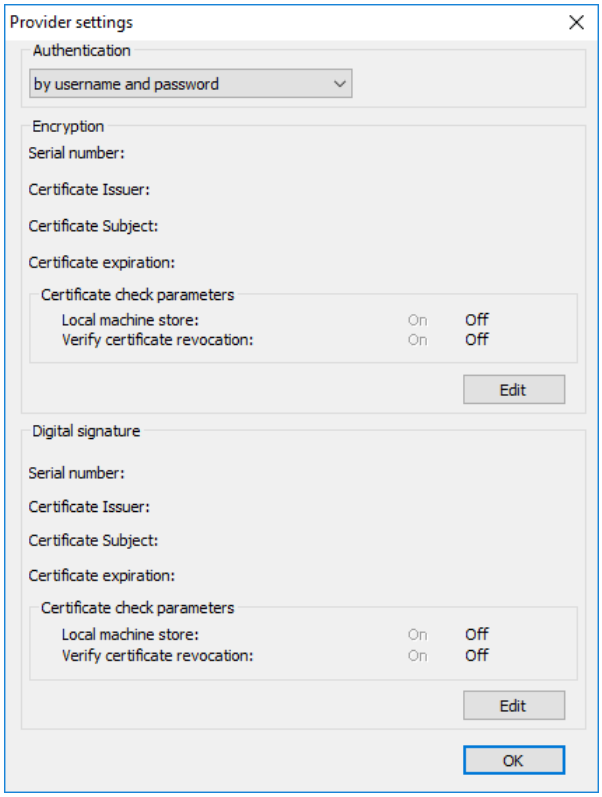
1.7 Configuration of encryption and digital signature carried out by means of MP library

1.7.1 Provider settings

In the **Cryptographic providers** window select the MP cryptographic provider and click the **Configure** button.



The opened window allows you to select the authentication scheme and view and edit the cryptographic provider settings for the encryption modes and digital signature:



In the **Authentication** dropdown list select the authentication scheme:

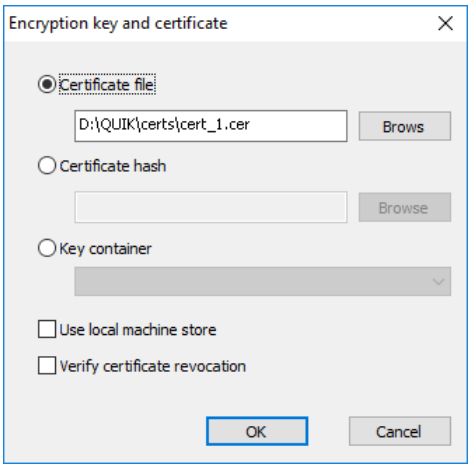
- defined by server – authentication scheme configured on the server by default;

- by user certificate – authentication scheme by user certificate. To operate according to this authentication scheme, the keys must be created and encryption certificate must be installed;
- by domain username and password – authentication scheme by domain username and password;
- by username and password – authentication scheme by username and password. This scheme is compatible with any authentication schemes used on the server.
- inside domain – authentication scheme by domain username.

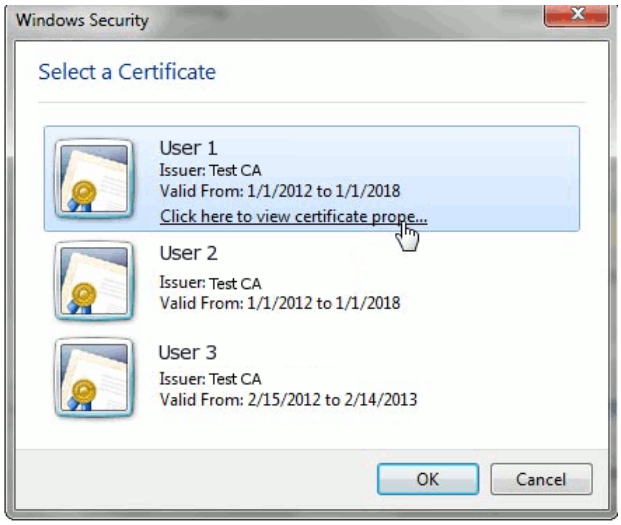
> **A single or different certificate can be used to work in encryption and digital signature modes. The cryptographic provider parameters are configured separately and independently for the encryption mode and digital signature mode.**

If 'by user certificate' authentication method is used, in the cryptographic provider configuration dialog box (the **Edit** button), specify the key container for encryption and / or digital signature by using one of the following methods:

- Certificate file – select a file of certificate which is linked to the key container.



- Certificate hash – select a hash of certificate linked to the key container:



- Key container – select the key container.

Additionally, the following settings can be set up in the **Encryption / Digital signature key and certificate** dialog box:

- **Use local machine store** – if the checkbox is enabled, the key is located in a local computer store, otherwise – in a current user store.
- **Verify certificate revocation** – if the checkbox is enabled, the certificate is checked on the revoked certificates list by the cryptographic provider.

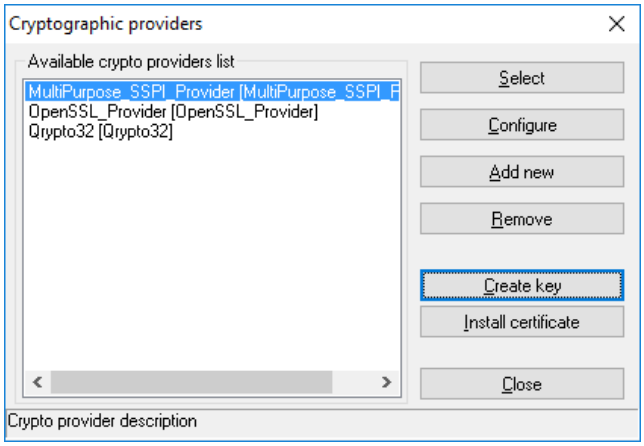
Click **OK** to complete the setting.

1.7.2 Generation of key pair and certificate request

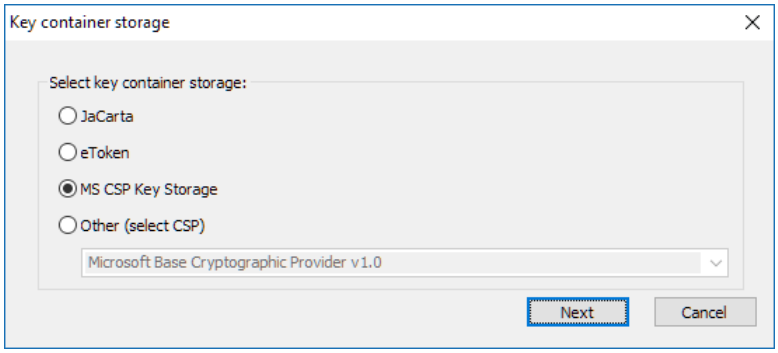
To work with the server through the channel protected by the **MP** provider and/or send transactions to the server using the digital signature through the MP provider do the following:

1. Create a certificate key.
2. Receive a certificate.
3. Install the certificate.

To create a key, select the cryptographic provider in the **Cryptographic providers** window and click the **Create key** button.

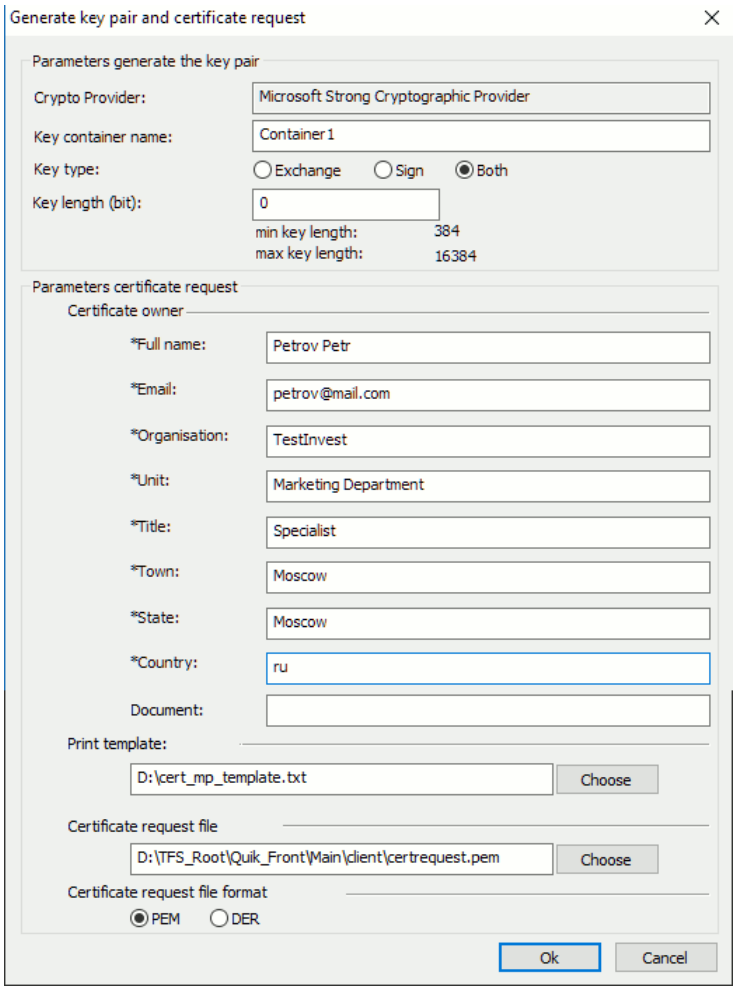


In the opened window select a location where the key container will be created and stored (using of JaCarta or eToken requires pre-installation of appropriate software products):



- JaCarta – a private key is stored in non-recallable memory (key fob);
- eToken – a secure key is stored in non-recallable memory (key fob);
- MS CSP Key Storage – a standard carrier of the key container. Processed using Crypto API and CSP Microsoft Strong Cryptographic Provider;
- Other (select CSP) – select another cryptographic provider.

Click the **Next** button and specify parameters of the key pair and certificate request. Required parameters are marked by *:



1. **If the user previously created the key pairs using this interface, and the values of parameters are specified in the settings file, and a cryptographic provider is the same as the one selected by the user in step 1, then the dialog box fields are automatically filled in by the appropriate values of the settings file (with the exception of the Key container name field).**
2. **In the Country field, the two-letter country code according to the standard ISO is to be specified (ru for Russian Federation).**

Then the user should give the certificate request file to the broker via the agreed communication channel and receive a certificate file from the broker.

If the broker creates a certificate for the client by himself, the client receives the container with a private key (*.pfx file extension). The client should install the received file following the instructions of the installation wizard:

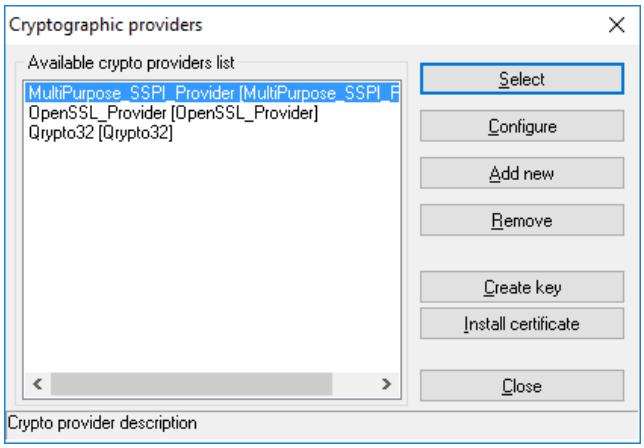


You can also get a certificate via web interface of Certification Authority.

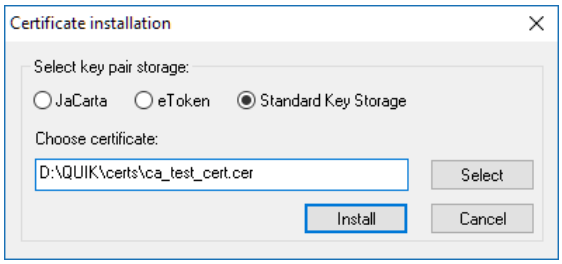
After that, the user can move on to the certificate installation using the form.

1.7.3 Certificate installation

In the **Cryptographic providers** window select the required cryptographic provider and click the **Install certificate** button.



In the opened window specify the key pair carrier and certificate:



To install a certificate, click the **Install** button (depending on the used carrier and certificate you may be asked to enter your password).

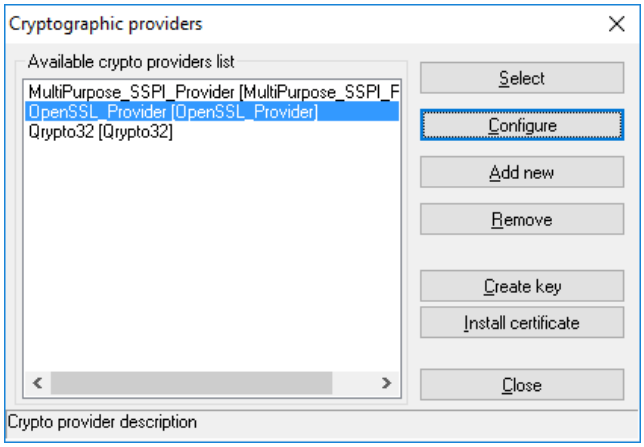
1.7.4 Restrictions working under WINE

When the MP cryptographic provider is used with **CryptoPro CSP** software, key storages with non-extractable keys such as Rutoken, JaCarta, MS_Key, and other tokens compliant with interface with the PKCS#11 standard. For more information, see the **CryptoPro** developer company website: https://cryptopro.ru/products/csp#fkc. However, the **CryptoPro CSP** software is currently not supported under the WINE.

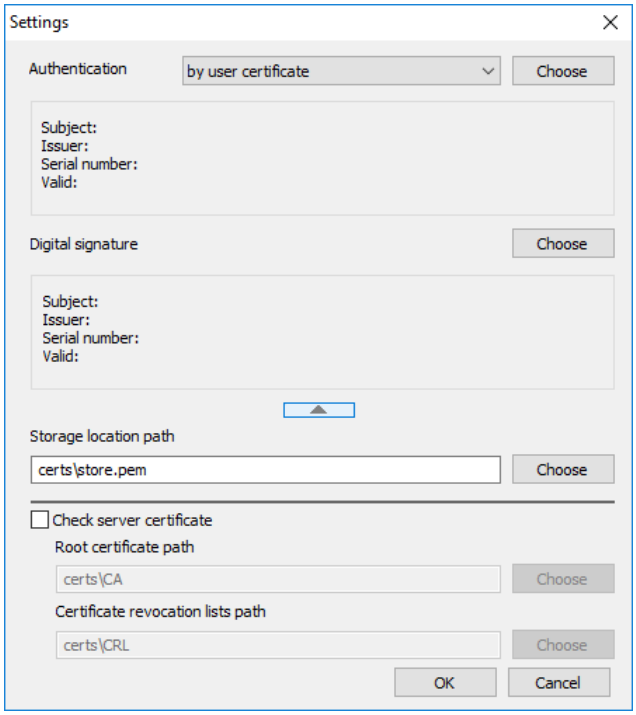
1.8 Configuration of encryption and digital signature carried out by means of OpenSSL library

1.8.1 Provider settings

In the **Cryptographic providers** window select the OpenSSL cryptographic provider and click the Configure button.



The opened window allows you to select the authentication scheme and view and edit the cryptographic provider settings for the encryption modes and digital signature:



In the **Authentication** dropdown list select the authentication scheme:

- defined by server – authentication scheme configured on the server by default;
- by user certificate – authentication scheme by user certificate. To operate according to this authentication scheme, create the request for encryption certificate and install the received certificate;
- by domain username and password – authentication scheme by domain username and password;
- by username and password – authentication scheme by username and password;
- inside domain – authentication scheme by domain username.

> **A single or different certificate can be used to work in encryption and digital signature modes. The cryptographic provider parameters are configured separately and independently for the encryption mode and digital signature mode.**

If 'by user certificate' authentication method is used, the request for encryption certificate must be created by clicking Choose. If a certificate is installed, then **Choose** button opens the certificate selection dialog box. After selection a certificate its parameters are displayed in the corresponding frame.

Clicking the arrow opens the parameters of 'by user certificate' authentication method settings for setting the attribute of server certificate checking, as well as for selection of file paths to the directories with root certificate and revocation lists.

Click **OK** to complete the setting.

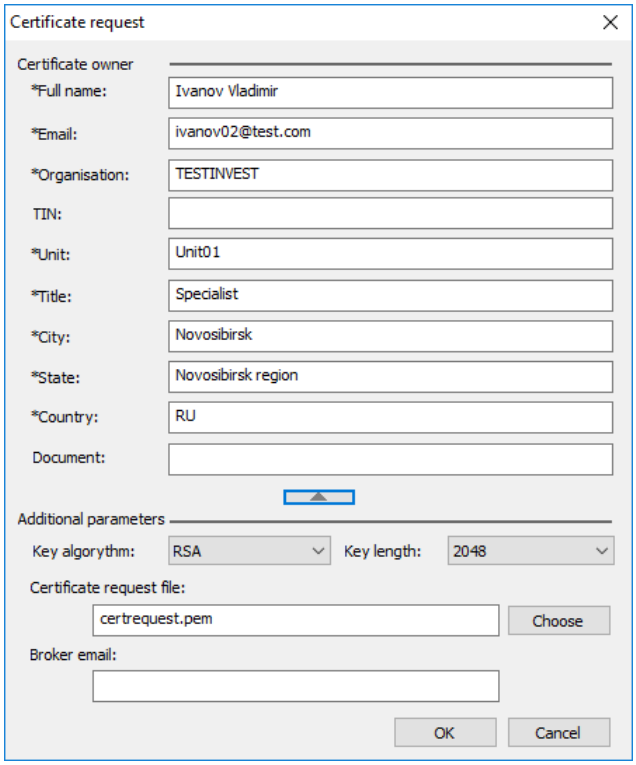
1.8.2 Certificate request generation

To receive the certificate from broker it is necessary to send him the request for certificate, created in the QUIK workstation, via the pre-agreed communication channel.

The certificate request dialog can be opened in the workstation settings in the following ways:

- In the **Cryptographic providers** dialog box select OpenSSL cryptographic provider and click **Create key**;
- In the **Trading / Digital signature** section click **Load**. In the opened dialog box, click **Request**.

Required parameters are marked by *:



> **In the Country field, the two-letter country code according to the standard ISO is to be specified (ru for Russian Federation).**

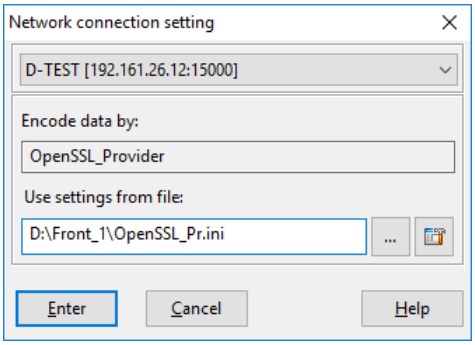
1.8.3 Certificate installation

Copy the certificate received from broker to the QUIK workstation root directory.

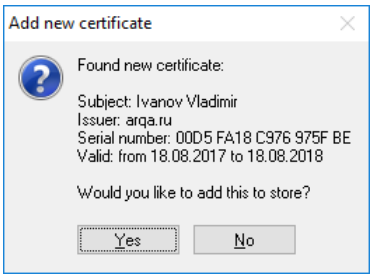
The certificate can be installed in two ways:

1. In the **Cryptographic providers** dialog box select OpenSSL cryptographic provider and click **Install certificate**.
2. Certificate can be installed when connection establishing:

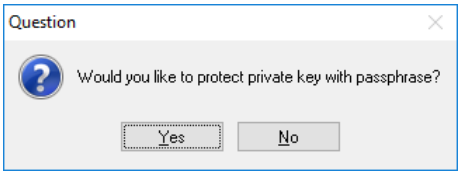
– Launch the QUIK workstation. Click to establish connection. The dialog of the following view will be opened:



– Select settings file in the **Use settings from file** dialog box and click **Enter**. The program finds the certificate file automatically and displays the request for adding it to the store. Click **Yes**.

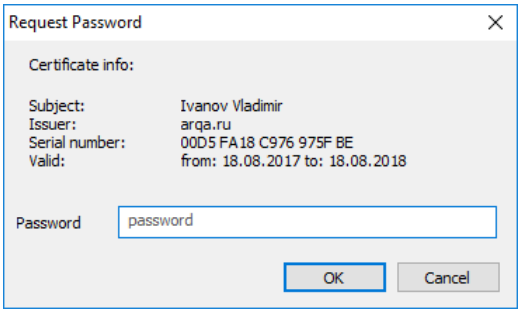


– The request for the private key protection by password is opened. If you click **No** the certificate is added without password.



– To enable the protection click **Yes** and enter password.

The password should contain at least one digit, one capital letter and one lower-case letter of the Latin alphabet. Space (" ") and hyphen ("-") are allowed. The password must contain at least 8 symbols.



– Select the certificate and click **OK**.

This method is also used for planned certificate change.

1.9 Running keys of the QUIK workstation

When running the QUIK workstation from the command line the following keys can be used:

- **-clear** – clears service files that contain trading data (info.log (or curr_data.log depending on the terminal settings), acnt.dat, alert.ik, alltrade.dat, trades.dat, orders.dat). It speeds up loading of the program.
- **-full-dump** – in error cases .DMP file is formed, that contains all information on the program.
- **-security-replace** – the instruments in .WND settings file are replaced according to the rules specified in a replacement file.

  The format:

  ```
  info.exe -security-replace [name of the file with replacement rules>]
  ```

  If the replacement file is not specified, then the **replacements.txt** file from the QUIK workstation directory will be used.

  Replacement file format:

  ```
  <Old class code 1>,<Old instrument code 1>=<New class code 1>,<New instrument code 1>
  …
  <Old class code N>,<Old instrument code N>=<New class code N>,<New instrument code N>
  ```

  The following parameters are to be replaced:

  - Instrument code;
  - Short and full names of the instrument;
  - Class code;
  - Class name.

  > **To correctly replace the instruments in the Options board table, specify the options class code as a class code, and the code of underlying asset as an instrument to be replaced.**

  If the instrument specified in the replacement file is not found in the instruments dictionary of the QUIK workstation, then the replacement operation will not be performed.

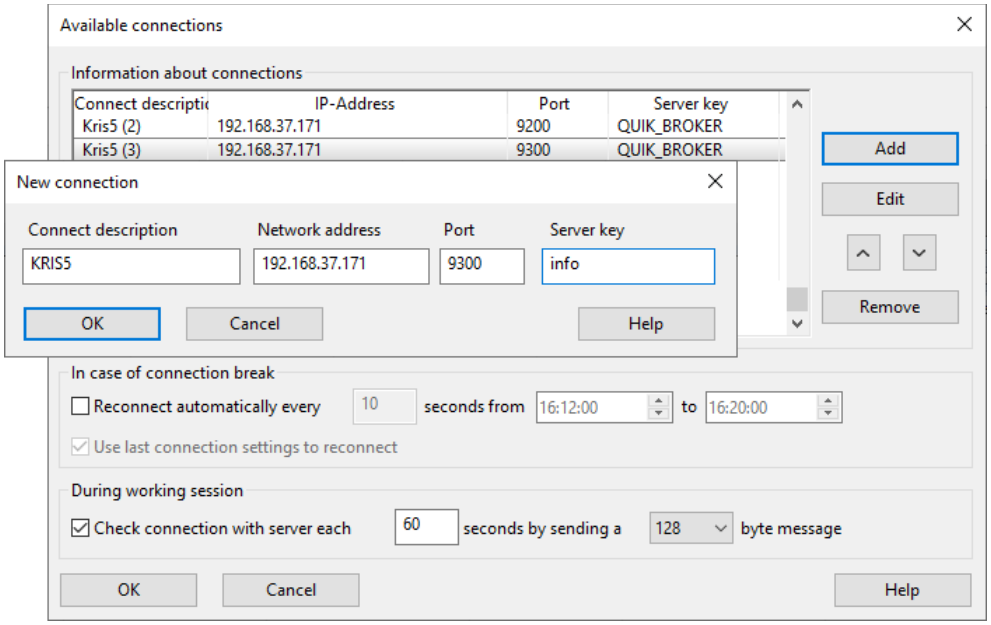
  File sample:

  ```
  SPBOPT,GZ10250BJ6=SPBOPT,GZ10250BL6
  SPBFUT,SiZ6=SPBFUT,SiH7
  ```

To save the changed settings file, use the functionality of saving the configuration of the QUIK workstation into a .WND file (see Chapter 2, "Basic Operating Principles", section Saving / restoring the configuration).

1.10 Configure connection

1. **By default, QUIK system connects to the sever using the settings of the previous connection. If a connection was edited or added, it would be the default for the next connection.**
2. **It is advisable to arrange the list of connections in descending order relative to their use by moving the lines using the ^ and v arrow buttons.**



1. Click **Connections...** in the **System** menu.
2. To edit connection parameters, click the required line in the list of **Information about connections** and then click **Edit**.
3. To create a new connection, click **Add**.
4. The **Network Address** and **Port** fields must contain the server address and port. If working on a local network through a proxy server, select **Internet connection...** from the **System / Settings** menu (for description, see Configuring the Connection through a Proxy Server) to specify the proxy address and port.
5. Specify the server key identifier provided by the QUIK server's Administrator in **Server key** box.

In the Network address field, specify either a hostname or IP-address of the QUIK server.

6. Click **OK** to save changes or **Cancel** to close the window without saving the settings.
7. To delete a connection that you do not require any longer, highlight its description in the list of **Information about connections** and then click **Remove**.

1.10.1 Setting up automatic reconnection to the server

1. Select the **Reconnect automatically after … seconds from … to …** checkbox.

   - In the **Seconds** box, specify the timeout period in seconds. The recommended value is 15 to 60 seconds. Minimum interval: 5 seconds;
   - In the **From** and **To** boxes, specify the period (according to system time of your computer) during which the reconnection is enabled. It is recommended that this period be equal to the time of exchange trading, because the server disconnects all users automatically once the trading is over. The connection will be set automatically the next day at the specified time;
   - If the **Use last connection settings to reconnect** checkbox is enabled (default setting), the next connection has the same settings as the previous one.

2. If the checkbox is not checked, the next connection will be established using the settings shown in the next line in the Information about connections list. For this purpose, the list of available connections should be sorted, using the  and  arrows, in conformity with the preferred order of connections. This feature is convenient in case different providers are used to establish connection with the server.

1.10.2 Monitoring channel delays

If the **Check connection with server each … seconds by sending a … byte message** checkbox is selected, the program regularly measures connection delays in the channel between the server and the client using the standard PING command. Results of the measuring are displayed in the **Information window** (see Monitoring the connection status). The function has the following parameters:

- inter-messaging interval (in seconds); the recommended value is 60;
- size of a package (in bytes); the recommended value is 128.

1.10.3 Configuring the Data Reception and Saving Data Parameters

Data reception

To configure the reception of data, click **General…** in the **System / Settings / General settings** menu, and then click the **Program / Receiving Data** tab.

1. The settings in the **Refresh interval for current data** group box define how frequent the **Quotes** table should be updated:

   - Select the **Refresh data once in … sec** checkbox to update data in the Quotes Table only at specified intervals (in seconds). Maximum update period is 60 seconds. This feature is enabled by default. Value by default: 1.

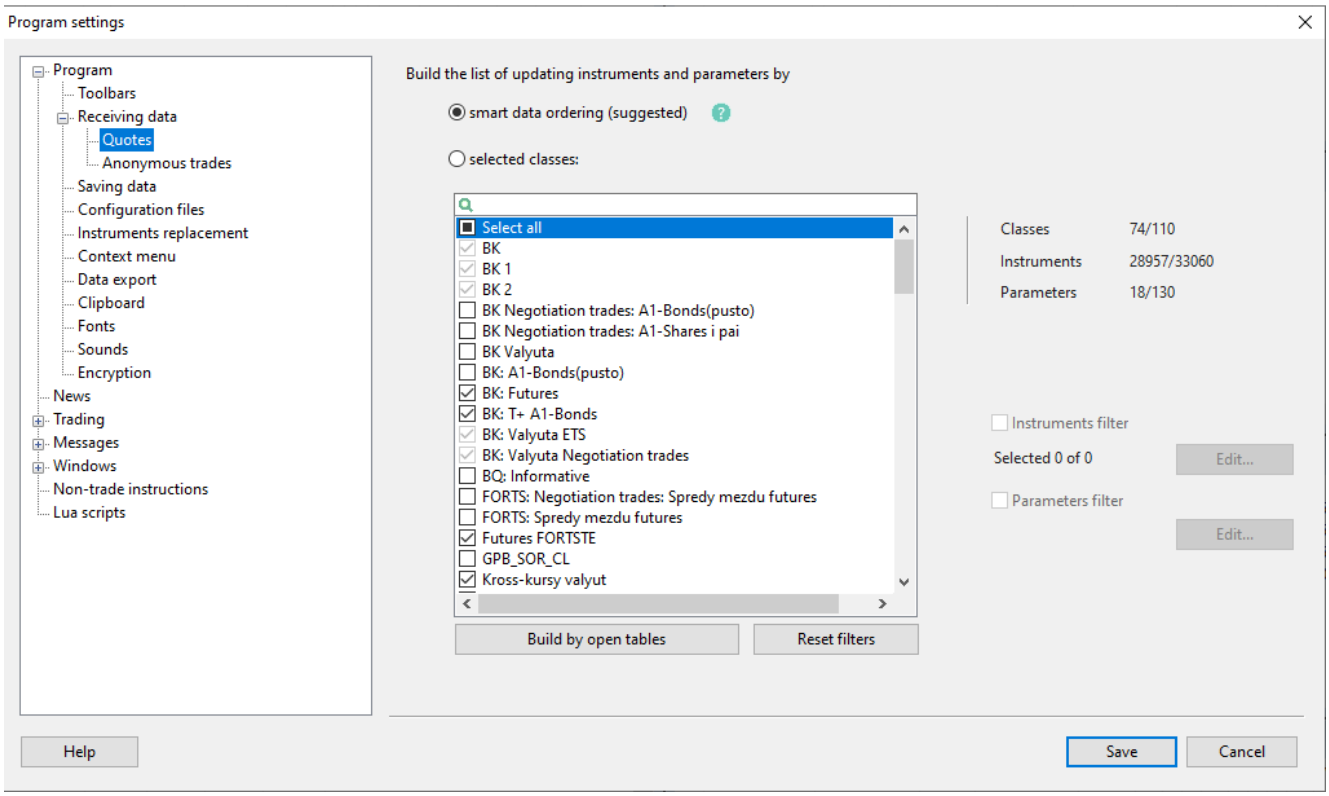
2. The **Upon receiving a new instrument** group box contains parameters for addition of new instruments to the existing tables:

   _ Select the **Add to all tables** checkbox to include a new instrument of a certain class that appears in the trading system into all existing tables with instruments of the same class and into the list of instruments shown in the **Quotes** table.

3. If the **Request positions by global clients filter** checkbox is selected, the user receives only positions by the code specified in the global filter. The setting is also applied to the **Client profiles** table (for details, see Chapter 3, "Viewing Information", section **Client profiles table**). If the <Not chosen> is selected in the **Global Client Filter**, positions are not retrieved. When you change the client code in the filter or switch to a tab with a different client code, positions are received using the new client code. When the **Request positions by global clients filter** checkbox is enabled, setting filter through the **Global filters...** menu item from the **Services** menu or by pressing Ctrl+G key combination and enabling the option **Exclude selected from filter** (for details, see Chapter 2, "Basic Operating Principles", section **Operations with filters in a table**) are not used. By default, the setting is disabled.

Quotes

To configure the lists of instruments for obtaining information on quotes, click **General settings...** in the **System / Settings** menu, and then click the **Program / Receiving Data / Quotes** tab.



Build the list of updating instruments and parameters by setting allows you to set the amount of data received from the server. Allows you to limit the list of received data to reduce stream:

1. **smart data ordering (suggested)** allows you to receive new values for instruments and their parameters, that are displayed in tables and necessary for calculating margin

parameters, purchasing capacity, used in Lua and QPILE scripts, displayed on charts, exported to technical analysis systems and used by external plug-in modules.
List of tables whose contents affect the set received instruments and parameters:

- Quotes table;
- Quotes changes table;
- Quotes history table;
- Client portfolio table;
- Buy/Sell table;
- Options board table;
- Alerts window of the Quotes table parameters.

2. **selected classes** allow you to receive new values for instruments and their parameters of data selected in the window. The window contains a list where you can use the checkboxes to select the classes of the data to be received. Search is also available.

- **Select all** item allows you to select all classes / clear all;
- **Build by open tables** button to automatically customize the instrument and parameter filters, so that only those instruments and parameters already displayed in the open tables are selected. If the user alters the settings for the tables, the settings for the data reception filters are altered in the same way.

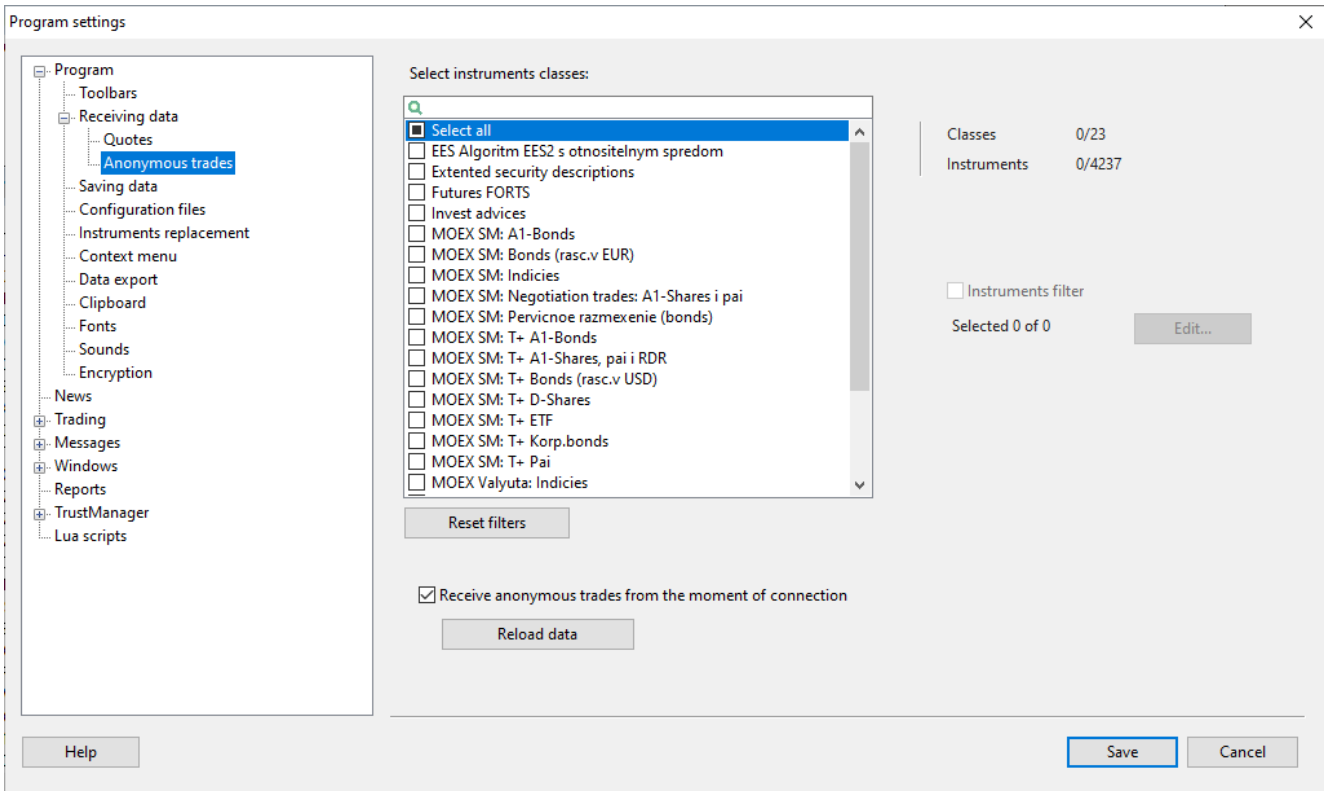
> **If the option is enabled, not only opened windows are taken into consideration but parameters required for the calculation of margin indicators and purchasing power as well.**

- **Reset filters** button resets all configured filters by class.
- Common information on all selected and available parameters is next to the list:
  - classes selected / classes available – number of selected classes / of available classes;
  - instruments selected / instruments available – total number of selected instruments / available instruments;
  - parameters selected / parameters available – total number of selected parameters / available parameters;
- For each class configure:
  - **Instruments filter** – if the checkbox is selected, data is received for only selected instruments. If the checkbox is cleared, data is received for all instruments available for the class. Those classes with set filters are shaded grey;
  - **Parameters filter** – if the checkbox is selected, data is received for only selected parameters. If the checkbox is cleared, data is received for all parameters available for instruments of the class. Use this filter to cancel the receipt of unused parameters.

To save the flow of data settings, click **Save.**

Anonymous trades

To configure the lists of instruments for obtaining information on anonymous trades, click **General settings...** in the **System / Settings** menu, and then click the **Program / Receiving Data / Anonymous trades** tab.



1. **Select instruments classes** allows to select the instrument classes that available in the window. A search is also available.

   - **Select all** item allows you to select all classes / clear all;
   - **Reset filters** button resets all configured filters by class.
   - Common information on all selected and available parameters is next to the list:
     - classes selected / classes available – number of selected classes / of available classes;
     - instruments selected / instruments available – total number of selected instruments / available instruments;
   - For each class configure:
   - **Instruments filter** – if the checkbox is selected, data is received for only selected instruments. If the checkbox is cleared, data is received for all instruments available for the class. Those classes with set filters are shaded grey.
   - Statistics of instruments of the selected class are displayed under the filters.

2. Tick the **Receive anonymous trades from the moment of connection** checkbox to configure receiving of anonymous trades. If the checkbox is selected, information on anonymous trades will be sent from the QUIK server immediately from the instant a connection is made to the server. If the checkbox is empty (default settings), new information should be requested each time for anonymous trades after the last trade is available on QUIK workstation.

3. Click **Reload data** to delete all available information on anonymous trades (clear all tables and stored files) and request trade data again selecting the **Receive anonymous trades from the moment of connection** checkbox.

Save the settings by clicking **Save**.

Comments:

- List of instruments selected by default in dialog of creating Time and Sales table. Instruments in the list are the same as those selected by the user in configuration dialogue for anonymous trade request. If the instruments for which there are trades that are not requested (i.e., those instruments have not been specified in the configuration dialogue for anonymous trades) are added to Time and Sales table, those instruments will be automatically added to the list of instruments for requesting anonymous trades;
- If the Time and Sales table is used as the basis for creating charts and configuring the export of data for technical analysis systems or the user selects an instrument for which anonymous trades have not been requested, such instruments will be automatically added to the list of instruments for which anonymous trades are requested;
- When **Reload data** is set, the automatic cleaning of exported data on anonymous trades using ODBC and DDE is not provided. The user should clean that data manually. Restarting the QPILE portfolio should also be completed manually by the user.

Saving data

To configure the settings to save data, click **General settings...** in the **System / Settings** menu, and then click the **Program / Saving Data** tab.

1. The settings under **Save for received instruments and parameters** define the amount of information saved by the QUIK workstation for subsequent use.

   - Select the **Only current data** option to save only the most recent values;
   - Select the **Current and historical data** option to save all of the values captured. This feature is necessary when using the Quotes History and Quote Changes tables, plotting parameter charts based on the Quotes Table, and when exporting data (if taken from the Quotes Table) to systems for technical analysis;
   - Select the **Get missing data** checkbox to receive all data from the moment a trading session is opened (it affects the speed of the application). To get new data only, disable this checkbox.

     This feature is necessary if the Quote Changes or Quotes History table is used, or if any charts contain parameters from the Quotes History table. If these tables are not used, disable this checkbox to reduce traffic.

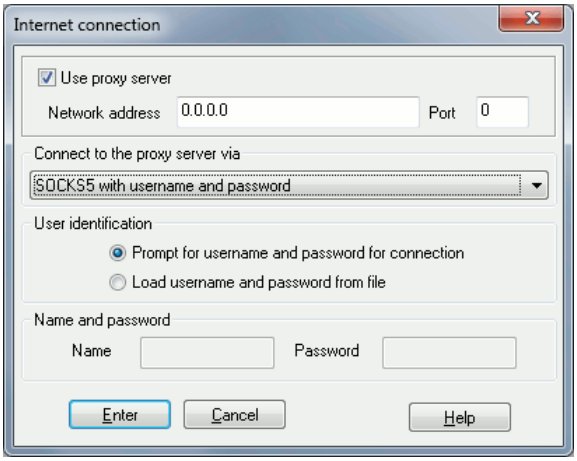
2. The settings under **Clear data after date change** control the deletion of data:

   - Select the **On local computer** option to clear data from the previous trading session upon program launch before connecting to the server. This option is recommended for use if information about the previous trading session is not needed before the current trading session begins;
   - Select the **On server (upon establishing connection)** option to clear data from the previous trading session after the next trading session's data appears on the server. This option is recommended for use if trading information is received the next morning (because of a considerable difference between time zones, for example).

1.10.4 Configuring the Connection through a Proxy Server

When running QUIK on a local network with restricted access to the internet, the network administrator will most likely need to set up and configure a proxy server. If it is possible to connect without using a proxy server, such configuration is not required.

1. Open the options for **Internet connection** in the **System / Settings** menu.



2. Select the **Use proxy server** checkbox.
3. In the **Network address** and **Port** fields, enter the address and port for the proxy server (available from the local network administrator). You may also find them in your browser settings. If you use MS Internet Explorer, for example, select **Internet Options** in the **Tools** menu and then click **Network settings** on the **Connections** tab. Copy the address and the port number from the **Proxy server** pane to the QUIK settings dialogue box.

> **In the Network address field, specify the network name or computer's IP address upon which QUIK will be launched.**

4. Select the connection type:

   - Select **SOCKS5 with username and password** if the proxy server supports SOCKS5 and requires user authentication. In this case, if **Prompt for username and password for connection** is selected, the user will be prompted to enter their user name and password manually in order to establish an internet connection. If **Load username and password from file** is selected, the information will be stored in and retrieved from the QUIK configuration file;
   - Select **SOCKS5 protocol without user identification** if the proxy server supports SOCKS5 and does not require user authentication;
   - Select **Connect through HTTP port** if the proxy server does not support SOCKS5 but still allows for CONNECT command protocols. The proxy servers listed below have been tested for compatibility with QUIK (see configuration examples in the next section):
     - Squid proxy (additional configuration required);
     - MS Proxy (additional configuration required);
     - WinGate (configuration is not required).
   - Select **CONNECT through HTTP port with user name and password** if server does not support protocol SOCKS5 but allows using the command of CONNECT protocol and requires user authentication. In this case, if **Prompt for username and password**

for connection is selected, the user will be prompted to enter their user name and password manually in order to establish an internet connection. If **Load username and password from file** is selected, the information will be stored in and retrieved from the QUIK configuration file.

Information for a local network administrator for proxy server configuration

It is necessary to include the QUIK port (its number is provided by the QUIK system administrator) into the list of ports through which an SSL connection can be established.

1. **Settings for Squid Proxy**

   The squid.conf file (usually located in the / usr / local / squid / etc / squid.conf folder) must contain the following lines:

   _ Enter (for example) port 200 into the list of SLL ports:

   ```
   acl SSL_ports port 443 563 200
   acl Safe_ports port 80 21 443 447 563 1025-65535 200
   ```

   _ Allow the CONNECT method to be used for the SSL ports defined above:

   ```
   acl CONNECT method CONNECT
   http_access deny CONNECT !SSL_ports
   ```

2. **Settings for MSProxy**

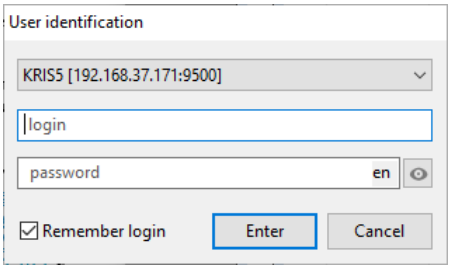
   It is necessary to change one of the keys in the Windows Registry (using the Regedit program) on the computer where the MS Proxy is installed:

   ```
   HKEY_LOCAL_MACHINE / SYSTEM / CurrentControlSet / Services / W3Proxy / Parameters / SSLPortListMembers
   ```

   The port being used (for example, 200) must be added to the list of ports. If the access control for the Web Proxy service is on, then the group EVERYONE must be added for the SECURE protocol. In the service logs, these connections will be registered as originating from an 'anonymous user'.

1.11 Connecting to the QUIK Server

1. Click  on the Toolbar, or select **Connect...** from the **System** menu, or press CTRL+Q.
2. If you use MP cryptographic provider saving the private key in non-recallable memory, insert the key external storage device. Connection to the server is established automatically.
3. If you use Qrypto32, MP or OpenSSL cryptographic providers ("by name and password in domain" or "by name and password" authentication schemes are used), set up the connection parameters in the **User identification** window:



– Select the required connection. Consult the QUIK server administrator about the preferable connection.

  Program configuration delivered as a part of distribution contains a list of configured connections. Connections may be added/deleted if necessary, their settings may be edited (see Configure connection).

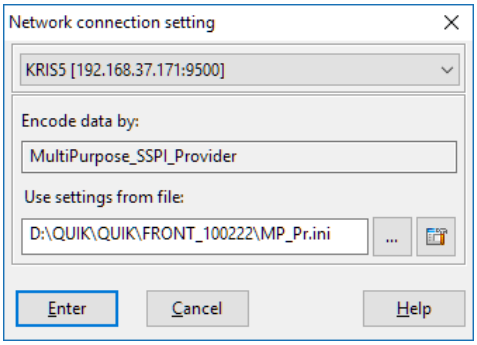
– Type your login and password that were used to register the key. Pay attention to the character case and language. At the end of the box, the alphabetic code of the layout and the mode of entering letters is displayed; when the Caps Lock key is pressed, the layout code is displayed in capital letters (for example, RU/EN). To show / hide the password, click on the eye / icon. The password can be changed.

  If the **Remember login** checkbox is enabled, the **login** box will be automatically filled by previous value the next time the dialog box is opened.

  > **Click Enter to remember the value of the login box.**

– Click **Enter**. After the connection is established, you will see a corresponding message with the previous login data. For information about possible errors, see Error Messages.

4. If you use MP or OpenSSL cryptographic provider ("by user certificate" authentication scheme is used) or other cryptographic providers (other than Qrypto32), set up the connection parameters in the **Network connection setting** window:



– Select the required connection. Consult the QUIK server administrator about the preferable connection.

  Program configuration delivered as a part of distribution contains a list of configured connections. Connections may be added/deleted if necessary, their settings may be edited (see Configure connection).

– The name of the cryptographic provider (system for information cryptographic protection) used for encryption is shown in the **Encode data by** box. Specify the path and name of the configuration file of this cryptographic provider in the **Use settings from file** box or select the file using the "…" button.

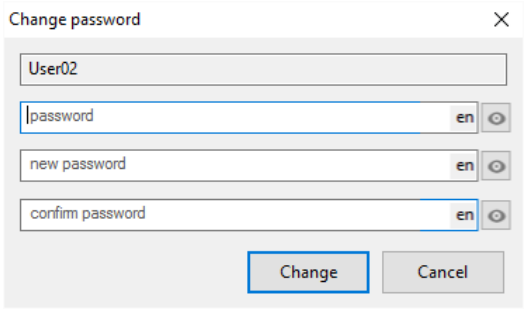
– Press ENTER. After the connection is established, you will see a "Connection established" message on the screen. For information about possible errors, see Application 1 Error Messages.

To disconnect from the server, click or select the menu item **System / Disconnect...** or press Alt+Q.

1.11.1 Password change

The **Change password** dialog can be opened in the following ways:

- Select **Services / Change password** menu items. This menu item is available if the connection to the QUIK server is established and MP or OpenSSL cryptographic provider with "by name and password" authentication scheme is used.
- When the password expires or the **Must change password at next logon** attribute is enabled in the user settings on the server, the user will be asked to change the password after entering the current login and password.



The following parameters are to be configured in the dialog box:

> 1. **When entering, pay attention to the correct selection of the keyboard case and language, at the end of the box the alphabetic code of the layout and the mode of entering letters is displayed, when the Caps Lock key is pressed, the layout code is displayed in capital letters (for example: the English layout with the Caps Lock key pressed will be displayed as EN on the right in the password entry box, and the Russian layout without the Caps Lock key will be displayed as ru).**
> 2. **To show / hide the password, click on the eye / .**

- password – the user's current password;
- new password – the user's new password;
- confirm password – re-enter the new password for confirmation.

Click **Change** to change the password to a new one.

> **IMPORTANT! Clicking the Change button initiates automatic reconnection to the QUIK server.**

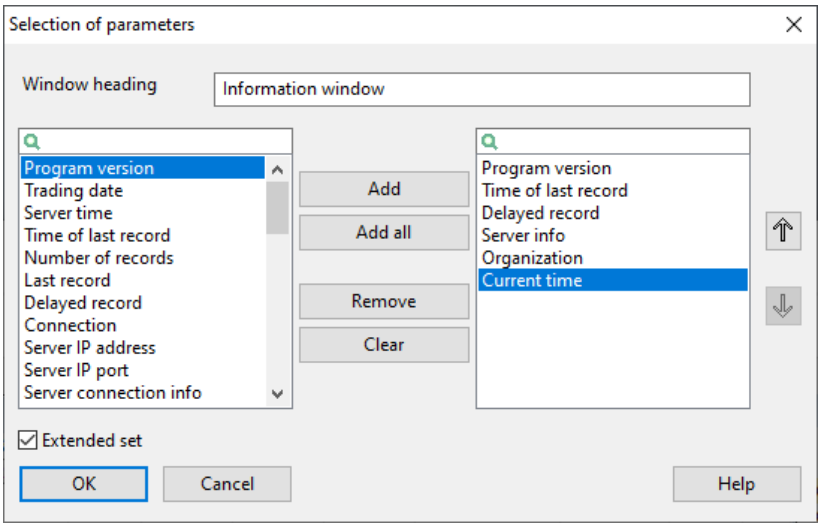
1.12 Monitoring the connection status

The connection to the server is monitored in several ways.

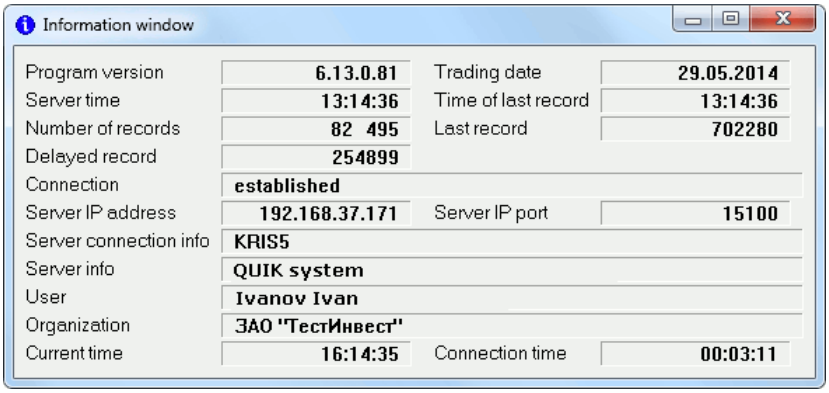
1. The **Connection status indicator** is located on the right-hand corner of the status bar, and shows the date of the trading session received from the QUIK server (for example, data from the previous trading session may be downloaded on the following morning).
   If the indicator does not show a date, no data has been received. The LED colour indicates the connection status:

   - green indicates that a connection has been established and the information is up-to-date;
   - yellow indicates that a connection has not been established and the information is not up-to-date (the date of the last update is shown).

2. The **Information window** shows the full set of statistical parameters used to monitor the connection status. To configure the window, select **System / About program / Information window...**.
   In the window that follows, select the list and order of parameters displayed in the Information window. When the **Extended set** checkbox is selected additional parameters are added to the list of available parameters:



   After setting parameters the following Information window is opened:



Information window available fields:

Field	Description
Program version	Program version serial number
Trading date	Trading session date
Server time	The value is calculated on the basis of time, when the actual data of the Quotes Table is received from the server. Time format is defined by settings of the operational system
Time of last record	Time of receipt from the server for the last record (data chunk). Time format is defined by settings of the operational system
Number of records	Number of records received from the server
Last record	Number of the last record received
Delayed record	Number of the last delayed record received (as a result of restoring missing data after a connection time out)
Connection	Status: Connected / Disconnected
Server IP address	Internet address of the QUIK server
Server IP port	Number for the QUIK server access port
Server connection info	Description from the list of available connections
Server info	Server name
User	User name (entered when signing on)
Organization	User's organization or firm (entered when signing on)
Current time	Time from the user's computer clock. Time format is defined by settings of the operational system
Connection time	Duration of the connection to the server. Time format is defined by settings of the operational system
* Trading session identifier	Unique identifier for an individual trading session
* User code	User code on the QUIK server
* Storage reserved	Reserved memory space, not used
* Messages sent	Number of sent messages
* Total bytes sent	Total amount of outgoing traffic sent during the current connection
* Useful bytes sent	Amount of significant outgoing data sent during the current connection

Field	Description
* Data sent per second	Amount of data sent during the last second
* Messages received	Number of received messages
* Useful bytes received	Total amount of significant incoming data received during the current connection
* Total bytes received	Total amount of incoming traffic received during the current connection
* Data received per second	Amount in bytes received during for the last second
* Average transfer rate	Ratio of amount in bytes sent / connection time (sec)
* Average receive rate	Ratio of amount in bytes received / connection time (sec)
** Time of Last Round-Trip	Time of the last Round Trip Time test (data delay measurement). Time format is defined by settings of the operational system
** Round-Trip Time	Last Round Trip Time value in seconds
** Average Round-Trip Time	Average Round Trip Time value in seconds for the current connection
** Maximum Round-Trip duration	Time of the maximum Round Trip Time occurred during the current connection
** Time of Maximum Round-Trip duration	Maximum Round Trip Time for the current connection in seconds
* String converting mode	Convert data received from QUIK Server from CP866 to CP1251 encoding. Valid values: _ Yes; _ No
* Cash positions	Amount of cash
* Positions in instruments	Number of instruments
* Futures limits	Number of futures limits
* Futures positions	Number of futures positions
* Trade accounts	Number of trading accounts
* Orders	Number of orders
* Trades	Number of trades

Field	Description
* Marginal rows (all; queue)	Service parameter. Intended for technical support staff only
* Markers (cash positions)	Service parameter. Intended for technical support staff only
* Markers (futures positions)	Service parameter. Intended for technical support staff only
* Markers (instrument positions)	Service parameter. Intended for technical support staff only
* Markers (trading accounts)	Service parameter. Intended for technical support staff only
* Markers (futures limits)	Service parameter. Intended for technical support staff only
* Network messages queue	Service parameter. Intended for technical support staff only
* Service tasks queue	Service parameter. Intended for technical support staff only

* – extended data set.

** – server connection monitoring parameters, see Configuring the Data Reception and Saving Data Parameters.

3. The **Train**  indicator located on the left-hand side of the toolbar looks like a moving train. Moving train indicates that data is being downloaded from the server. If the train is not moving, new data is not being transmitted and a problem with the connection has been detected. If a connection has not been established, the train does not appear.

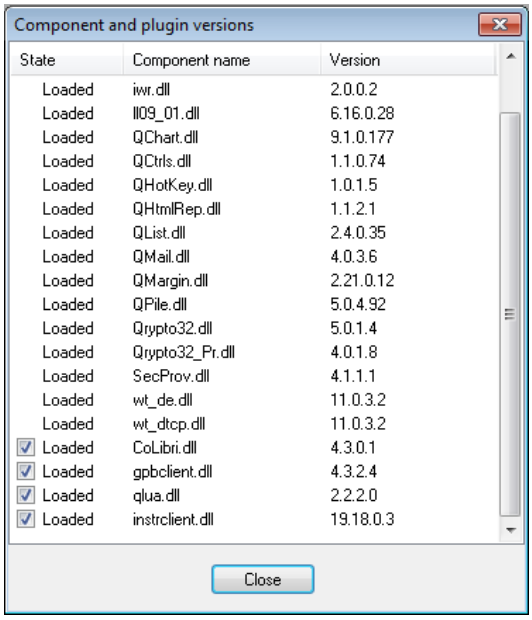
1.13 Versions of components and plugins

menu **System/About program/Components and plugin versions...**

1.13.1 Purpose

The dialog contains information about components and plugins of the used program version.

1.13.2 Table format



Each row of the table corresponds to a particular component/plugin. The table columns show names of the following parameters:

Field name	Description
State	State of the component/plugin. Valid values: _ Loaded – enabled by user, loaded by workstation and presently working; _ Offline – not loaded by workstation as it is disabled by user; _ Reject – enabled by user but an error occurred when loading by workstation (for example, no licenses on server), presently does not working
Component name	Name of the component/plugin
Version	Version of the component/plugin

To enabled or disabled a particular plugin use the checkbox in 'State' column. If a plugin is disabled, its menu is removed; windows are closed and not automatically restored when enabling it next time.

1.14 Program updates

1.14.1 Automatic update

QUIK has a built-in update procedure. After a connection to the server is established, the program compares the module versions installed on the client computer to those on the server.

If any new modules are available from the server, the program suggests downloading and installing them. Thus, to update the program, reinstallation from the distribution kit is not necessary. To download the updated modules and to let QUIK install them, just click **Receive files**.

After the files are downloaded to the client computer, a prompt to restart the program appears so that the new files can replace the outdated segments. Click **OK**. When updating is complete, the program prompts the user to restore the connection to the server to continue operation.

> **After the program is updated, the computer does not need to restart.**

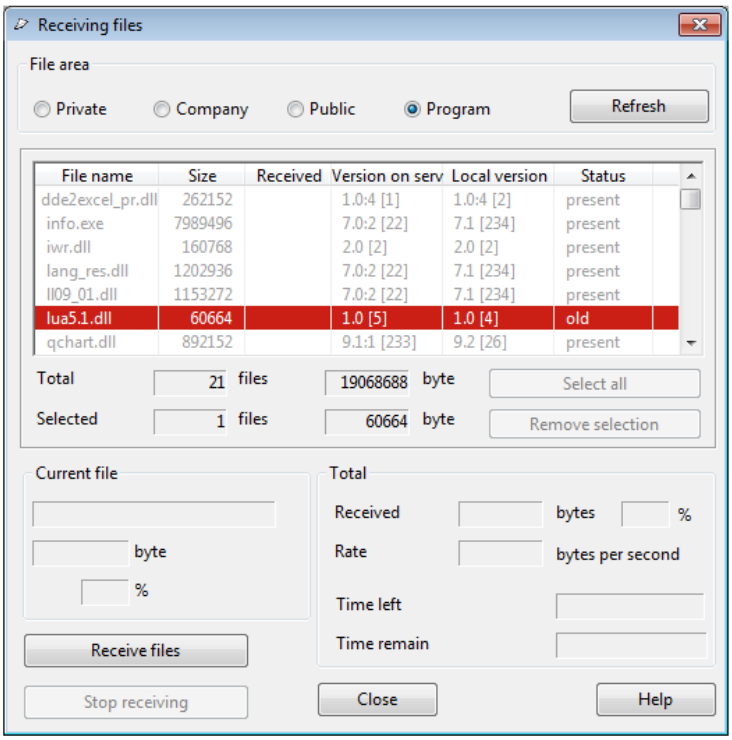
To disable the automatic update, click **General settings...** in the **System / Settings** menu and then uncheck the **Check for updates** checkbox under the **Program** tab.

1.14.2 Manual update

To update the program manually, select **System / About program / Update program version** menu item.

1.15 Receiving files

The **Receiving Files** window (accessible through the **Receiving files...** menu item from the **System** menu) allows the QUIK system administrator to use the program update mechanism to deliver various files to QUIK users.



1.15.1 Purpose of file areas

- The **Private** area is intended for documents and files addressed only to a specific user (for example, broker reports). The received files are saved to the FILES\PRIVATE folder located in the QUIK directory;
- The **Company** area is for documents and files for the company's employees. Received files are saved to the FILES\COMPANY folder located in the QUIK directory;
- The **Public** area is reserved for files and documents which are commonly shared, such as broker service regulations, rates and program documentation. Received files are saved to the FILES\PUBLIC folder located in the QUIK directory;
- The **Program** area is reserved for program updates.

To request the current status for a file area (for example, if you expect a new file to be added to the area), click **Refresh**.

1.15.2 Purpose of file area fields

- The **File name** field shows the file name;
- The **Size** field shows the file size in bytes;
- The **Received** field shows the size of the received portion of the file in bytes;
- The **Version on server** field shows the version of the file available on the server;
- The **Local version** field shows the version of the file available on the client's computer;
- The **Status** field shows the current state of reception (‘present’, ‘not received’, ‘old’, ‘in transit’, ‘received’).

1.15.3 Receiving a file

To select a file for retrieval, left-click on it. The selected files are highlighted in red. The **Total** and **Selected** fields will provide information about the number of available and ordered files selected for retrieval.
To get the files, click **Receive files**. The **Current file** and **Total** group boxes will display the status of file retrieval. The process will complete automatically; therefore, the window may be closed by clicking the **Close** button. If necessary, this window may be re-opened again from the program menu. To stop the process, click the **Stop receiving** button.

> **Files are received in background mode which does not affect the delivery time of information from an exchange during a trading session. However, when working via low-bandwidth connections, the process may take longer. In such cases, we recommend receiving files either before or after the trading session. The system administrator may restrict file receipt to a specified time period.**

Appendix 1. Error messages

Name and password entry errors

1. 'File with key not found'

   - The program is unable to locate the file with the specified keys indicated in qrypto.cfg. If the keys are stored on an external storage device, check whether it has been inserted to the computer;
   - If the keys are not stored on an external device, ensure that they are available at the location specified in **Program / Encryption** under the **System / Settings / General settings...** menu. In the window that follows, select **Default Settings** and find the lines '**Public key file**' and '**Secret key file**'. If these lines are empty, by default the program will search for the key files on the A: drive. The file path should not contain any spaces or Cyrillic characters. You can only change these settings when disconnected from the QUIK server;
   - The storage device or the file containing the keys is damaged. If damaged, it is impossible to use this key and you will need to create and register a new access key on the server.

2. 'User or server key not found'

   - The public key file pubring.txk does not contain the key file for the server ID specified in the connection settings;
   - The secret key file secring.txk does not contain the secret key for the user whose ID was entered.

3. 'IO error when trying to access a key file'

   - Failure to access the key file. May be denied access to the file.

4. 'Incorrect key file name'

   - Incorrect file name specified in the qrypto.cfg file.

5. 'Invalid key in the key file'

   - One of the keys specified in qrypto.cfg is incorrectly formatted or damaged. You will need to create and register a new access key.

6. 'Invalid password'

   - An incorrect password was entered. Make sure that the password is entered using the correct capitalisation and language and then retype the password.

7. 'Encryption error N...'

   - An encryption error occurred. If this message appears, please send a screenshot to the QUIK technical support: quiksupport@arqatech.com.

Server connection errors

1. 'Connection failed'

   - IP address and port specified in the connection parameters are available on computer where the QUIK workstation is launched but QUIK Server is not launched with such parameters. Contact the QUIK system administrator;
   - The user's key is not registered on the server. Please contact the QUIK system administrator to register the key.

2. 'Connection refused' (Connection rejected)

   - IP address and port specified in the connection parameters are available on computer where the QUIK workstation is launched but not supported by QUIK Server. Please contact the QUIK system administrator;

3. 'No Route to Host'

   - IP address and port specified in the connection parameters are not available on computer where the QUIK workstation is launched. Please contact the QUIK system administrator.

4. 'You are already working in the system'

   - A user may log on only once or from one machine at a time. If you receive this message while reconnecting immediately after a connection has been lost (most likely when connecting via dial-up), try again a few seconds later allowing the server to stop processing your previous connection;
   - If you receive this message while connecting to the server for the first time, contact the system administrator.

5. 'License expired'

   - Your license to use the QUIK terminal has expired. To renew your license, contact the QUIK system administrator

6. 'Access blocked by administrator'

   - The user's account or IP address has been blocked by the system administrator. Contact the QUIK system administrator.

7. 'Protocol error', 'Out-dated protocol', 'Incorrect protocol' or 'Unsupported protocol' (Protocol mismatch)

   - The server does not support the client's workstation. Older versions of QUIK may be compatible with more recent versions of the server, while newer versions of the client's workstation may not necessarily be compatible with older versions of the server.

   > **To check version compatibility, update the program automatically (using the Update program version command in the System / About program menu). In this way, the compatibility of versions is ensured.**

8. 'Unknown encryption provider'

   - The settings for the client program's encoding system do not suit those for the QUIK server. Modify the settings according to the system administrator's recommendations.

9. 'Corrupted certificate'

- The encryption certificate is invalid. Please contact the QUIK system administrator.

10. 'User not found'

- The SSL authorisation could not find the user. Please contact the QUIK system administrator.

11. 'Error during context creation'

- An authentication error occurred. Report the error to the QUIK system administrator indicating which encryption system was used.

Runtime errors

1. 'Connection timed out'

- The connection to the server is lost because of a poor quality connection. Re-establish the connection. If you experience frequent connection time outs, consult the QUIK system administrator about your system settings and selecting a provider.

2. 'Connection reset by peer'

- The connection to the server is lost. Try to reconnect;
- Users are automatically disconnected at the end of a trading session.

3. 'Unable to write the connection settings to the configuration file <file path> info.ini'

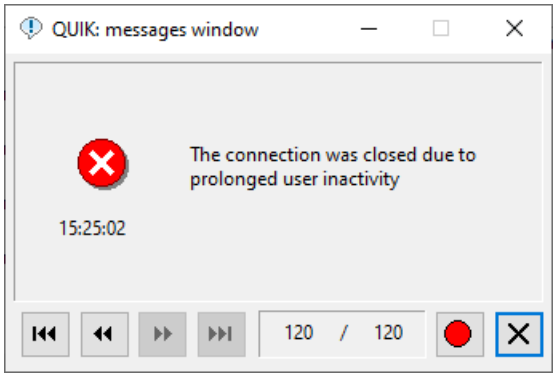
- The 'Read only' attribute is set for the file. Remove this attribute;
- The user does not have permission to write to the directory where the program is installed. Ask the system administrator to grant you permission to write to this folder;
- The file is in use by another program. Ensure that info.ini is not opened in another application, such as Text Editor

4. Upon launch, the program reports an error and stops.

- The received data is corrupt. Delete the info.log file from the QUIK directory and restart the program;
- The program has been incorrectly updated. Restore the previous version. In the QUIK directory, find the **BACKUP** folder. This folder contains the subdirectories labelled in the format <**DDMMYYYY>,** where <DD>, <MM>, and <YYYY> are the day, month, and year of the specific updates. Select the folder with the date of the last update, and copy all of the files from that folder to the QUIK working directory. Then, relaunch the program;
- A system malfunction occurred. Please contact the QUIK system administrator.

5. 'The terminal will be disconnected in N seconds'

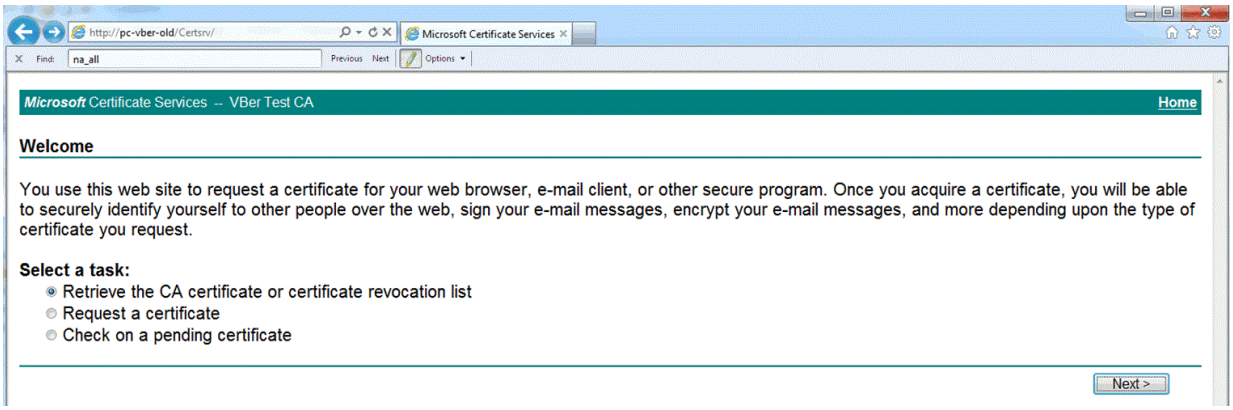
- The user was inactive when the **Disconnect after the specified inactivity period has expired** checkbox was enabled (see Chapter 2, "Basic Operating Principles", sub-section **Program**). To continue operation, press "OK" button in the opened window. Otherwise, after the time has passed, the connection to the server will be closed and the messages window will open:

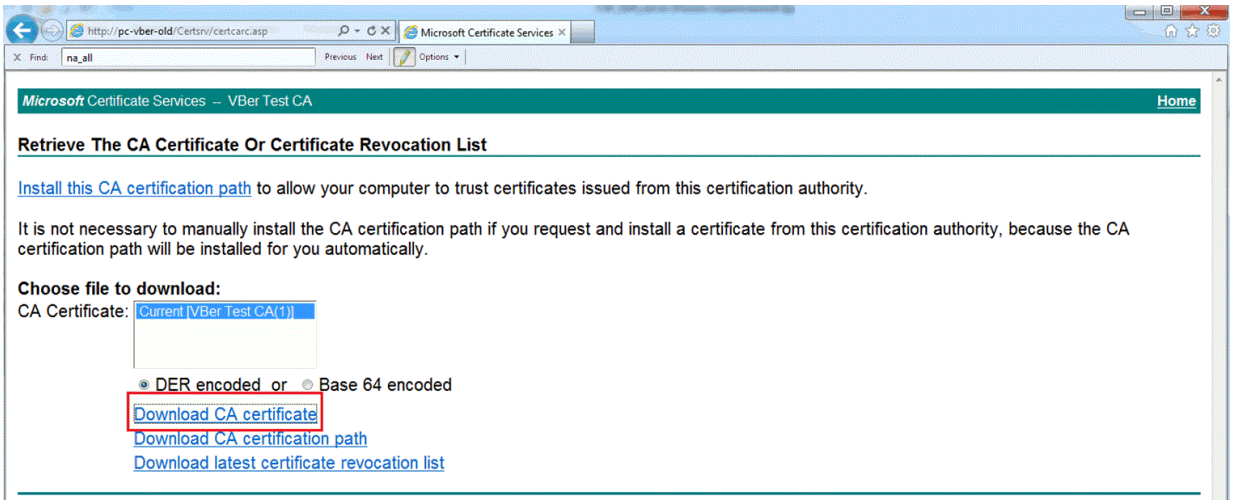


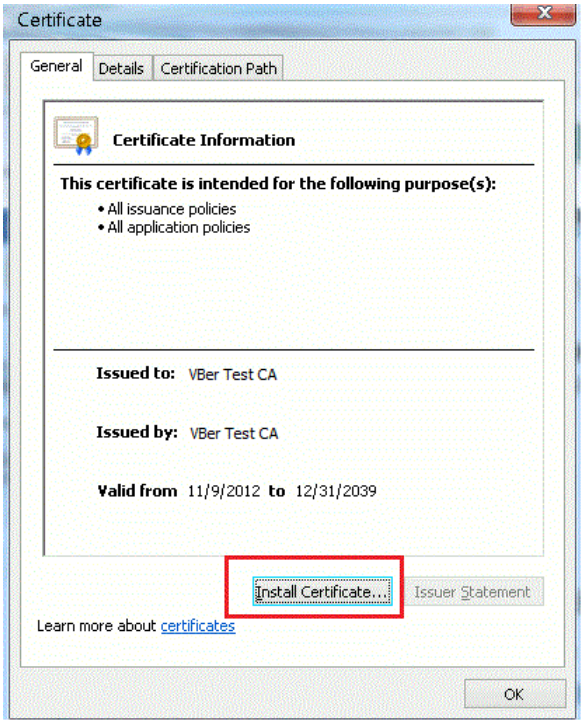
The connection to the QUIK server can be configured only manually.

Appendix 2. Example of certificate retrieval via web interface of Certification Authority

1. Open Internet Explorer (it is guaranteed to correctly receive a certificate only in this browser).
2. Insert the link received from your broker to the Address bar. In the opened window allowing to select tasks check the values shown in the screenshots:

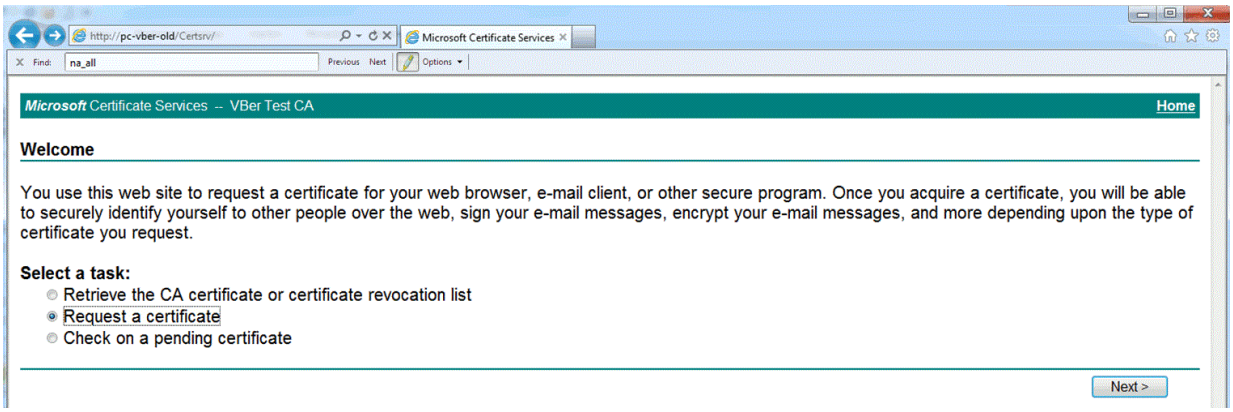




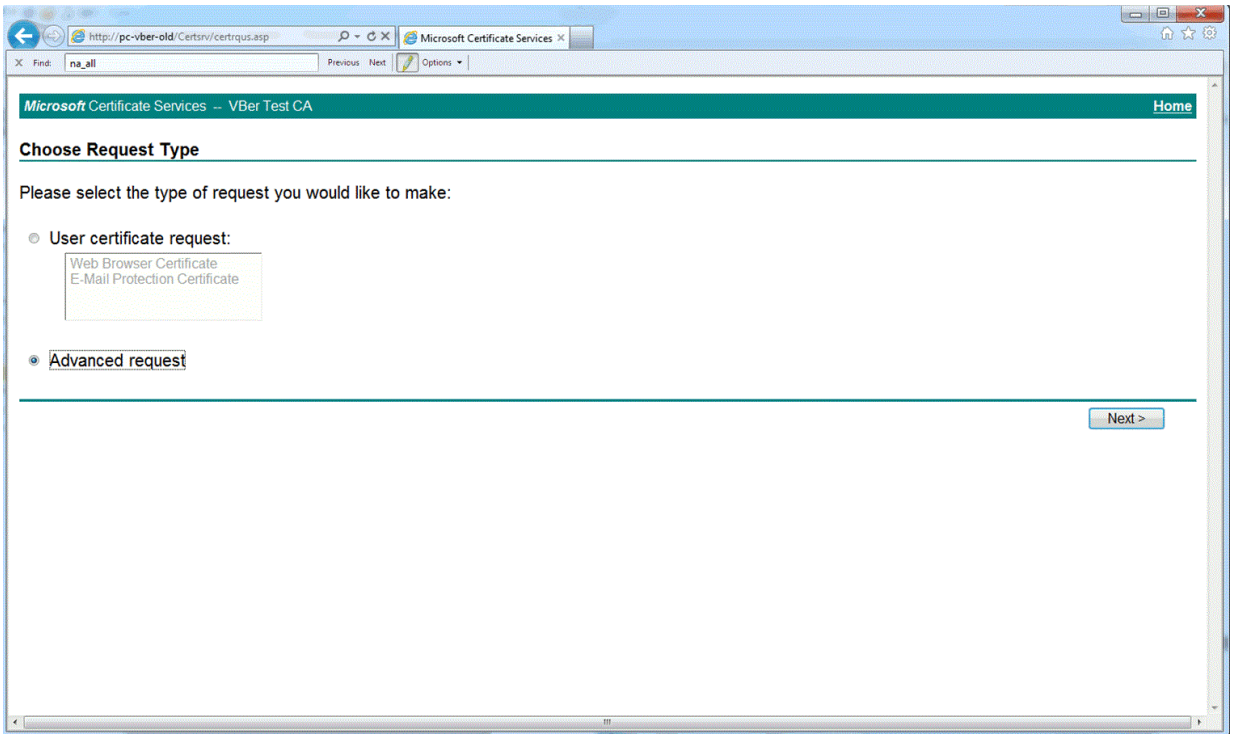


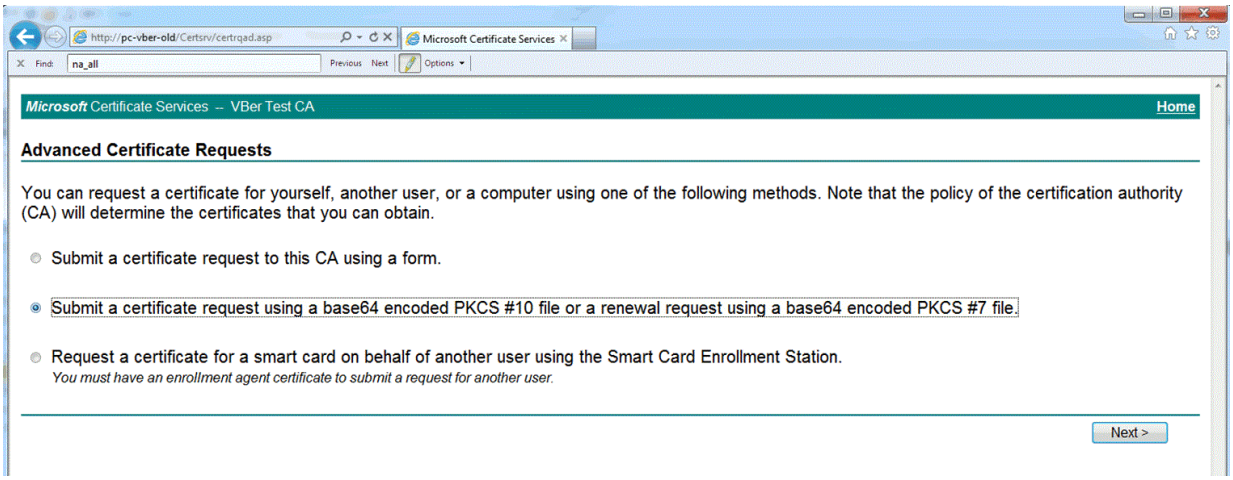
Install the certificate of the Certification Authority using the Certificate Import Wizard by selecting the Trusted Root Certification Authorities store.

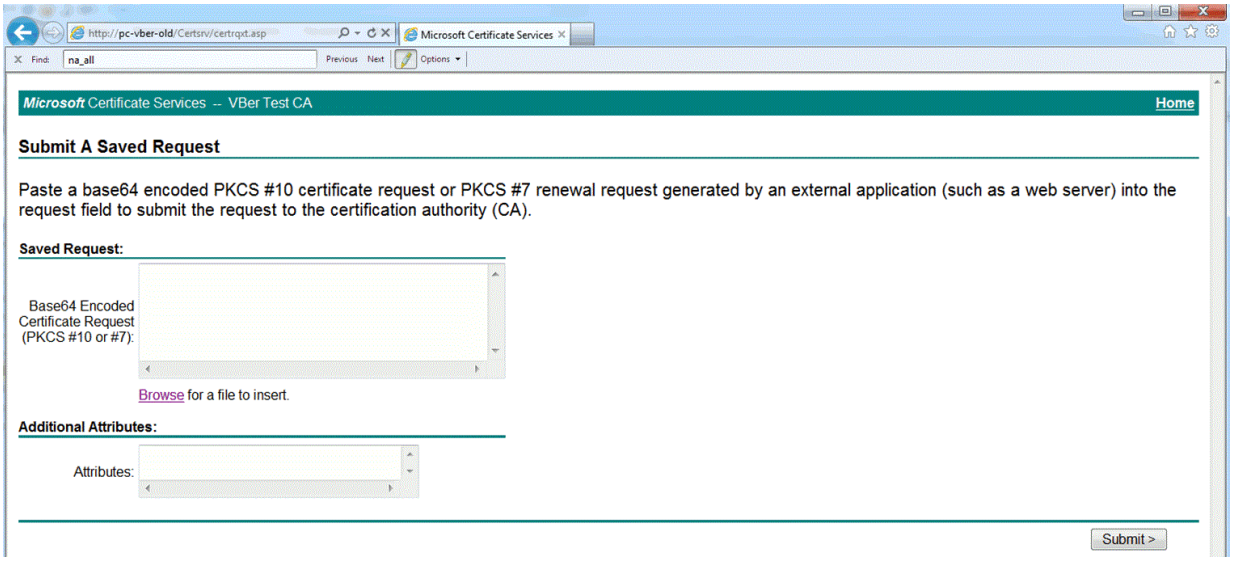
3. The certificate of the Certification Authority is installed. Then, install the client certificate:



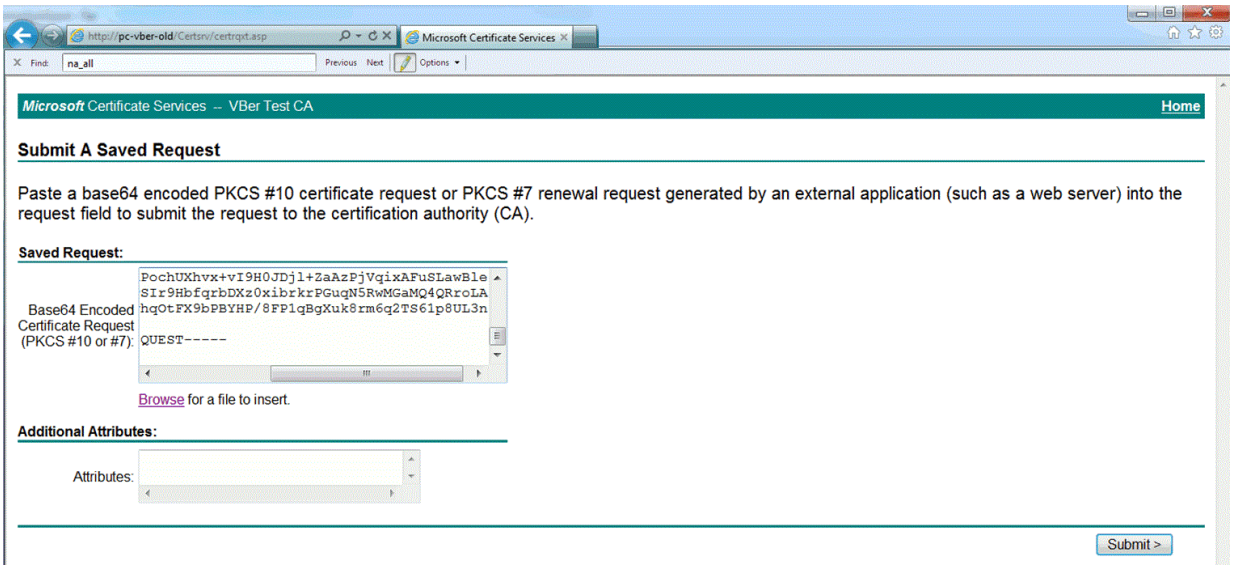
Select the values as shown in the screenshots:

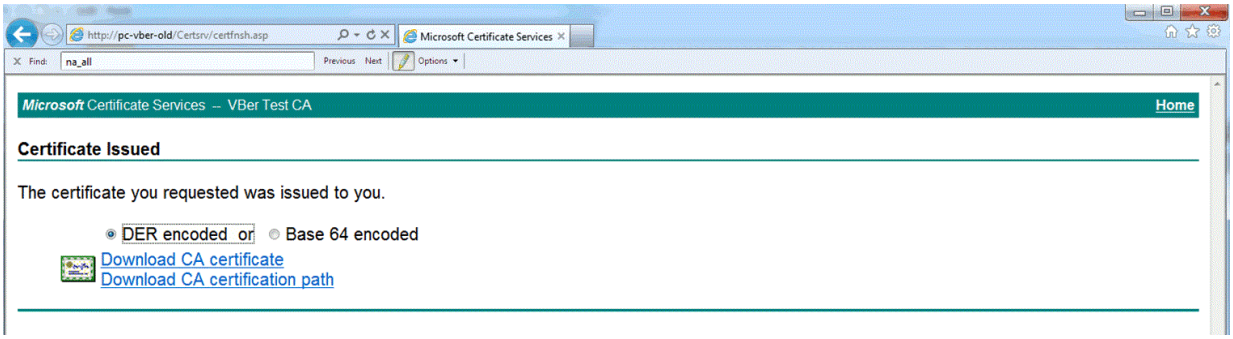






In this window, click **Browse** and specify the path to the generated request on a certificate. If your browser reports that this action is not allowed for security policy reasons, the contents of the certificate request file can be copied to a corresponding box:





In the opened window, select **Download CA certificate**, then the security certificate is saved to the directory specified by the user.