UniCredit Mobile App Customer Information

The UniCredit Mobile App can be downloaded to any suitable smartphone or tablet device (with an Android or iOS system) connected to the internet. The UniCredit ATM and branch office search and the exchange rate information are available to users without identification or sign-in. Activation is necessary for other functions which will become available after login.

UniCredit Mobile application
UniCredit Bank Hungary Zrt.'s UniCredit Mobil app can be used 24/7 to obtain information about the current balance of your bank account, initiate transfers or term deposits on your bank account or to withdraw money without your bankcard.
There are two services available through the app: the Mobil Bank and the mToken generator.
Users can install the UniCredit Mobile service to more than one devices. After 26th of June 2018, the application is no longer available in a format optimized for tablets. The application optimized for smartphones is compatible with tablet devices after re-activation. The terms of using the service are detailed in the General Business Conditions.

Would you like to use our service?
Both functions require activation. Activation can be initiated during opening times with our branch consultants, or every day between 8AM and 6PM through our Telefonbank (after identification).
You can also activate the services with your internet banking identification if you have an eBanking ID and use SMS authentication for your payment orders. Clicking on the code you receive via SMS (without copying) you can use it to simply activate the app.
The services are currently available for private UniCredit clients, and they can be required only by users of payment accounts or credit clearing accounts for their own usage.

Activation of Mobil Bank
Activation without eBanking credentials:

1. **Receiving your user ID:** please visit one of our branches or call the Telephone Banking service (+36 (1/20/30/70) 325 3200, any day from 8AM - 6PM), and after identification our advisor registers your personal data, request for activation and will give you your 9-digit user ID which you can use to activate the app.
2. **Initiating activation:** download and open the UniCredit Mobile application, then click on the "Activate Mobile Bank" option. On the next screen, untick the "Activation with eBanking ID" option, as you will activate the app with your user ID.
3. **Receiving your activation code:** we will send you your personal activation code in a text message (SMS) to your domestic mobile phone number.
4. **First access**: to enter the application please insert your user ID and the activation code received in SMS. The activation code is valid for 3 days after sending. If the activation does not happen over the course of these 3 days, you will need to apply for a new activation code. After the 15th of November 2016, the bank will automatically send new activation codes up to 3 times after the sending of the first code.
5. **Setting the PIN code and the biometric ID:** in order to ensure the safety of your personal data please set a PIN code for later use. Furthermore, you can also set a biometric ID. From now on you will have to sign in with one of these identification methods (PIN code, fingerprint/face recognition) when accessing the application or authorizing transactions.
6. **Security flag:** After entering your PIN, a security flag will appear on the screen. This will let you know if you have entered a correct PIN.

Activation with eBanking credentials:

1. **Starting the activation process:** download and start the application, and select Activate app with eBanking username and password option. Enter your eBanking username and password. Then you have to accept the terms and conditions of the service to proceed.
2. **Receiving your activation code:** if the data provided are valid and you use eBanking with SMS authorization, we will send you your personal activation code in a text message (SMS) to your domestic mobile phone number.
3. **First access:** to enter the application please insert the activation code received in SMS.
4. **Setting the PIN code and biometric ID:** in order to ensure the safety of your personal data please set a PIN code for later use. Furthermore, you will need to set a biometric ID. From now on you will have to sign in by one of these identification methods (PIN code, fingerprint/face recognition) when accessing the application or authorizing transactions
5. **Security flag:** After entering your PIN code, a security flag will appear on the screen. This will let you know if you have entered a correct PIN.

Please note that activation with eBanking credentials can be slower outside of the period from 8AM to 6PM.

If you want to use the application on more devices, you have to activate it on each device separately following the steps above.

The bank will send the activation code in an SMS during activation. Please note that distributing the code to a third party or displaying it on any other interfaces (e.g. websites) may result in unauthorized access!
The PIN code must be minimum 6, maximum 16 numeric characters and may not contain 6 sequential numbers (e. g. 123456), groups of the same 2 sequential numbers (e. g. 112233), or 4 identical consecutive number (e. g. 111123).

The following services are available through the app:
Functions not requiring sign-in:

- Exchange rate query
- Extended ATM and branch location finder - Locations from all UniCredit countries are shown in mobile location finder
- Call Center and social network contacts
- mToken and Mobile Bank demo

Functions requiring sign-in:

- Account history
    - Account balance and detailed account information
    - Account history and transaction details
    - Management of credit notes
- Bankcard information
    - Card overview and detailed information
    - Booked transaction history overview and detailed information
    - Pending Debit and Credit Card transaction details
- mCash
  With this function, you can withdraw cash from UniCredit ATMs by generating an identification code without using your bankcard.
- Modification of Debit card limits
    - Daily ATM cash withdrawal limit
    - POS daily limit
    - Daily Internet purchase limit
- Debit card activation
- Credit card repayment
- Managing term deposits
    - Term deposit query
    - Deposit order for existing deposit account
- Transfers
    - Ad-hoc bank-to-bank HUF transfer (regular and VIBER)
    - Ad-hoc in-bank HUF transfer
    - HUF transfers between own accounts
    - Transfer between own different currency accounts with currency exchange, calculated in HUF or foreign currency
    - Creating new standing orders, handling, editing and deleting existing standing orders
    - Managing group direct debit orders, detailed information on direct debit orders
- Managing forms and FastPay
    - Saving created orders as templates
    - Creating an order from template
    - Creating an order with FastPay
    - Managing forms and FastPay
- Create QR codes to pay and share it with friends (FastPay)
  Templates for payment orders can be created by the app which can be saved and shared in form of a QR code. By using this QR code other UniCredit Mobile App users can easily transfer money to your bank account.
- Detection of hacked devices
  The app warns you during the activation if your device has been jailbreaked or rooted. As the service is not guaranteed where jailbreak or rooting has been implemented, the activation process continues only if you acknowledge this risk.

- Receiving in-app messages from the bank
- App settings
  - Choosing language
  - Changing PIN code
  - Switching biometric identification on/off
  - Credit Push notifications and setting limits
  - Setting third party provider (TPP) authorizations
    Third party providers (offering initiations of payments and information about the account) are market actors, who – after obtaining permission and authorization – are granted access to banking data and the usage of an open interface (API) to initiate payments to provide services for users with online accessible accounts. In this function you can manage permissions related to third party providers and their services of providing information, listing and filtering transactions.
- Enter with fingerprint/face identification
  The user can allow a suitable device to identify the user by recognising the face/fingerprint on their own responsibility.
  IMPORTANT: In this case, the recognised face/fingerprint will be equivalent to the signature given by the owner of the account or by those made eligible by the owner that is accepted by the bank. The user is required to ensure that only the face and fingerprints of the user are recorded and stored.
  The user is required to ensure that no other person uses face/fingerprint recognition on the device. When switching the function on, the user will be required to state that they use the face/fingerprint recognition function of the device exclusively. For a safer use, it is recommended to lock the device and to use identification when signing in.
- Check Scan/Photo Pay
  The "Photo Pay" feature is using your smartphone's camera to scan the information from your postal remittance receipt (“check”), that you would like to pay. Based on this, an automatically filled payment form appears. The user should check, and if necessary change the scanned information before signing the transaction. After selecting this function, the scanning screen opens, where you can turn on the flash light if needed, if your device has a flash light. In order to successfully scan the check, it is important to hold your phone above the white/yellow check, so that the entire Beneficiary details fit into the frame seen on the screen, including OCR lanes (2 rows at the right-hand bottom of the check).
  IMPORTANT: Please always check the “Beneficiary Account Number” the “Amount” and the "Remittance Information” fields, so that the paid amount is correct, and the client can be clearly identified. For the field “Beneficiary name”, there may occur character errors more often, but this does not affect the payment fulfillment.
  This function is not suitable for scanning hand-written checks, only printed checks should be scanned with Photo Pay.
  The functions does not support reading QR codes.
- Segment Scan
  The "Segment Scan" feature is using your smartphone's camera to scan the information from your invoice that you would like to pay, field by field. In order to successfully scan the invoice details, it is important to hold your phone above the necessary fields, so that the entire segment content fit into the frame seen on the screen.
  IMPORTANT: Please always check the “Beneficiary Account Number” the “Amount” and the "Remittance Information” fields, so that the paid amount is correct, and the client can be clearly identified. For the field “Beneficiary name”, there may occur character errors more often, but this does not affect the payment fulfillment.
  This function is not suitable for scanning hand-written invoices, only printed invoices should be scanned with Segment Scan.
  The functions does not support reading QR codes.
- Template synchronization
  When applying for the activation code through the UniCredit branch or Telefonbank, unique daily and transaction limits can be rendered to the service; while if you activate with eBanking credentials, the service shall enter into force with the default limits described in the General Terms and Conditions. The daily and transaction limits are applied jointly for all the accounts managed in the UniCredit Mobile app by the given client. The default transaction and daily limits are specified in the General Business Conditions.

mToken (Mobile Token) Authentication

The mToken is a software-based and PIN-protected code generator application available via the UniCredit Mobile application. With mToken you can generate authorization codes for eBanking and e-Sign code for the transactions from eBanking which are valid for a maximum of 3,5 minutes.

In order to use the mToken, Users will need to download the UniCredit Mobile application and activate the mToken function. The mToken function may be activated independently of the UniCredit Mobile service.

Activation of mToken

Activation without eBanking credentials:

1. **Starting the activation process:** please visit one of our branches or call the Telephone Banking service (+36 (1/20/30/70) 325 3200, any day from 8AM - 6PM), and after identification our advisor registers your personal data, request for activation and will give you your 9-digit user ID which you can use to activate the app.
2. **Receiving your user ID:** download and open the UniCredit Mobile application, then click on the "Activate mToken" option. On the next screen, untick the "Activation with eBanking ID" option, as you will activate the app with your user ID.
3. **Receiving your activation code:** we will send you your personal activation code in a text message (SMS) to your domestic mobile phone number.
4. **First access:** to enter the application please insert your user ID and the activation code received in SMS. Clicking on the code in the SMS, it will automatically appear in the required field.
5. **Setting the PIN code and biometric identification:** in order to ensure the safety of your personal data please set a PIN code for later use. Furthermore, you can also set face/fingerprint recognition as biometric identification. From now on you will have to use one of these identification methods when accessing the mToken application.
6. **Security flag:** After entering your PIN code, a security flag will appear on the screen. This will let you know if you have entered a correct PIN.

Activation with eBanking credentials:

1. **Starting the activation process:** download and start the application, where the Activate app with eBanking username and password option is already selected. Clicking on the Forward button, the identification screen will appear. Enter your eBanking username and password.
2. **Receiving your activation code:** if the data provided are valid and you use eBanking with SMS authorization, we will send you your personal activation code in a text message (SMS) to your domestic mobile phone number.
3. **First access:** to enter the application please insert the activation code (or tap on it) received in SMS.
4. **Setting the PIN code and biometric identification:** in order to ensure the safety of your personal data please set a PIN code for later use. Furthermore, you can also set face/fingerprint recognition as biometric identification. From now on you will have to use one of these identification methods (face/fingerprint recognition or PIN code) when accessing the mToken application.
5. **Security flag:** After entering your PIN code, a security flag will appear on the screen. This will let you know if you have entered a correct PIN.

IMPORTANT: Only one mToken may be activated per User ID at any one time, and thus activation of the mToken on a given User ID will result in the deactivation of the mToken that may have been formerly activated on it.

If you have entered incorrect PIN code, the generated token code will be declined by eBanking. The PIN verification flag helps you to check if your PIN code was correct. In case of incorrect PIN another flag will be displayed as at your mToken activation. If the flag displayed is not your associated security flag, the PIN code that you used is not valid. Please check your PIN code and correct it in the previous screen if needed. You can correct the PIN by pressing the Back button.

Functions of the app:

- Generating a token code
  Those clients who do not use a physical token can generate the token code that is required when signing into our eBanking service. Furthermore, they can sign non-payment transactions (e.g. free cash withdrawal) here.
- Generating e-Sign signature code
  You can generate the e-Sign code required to sign payment orders in the eBanking system by entering a 6-digit code and the transferable amount.
- Receiving Push notifications for signing transactions in eBanking
  If you have enabled Push notifications in the mToken settings, you can sign the transaction without generating a code, by authorizing the Push notification.
  IMPORTANT: in this case, the process will also end on the eBanking platform, because it is necessary to click the "Finalize" button after authorizing the Push notification. If you miss this step, the transaction will not be sent to the bank and will remain as a pending order among the items that require signing.
- Enter with fingerprint/face identification

The user can allow a suitable device to identify the user by identifying the face/fingerprint on their own responsibility. When using biometric identification, the system will not display the security flag.
IMPORTANT: In this case, the identifying face/fingerprint will be equivalent to the signature given by the owner of the account or by those made eligible by the owner that is accepted by the bank. The user is required to ensure that only the face and fingerprints of the user are recorded and stored.
The user is required to ensure that no other person uses face/fingerprint recognition on the device. When switching the function on, the user will be required to state that they use the face/fingerprint recognition function of the device exclusively. For a safer use, it is recommended to lock the device and to use identification when signing in.

If multiple private/company accounts are assigned to one user, the changing of the way of signing will affect all accounts. In the case of two or more eBanking users (private + company/private + private), SMS + mToken or two mToken codes can be used as signature. Two or more eBanking users require an mToken for each user, so one user is managing one mToken on one mobile device.
In the case of company signatures, the eligibilities under 10 points remain valid when the signature mode changes. The mToken is used by one signing party on behalf of the company. If multiple people sign orders, we recommend keeping SMS-signature and/or physical Tokens.

General informations
Technical requirements for using the services:
When downloading and activating the application: internet access (network or WiFi); for the usage of mToken, no internet connection is required, as it can be used in offline mode.
For smartphones:

- Apple iOS 9.0 operating system or higher version, or
- Google Android 4.4.3 operating system or higher version,
- minimum 480x800 screen resolution with minimum 225ppi (pixel per inch).

For tablets:

- minimum 7” screen,
- Android 4.4.3 or newer OS, or
- iOS 9.0 or newer OS, iPad 2 or newer device,
- GPS availability.

The running of service is guaranteed only on devices where the official restrictions of the manufacturer are not unlocked. The service is not guaranteed where jailbreak (iOS) or rooting (Android) has been implemented.

Functions	**release Android smartphone from version**	**iOS smartphone from version**
Exchange rate query	v1.10.	v2.4.
ATM and branch location finder	v1.10.	v2.4.
Call Center and social network contacts	v1.10.	v2.4.
Account information	v1.10.	v2.4.
Bankcard information	v1.10.	v2.4.
Managing term deposits	v1.10.	v2.4.
Transfers	v1.10.	v2.4.
Transfer between own different currency accounts with currency exchange	v2.0.14.	v2.10.
Managing forms and FastPay	v1.10.	v2.4.
App settings (PIN change, select language, sounds)	v1.10.	v2.4.
Log in with fingerprint	3.1.61.0.	4.1.121.
Push notifications of authorizations	3.3.37.0.	4.2.127.
Log in with face authentication	-	4.8.2.
mCash	3.7.12.0.	4.5.0.113.
Two-factor identification	3.11.66.	4.9.0.200.
Push notification for signing transactions	3.11.66.	4.9.0.200.