

Information

about Password + SMS authentication

Hereby we would like to inform you about an important change in legal regulations¹ relevant to payment services that will come into force as of 14th September 2019. Based on the Act provisions, in order to make the electronic payments more secure the application of the provisions of strong customer authentication² will become mandatory as of this date. According to the change which directly affects our customers, from 14th September 2019 the Bank's electronic channels can be used only with strong customer authentication², also known as two-factor authentication process, for both login to the service and signing orders. **At our Bank the two-factor authentication process for KDB NetBank and KDB PC Kontakt (installed client program) services is implemented by using ViCA application or Password + SMS authentication.**

About Password + SMS in a nutshell

This authentication method is recommended for those clients, who has no smartphones with Internet connection (mobile net or wi-fi network). In this case strong client authentication is implemented by the client's login password and a one-time used SMS code sent to the client's specified mobile phone in our data base. However, it is highly recommended to switch ViCA app, because it provides a more secure way to manage financing.

Login with Password + SMS authentication

Choose "Login with password"! After that, enter your user identifier in GROUP:USERNAME format.





Click on the login button! A one-time used code will be sent via SMS. Please, type in the SMS code, and click on the login button!



If the password and code were typed well, entering to the NetBank is successful!

Signing orders

Signing orders can be done with SMS authentication too.

In case one or more transaction orders are needed to sign, you can use NetBank service as usual. Please, click on "Send now" button, if all the details of the transaction were given.



Please type your **login password**, and the newly sent one-time used SMS code. After that, click on “OK” button.

 The authentication code required to sign the package(s) will be sent to your cellphone shortly, in the form of a text message. Please provide it in the field, labeled 'SMS code'.

Password

SMS code -

[Modification](#) [OK](#)

If the above steps were followed, order has been sent successfully!

How to set up password + SMS authentication?

Those clients who have not switched to ViCA, the Bank will set up automatically the Password + SMS authentication during the night from September 13 to September 14.

We will continuously inform our customers about the changes through several channels. Please give special attention to your messages in your KDB NetBank or KDB PC Kontakt mailbox, and the announcements published at our branches and on our homepage (www.kdbbank.eu).

Should you have any questions, please do not hesitate to contact our Call Center (at +3614734440 between 7:00 am and 8:00 pm on working days) or your relationship manager, or visit any of our branches.

Thank you for your kind cooperation in advance.

KDB Bank Europe Ltd.

¹ Act LXXXV of 2009 on the Pursuit of the Business of Payment Services

² The strong customer authentication means an authentication based on the use of two or more elements categorized as

- a) knowledge (something only the user knows, e.g. static password, PIN code),
- b) possession (something only the user possesses, e.g. SIM card, registered token application on mobile phone, bankcard chip) and
- c) inherence (something the user is, e.g. fingerprint, facial recognition)

that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.