MOBILE TOKEN USER MANUAL

Table of Contents

I General information about Ibank mToken application

1. Description

1.1. **Ibank mToken** is a mobile application of Investbank for authorizing transfers made through Internet Banking and the **Ibank Mobile** application (Mobile Banking).

1.2. **Ibank mToken** is an independent authorization tool and cannot be combined with other tools.

2. Where to download Ibank mToken application

- You can download Ibank mToken application for free from Google Play store (for Android operating system); App Store (for iOS) and App Gallery (for Huawei).

3. Security and limitations

3.1. The **Ibank mToken** application can only be registered on one mobile device.

3.2. The mobile token can be used by users authorizing transfers to more than one bank client.

3.3. If a client forgets the password to log in to **Ibank mToken**, it is necessary to deactivate the application through Internet Banking and make a new registration.

4. Technical requirements

- In order to download, install and activate **Ibank mToken** on your device, operating with the appropriate minimum version of the respective operating system:

4.1. For Android:

Minimum - Android 8.0. **Recommended** - Android 10 or higher

4.2. For iOS:

Minimum version: 12.3. **Recommended** - 14.4

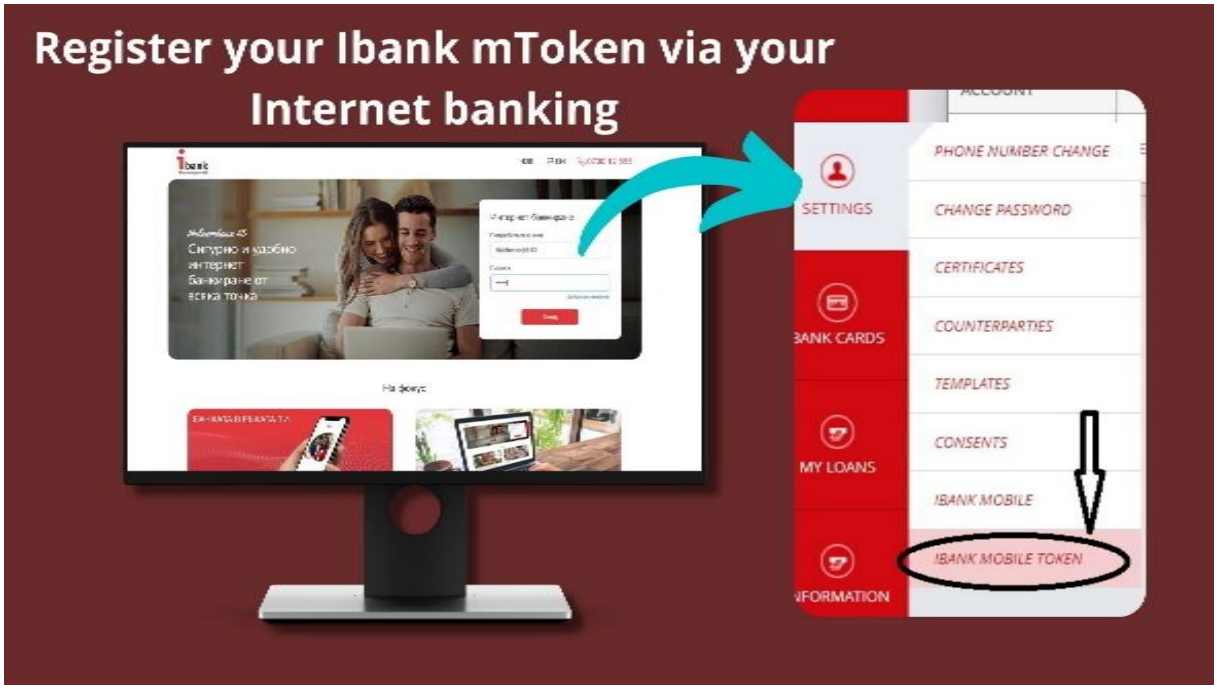
5. Filing Request for Use

5.1. Remote permission is granted to a User, an individual, who will authorize transfers only from his/her own accounts. This is executed automatically through Internet Banking, without confirmation from a bank employee.

5.2. Permission granted in the bank's office - when the User is attached to a client (company or individual), the permission to use the authorization Mobile Token method is granted in accordance with the valid rules for providing the Internet Banking service. After the client and the user present the relevant documents, the bank employee provides the permission to use Mobile Token in the system. After obtaining permission, the user registers the **Ibank mToken** application through Internet Banking.

II Registration of Ibank mToken

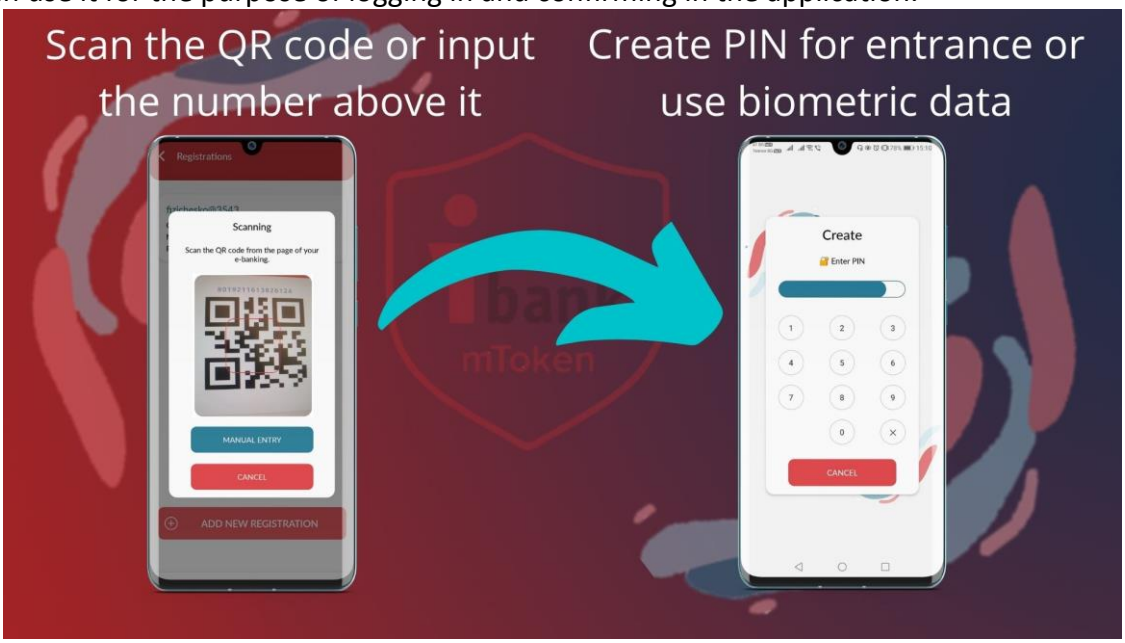
1. **Registration of Mobile Token** - After downloading the application on your



phone, you need to log in to Internet Banking. After login, the Settings / Ibank Mobile Token menu opens. If you are registering for the first time to authorize your accounts, you will first need to agree and sign the General Terms and Conditions of Use. After signing them with the current authorization method, click the **Registration on Mobile Device** button.

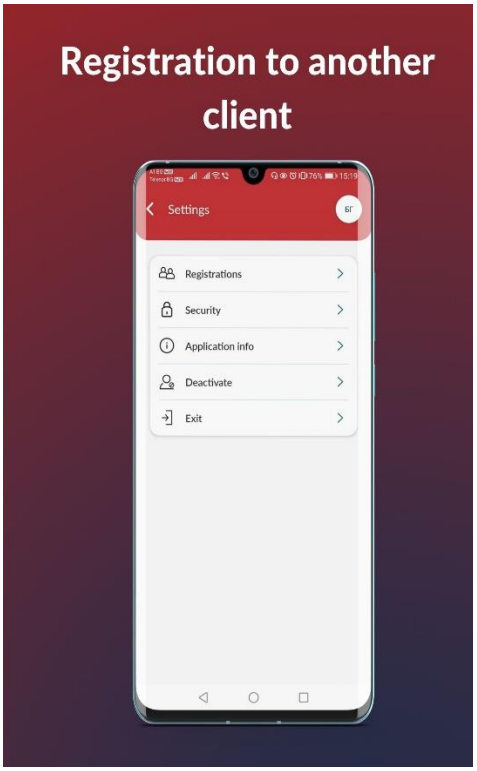
A screen is displayed warning that only one Mobile Token can be registered for each Client User. Click the **Next** button.

A screen containing a QR code valid for only 5 minutes is displayed. Open the already downloaded **Ibank mToken** application and press the Activate button. The application will require you to scan the QR code from Internet Banking. After scanning it, you need to enter **your Internet Banking username.** In the next step you have to create and confirm the **login and confirmation PIN** in the application. If your phone operates using biometric data, you can use it for the purpose of logging in and confirming in the application.



Registration of user connected to another client

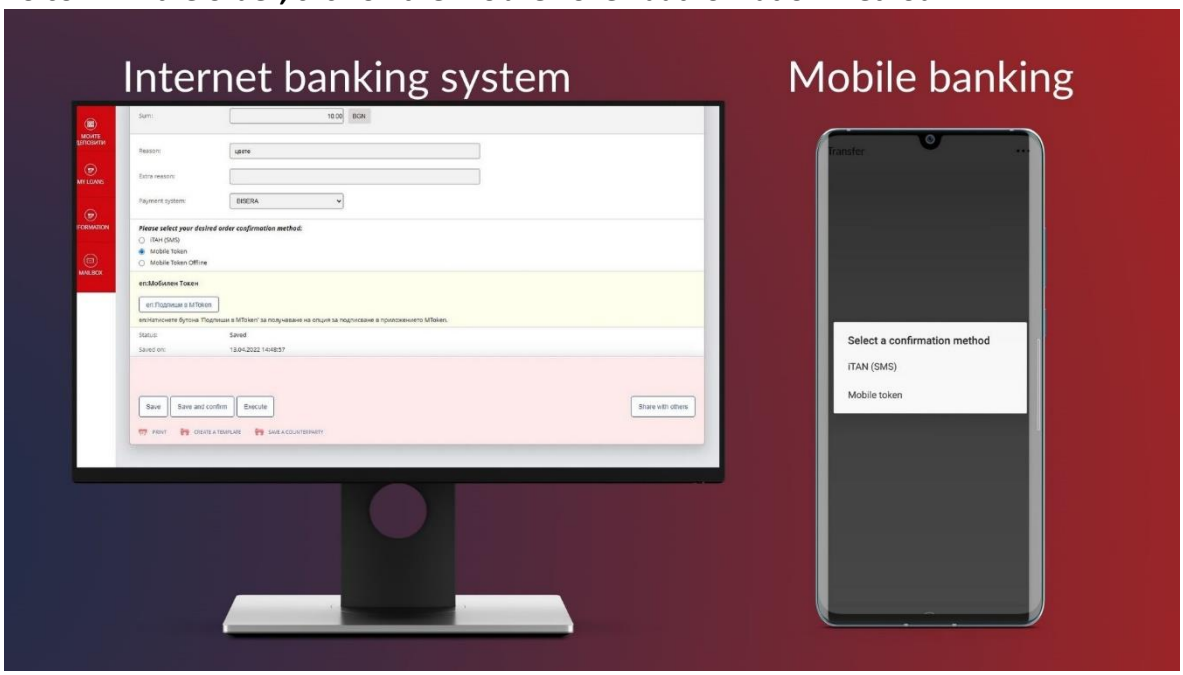
First you need to visit a bank office to get permission to use a Mobile Token for the relevant client.
After obtaining a permission, you can access the Internet Banking and follow the steps referred to in para. 6.1.
To scan the QR code generated in Internet Banking, open the application and press the **Settings** button at the top right. Select the **Registrations** menu and click the **Add New Registration** button and scan. The application will ask you to enter your username.



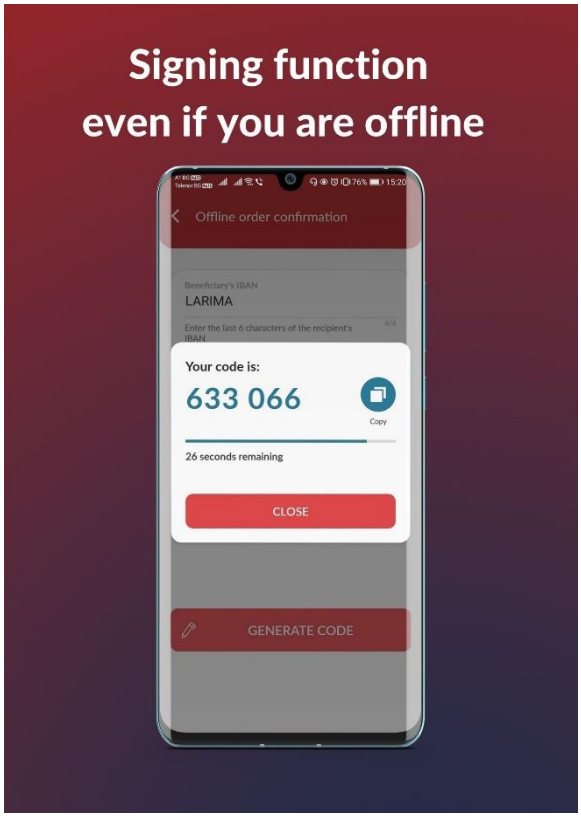
III Order confirmation

1. **Online order confirmation** – with this method you can confirm transfers ordered via Internet Banking and Mobile Banking.

   To confirm the order, click on the Mobile Token authorization method



After selecting this method, you will receive a notification that a confirmation order is waiting for you (if you have allowed notifications to be sent). Open the Ibank mToken application. On the home screen you will see the transfer that you need to confirm. Click the Sign button. Extended information about the ordered transfer will open on the screen. If you want to confirm it, press the Confirm button. The confirmation process is two-factor and the application will require you to enter the login PIN again. After its correct entry, the order is considered confirmed.



If you use the **Ibank mToken** and **Ibank Mobile** mobile applications on one and the same device, they will automatically transfer you to each other.

2. **Offline order confirmation**- offline confirmation is allowed for transfers ordered through the Internet Banking system.

To confirm the transfer, you need to select this option in Internet Banking via **Mobile Token - offline**. Then open the **Ibank mToken** application and select the icon at the top left. 

A screen opens asking you to fill in the last 6 digits of the recipient's IBAN and the exact amount of the transfer. Once you have filled in this information, click the **Generate Code** button. The application will first ask you for a login PIN and then a 6-digit code will be displayed on the screen subject to renewal in every 30 seconds.

The generated code must be entered in the One-Time Password field in Internet Banking.

IV Tips to protect your personal data

1. **Do not submit** confidential information relating to your access to the Internet banking services or your bank card via the Internet or phone.
2. **Lock your mobile device using a digital, graphic or biometric code,** so that you will make sure that even if you lose your device, no one will be able to use your data.
3. **Antivirus Protection** - Viruses can damage your device, destroy data or, in some cases, send personal information or passwords entered during the use of the system by unauthorized persons. The use of reliable and updated antivirus software will reduce the probability of such an adverse event.
4. **Secure Password** - Use secure passwords consisting of a combination of letters, numbers and other characters and do not share them to anybody.
5. **Pay more attention** - Do not leave unattended your personal mobile device to make sure that it is not used by another person without your knowledge!
6. **System log out** - It is essential after you have finished using the service, to close the session by pressing Exit instead of simply close the browser window.