Citadele

App “Citadele Phone POS” and “tapXphone” user guide

This section provides users with information on how to use the Application for accepting contactless payments on their own mobile devices.

Getting ready to use

Which devices does the application support?

The Application can be used on most smartphones. There are several general requirements listed below. There are no recommendations on which device to choose. The choice is made by the user.

We are not responsible for your choice in favor of the devices' poor characteristics of which may cause errors, interruptions in operation, slow and low performance of the Application or its individual functions.

Before you start using the Application, make sure that:

- Your device has an OS Android version 10.0 or higher.
- Your device provides NFC functionality.
- Your device supports:
    - Network services:
        - Global Positioning System (GPS).
    - Android services:
        - Hardware-backed Keystore.
        - Google Play Integrity API.
        - Google Play Store.

These are the minimum requirements for installing the Application. However, after the Application is installed, the system (server-side) will check the reliability of your device. And if its state does not meet the security criteria, further use of the Application can be restricted.

Application installation and launching

1. Download „Citadele Phone POS“ and “tapXphone” apps from the Google Play Store:
    - Installing the Application from outside the Google Play Store is prohibited. If you try to install the Application from other sources, you are violating the license agreement.
    - The Application is not available in the HUAWEI AppGallery. Devices without access to the Google Play Store are unable to use it. For example, such devices include, but are not limited to, the following:
        - P40 / P40 Pro / P40 Pro + / P40 Lite / P40 Lite 5G / P40 Lite E
        - P Smart 2021 / P Smart S
        - Mate XS
        - Mate 40 / Mate 40 Pro / Mate 40 Pro + / Mate 40 RS Porsche Design / Mate 30 Pro / Mate

30E Pro 5G
        - Nova 8 / Nova 8 Pro / Nova 8 SE / Nova 7 / Nova 7 Pro / Nova 7 SE / Nova 7 SE Vitality Edition / Nova 7i / Nova 6 / Nova 6 5G / Nova 6 SE
        - Y9a / Y8p / Y8s / Y7a / Y6p / Y5p
        - Enjoy 20 / Enjoy 20 Plus / Enjoy 20 Pro / Enjoy 20 SE / Enjoy Z
        - Maimang 9
        - MatePad Pro / MatePad 10.4 / MatePad T 8
2. Launch the „Citadele Phone POS“ app and click on Sign In. If you need to change the language, select it in the upper left corner before signing in.
    - The Internet must be enabled (through mobile network or Wi-Fi) on the device before launching the Application.
3. When the ‘’tapXphone’’ app opens:
    - Allow access to the device’s location while using the app.
    - Review the terms of the License Agreement and accept them to start using the Application.

After installing the Application, a unique number (ID) is assigned to your device. It is displayed next to the icon on the Application’s Sign in screen. If you have any questions on how to operate the Application, contact Citadele Bank Customer support to help you get a response faster.

Viewing the app version

You can view the current version of the “tapXphone” application:

- On the Sign-in screen by clicking the “i” icon.
- After logging into the Application, the “i” icon can be found in the extended menu.

We recommend regular updates of the application (including automatic updates) when the release of the new version is available.

To verify the authenticity of the “Citadele Phone POS” and “tapXphone” applications, check your last login date in the Merchant portal under the cashier menu. If a login date is present, you are using the official versions of the Applications rather than counterfeit or look-alike versions.

Trusted device criteria

The device's compliance with the requirements listed below, as well as adherence to the safe mode for using the application, minimizes the chances of restrictions on accepting payments on your device.

Device state requirements

The device must not:

1. Have an unlocked bootloader:
    - The bootloader must be locked.
2. Be rooted:
    - The device must not have root access, and the user must not have root privileges.
3. Be in developer mode:
    - How to check:
        - **Method 1:** Open Settings, go to About Phone or About Tablet, find the Build Number section (or MIUI version on Xiaomi devices), and tap it. If developer mode is enabled, you will see a confirmation message.
        - **Method 2:** Open Settings, select For Developers (or Advanced -> For Developers), and ensure the developer mode switch at the top is turned off.
4. Be in debug mode:

- How to check:
  - **Method 1:** Open Settings, select For Developers (or Advanced -> For Developers on some devices). In the Debug menu, ensure USB/Wi-Fi Debugging is not activated.
  - **Method 2:** Connect the device to the computer. Make sure that there is no USB/WiFi Debugging enabled notification on your smartphone.

5. Have SELinux Disabled or Permissive.SELinux must be set to enforcing mode. Devices with SELinux in "Disabled" or "Permissive" mode are not secure and will be blocked:
   - How to check:
     - Certain devices, such as Samsung smartphones, allow users to check the SELinux mode manually. To verify the SELinux state:
       1. Go to Settings -> About Phone.
       2. Find the section Software Information (or similar).
       3. Look for SE for Android or a similar entry. The SELinux mode should be listed as either “Enforcing” or “Permissive”:
          - If it shows “Enforcing”, the device is secure and compliant.
          - If it shows “Permissive” or “Disabled”, the device needs adjustment or replacement.
   - If a device is flagged due to SELinux misconfiguration, the following options are available:
     - Adjust SELinux Mode Manually**.** Advanced users may attempt to change SELinux mode from "permissive" or "disabled" to "enforcing." **Warning**: This process involves significant system modifications and could render the device unusable. It is not recommended for non-experts.
     - Visit a service center. You may seek assistance from a professional service center. Specialists at these centers may be able to reconfigure SELinux settings or provide a resolution.
     - Change the Device**.** The most straightforward and reliable solution is to replace the device with one that meets security requirements, where SELinux is properly enforced.
6. Pass Google Play Integrity API Checks. The device must successfully pass the Google Play Integrity API check with the MEETS_STRONG_INTEGRITY status:
   - How to check:
     - To verify the integrity verdict on your device, follow these steps:
       1. Enable Play Store's developer options by tapping your profile icon in the Play Store app, then select Settings.
       2. Open the About menu and tap Play Store version seven times to unlock developer mode.
       3. Open the Play Store app, tap your profile icon, then go to Settings > General > Developer options.
       4. In the Play Integrity settings, tap Check integrity to generate the verdict for the device.
7. Contain Apps Violating Google's Software Principles:
   - Apps installed on the device must comply with Google's Software Principles and Unwanted Software Policy.

Application installation source

The application must be downloaded and installed **only** from the Google Play Store.
Installation from other sources is strictly prohibited, as it violates the License agreement.

Safe usage of the “tapXphone”

When using the “tapXphone”, the user must not:

1. Allow Screen Overlay:
    - Apps or system functions (e.g., messengers) that overlay the tapXphone screen must be turned off during transactions.
2. Use Split Screen or Broadcast Modes:
    - Do not activate split-screen mode or use broadcast functionality from the mobile device.
3. Use the camera in unintended ways:
    - Background apps with camera access must be closed during a transaction.
    - Disable system functions that keep the screen active due to constant background camera usage (e.g., Face ID features).
4. Take screenshots or record videos:
    - Screenshotting or screen recording are prohibited while using the application.
5. Turn off previously granted permissions:
    - Ensure that all required permissions remain active for the application.
6. Use remote control applications:
    - Applications like TeamViewer or AirDroid are not allowed.

NFC requirements

The device must have:

1. A functional embedded NFC module.
2. NFC configured to read cards:
    - How to check:
        - Open Settings, go to Connection and Sharing, and ensure NFC is turned on.
        - If there is an option to choose between SIM and e-wallet, select e-wallet.

Security recommendations

- **OS Updates**: Regularly update the device’s OS and components to ensure the latest security improvements.
- **Trusted Apps**: Only download apps from trusted vendors in the Play Store, verified by Google Play Protect.
- **Malware Detection**: Install and update malware detection tools to protect the device.

The device is locked in the App

While using the Application, your device is constantly checked for compliance with the Security Criteria.

If the state of a device does not meet the requirements set by the system, it can be blocked in terms of using the Application, as the device may present a threat to the safe acceptance of card payments.

In some situations (instead of blocking), the application settings will be reset to their initial state, so you need to setup your device again.

To find out the possible reason for blocking and to request unlocking the device, contact Citadele bank. When addressing Citadele bank, please provide the device ID displayed on the application’s Sign-in screen.

Device setup

To begin using the application, you must register your mobile device in the system and activate an existing payment terminal using one of the available methods.

Method	Difference
Using the login and password of the Main Cashier	Confirmation codes are sent to Main Cashier's email. Need access to the email specified in the acquiring service agreement.
Using the Device code	The device code is entered in the Merchant's web portal. Need access to the Merchant's web portal account to enter the Device code.

Device setup using the login and password of the Main Cashier

The device setup must be performed by the Main Cashier. If you are not the Main Cashier, then let him/her know you need to pass the process on your device.

1. Enter the Username/Login and Password of the Main Cashier.
    - When you enter the password, remember it is sensitive to upper and lower case.
    - If you are logging into the Application for the first time as the Main Cashier, then the default Password is equal to the Login/Username (case sensitive).
    - The password that you received via email is not for Application; it is for Merchant web portal.
2. If you have successfully entered credentials, the Application will ask you to enter the initialization code (4 digits). Enter it into the appropriate field and continue to login.

The initialization code is sent by email, specified in the acquiring service agreement.

Payment terminal activation

The payment terminal activation can be required in the following cases:

- Passing the initialization process on the device for the first time.
- The device was unbound from the payment terminal.

If payment terminal activation is needed, the system will ask to enter the activation code (6 digits). Enter it in the appropriate field and continue to login. The activation code is sent by email, which is specified in the acquiring service agreement.

The activation of the payment terminal must be performed by the Main Cashier. If you are not the Main Cashier, then let him/her know you need to pass the process on your device.

You may be notified that there are no available terminals to bind to your current mobile device. This message may occur when all the payment terminals generated by Citadele bank are already bound to other mobile devices. In this situation you can:

- Contact Citadele bank with a request to increase the number of payment terminals.
- Or unbind the existing payment terminal from another mobile device.

The list of available payment terminals is in the Merchant's web portal.
If you need to activate a payment terminal with a specific identifier, then you need to use the device setup using the Device Code.

After successful completion of device initialization and/or payment terminal activation, the Application will display the Amount entry screen. This means the device is ready to use as a payment terminal. Main Cashier can log out of the account and hand in the device for further use of the Application as it is intended to another user/cashier.

Device setup using a Device Code

1. On the login screen, click the Use Device Code button.
2. The device will generate a temporary Device Code consisting of 8 digits.
3. Go to the Merchant Portal or give this code to the person who has access to the Merchant Portal.
4. On the Merchant portal, need to activate the payment terminal using the device code:
    - Go to the Payment terminals section.
    - Find a terminal available for binding and click the Bind button.
    - Enter the Device Code.
5. If the Device Code is successfully entered on the Merchant Portal, then on the mobile device, click the Update device status button to complete the setup.

Upon successful completion of the device setup, the application will display a screen for entering the login and password of the cashier to enter the application.

The code is valid for the time indicated on the screen at the time of its formation. During this period, the Code must be entered in the Merchant's portal and click the Update status button on the mobile device. If both or one of the steps were completed after the specified period, the device setup procedure must be started again.

Reconfiguring the device
There are situations when there is a need to reconfigure the device (for example, they deleted, re-downloaded the application, cleared its memory, etc.) In this case, you can use the Device Activation section in the Merchant's portal, having previously generated a code on the device. You can also use this section if it does not matter which terminal the device will bind to. If you enter the code in this section, the system will link the device to a free terminal.

Sign in

The Application can be used by any cashier when the subheading of the Sign in screen does not contain indication that the device needs to be setup (or that the device is locked or disabled).

To sign into the Application, enter the cashier's Username and Password.

- When entering the password, please note that it is sensitive to upper and lower case.
- If this is a Cashier's first login to the Application, then the default Password is equal to the Login (case sensitive) that was set in the Merchant's portal.

You have 5 attempts to enter the correct Username/password, after which the account will be locked (in this case, the Application will display a message with the code 203). The cashier's account can be unlocked in the Merchant's portal. In this case, you should contact the employee of your company who has access to it.

If the application displays an error message with the number 101, indicating that the login and password were entered incorrectly, the device should be given to the Main Cashier for reinitialization by logging in with the Main Cashier's credentials.

Upon successful signing in, the Application will display the Amount entry screen. You can start accepting payments.

Biometric Authentication

Biometric authentication can be enabled in the application in the following ways:

- During device initialization: after the device setup is complete, a pop-up screen will appear prompting the user to enable biometric authentication.
- From the application settings: navigate to the Settings section in the application menu and switch on the Biometric Authentication option.

Authentication is enabled by scanning a fingerprint using the device's biometric sensor, following the on-screen instructions.

Future logins to the application can be performed using biometric authentication (fingerprint scan), eliminating the need to enter a password.

Change and recover password

Change password

When signing in for the first time, the system will prompt you to change the default password. On the Change Password screen, enter your current password, then enter the new password twice, and apply the change. The password must contain letters, numbers/symbols and must be at least 8 characters long.

You can also go to the Change password section via the menu "Point of Sale" of the Application by clicking on the icon.

Recover password

If you do not remember your password, you can recover it with the help of the password reset function in the Merchant's portal. Contact the employee who has access to it.

If the password is reset, then by default it becomes equal to the Login (case-sensitive) that is set in the Merchant's portal.

Payment acceptance

The Application can only be used for contactless payments.

Payment cards that support contactless payments have an "contactless payment" icon.

Preparing to accept payments

Before you start to accept payments, make sure that:

- The Internet is enabled.
- The NFC module has been enabled and configured to read cards.
- The device is in the safe mode for the Application.

Amount entering

On the Amount entry screen, type in the required payment amount and confirm it by clicking the PAY button.

Before accepting payments, we recommend checking and understanding the current limits for:

- The maximum amount for a single payment.
- The payment amount that requires the application to request a PIN from the cardholder.
- The total daily payment limit.

You can get this information from Citadele bank.

Payment card tapping

When you see the prompt on the screen to tap a card, ask the customer to tap their card or mobile device (with the payment app installed) on your device, over the NFC module area.

A card must be tapped after the first color indicator lights up on the screen ● ○ ○ ○ (the color of the indicators may differ).

Before tapping a card, make sure that the payment card is contactless and belongs to payment systems supported by your payment terminal. You can check this by matching the payment systems displayed on the Application's screen with the logo on your customer's payment card.

For better card reading, you should bring it as close to the location of the NFC module on the device as possible and hold it until it is read in full. The result of the complete reading of a card is confirmed by lighting up of four-color indicators ●●●● and displaying the message about the successful transaction (the indicators' color may differ). In the new version of the Application, it is additionally accompanied by a single sound signal and a single vibration of the device. After that, the card can be removed from the device.

Where to bring the payment card

Below are examples of some possible locations for the NFC module.

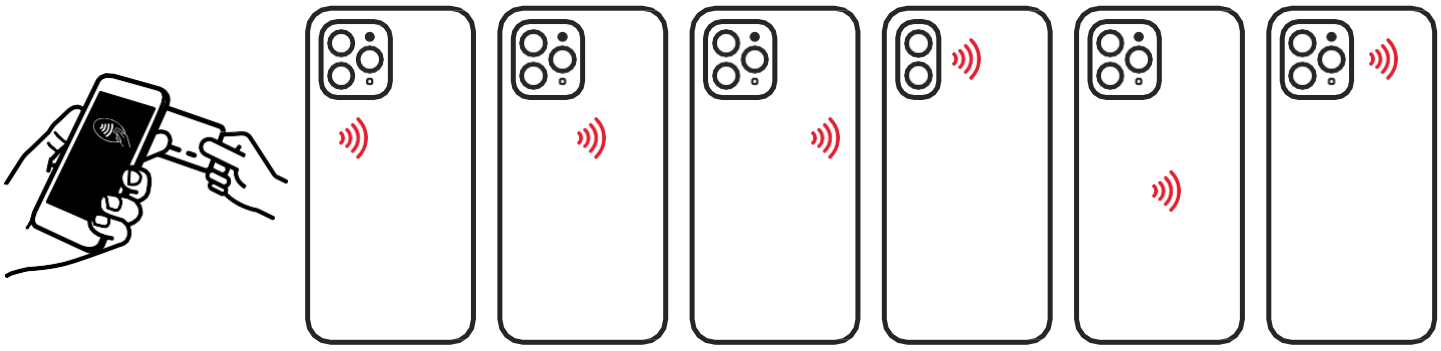
The exact location of this module should be specified in the manufacturer's instructions.

For such practice when finding the NFC module location, you can:

- Take an expired card and try to complete several Payments by entering the minimum amount allowed.
- If you have no such card, you can use a valid card and try to accept Payments with the minimum amount allowed and then (in case the payments have been successful) you can cancel transaction.

All NFC modules are typically located on the back of the devices.

The possible locations of the NFC module are shown in the illustration below.



Unsuccessful card reading

In case the payment card reading fails, you will receive a corresponding information message, which may contain the following codes: 1926, 1929, 1943, 1976. The main reasons why the payment card is not successfully read in may be the following:

Reason	Recommended actions
The card is not brought to the NFC module location	Find the location of the NFC module in your device where the strongest antenna signal for reading cards is detected.
The payment card was removed too early	Ask your client to bring the card and do not remove it until the result of a successful reading of the card is displayed on the screen.
The client's card has very low signal in process of contactless payments	As experience has shown, very often some cards have a weak signal of the internal antenna. In such a situation, you can try to tap the card with the other side, while maintaining the minimal distance between the microchip and the NFC module. If the card cannot be read in, suggest that the customer use another one.

The contactless interface on the card is disabled (error code 1943)	This may occur if the contactless interface is not activated on the card or was disabled by the cardholder. Please advise the client to enable the contactless feature via their mobile banking app or by contacting their issuing bank.
NFC module is not activated	Go to the settings of your device and enable the NFC function. If you have a choice between paying with "sim" or "e-wallet" when activating the function, then you should choose "e-wallet".
Application has no permissions for NFC	Open the system menu, in the section with the applications list find the tapXphone application and make sure that in the Application permissions the access to NFC is allowed.
Payment card that is used does not have a contactless interface	Check the presence of the icon on the payment card.
Payment card of an unsupported payment system is used	Make sure that the payment card belongs to a payment system that is supported by your payment terminal.
The NFC module does not work	Install a third-party application that can be used to read regular NFC tags. Run it and try to read the NFC tag/any contactless card (but not the card of your client).
There are objects that block the signal between the device and the payment card	Remove items that may affect the processing of the payment card. For example, the device case.

Any repeated attempt to use the payment card must begin with removing it from the field of the NFC module on your device and then bringing it back to it.

PIN entering

The Application may ask the customer to enter PIN code if the payment amount exceeds the limit for no-PIN transactions set by Citadele bank. This is a prerequisite for verifying the cardholder to confirm the transaction.

When the PIN entry screen appears, allow your customer to enter PIN on your device.

If the customer refuses to enter the PIN code, click the Cancel button or the **X** icon. In this case, the purchase cannot be considered complete.

Payment result

Upon successful processing of the transaction and confirmation of the completed payment by Citadele bank, the Application will offer you the function of sending/displaying the receipt to your customer.

The Application's receipt is not a fiscal receipt.

If the customer does not need the receipt, you can start a new transaction by clicking the New Purchase button.

Payment cancelation

If the customer wants to cancel the purchase, you can use the Reversal function.

- The Reversal function is available only while the business day is still open. Once the business day is closed, Citadele bank settles the transactions, and payment cancellation is no longer available.
- Payment reversal returns the full amount to the customer.

There are two ways to cancel a purchase:

1. By selecting the required purchase from the list of transactions in the current business day.
    - Go to the menu Point of Sale in the Application menu -> List of transactions. Then select the required purchase and click Reversal.
2. By specifying the receipt number.
    - Click on the folder icon with an upwards arrow in the amount entry screen. Enter the receipt number from the customer's receipt and confirm the action by clicking Reversal.

To send a cancellation receipt to the customer, click on the receipt icon and enter the customer's phone number or email.

To check payment status, go to the menu Point of Sale -> Transactions. The canceled payment will have a status “Reversed”.

If the payment reversal processing has failed, the purchase cannot be considered canceled. In this case, we recommend trying to cancel the purchase again.

Why and how to close the business day

Business day - usually a 24-hour period after which the business day is automatically closed, and all performed operations are transferred to processing.

Business day may be closed:

- Automatically at midnight (00:00).
- Manually in the application.
    - Click on the Application menu ⋮ and select “Close business day”. Confirm the action.
- Manually on the Merchant's web portal.
    - When a message about an issue with closing the business day appears in the Application (message 705), it must be closed on the Merchant's portal.

In the Application, the Transactions menu displays only transactions for the current (open) business day. Once the business day closes, transactions for that day will no longer be accessible.

To view a summary of your transactions for the current business day, simply click the "Business Day Results" button in the Application menu ⋮.

You can access all transactions, both for open and closed business days, through the Merchant's portal. For further details, refer to the Merchant Portal User Guide – Transactions Log.

If you have any questions, please contact Citadele Bank client support, indicating the device ID number, which will allow you to receive a quicker response.