



VISTA BANK

#faster

VISTA 3D SECURE

You make card online payments
easy and strictly secure
with biometric authentication

TOGETHER WE ARE STRONGER



**Vista 3D Secure
User Manual**



Contents

I. Vista 3D Secure mobile application	3
A. Registration.....	3
B. Using Vista 3D Secure for e-commerce authentication	6
C. Other features offered by Vista 3D Secure.....	9
II. Static password and SMS (one time password) authentication	10
A. Registration.....	10
B. Authorization of transactions after registration.....	12
C. Change password.....	12
D. Forgot your password.....	13
III. Troubleshooting	14

I. Vista 3D Secure mobile application

The **Vista 3D Secure** mobile application is compliant with the latest security standards in the field, ensuring you better protection when making transactions with online merchants.

The new legislative regulations for electronic payments require, among others, the use of Strong Customer Authentication (SCA) when conducting online card transactions in the European Economic Area. More information about the new legislative framework can be found on our website, [here](#).

Strong Customer Authentication (SCA) in the case of online card payments (online payment at merchants / e-commerce payment) means that the identity of cardholders must be more strictly verified in the European Economic Area, using two of the three authentication methods presented below:

- Authentication methods based on **knowledge** (something only the customer knows): for example, password or PIN
- Authentication methods based on **possession** (something only the customer has): for example, a mobile device (smartphone, tablet) or other physical authentication device
- Authentication methods based on **inherence** (something the customer is): for example, digital fingerprint or facial recognition (biometric authentication).

Vista 3D Secure meets the new requirements, being a SCA compliant mobile application, certified by VISA International for the VISA Secure protocol and using:

- two **authentication factors** , the first based on **possession** (the application installed on a mobile device identified as being in the customer's possession at the enrollment stage, based on the phone number registered at the bank and the last 6 digits of the card, application that automatically generates a OTP unique code (one time passcode) for authorizing each transaction), and the second based on **inherence** (confirmation of the transaction by digital fingerprint / facial recognition) or **knowledge** (mobile phone security code).
- **dynamic correlation protocol**, a security measure by which you are informed on a second communications channel (in the Vista3D Secure application installed on your smartphone / tablet) about payment details (merchant name and payment amount) in the payment confirmation phase (to allow you to decide whether or not to authorize the respective online card payment)..

Since Vista Bank had already a 3D-Secure solution with dynamic correlation via SMS previously implemented, authentication through the Vista 3D Secure application will seem largely familiar to you. In short, the Vista 3D Secure mobile app will replace previous 3D Secure SMS authentication for customers who install their Vista 3D Secure app on an Android or iOS smartphone / tablet.

Note: The Bank does not process biometric data (digital fingerprint, facial recognition). This verification, part of the SCA, is performed strictly at the level of the user's mobile device (smartphone, tablet), the bank not having access to this data.

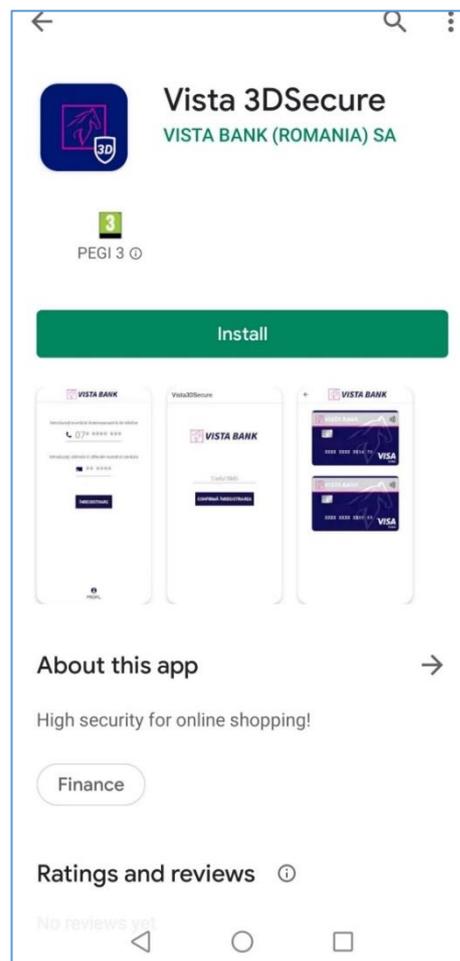
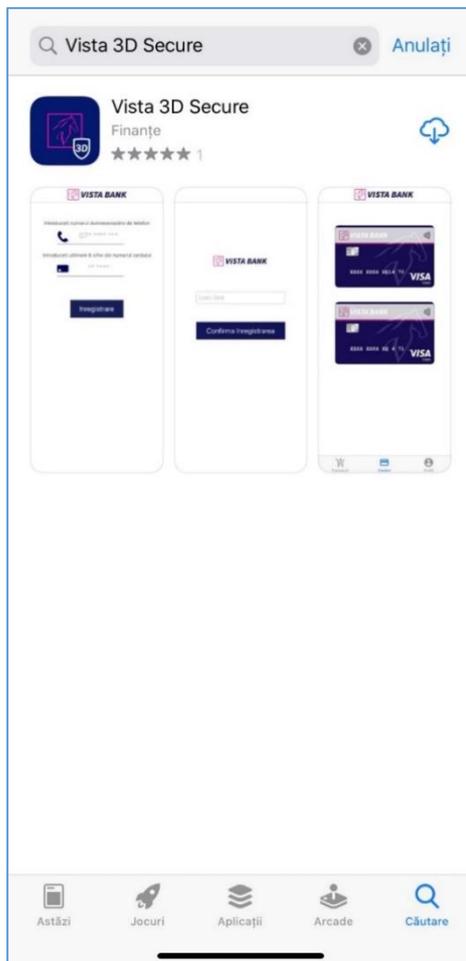
Next, we will describe the steps for installing, registering, and using Vista 3D Secure.

A. Registration

1. Set up a method of securing your smartphone/tablet on which Vista 3D Secure application is going to be installed (fingerprint, facial recognition or security code).

We recommend not allowing access to your mobile device to other people who could authorize payments in your behalf.

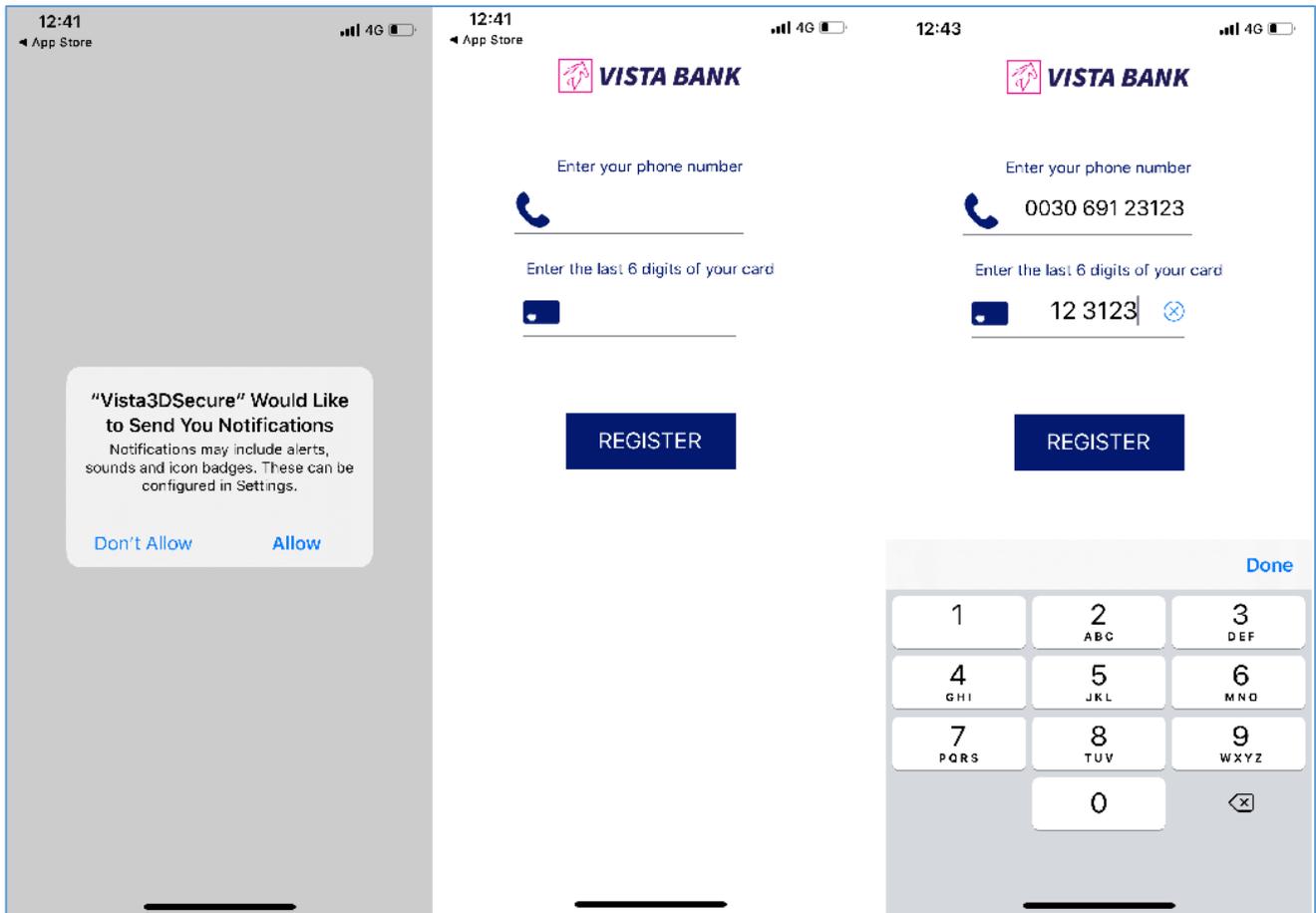
2. Download free of charge the Vista 3D Secure mobile app from the App Store (iOS) or Google Play Store (Android) on your smartphone/tablet.



3. Enter in the mobile application the valid mobile phone number (country code + phone number) registered with the Bank and the last 6 digits of the Vista Bank card number.

Important: Before registering, make sure that you have updated your personal data with Vista Bank, including the mobile phone number.

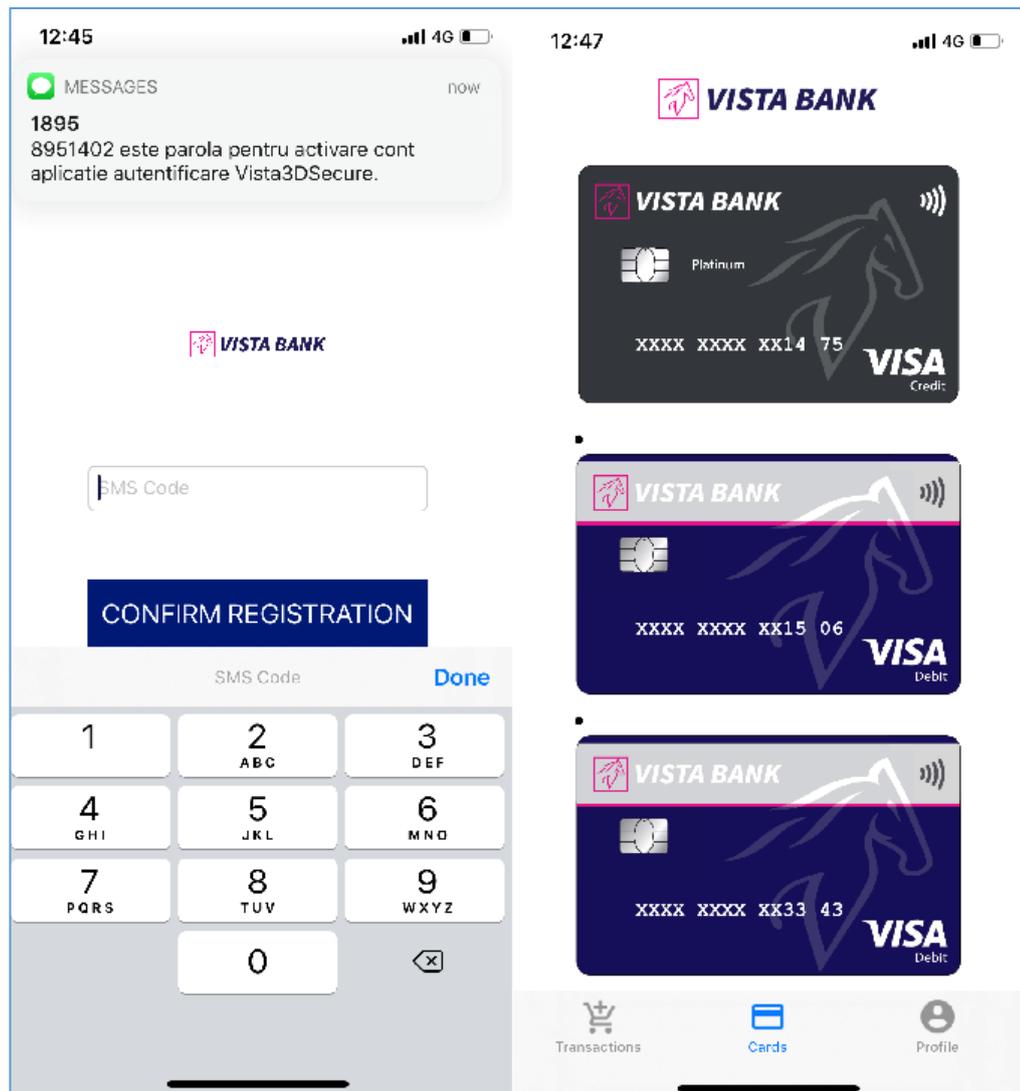
4. Allow notifications from the app: during an e-commerce transaction, you will receive a “Push” notification via Vista 3D Secure application to confirm the payment.



- You will receive on your mobile phone a unique, automatically generated SMS code. Enter this SMS code in the mobile application in the "SMS code" field.

Notes:

- If you receive an error message or you don't receive the SMS code please contact us (+4021 222 33 10/ info@vistabank.ro) because it's possible that your personal data isn't updated with the Bank.
- If you received a SMS message (without knowing that you tried to register your card in the Vista 3D Secure application), notify the Bank immediately!



Registration is complete! The above steps will be performed only once, when registering into the application.

Note: If you have more than one card at Vista Bank, all your cards will be automatically enrolled in the application upon completion of registration according to the steps above. Supplementary cards will have to be registered separately by the cardholder using his mobile device/telephone number.

B. Using Vista 3D Secure for e-commerce authentication

1. Access the merchant's website to buy goods or services, add the products in the cart and choose payment by card. We recommend that you make sure that the "Visa Secure" or "Verified by Visa" logo appears on the merchant's website, which means that payment will be authorized by you through 3D-Secure.
2. In the payment page enter the data requested by the merchant: card number, name on the card, CVV2 code, expiration date.

3. You will receive a "Push" notification through the mobile phone application.

Important: The transaction cannot be performed without a valid mobile phone number registered with the Bank. Make sure your personal data is up to date with Vista Bank, including your mobile phone number. Also, you need to be connected to the Internet on your smartphone/tablet when using the application.

4. Tap the received notification and you will be redirected to the Vista 3D Secure mobile application.

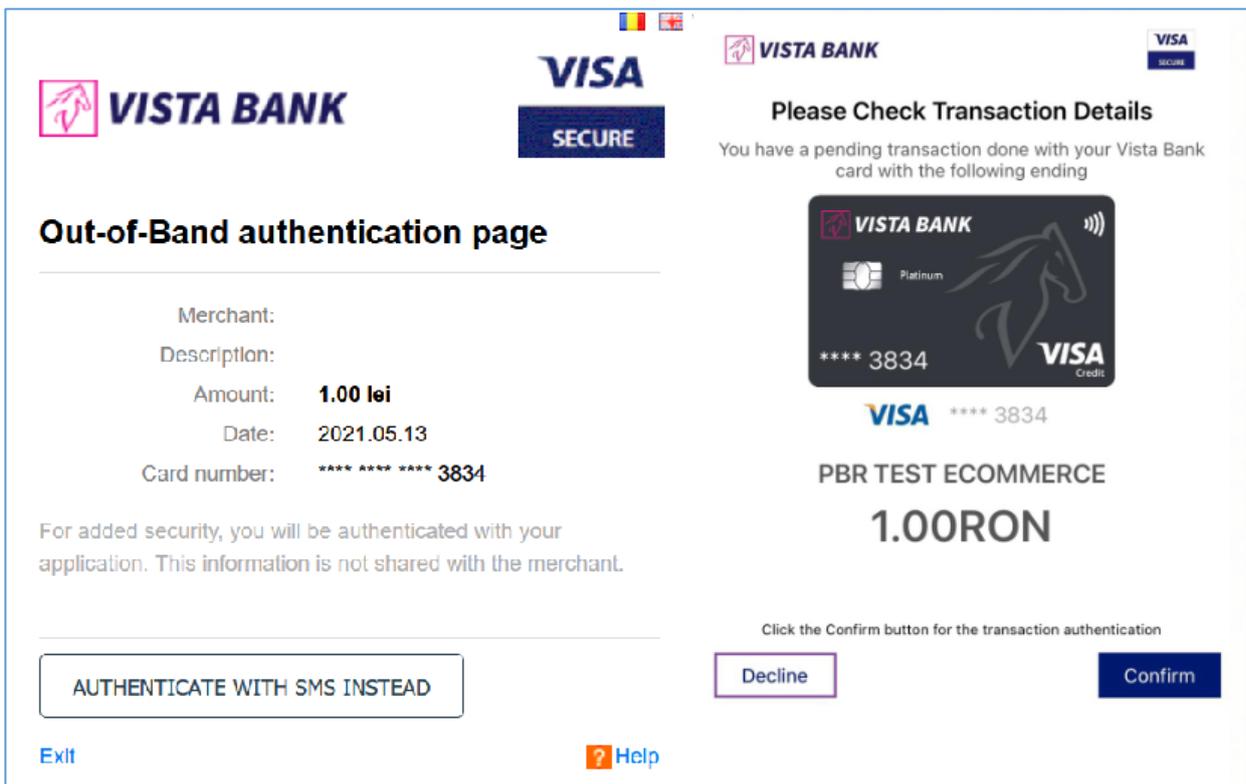
5. Thanks to the dynamic correlation protocol (security measure by which you are informed on a second communications channel about the payment details), the details of your transaction will be displayed on the screen: the name of the merchant (payment beneficiary) and the payment amount. At the same time, you will have the options to "Decline" or "Confirm" the transaction.

Note: For security reasons, the card number will appear on the Vista 3D Secure screen only with the last four digits.

6. Check carefully the amount, currency and the name of the merchant:

(a) If you choose **"Confirm"**, you will be asked to authorize the transaction by authentication using digital fingerprint / facial recognition or, if the device does not have biometric authentication feature, by entering the security code of the mobile phone.

The completion of the transaction must be confirmed by the merchant's website - check the Merchant Authentication Page.



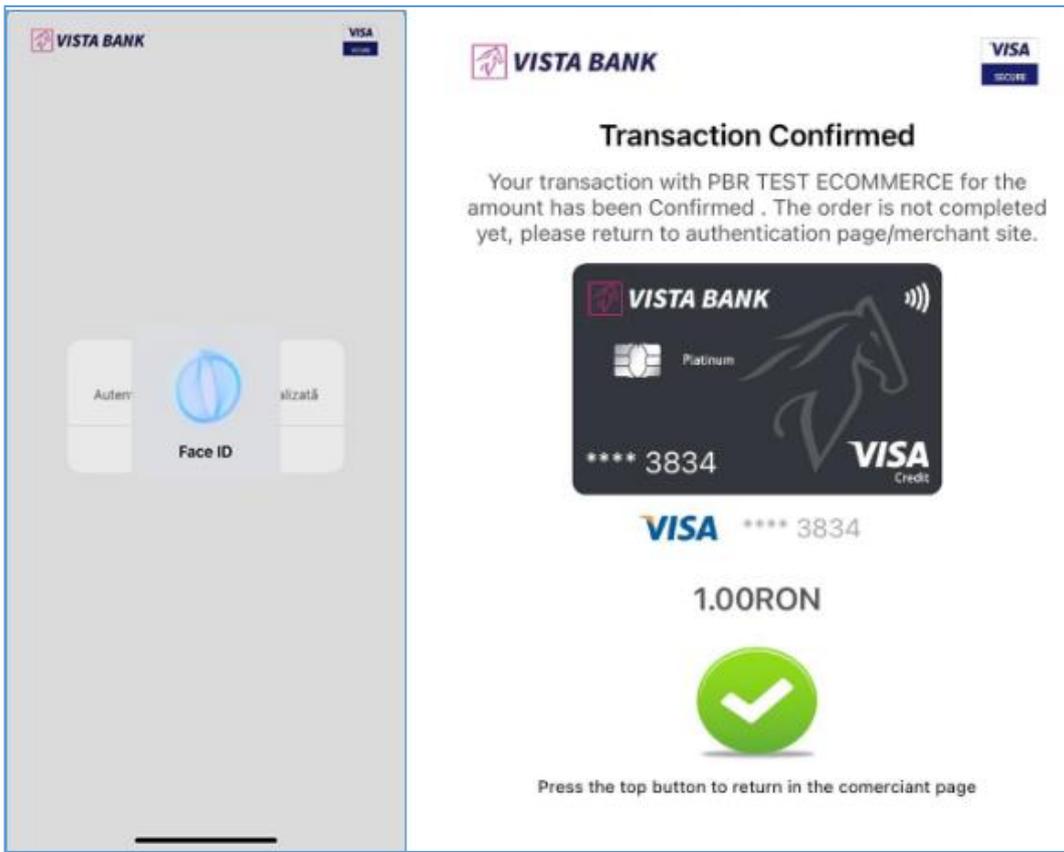
Out-of-Band authentication page

Merchant:
Description:
Amount: **1.00 lei**
Date: 2021.05.13
Card number: **** * 3834

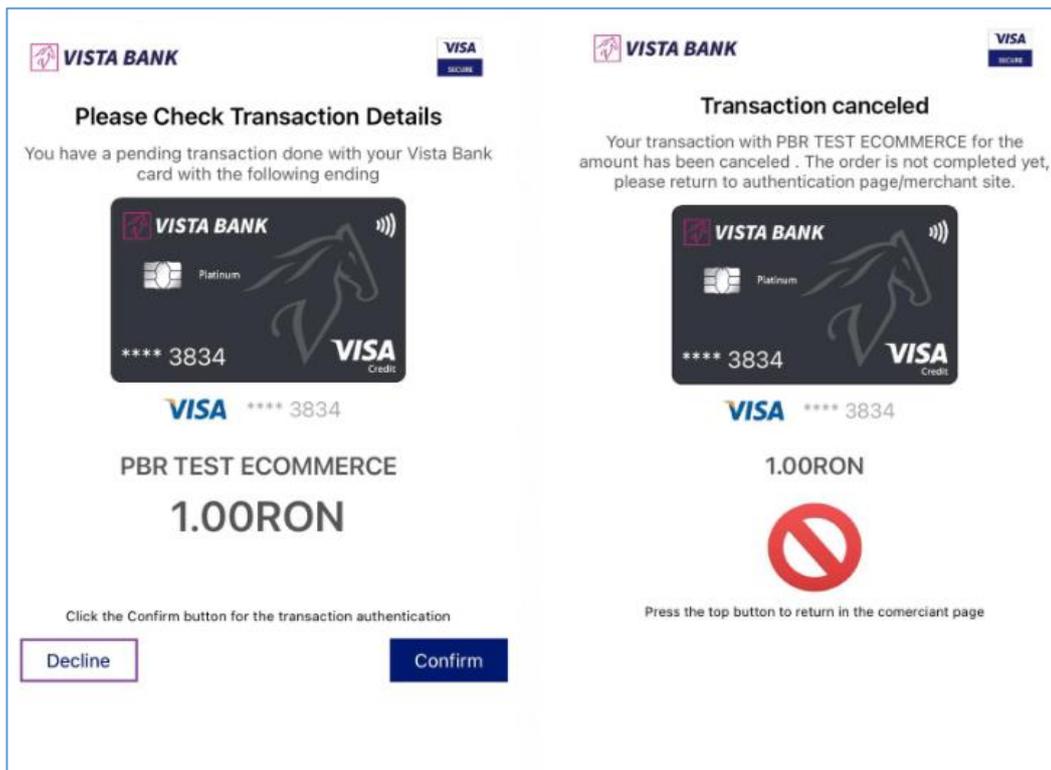
For added security, you will be authenticated with your application. This information is not shared with the merchant.

Decline **Confirm**

[Exit](#) [? Help](#)



(b) If the transaction data is incorrect, press “**Decline**” and the transaction is canceled automatically.

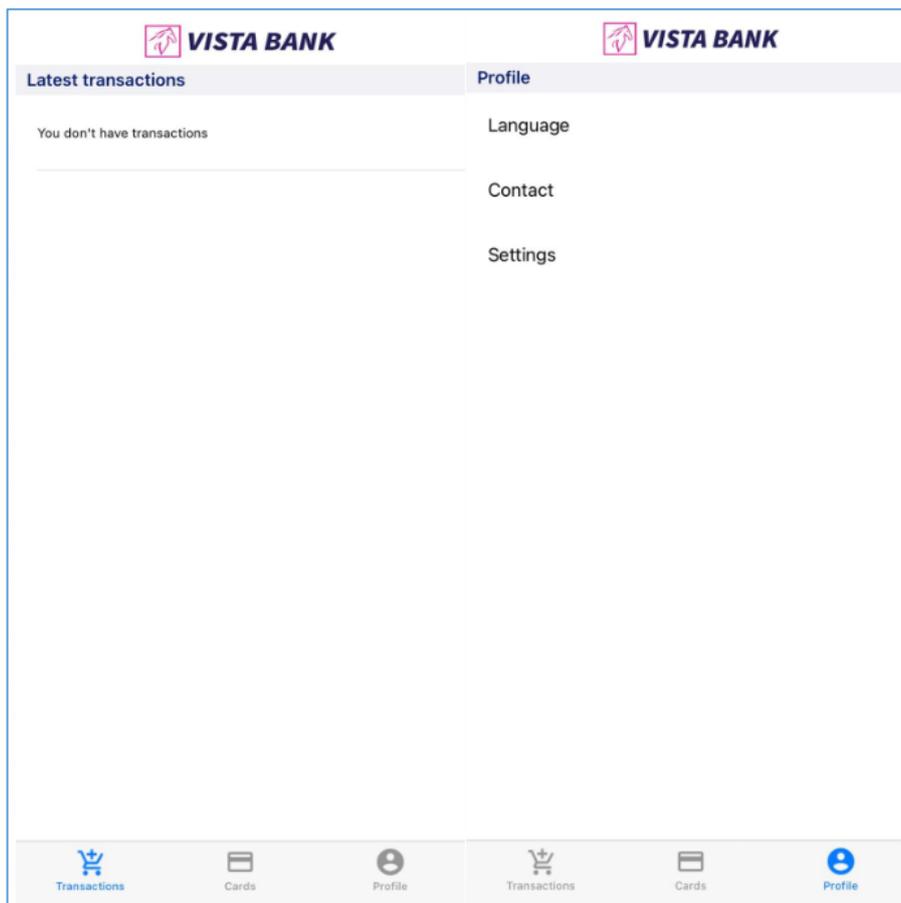


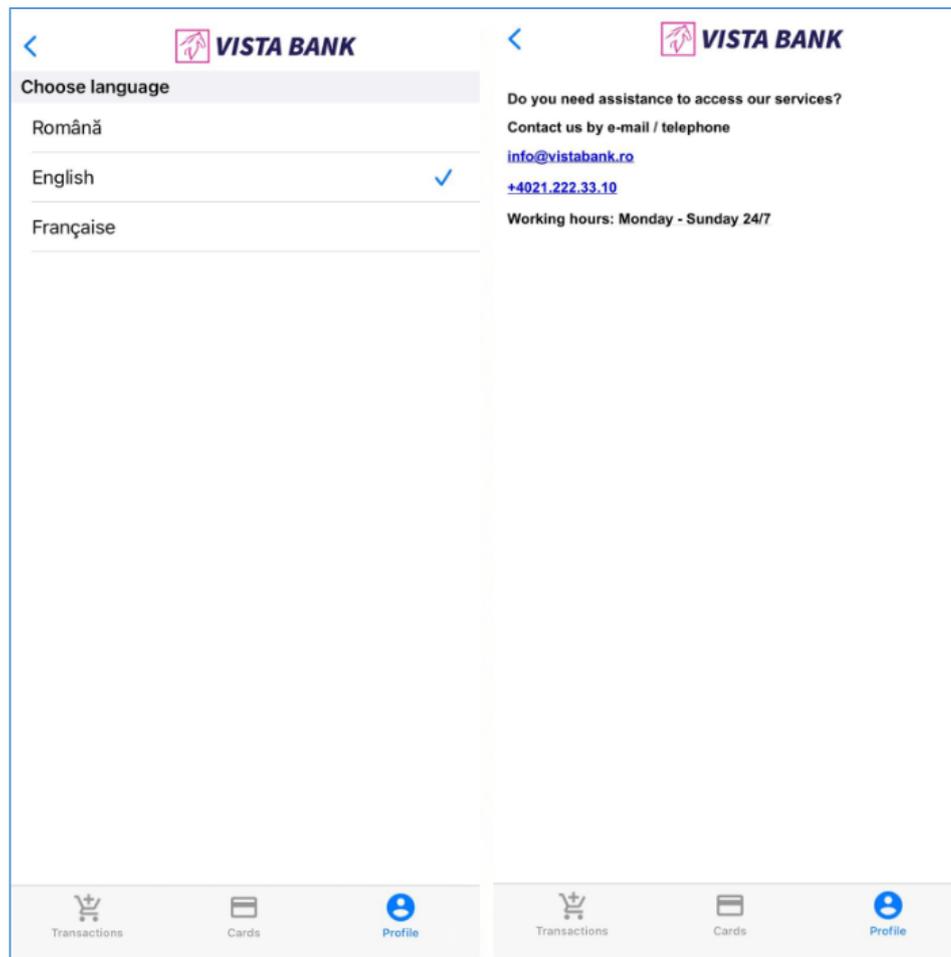
Important:

- If the transaction data is incorrect, click "Decline" and the transaction will be canceled.
- If you see different a different Merchant / Beneficiary/ Amount or Currency displayed by Vista 3D Secure application, Decline the transaction and notify the Bank immediately.
- Notify the Bank immediately if you have not initiated an e-commerce payment but you have received in Vista 3D Secure a request for a payment confirmation that you do not recognize.
- The method of securing your smartphone / tablet on which the Vista 3D Secure application is installed (fingerprint, facial recognition or security code) is your responsibility. We recommend that you **make sure that you have not allowed access to your mobile device and to other people who could even authorize payments with your card.**

C. Other features offered by Vista 3D Secure

- Viewing pending transactions - maximum 5 minutes after initiating the transaction;
- Viewing credit and debit cards held at Vista Bank;
- Language configuration - Romanian, French, English;
- Bank Contact Details;
- Vista 3D Secure application settings.





II. Static password and SMS (one time password) authentication

A. Registration

This is an alternative solution that can be used as a backup for the mobile phone application or in case you do not want to use the Vista 3D Secure mobile application (the solution recommended by the bank).

In order to meet the new legal requirements for strict customer authentication (SCA), the alternative solution for authorizing online card payments (payment to online merchants / e-commerce payment) will use:

1. **Knowledge**-based authentication method (something only the customer knows): static / initial password
- and
2. **Possession**-based authentication method (something only the customer has): the unique code received via SMS

For the first transaction, you will need to follow the steps on the login page of your mobile phone or computer.

You will enter the initial password set by the Bank and **you will change it with a new password**, which will be known only by you.

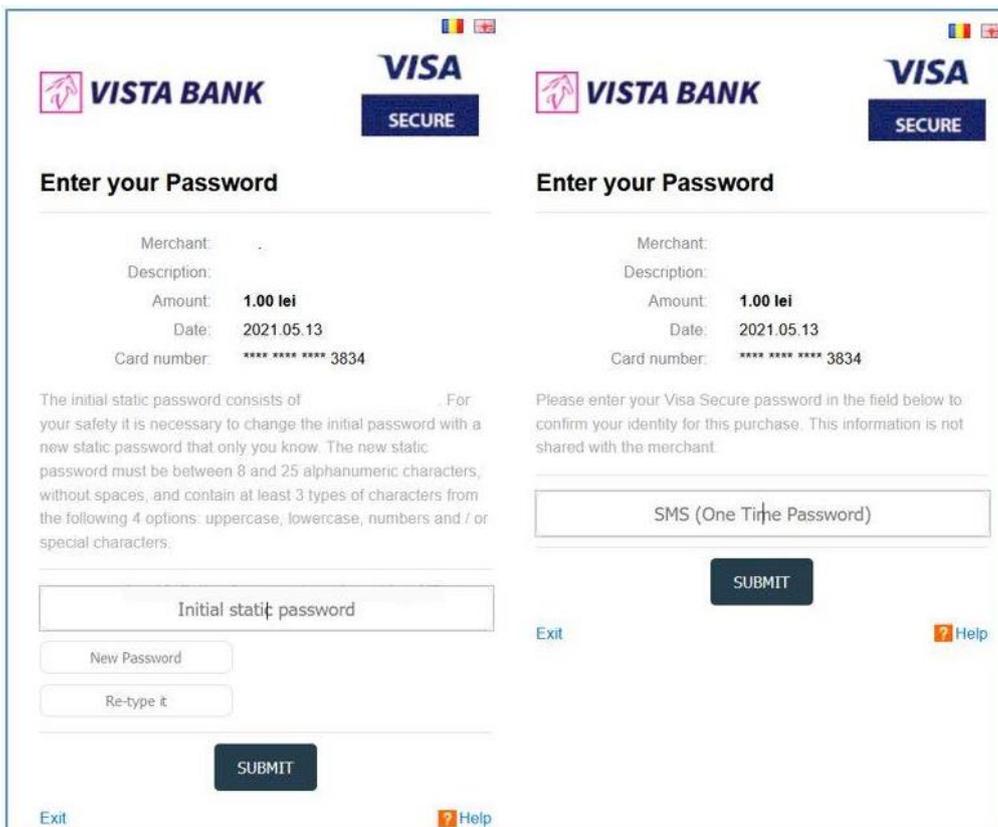
Note: If the initial password is not validated, please contact us (+4021 222 33 10/ info@vistabank.ro) to confirm it.

The new password must meet the following conditions:

- 8 to 25 characters long
- To have at least one capital letter, one small letter and a digit
- To be different from the initial password

After setting the new password, you will press the "**Confirm**" button and you will receive the SMS message to approve the transaction and save the new password. For the delivery of the SMS, the Bank will use the telephone number registered with the Bank. If you do not receive the SMS message, please contact us (+4021 222 33 10/ info@vistabank.ro) to check the phone number and how it can be updated.

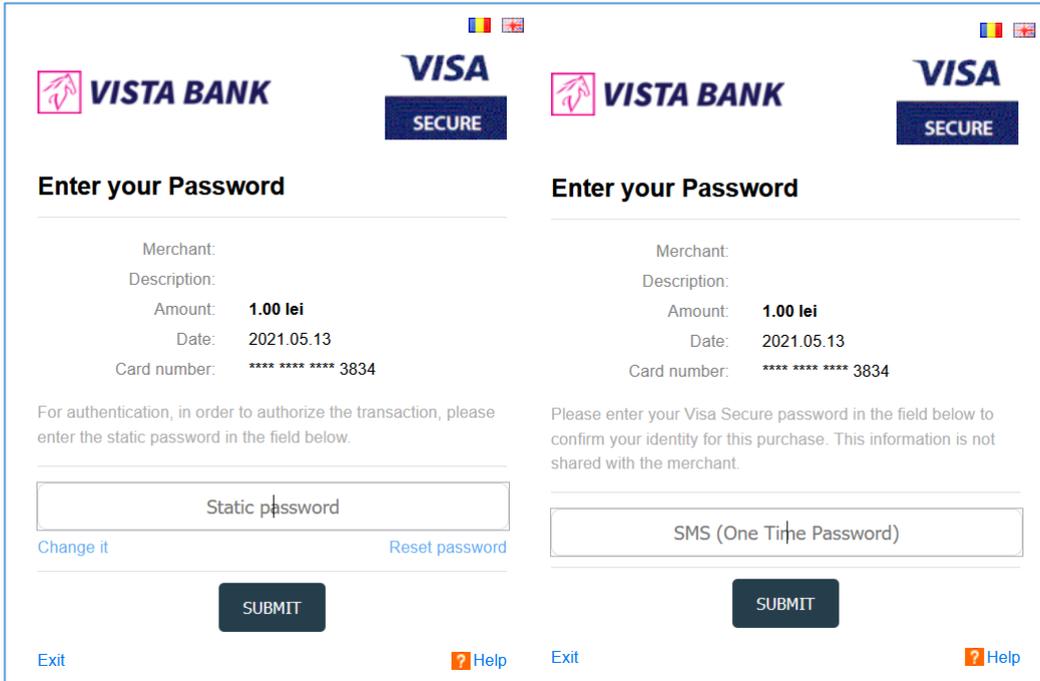
Before you enter the code received by SMS, please check the payment data received by SMS: MERCHANT NAME, AMOUNT and TRANSACTION CURRENCY.



The image shows two side-by-side screenshots of the Vista Bank mobile app interface. Both screens feature the Vista Bank logo and a 'VISA SECURE' badge at the top. The left screen is titled 'Enter your Password' and displays transaction details: Merchant, Description, Amount (1.00 lei), Date (2021.05.13), and Card number (**** * 3834). Below the details, it explains that the initial static password must be changed to a new one between 8 and 25 characters, containing at least 3 types of characters (uppercase, lowercase, numbers, and/or special characters). It includes input fields for 'Initial static password', 'New Password', and 'Re-type it', along with a 'SUBMIT' button. The right screen is also titled 'Enter your Password' and shows the same transaction details. It prompts the user to enter their Visa Secure password to confirm the purchase. It features an 'SMS (One Time Password)' input field, a 'SUBMIT' button, and 'Exit' and 'Help' options at the bottom.

B. Authorization of transactions after registration

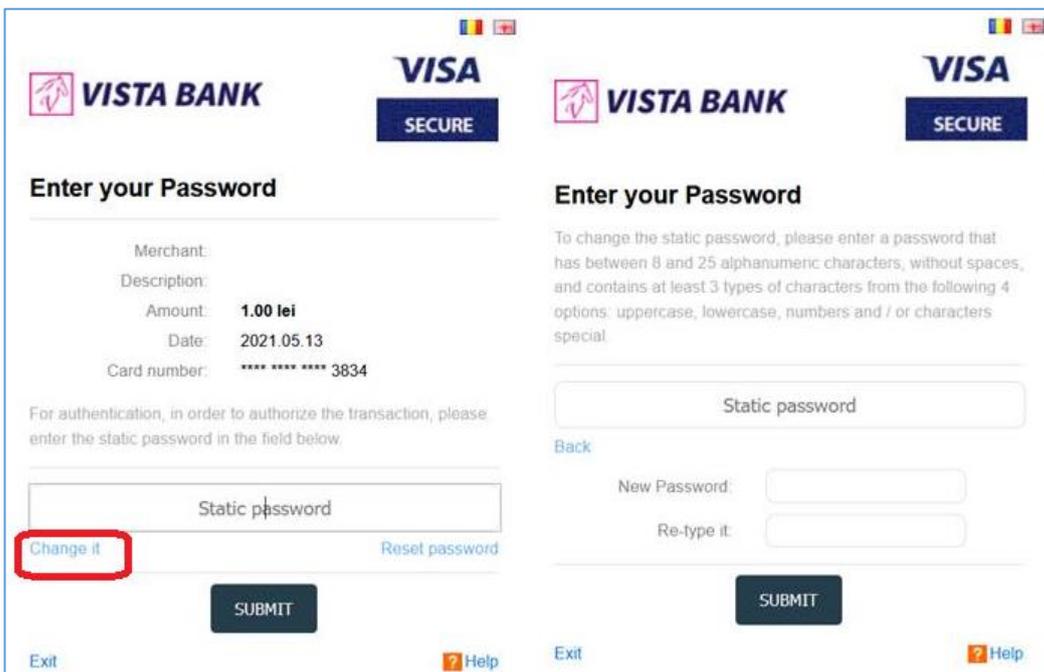
Once the new password is saved, all future transactions will be authorized using the new password and the unique code received via SMS.



The image displays two side-by-side screenshots of the Vista Bank payment authorization interface. Both screens show transaction details: Merchant, Description, Amount (1.00 lei), Date (2021.05.13), and Card number (**** * 3834). The left screen is for a static password, with a text input field labeled 'Static password' and a 'Change it' link below it. The right screen is for an SMS (One Time Password), with a text input field labeled 'SMS (One Time Password)'. Both screens have a 'SUBMIT' button and 'Exit' and 'Help' links at the bottom.

C. Change password

The static password can be changed when initiating an online payment by clicking the "Change it" button. To change the password you need to know the current password.

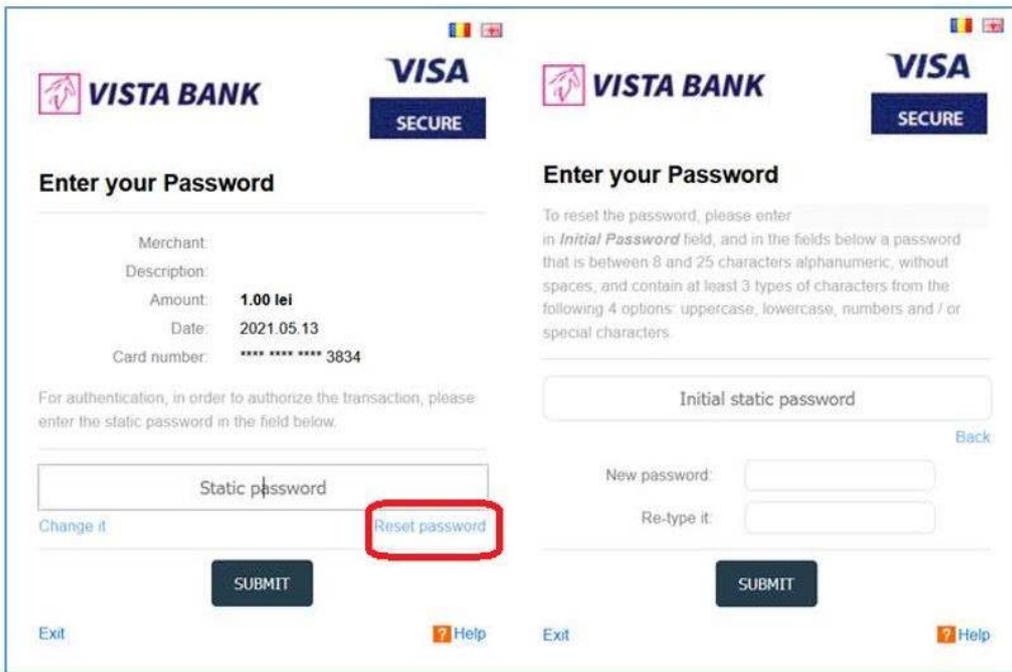


The image displays two side-by-side screenshots of the Vista Bank password change interface. Both screens show transaction details: Merchant, Description, Amount (1.00 lei), Date (2021.05.13), and Card number (**** * 3834). The left screen is for a static password, with a text input field labeled 'Static password' and a 'Change it' link below it, which is highlighted with a red box. The right screen is for changing the static password, with a text input field labeled 'Static password' and a 'Back' link below it. Below the 'Back' link are two text input fields labeled 'New Password' and 'Re-type it'. Both screens have a 'SUBMIT' button and 'Exit' and 'Help' links at the bottom.

D. Forgot your password

If you no longer remember your password, you can reset it by pressing the "Reset password" button. You will enter the initial password set by the Bank and then the new password set by you, followed by the unique code received via SMS.

Note: If the initial password is not validated, please contact us (+4021 222 33 10/ info@vistabank.ro) to confirm it.



The image displays two side-by-side screenshots of the Vista Bank 3D Secure interface. The left screenshot shows a transaction confirmation page with the following details: Merchant, Description, Amount: 1.00 lei, Date: 2021.05.13, and Card number: **** * 3834. Below the details is a 'Static password' input field and a 'Reset password' button, which is highlighted with a red rectangle. The right screenshot shows the 'Enter your Password' page for password reset. It includes instructions: 'To reset the password, please enter in *Initial Password* field, and in the fields below a password that is between 8 and 25 characters alphanumeric, without spaces, and contain at least 3 types of characters from the following 4 options: uppercase, lowercase, numbers and / or special characters.' The form contains an 'Initial static password' field, 'New password' and 'Re-type it' fields, and a 'SUBMIT' button.

III. Troubleshooting

1. Error message Vista 3D Secure application:
 - “Your card is not compatible” – please contact us to check the phone number registered with the Bank.
 - Your authentication method is not validated – please make sure that your device has setup (device settings) the method of security you are trying to use (fingerprint, facial recognition or security code).
2. Transaction is not authenticated by Vista 3D Secure application – please use the backup with the static password and one time password. You might not have access to internet.
3. A new card was issued but is not displayed in Vista 3D Secure application – please uninstall the application and register again.
4. You don't receive the SMS code for Vista 3D Secure application activation – please contact us to check the phone number registered with the Bank.
5. Wrong initial static password – please contact us to confirm it.
6. Wrong static password – you can reset the password using the initial static password.
7. You have entered 3 times the wrong static password – you will need to start the transaction again from the merchant's website.

We trust that the new authentication methods will improve your online experience with Vista Bank.

Thank you!

