

Guide for OTP Token usage in the Remote Banking System of AO Mizuho Bank (Moscow)

One-Time Password (OTP) is a sequence of symbols dynamically generated for one login session.

One-time passwords are used for additional authentication of system users who have the authority to sign electronic documents. That provides additional security in case a user's password and login are compromised.

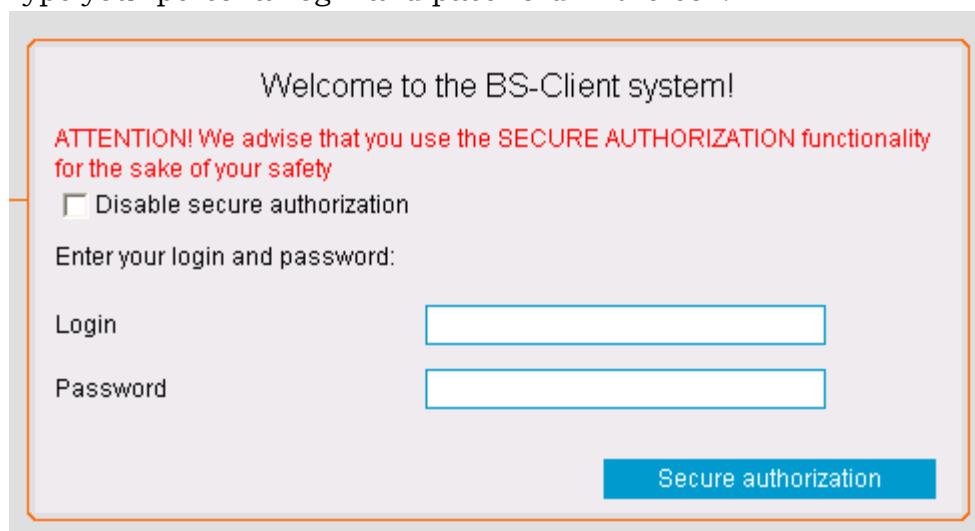


A special device is used for one-time password generation – an OTP-token. In the RB System of AO Mizuho Bank (Moscow), eToken PASS devices by Aladdin-RD are used.

The device is self-contained and does not require any connection to a computer. RB System access with eToken PASS has almost no differences from the regular order except one additional step - the System will prompt for the key generated by the eToken Pass device.

How to access the system:

1. Type the RB system server address in the Internet Explorer address bar <https://online.mhcbr.ru>
2. Type your personal login and password in the box:



Welcome to the BS-Client system!

ATTENTION! We advise that you use the SECURE AUTHORIZATION functionality for the sake of your safety

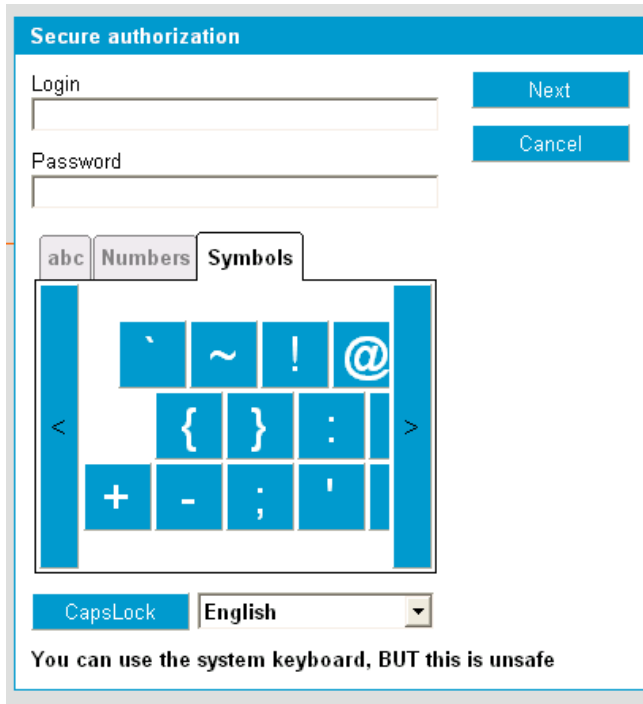
Disable secure authorization

Enter your login and password:

Login

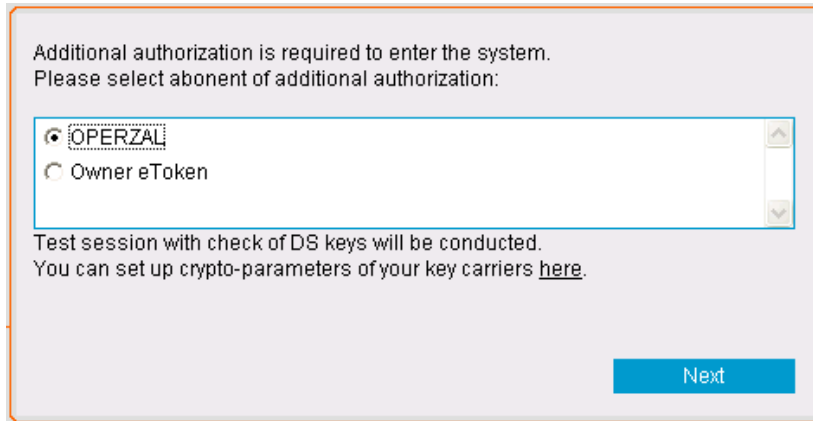
Password

We strongly recommend to use safe authorization (data input using a virtual keyboard). Press the “Secure authorization” button and use mouse to enter your Login and Password via clicking buttons on virtual keyboard.



The image shows a 'Secure authorization' window. It has a title bar with the text 'Secure authorization'. Below the title bar, there are two input fields: 'Login' and 'Password'. To the right of the 'Login' field is a blue 'Next' button, and to the right of the 'Password' field is a blue 'Cancel' button. Below the input fields, there are three tabs: 'abc', 'Numbers', and 'Symbols'. The 'Symbols' tab is selected, and it shows a grid of symbols including apostrophe, tilde, exclamation mark, at-sign, left and right angle brackets, curly braces, colon, plus, minus, semicolon, and apostrophe. Below the grid, there is a 'CapsLock' button and a language dropdown menu set to 'English'. At the bottom of the window, there is a warning message: 'You can use the system keyboard, BUT this is unsafe'.

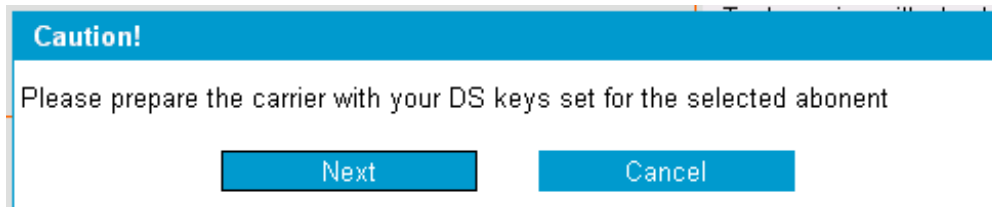
3. The page for additional authorization will appear.



The image shows a dialog box for additional authorization. It contains the text: 'Additional authorization is required to enter the system. Please select abonent of additional authorization:'. Below this text is a list box with two options: 'OPERZAL' (selected with a radio button) and 'Owner eToken'. Below the list box, there is more text: 'Test session with check of DS keys will be conducted. You can set up crypto-parameters of your key carriers [here](#).'. At the bottom right of the dialog box is a blue 'Next' button.

Choose your account and press “Next”.

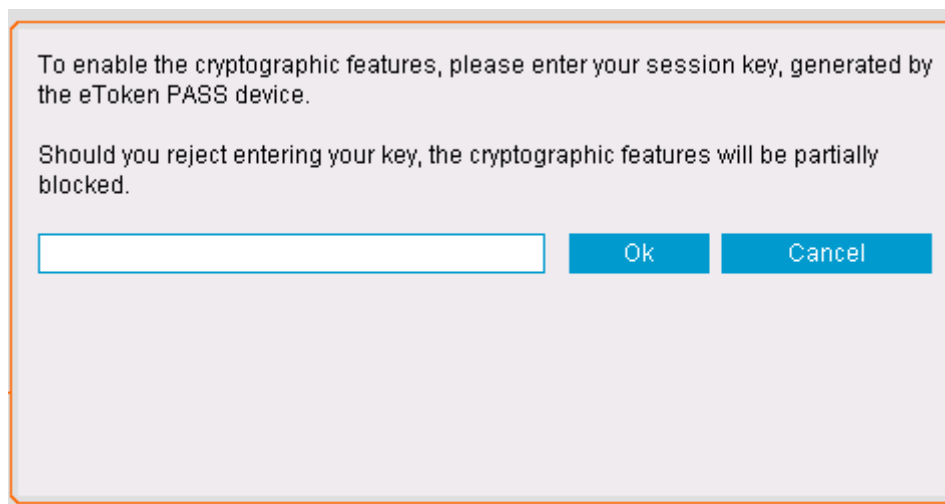
4. You will see the following message in the system:



The image shows a 'Caution!' dialog box. The title bar is blue with the text 'Caution!'. The main text area is white and contains the message: 'Please prepare the carrier with your DS keys set for the selected abonent'. At the bottom of the dialog box, there are two blue buttons: 'Next' and 'Cancel'.

Insert the signature key media, if you didn't do it yet and press “Next” button.

5. The System will prompt for the PIN code generated by the eToken Pass device



In order to generate the PIN code, press the button on eToken Pass. You will see the generated PIN code on the screen of the device. Type it in the entry line and press "Ok".

In case of successful authorization the system will forward you to the main page of your company profile.

In case of any problems with eToken PASS, please contact the RB System customer support.

IMPORTANT! It is strongly forbidden to pass a personal password generator to third parties and to generate passwords (press the device button) for purposes other than entering the RB System.