INTESA SANPAOLO BANK

Card mToken
User Guide

mToken

Version 2 – 02 2021

CONTENTS

1. What is Card mToken application and what it's good for?

Card mToken is an application that can be used to confirm online transactions performed with any bank card issued by Intesa Sanpaolo Bank Romania.

This application is a faster and friendlier alternative to the physical token (3D Secure token), which you need to always remember to take with you to complete payments through **3D Secure.** Once installed, Card mToken will send a notification to your phone to sign transactions performed in online stores.

The two ways to confirm transactions will work in parallel, so you can choose what's easier for you.

The application is available on phones (or tablets) that benefit from the following operating systems: Android 6.0 and newer or iOS 11.0 and newer.

To benefit from the entire experience and the high level of security of signing transactions using the Card mToken application, your mobile device used needs to benefit from biometric authentication methods (print, facial recognition, retinal scan etc.).

Attention: There is a possibility that certain Android devices, which have biometric methods implemented, are not active or don't work with the Card mToken application, these devices having proprietary biometric authentication systems that are not shared with other developers. This does not mean you will not be able to use the application, but only that when you install the application the biometrics must be uninstalled.

You can download the **Intesa Sanpaolo Bank Card mToken** application here:

GET IT ON Google Play

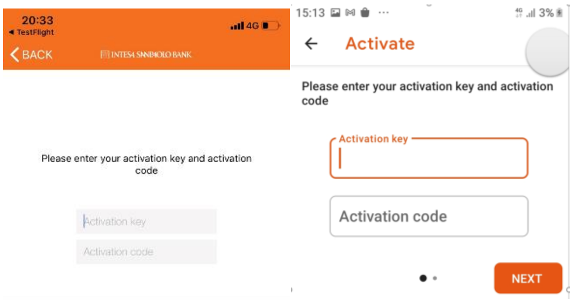
Download on the App Store

2. Activation of Card mToken application

Enrollment in the application is done by phone, free of charge at the phone number **0 800 800 888** or **+40 372 712 194**. After you have been identified by Call Center advisers, you will receive by phone an **Activation Key** and by SMS, at the phone number with which you are registered with the bank's systems, an **Activation Code**.

ATTENTION! For the moment you may activate the application on a single phone.

Examples of device enrollment screen (iOS & Android)



Please enter your activation key and activation code

Activation key

Activation code

Please enter your activation key and activation code

Activation key

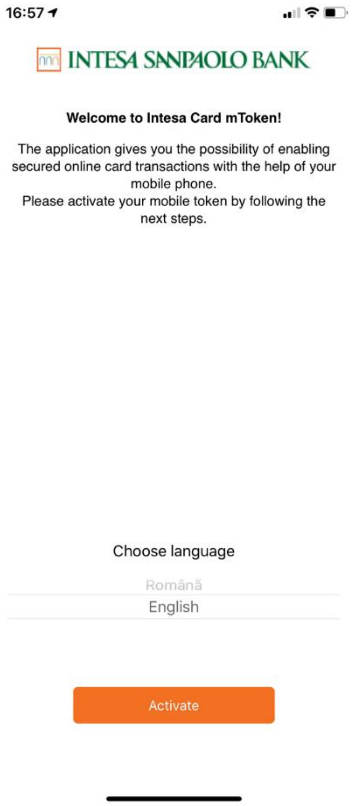
Activation code

The activation code sent by SMS is sent from the phone number **+40 371 700 200** and is an alphanumeric code (*e.g.: 06e28749f6*).

ATTENTION! The generated codes have a validity of 15 minutes and it does not matter if they are written in uppercase or lowercase.

We recommend to carefully follow the steps in the application.

a. Apple iOS phone enrollment



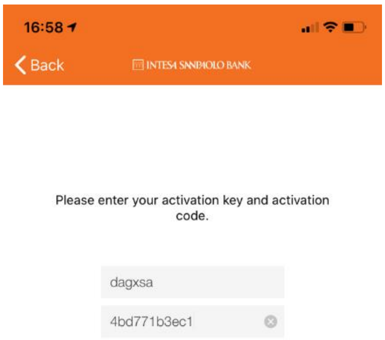
Welcome to Intesa Card mToken!

The application gives you the possibility of enabling secured online card transactions with the help of your mobile phone.
Please activate your mobile token by following the next steps.

Choose language

Română
English

Select the language you want to use in the application.



Please enter your activation key and activation code.

dagxsa

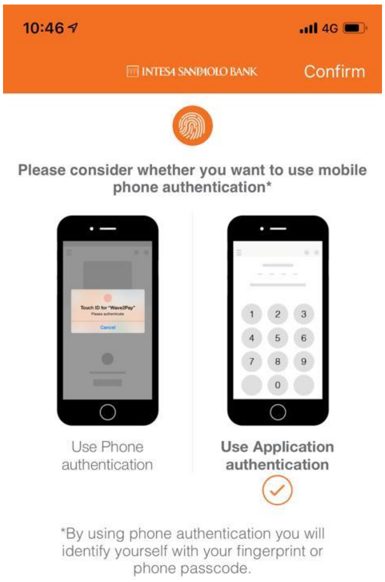
4bd771b3ec1

In the first field fill in the *Activation Key* sent by phone by the Call Center adviser and then the *Activation Code* automatically sent by SMS on the phone number registered in the system.

Error 1500 will appear if you entered incorrectly the activation key or activation code.

Error 2001 will appear if you use an expired activation code or activation key, which exceeded the 15 minutes. In this situation you need to request the Call Center advisers to regenerate the activation codes.

ATTENTION! The activation keys and codes are unique and they cannot be reused.

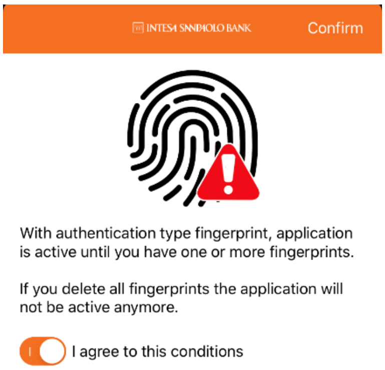


Please consider whether you want to use mobile phone authentication*

*By using phone authentication you will identify yourself with your fingerprint or phone passcode.

You have the possibility to use authentication with biometrics (fingerprint or Face ID, according to the device), or you can define a 4-digit PIN.

ATTENTION! For safety of online payments, we recommend using biometric authentication.

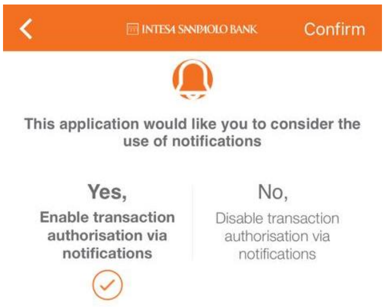


With authentication type fingerprint, application is active until you have one or more fingerprints.

If you delete all fingerprints the application will not be active anymore.

I agree to this conditions

Once biometric authentication is selected, the device will request a confirmation regarding the conditions of use of the application.



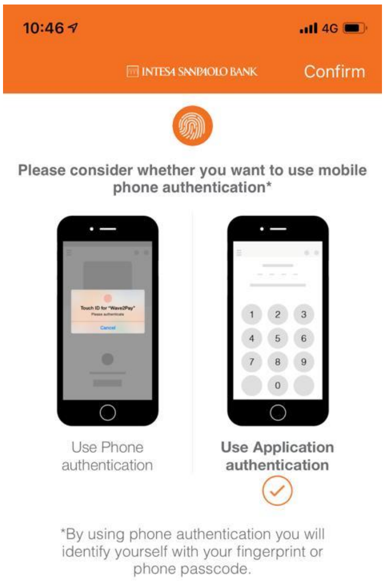
This application would like you to consider the use of notifications

Yes, Enable transaction authorisation via notifications ✓

No, Disable transaction authorisation via notifications

To receive in real time notifications on the confirmation of online card transactions, you will need to make sure that notifications are active.

ATTENTION! If by accident at the time of enrollment you select that you don't want to be notified by the application, and then you change your mind, then you have the possibility to activate the notifications in the device's settings: *Settings > Notifications > Card mToken > Allow Notifications*



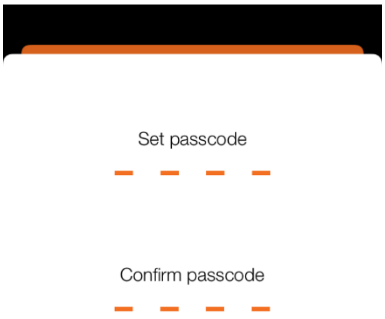
Please consider whether you want to use mobile phone authentication*

Use Phone authentication

Use Application authentication ✓

*By using phone authentication you will identify yourself with your fingerprint or phone passcode.

If you don't want the use or the device is not provided with biometric authentication, then you will be redirected to the screen of authentication by PIN code.



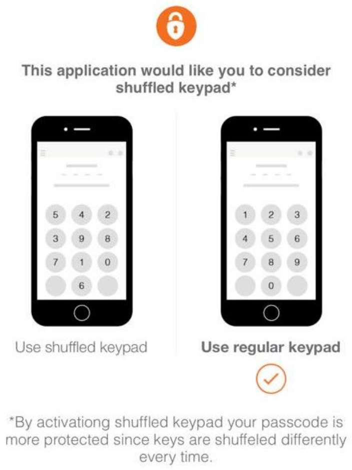
Set passcode

_ _ _ _

Confirm passcode

_ _ _ _

Following confirmation, you will need to set and confirm a 4-digit password.

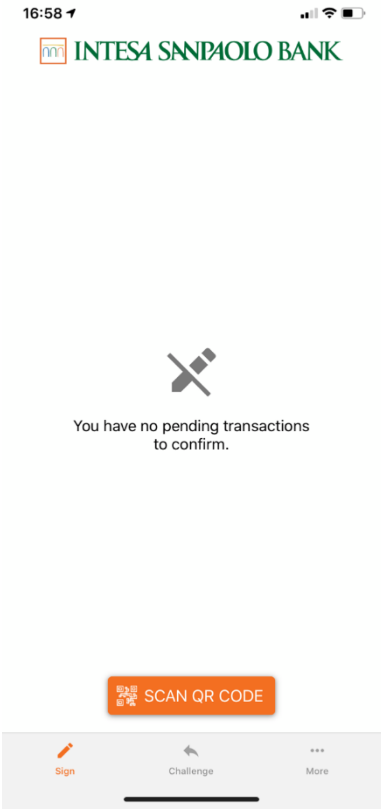


This application would like you to consider shuffled keypad*

*By activationg shuffled keypad your passcode is more protected since keys are shuffeled differently every time.

For increased security, you have the possibility to select that the digits in the PIN keypad to be shuffled each time you need to enter the authentication code.

ATTENTION! If this option is selected, please be very careful when you enter the PIN code.

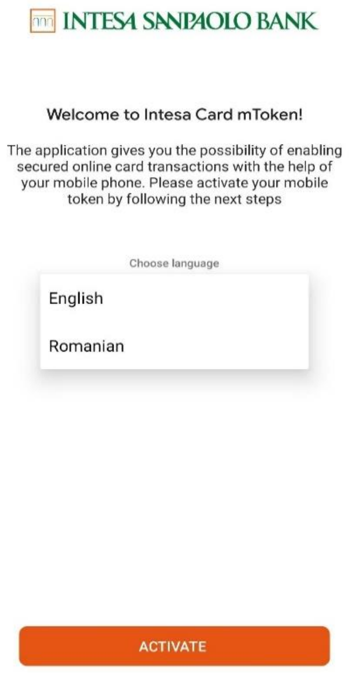


16:58

You have no pending transactions to confirm.

CONGRATULATIONS! If you reached this screen, it means that enrollment was successful and from this moment you can perform online card transactions, which will automatically appear here.

b. Android phone enrollment



INTESA SNNPAOLO BANK

Welcome to Intesa Card mToken!

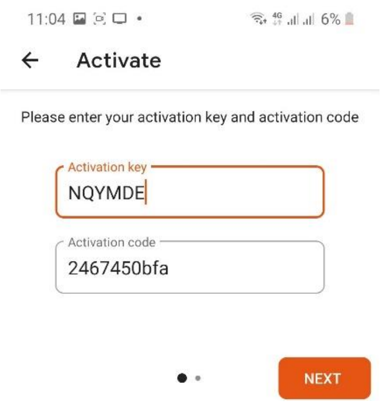
The application gives you the possibility of enabling secured online card transactions with the help of your mobile phone. Please activate your mobile token by following the next steps

Choose language

English

Romanian

Select the language you want to use in the application



11:04 6%

Activate

Please enter your activation key and activation code

Activation key: NQYMDE

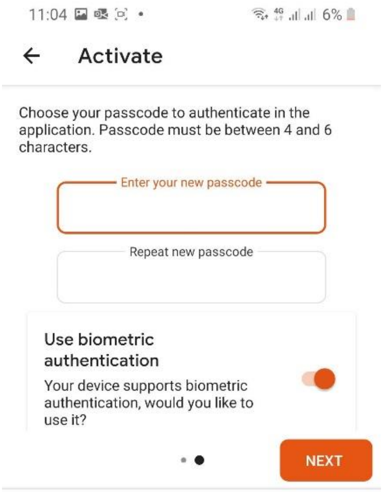
Activation code: 2467450bfa

In the first field fill in the *Activation Key* sent by phone by the Call Center adviser and then the *Activation Code* automatically sent by SMS on the phone number in the system.

Error 1500 will appear if you entered incorrectly the activation key or activation code.

Error 2001 will appear if you use an expired activation code or activation key, which exceeded the 15 minutes. In this situation you need to request the Call Center colleagues to regenerate the activation codes.

ATTENTION! The activation keys and codes are unique and they cannot be reused.



11:04 6%

Activate

Choose your passcode to authenticate in the application. Passcode must be between 4 and 6 characters.

Enter your new passcode

Repeat new passcode

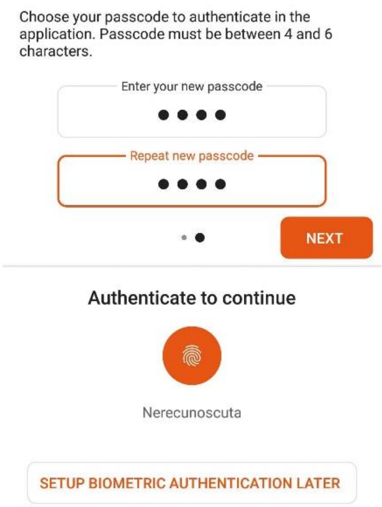
Use biometric authentication

Your device supports biometric authentication, would you like to use it?

NEXT

In this step, you will need to define a password consisting of 4 characters and you have the option to select to use biometric authentication (fingerprint, retinal scan or facial recognition, depending on the device).

ATTENTION! For safety of online payments, we recommend using biometric authentication.



Choose your passcode to authenticate in the application. Passcode must be between 4 and 6 characters.

Enter your new passcode ●●●●

Repeat new passcode ●●●●

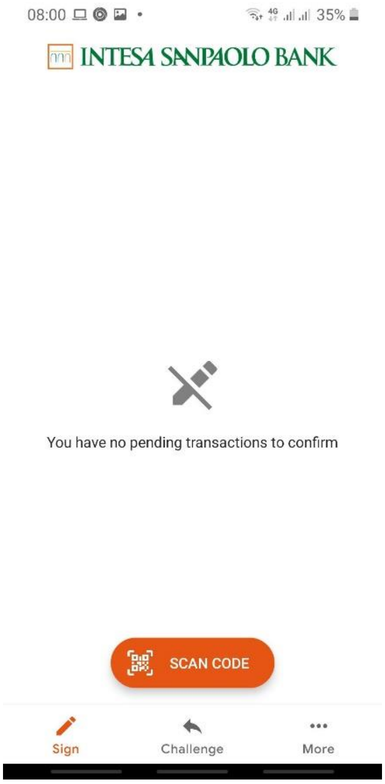
NEXT

Authenticate to continue

Nerecunoscuta

SETUP BIOMETRIC AUTHENTICATION LATER

Once biometric authentication is selected, the device will request a confirmation on the user conditions of the application.



08:00 35%

INTESA SANPAOLO BANK

You have no pending transactions to confirm

SCAN CODE

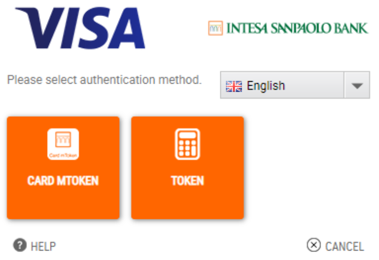
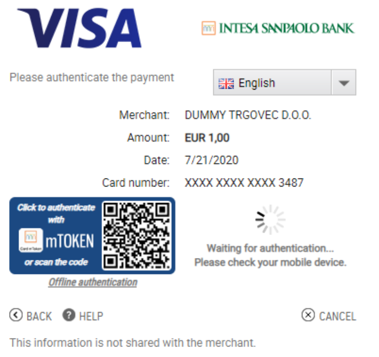
Sign Challenge More

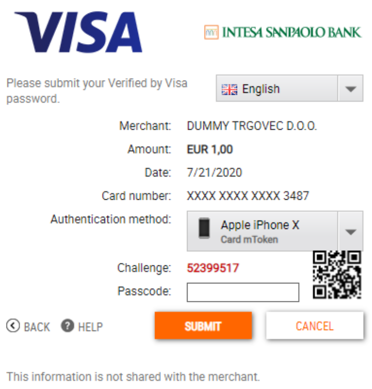
CONGRATULATIONS! If you reached this screen, it means that enrollment was successful and from this moment you can perform online card transactions, which will automatically appear here.

3. Authorization of transactions

Please follow carefully the steps in the payment platform, to make sure that you authorize the desired transaction.

a. Payment page (3D Secure)

 VISA INTESA SANPAOLO BANK English CARD MTOKEN TOKEN HELP CANCEL Please select authentication method.	When you make the payment, after you fill in the card details, to sign the transaction you will be redirected to the 3D Secure page. Here you have the possibility to select the method through which you wish to authorize the online transaction. You can do it through the Card mToken application, and also by using the 3D Secure Token (Hard Token), as we mentioned at the beginning of this guide. ATTENTION! If you don't see both buttons, it means that one of the options for authorizing transactions is not available.
 VISA INTESA SANPAOLO BANK English Click to authenticate with mTOKEN or scan the code Offline authentication BACK HELP CANCEL Please authenticate the payment Merchant: DUMMY TRGOVEC D.O.O. Amount: **EUR 1,00** Date: 7/21/2020 Card number: XXXX XXXX XXXX 3487 Waiting for authentication... Please check your mobile device. This information is not shared with the merchant.	For authorizing the transaction using the Card mToken application, you will receive an automatic notification on the mobile device on which you have the application installed and enrolled and where you will have to sign (authorize) it. At the end of the transaction, if it is successfully confirmed, you will receive a message of confirmation and be redirected to the page of the online store. ATTENTION! If you did not receive the automatic notification (lack of data connection or other technical issues), you have the possibility to sign manually the transaction by scanning with the Card mToken application the QR code displayed and accessing in the Card mToken application the *Code Generation* menu following precisely the steps in the application.



Please submit your Verified by Visa password.

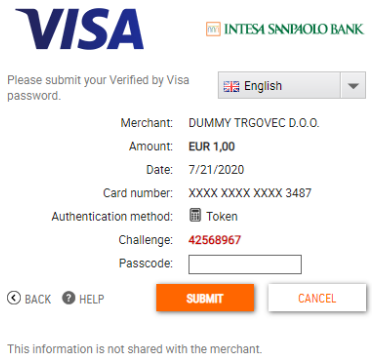
English

Merchant: DUMMY TRGOVEC D.O.O.
Amount: EUR 1,00
Date: 7/21/2020
Card number: XXXX XXXX XXXX 3487
Authentication method: Apple iPhone X Card mToken
Challenge: 52399517
Passcode:

This information is not shared with the merchant.

Additionally, if you did not receive the notification and you failed to scan the QR code, you may authorize the transaction manually using the *Challenge / Response* method and you will need to follow the steps in the *Code Generation* menu in the Card mToken application and then confirm the code of the transaction in the 3D Secure page.

At the end of the transaction, if it is successfully confirmed, you will receive a message of confirmation and be redirected to the page of the online store.



Please submit your Verified by Visa password.

English

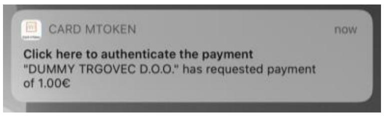
Merchant: DUMMY TRGOVEC D.O.O.
Amount: EUR 1,00
Date: 7/21/2020
Card number: XXXX XXXX XXXX 3487
Authentication method: Token
Challenge: 42568967
Passcode:

This information is not shared with the merchant.

If you want to use the Hard Token, then you will enter the card with which you make the payment into the Hard Token device, press the *BUY* button, enter the PIN of the card and then follow the steps described on the device screen and correlate them with the messages generated in the 3D Secure page.

At the end of the transaction, if it is successfully confirmed, you will receive a message of confirmation and be redirected to the page of the online store.

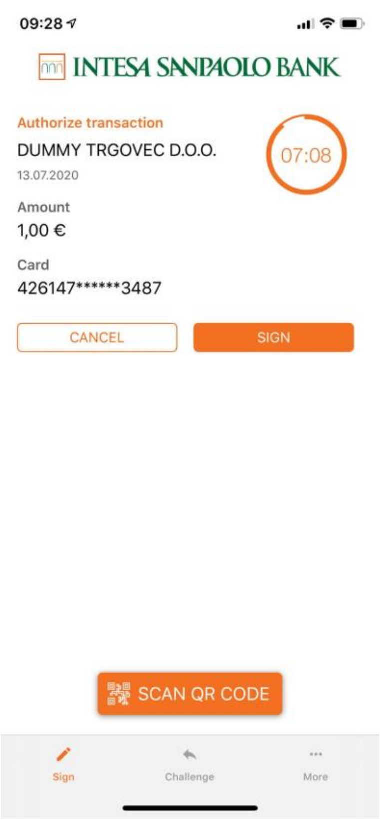
b. Authorization of transactions in Apple iOS



Click here to authenticate the payment
"DUMMY TRGOVEC D.O.O." has requested payment of 1.00€

When you make the payment, to authorize the transaction you will automatically receive on the mobile device a notification that you may access to be redirected in the Card mToken application.

ATTENTION! If you haven't received the message automatically or maybe you have deleted it by mistake, access the application and the transaction will appear automatically on the first screen.



Authorize transaction

DUMMY TRGOVEC D.O.O.

13.07.2020

Amount

1,00 €

Card

426147******3487

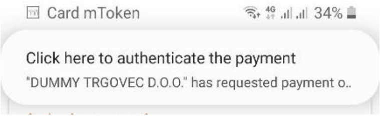
After you have opened the application, the transaction will be displayed on the first screen. You have the possibility to sign it or cancel it.

You will sign the transaction using the biometric confirmation (fingerprint or FaceID) or the PIN of the application, according to the option selected by you upon enrollment.

Once signed, you will receive a confirmation message in the application, as well as a message in the 3D Secure page, where you entered the transaction confirmation data.

ATTENTION! The transaction has a signing deadline of 10 minutes - after this term, if it is not confirmed or refused, it will be automatically cancelled.

c. Authorization of transactions in Android OS



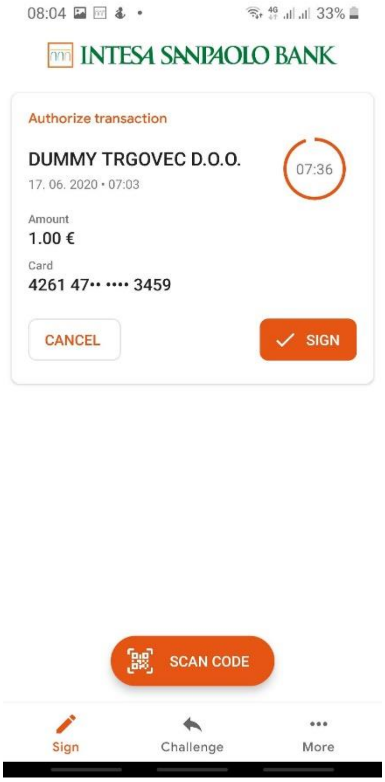
Card mToken 34%

Click here to authenticate the payment

"DUMMY TRGOVEC D.O.O." has requested payment o..

When you make the payment, to authorize the transaction you will automatically receive on the mobile device a notification that you may access to be redirected in the Card mToken application.

ATTENTION! If you haven't received the message automatically or maybe you have deleted it by mistake, you may access the application and the transaction will appear automatically on the first screen.



08:04 33%

INTESA SNNPAOLO BANK

Authorize transaction

DUMMY TRGOVEC D.O.O.

17. 06. 2020 • 07:03

07:36

Amount

1.00 €

Card

4261 47•• •••• 3459

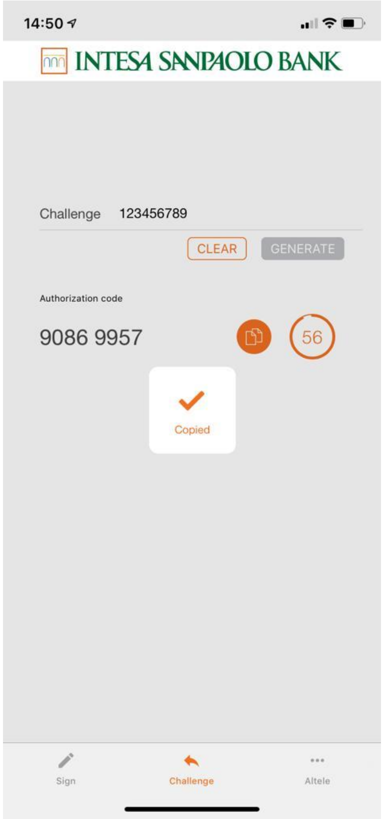
After you have opened the application, the transaction will be displayed on the first screen. You have the possibility to sign it or cancel it.

You will sign the transaction using the biometric confirmation (fingerprint, retinal scan or face recognition) or the PIN of the application, according to the option selected by you in the application.

Once signed, you will receive a confirmation message in the application and a message in the 3D Secure page, where you entered the transaction confirmation data.

ATTENTION! The transaction has a signing deadline of 10 minutes - after this term, if it is not confirmed or refused, it will be automatically cancelled.

d. Other ways to authorize transactions in Apple iOS



Challenge 123456789

Authorization code

9086 9957

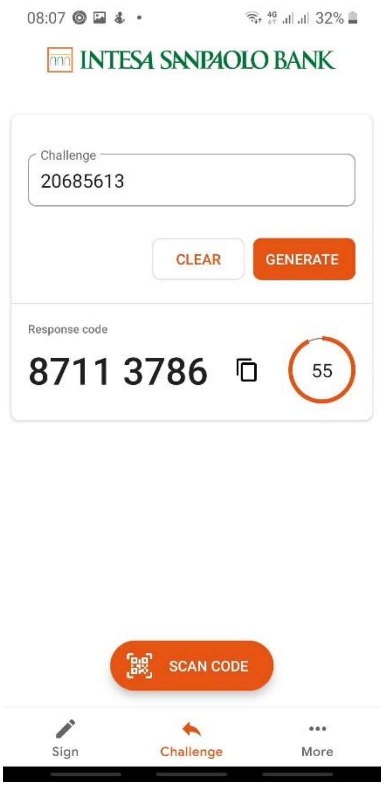
If you haven't received the notification and failed to scan the QR code, you may authorize the transaction manually using the *Challenge / Response* method and you will need to follow the steps in the *Code Generation* menu in the Card mToken application and then confirm the code of the transaction in the 3D Secure page.

You will fill in in the *Verification Code* field the code displayed in the 3D Secure page, generate the *Authorization Code*, which you will enter in the field that must be completed in the 3D Secure page.

At the end of the transaction, if it is successfully confirmed, you will receive a message of confirmation and be redirected to the page of the online store.

ATTENTION! The generated code has a signing deadline of 60 seconds - if you fail to confirm it in this period, the code will have to be regenerated in the application.

e. Other ways to authorize transactions in Android OS



Challenge
20685613

Response code

8711 3786

If you haven't received the notification and failed to scan the QR code, you may authorize the transaction manually using the *Challenge / Response* method and you will need to follow the steps in the *Code Generation* menu in the Card mToken application and then confirm the code of the transaction in the 3D Secure page.

You will fill in in the *Verification Code* field the code displayed in the 3D Secure page, generate the *Authorization Code*, which you will enter in the field that must be completed in the 3D Secure page.

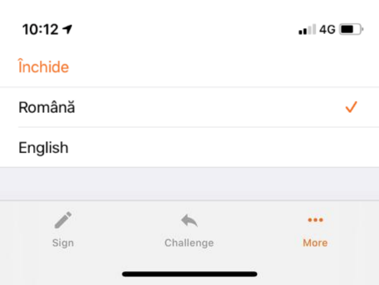
At the end of the transaction, if it is successfully confirmed, you will receive a message of confirmation and be redirected to the page of the online store.

ATTENTION! The generated code has a signing deadline of 60 seconds - if you fail to confirm it in this period, the code will have to be regenerated in the application.

4. Select language

If you are tired of the language you have selected upon enrollment, you have the possibility to change it.

iOS



10:12

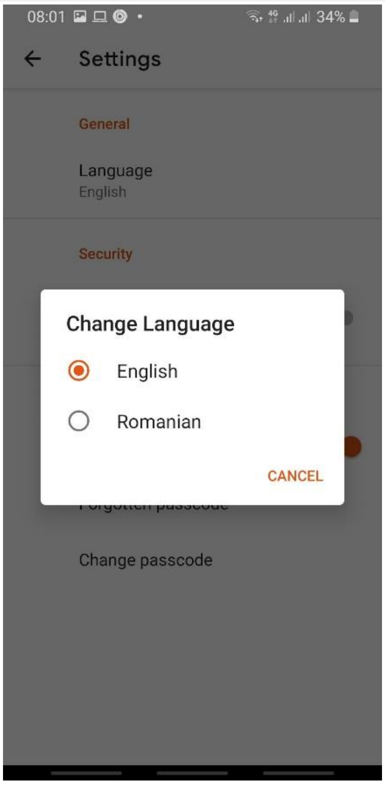
Închide

Română ✓

English

In the *Other* menu you may select another language instead of the one you already have. Once you save it, when you will restart the application you can use your new selection.

Android



08:01 34%

Settings

General

Language
English

Security

Change Language

● English

○ Romanian

CANCEL

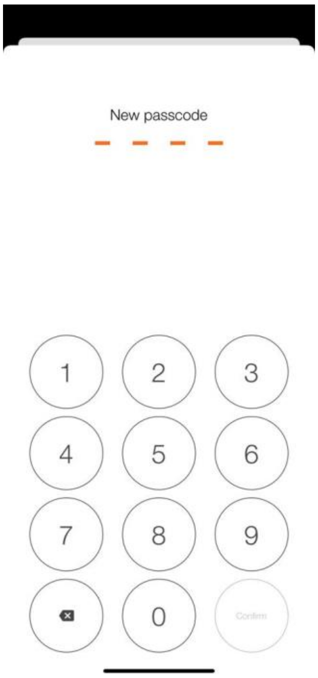
Change passcode

In the *Settings* section you may select another language instead of the one you already have. Once you save it, when you will restart the application you can use your new selection.

5. Password change

If you want to change your password, here's how you can do it in the application:

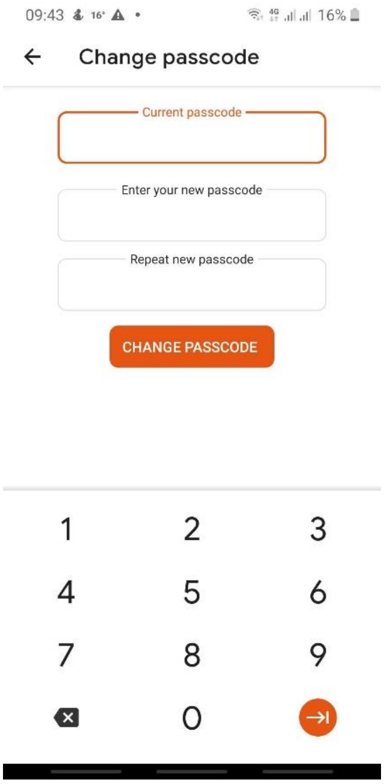
iOS



If you wish to replace the initially defined password, you can do it in the *Other* menu in the *Change the password* section. Initially you will enter the existing password, then the new password and its confirmation.

ATTENTION: If upon enrollment in the application you selected biometrics as a way of authentication, the *Change the password* section is only available after deactivating the biometrics.

Android

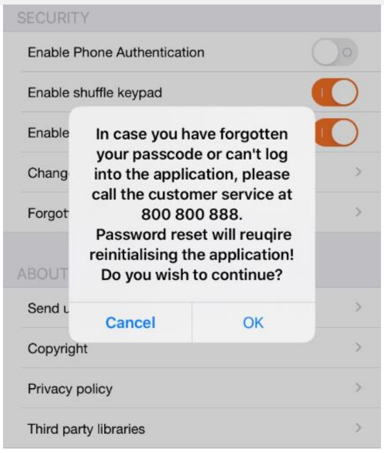


If you wish to replace the initially defined password, you can do it in the *More* menu, the *Settings* section, in the Authentication section by pressing *Change the password*. Initially you will enter the existing password, then the new password and its confirmation.

6. Password reset

If you wish to reset the existing password because you forgot it, it's very easy:

iOS



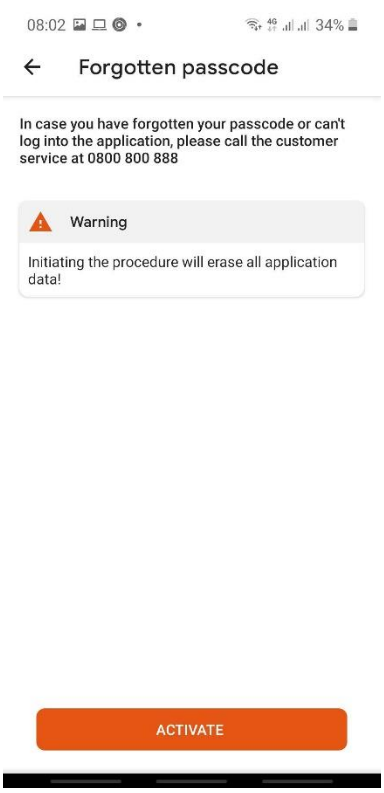
In case you have forgotten your passcode or can't log into the application, please call the customer service at 800 800 888. Password reset will reuqire reinitialising the application! Do you wish to continue?

If you forgot the initially defined password and wish to define a new password, you can do it in the *Other* menu, at the *You forgot the password* section.

Please note that the application will be reinitialized and you will need to contact us to receive a new set of *Authorization Key & Code*.

This procedure will also be used if you receive a message that the application has been out of sync.

Android



In case you have forgotten your passcode or can't log into the application, please call the customer service at 0800 800 888

Initiating the procedure will erase all application data!

If you forgot the initially defined password and wish to define a new password, you can do it in the *More* menu, *Settings* section, in the *Authentication* section, by pressing *Forgotten password.*

Please note that the application will be reinitialized and you will need to contact us to receive a new set of *Authorization Key & Code.*

This procedure will also be used if you receive a message that the application has been out of sync.

____//____