User guide for BKS mToken

July, 2022

BKS Bank

Naše srce kuca za vaše želje.

Content

1. BKS mToken application in general

BKS mToken (SW token) is a service intended for clients who have an open payment account with BKS Bank AG, Main Branch Croatia.

BKS mToken is an application used for digital signing of financial transactions via **Challenge response** and for user authentication when authorizing a purchase transaction at Internet points of sale. It is also used to log in to Internet banking via **OTP** (One Time Password). It is activated by entering a PIN, fingerprint or facial scan (biometrics). The SW token can also be used to auto-create an order initiated by a payment initiation service provider. You can contract the BKS mToken service at any BKS Bank AG branch in Croatia.

1.1. Mobile banking application functionalities:

- Authorization of Internet payments,
- Application for Internet banking,
- Overview of the Bank's branches and ATMs as well as navigation to the selected location,
- Contacts of the Bank,
- Change PIN,
- Biometrics,
- Change the application language,
- Selecting the main authorization device for authorizing Internet payments if you use both BKS Bank AG applications (mBanka and mToken)

1.2. Technical prerequisites for using the BKS mBank application

- Smartphone with mobile platform: Android 4.4.2 or newer and iOS (iPhone) 5.0. or newer;
- For Android the application is available on GooglePlay;
- For iOS the application is available on the AppStore;
- For Huawei the app is available on the AppGalery;
- Internet access with appropriate data tariff

# 2. Working in the BKS mToken application

2.1. Login to the application

After contracting the service in any branch of BKS Bank AG, in Croatia, you will receive an activation key on your mobile device via SMS, by entering and setting your user PIN, the application is ready to work. After setting the user PIN, depending on whether the device supports biometrics, it is possible to set biometrics as a way to log in to the application.
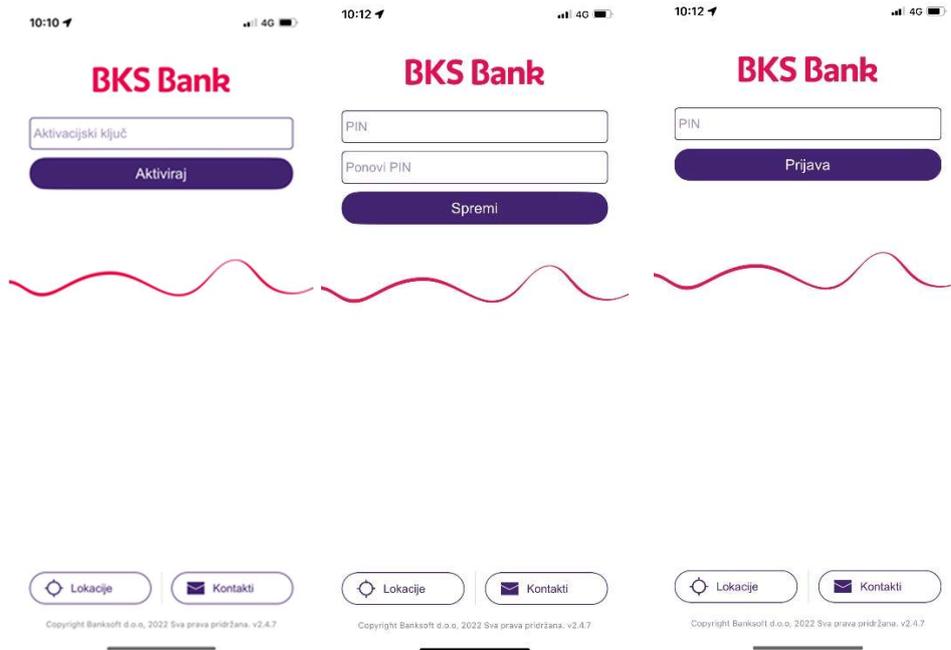
If you enter the wrong PIN to access BKS mToken 3 times in a row, the application will be blocked. In that case, contact your account menager at BKS Bank AG Croatia.

2.2. Home page

After entering the user PIN or logging in via biometrics, the homepage opens:
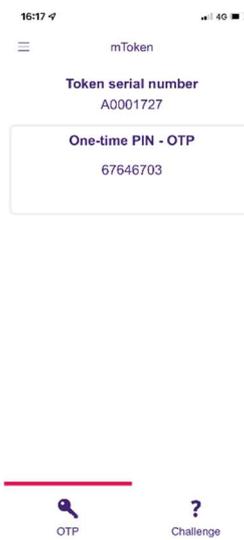
The home page contains information of the serial number of the token and the automatically generated **APPLI 1 (One-time PIN - OTP)**. The displayed One-Time PIN - OTP is used when logging in to electronic banking.
In the lower left corner of the screen there is an option to generate a new OTP. The new OTP (APPLI 1) can also be generated by clicking on the existing APPLI 1.

In the lower right corner of the screen there is an option to enter the **challenge set** by the electronic banking application when authorizing the execution of orders. There is a menu icon in the upper left corner.

2.3. Creating a response to a challenge

Pressing the "Challenge" button opens the screen for entering the challenge set by the e-electronic banking application when authorizing the execution of the order.
You need to enter the number you will receive in the electronic banking application and press the unlocked padlock icon (🔓).
When you enter the challenge (default number) and press the padlock icon, the answer you need to enter in the electronic banking will be generated. After entering the answer, the order is authorized.
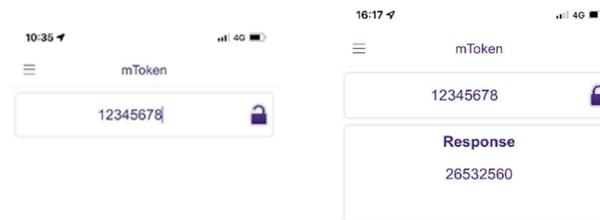

Enter of challenge

Response (APPLI 2)

2.4. Menu

Clicking on the icon in the upper left corner displays a menu with the following options:

- mToken - option to generate OTP and respond to the received challenge.
- Locations - display of data on ATMs and bank branches.
- Contacts - view information on how to contact the bank.
- Settings - change the application language, change the PIN, Select the main author-ization device, and Select the biometric authorization
- Logout - logout from the application
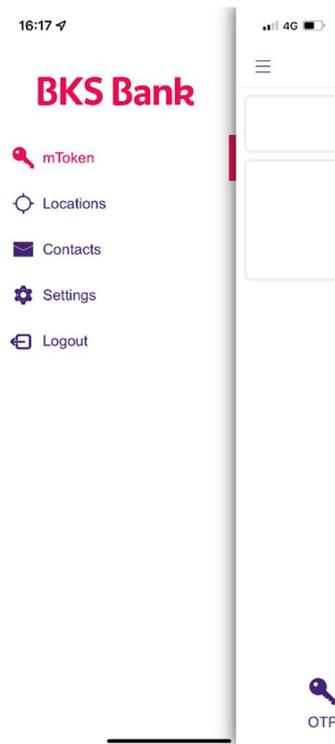
Menu display

2.5. Locations

The application shows on the map your current location, the location of BKS Bank Main Branch Croatia and ATMs BKS Bank Main Branch Croatia as well as ATMs from the EGCP network. Selecting navigation apps will guide you from your current location to your chosen ATM or branch.

2.6. Contacts

Contacts and e-mail address of BKS Bank AG, Main Branch Croatia are displayed with the possibility of direct calling / sending e-mail.

2.7. Settings

In the settings it is possible to change the PIN, choose between Croatian and English, change the e-mail address, set biometrics and select the main authorization device for authorizing Internet payments if you use both BKS Bank AG applications (mBanka and mToken).

2.8. Internet payment authorization

If you have a debit and / or credit card BKS Bank AG, Main Branch Croatia, the authorization of Internet payments can be done via mToken application. In order for this option to be possible, it is necessary to **allow the mToken application to send you notifications**. After all the necessary data has been entered on the online store, the **"Authorization Request"** notification arrives in the mToken application. After opening the notification, the login screen for the mToken application automatically opens. After logging in, a screen appears on which it can be chosen whether the card transaction will be approved or rejected. Depending on the selected option, the authorization of the Internet payment is completed.
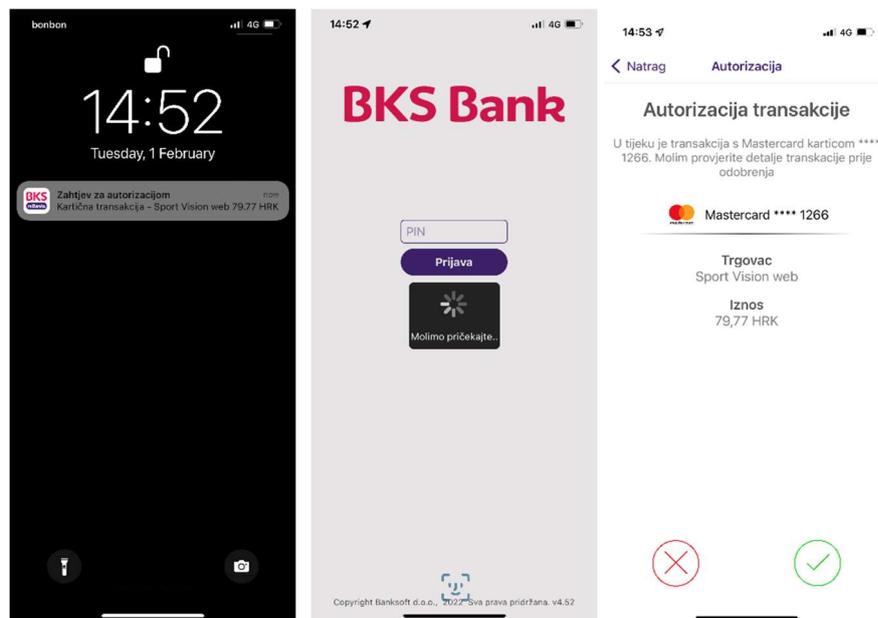
3. Log out of the application and user guide

If you use BKS mToken on the Android platform, you can log out of the application by pressing the back button. If you exit the application by pressing the home button, it will still be active until you log out automatically.

If you use the iOS platform to access the BKS mToken application, you can log out by clicking the Unsubscribe option. If you exit the application by pressing the home button, it will still be active until you log out automatically.

In case of user inactivity after 5 minutes, the automatic logout of the application is started.

Instructions for the use of the application and fees for the execution of payment orders are regulated by the Bank's Tariff and are published in the Bank's branches and on the Bank's website www.bks.hr.

4. Security of using the application and changing the mobile device

All communication between the mobile device and the application server gateway is protected using SSL / TLS encrypted protocol.

Access to all functionalities in the mToken application is via a secure channel. The user logs in to the application with the selected PIN when launching the application for the first time, or via biometrics if the mobile device supports it. Connecting the mToken to your smartphone and phone number (possession factor) and accessing the application by free choice of PIN (knowledge factor) or fingerprint / face scan (biometric authentication) are two components that provide 2 factor authentication according to PSD2 (Directive on payment service 2), RTS (Regulatory Technical Standards) and SCA (Strong Customer Authentication).
In case the user enters an incorrect PIN three times, the mToken service will be blocked. In case of inactivity of the application, the user will be automatically logged out of the system.

In case losing a mobile phone or suspicion of misuse of the PIN, the user is obliged to inform the Bank as soon as possible and request a blockade of the service. The user bears all damage that may occur due to loss, theft or any other unauthorized or improper use of the mobile device.

BKS mToken service is related to the phone number and mobile device on which the application is installed and the activation key is entered. **When changing the phone number or mobile device, it is necessary to ask the Bank to reactivate the service.**

5. Contact information

Our HelpDesk support is at your service on weekdays from 8:00 to 16:00.

BKS Bank AG,   **BKS mToken:**
Glavna podružnica Hrvatska   www.bks.hr
Mljekarski trg 3   podrskaplatni@bks.hr
51 000 Rijeka   0800/257-257