AO Mizuho Bank (Moscow)

Remote Banking Service System Setup Manual

User Manual

Moscow

Table of contents

General information

Current manual describes the process of installment and initial set up of the client's workplace in the Remote Banking Service System (later RBSS) of AO Mizuho Bank (Moscow) (later the Bank) on Windows platform.

The target audience is the RBSS users, also technical specialists servicing the equipment that provides the access to RBSS of the Bank.

- Interaction with RBSS is carried out by using Microsoft Internet Explorer 11, Google Chrome or Mozilla Firefox

. All data of clients' part of the system is stored on RBSS server of the Bank.

To protect information in RBSS is used:

- Data encryption software "RuToken ECP 2.0". Additional information on "RuToken ECP 2.0" and technical documentation are available on the developer's site https://www.rutoken.ru/
- Data encryption software "Message-Pro". Additional information on "Message-Pro" and technical documentation are available on the developer's site http://www.signal-com.ru/.

Technical requirements

Below are the minimal PC requirements for working with the RBS system:

Hardware configuration:

- IBM computer or 100% compatible with it
- processor speed 600 MHz and higher
- RAM (memory) 128 Mbyte and higher
- Video adapter not lower than SVGA (800*600, 256 colors)
- Not less than 100 Mbyte of free space on a hard drive
- Available USB port

System software:

- Microsoft Windows 10 and Microsoft Windows 11
  Attention! Only English and Russian versions of the operating system are supported!
- Microsoft Internet Explorer 11, Google Chrome, Mozilla Firefox

Communication requirements:

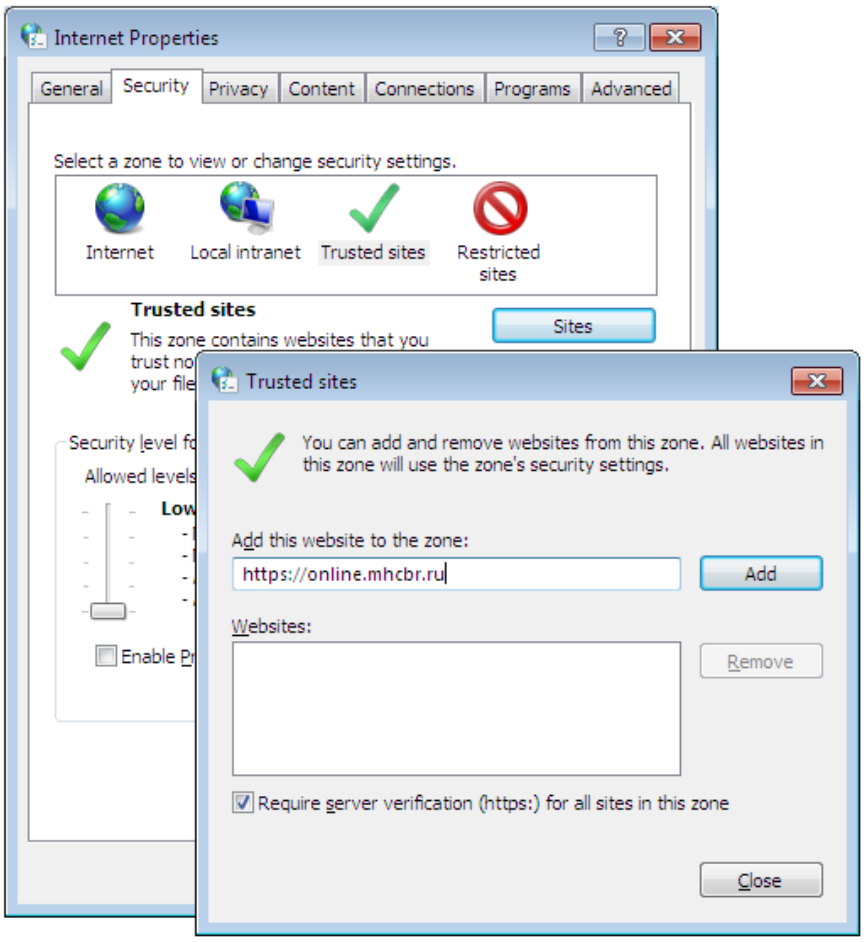
- Internet access.

A supported browser security settings

Before connecting to the Remote Banking Service system, it is necessary to set up a supported browser security settings

A supported browser security set up:

- Open Internet options (through Windows control panel)
- Go to **Security** tab
- Choose **"Trusted sites"** zone
- Add the site address **https://online.mhcbr.ru/** to the **Trusted sites** zone
- Set up the security level for **Trusted sites** zone-**Low**



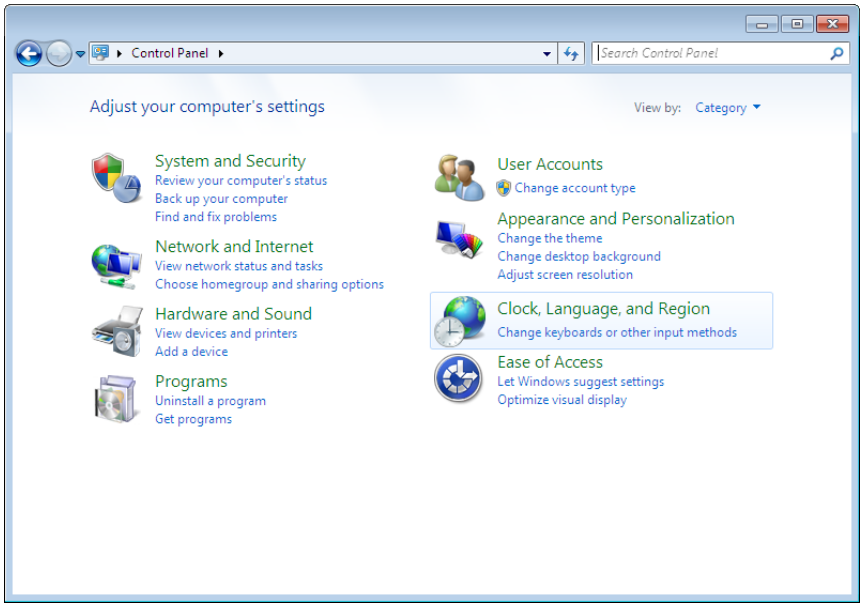
- Close tab
- Consecutively click **Apply** , then **OK** button to save the changes

Technical support of RBSS: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru

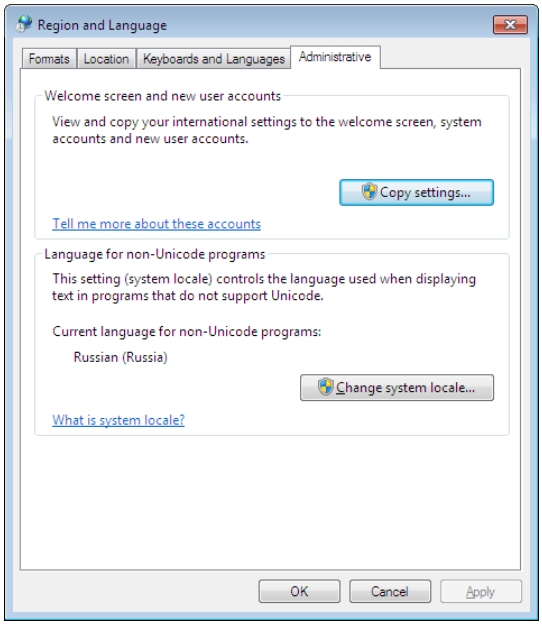
OC Windows settings

Choosing the language of the programs, not supporting Unicode (restart needed if changes occur):

- Open Windows Control Panel
- Choose **Change keyboards or other input methods** group



- Go to **Administrative** tab
- In **Language for non-Unicode programs** click **Change system locale**
- **Russian** should be installed as a **Current language for non-Unicode programs**



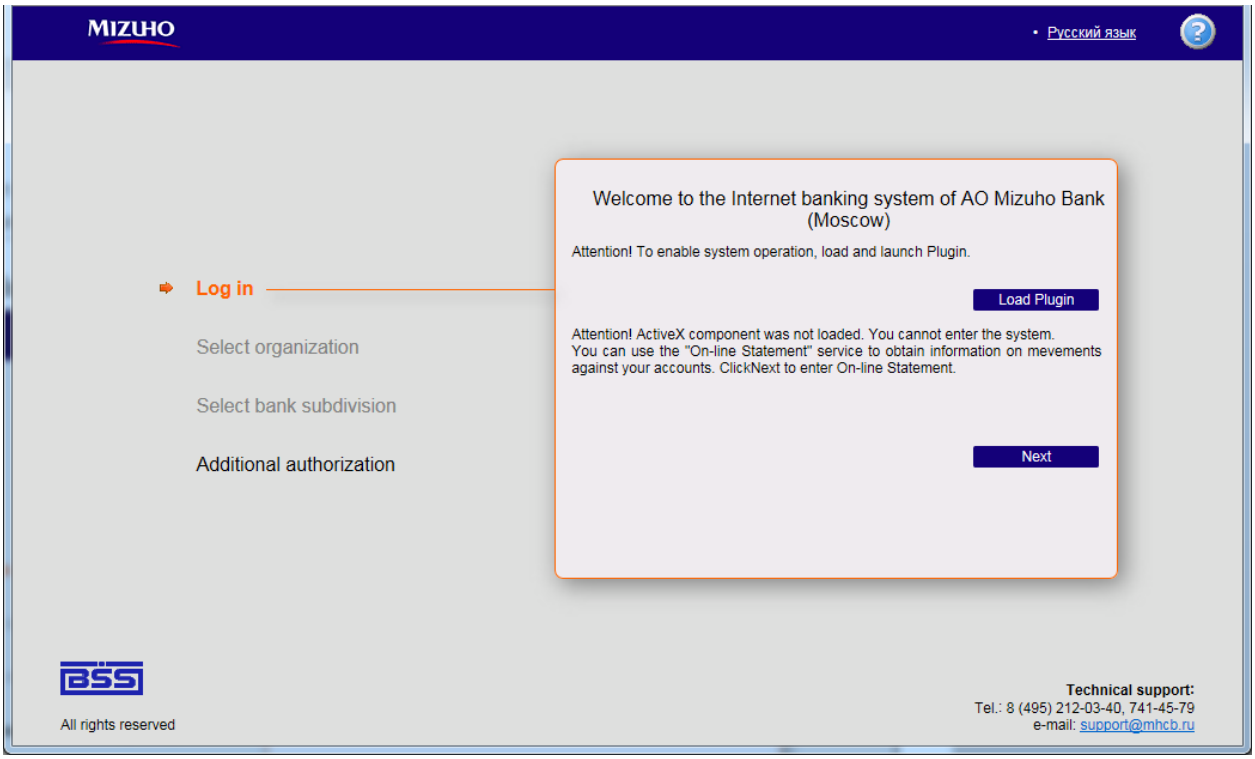
- Click **OK-Apply-OK** to save the settings

Technical support of RBSS: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru

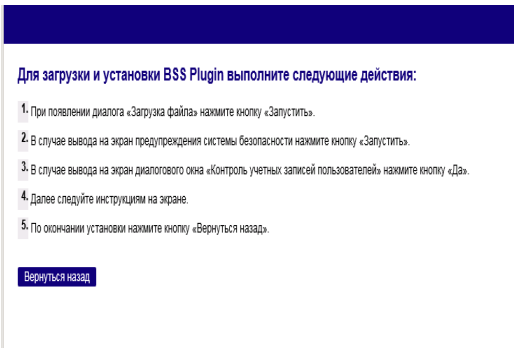
Installation/update of Internet-client components

To connect to Remote Banking Service system it is necessary to do the following:

1. Open a supported browser and go to https://online.mhcbr.ru
2. Click "**Load Plugin**"



3. Follow the instructions from the opened tab



To download and install BSS Plugin follow the steps below:

1. When the “File downloading” dialog appears click “Download”
2. In case the security system warning comes up on the screen click “Download”
3. In case “User accounts control” dialog comes up on the screen click “Yes”
4. Then follow the instructions on the screen
5. After the download is finished click “**Вернуться назад**” (Go back)

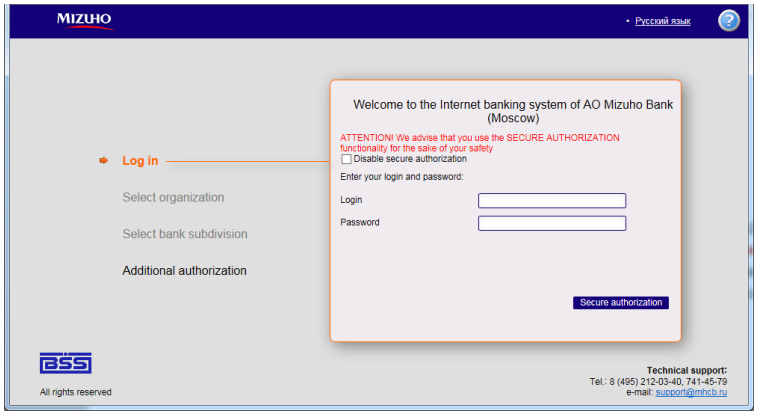
4. Wait until the plug-in installation is finished

The primary log in into the system/ Primary key generation

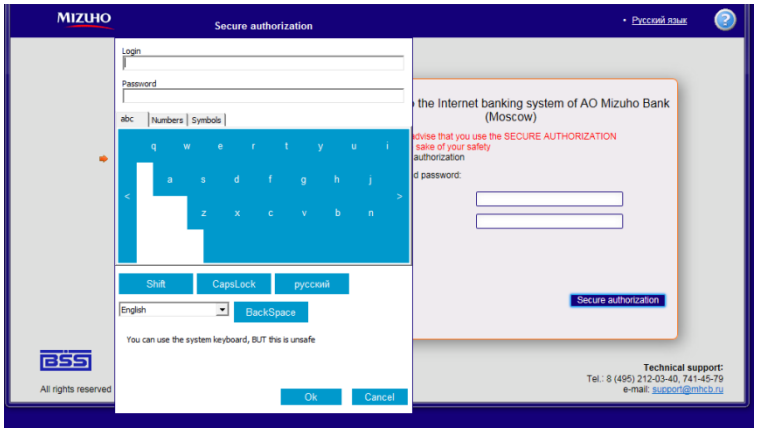
1. Insert the RuToken received at the Bank into the USB port before connecting to RBSS.

If it is a primary connection, it is necessary to wait for OC Windows to install the key driver. In case of a problem with the driver, set up it is necessary to contact technical support service.

2. Open a supported browser and go to **https://online.mhcbr.ru/**
3. In the open tab of log in into the system:

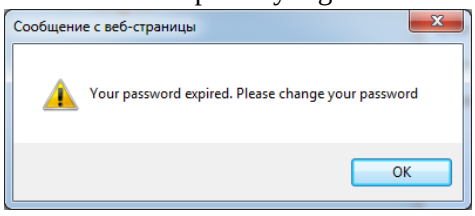


Version 1: click **Disable secure authorization** **(not recommended)** then enter login and password (indicator of RBS system access received at the Bank) and click **Continue**

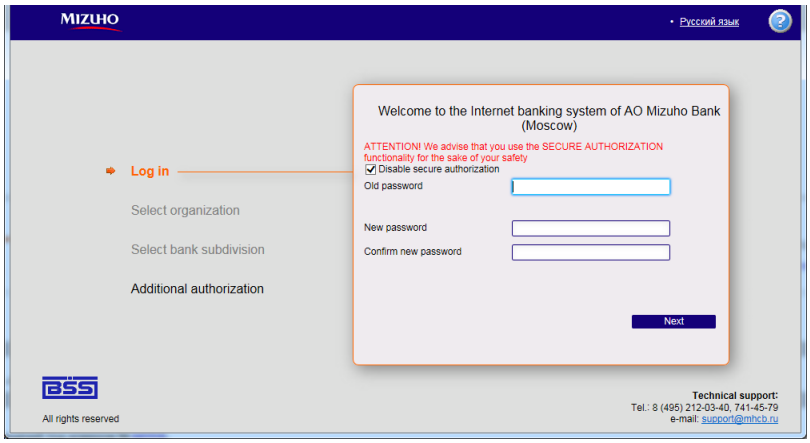


Version 2: click **Secure authorization** and in open tab using the onscreen keyboard enter login and password with the help of a mouse cursor

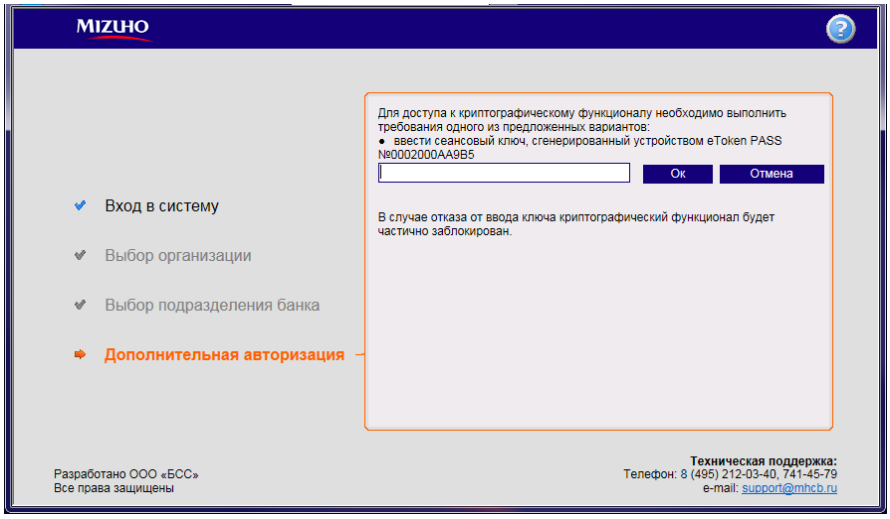
4. In case of a primary log in into the system a Change password tab opened up - click **OK**



5. Using the **safe authorization (recommended)** or disconnecting it, change the password entering **the Old password, New password and Confirm of a new password** (letters, numbers and special symbols can be used for password, length of password 8-10 symbols).



6. In case of using an isolated generator of one-time passwords e-Token PASS, it is necessary to enter a session key by clicking the button on the device.



eToken PASS

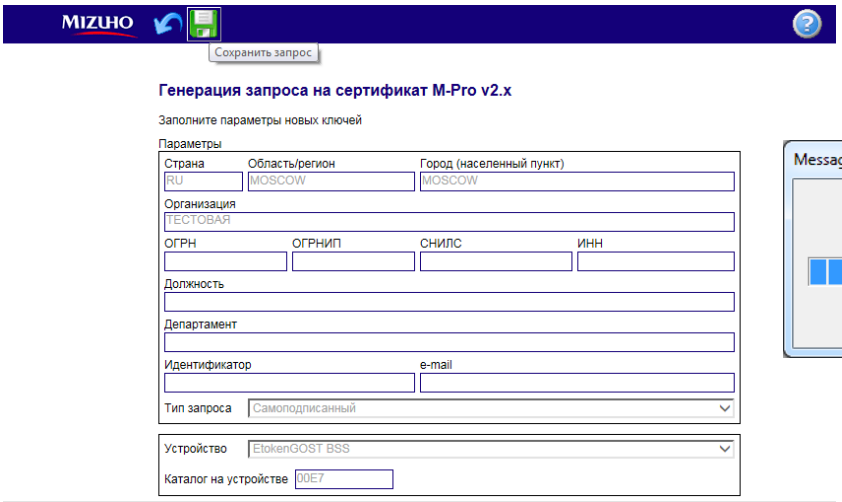
ATTENTION! THIS DEVICE IS USED ONLY ONCE DURING EACH LOG IN INTO THE SYSTEM. **IN CASE OF MULTIPLE CLICKING THE DEVICE WILL BE BLOCKED!**

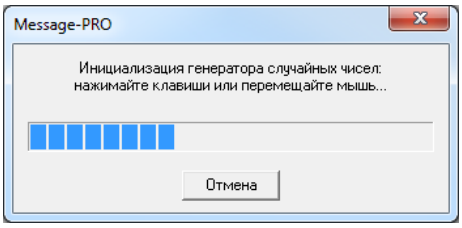
7. In case the generation or regeneration of the user's key is needed, in open tab it is necessary to mark the user (by clicking once on the last name of the user) then click ***Create request for generation /regeneration.***

Attention! At this stage the **RuToken ECP 2.0** received at the Bank or other removable device key should be connected the USB port

RuToken ECP 2.0

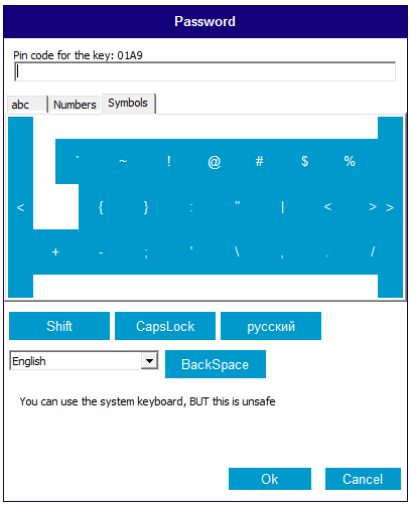
8. *In the open tab click* ***Save request***





If you use USB Flash Drive, in the setting **Устройство** change the letter of drive **A** to the letter of the disc of the USB Flash Drive

9. Enter password received at the Bank **on e-Token GOST- PIN CODE of the key stated in the passwords form.**

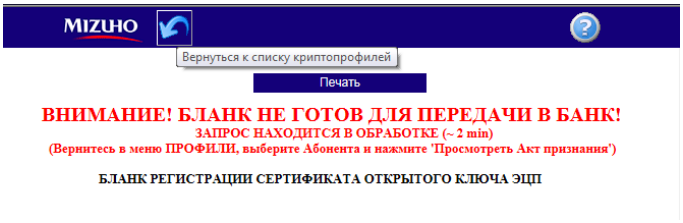


IMPORTANT!! PIN CODE IS WRITTEN ON THE PASSWORDS FORM!!! AT THIS STAGE DO NOT USE THE GENERATOR OF ONE-TIME PASSWORDS - E-TOKEN PASS DEVICE!!!

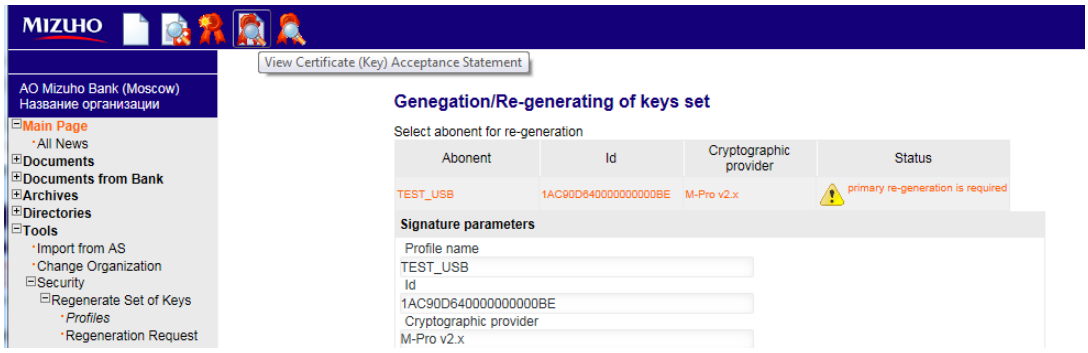
RuToken ECP 2.0

Technical support of RBSS: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru

10. In the process of generation a new closed key will be created on the carrier and a request for registration will be sent to the bank. On client's side a certificate registration form will open. If you see a red writing then the request is still in process. Click ***Return to the list of crypto profiles***



11. It is necessary to wait 2-3 minutes, then mark the user (by clicking once on the last name of the user with the left click of a mouse) and click ***View the certificate acceptance act (key)***

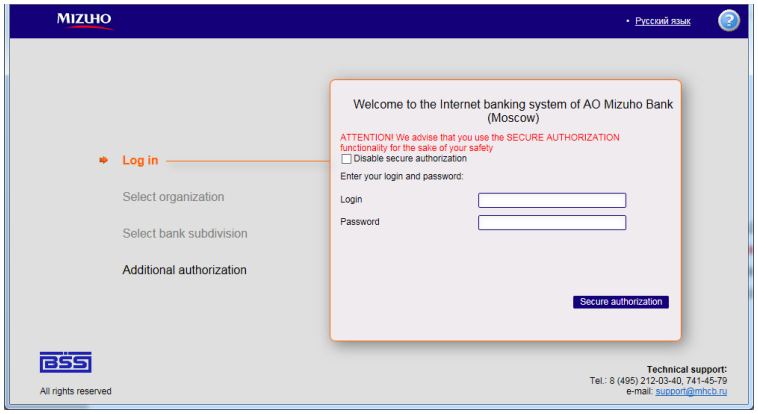


12. It is necessary to print out two copies of the opened form (without red writing). Each form has to be signed by the owner of the key and the head of the organization and sealed. It is necessary to bring the forms to the Bank.

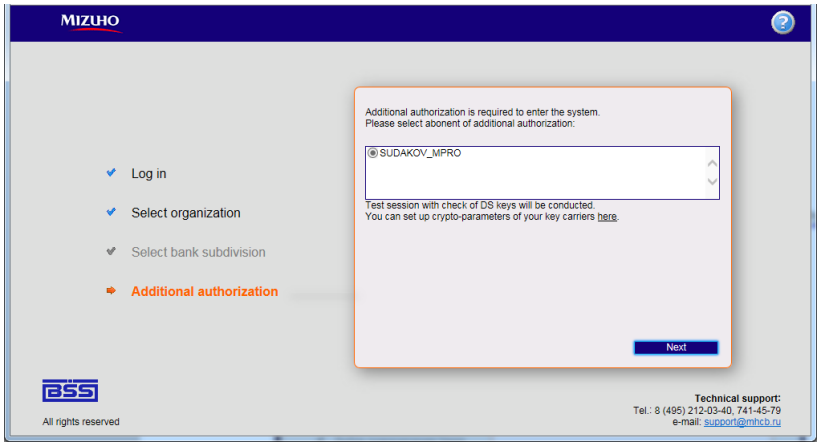
Technical support of RBSS: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru

LOG IN INTO THE SYSTEM AND CONCLUSION OF REGISTRATION OF USER'S KEY SIGNATURE

1. After receiving the originals of the electronic signature key certificate forms the Administrator finishes the registration of a new user's key.
2. To finish the procedure of the new key registration a user should enter the RBS system:



Enter login/password

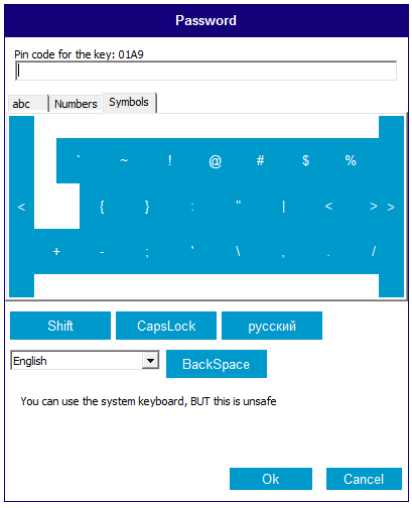


Click ***Next*** on the page of additional authorization

At this stage an **RuToken ECP 2.0** received from the bank or other key carrier should be installed

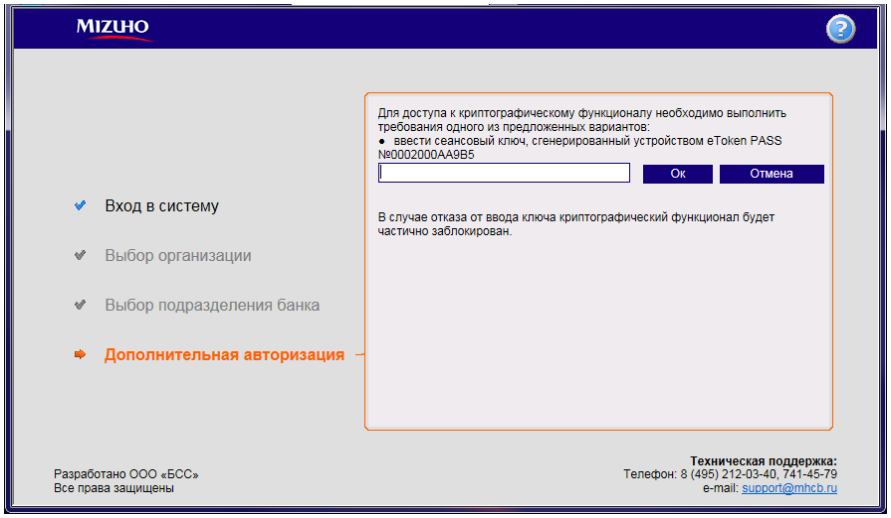
RuToken ECP 2.0

3. Enter password on **RuToken ECP 2.0**, **PIN-CODE stated in the password forms**, received at the bank.



IMPORTANT! THE PIN-CODE IS STATED IN THE PASSWORDS FORMS!
AT THIS STAGE DO NOT USE THE GENERATOR OF ONE_TIME PASSWORDS –e-Token PASS DEVICE!!

4. In case of using an isolated generator of one-time passwords e-Token PASS, it is necessary to enter a session key by clicking the button in the device.



eToken PASS

ATTENTION! THIS DEVICE IS USED ONLY ONCE DURING EACH LOG IN INTO THE SYSTEM. **IN CASE OF MULTIPLE CLICKING THE DEVICE WILL BE BLOCKED!**

5. The procedure of key regeneration is now finished; you may start working in RBSS.