UniCredit mBanking mobile application Customer Information

Valid from 10th of December 2020

The UniCredit mBanking mobile application can be downloaded and used on 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 mBanking mobile application

UniCredit Bank Hungary Zrt.'s UniCredit mBanking mobile application can be used 24/7 to obtain information about the current balance of your bank accounts, savings and loans, 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 Mobile Application Services [UniCredit mBanking] and the mToken code generator.

The following functions are available in the application without activating the services:

- 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.

Users can install the UniCredit mBanking mobile application 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 activation. The terms of using the service are detailed in the General Business Conditions.

Would you like to use our services?

Both functions require activation. The services can be activated via Internetbank Services [UniCredit eBanking] user ID without visiting our branches, if you use SMS or mToken authentication for your payment orders..

If you do not have [UniCredit eBanking] user ID, but you would like to use [UniCredit mBanking] service, activation can be initiated during opening times with our branch consultants, or every day between 8AM and 6PM through our [UniCredit Telephone Banking] (after identification).

The [UniCredit mBanking] 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 [UniCredit mBanking]

Activation without [UniCredit eBanking] user ID:

1. **Receiving your user ID:** if you **do not own** a [UniCredit eBanking] user ID, please visit one of our branches or call the [UniCredit 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 digital user ID which you can use to activate the services.
2. **Initiating activation:** download and open the UniCredit mBanking mobile application, then click on the "Activate mBanking" option. Choose the „with digital user ID" option on the first screen, and enter your digital user ID on the next screen.
3. **Receiving your activation code:** we will send you your personal activation code in a text message (SMS) to your domestic mobile phone number. Clicking on the code will automatically paste the code into the appropriate field. 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 but the bank will automatically send new activation codes up to 3 times after the sending of the first code.

Setting the PIN code and the biometrical identifier: in order to ensure the safety of your personal data please set a PIN code for later use. Furthermore, you can also set a biometrical identifier on suitable devices. From now on you will have to sign in with one of these identification methods (PIN code, fingerprint, and face recognition on iPhone X or later iOS devices) when login the service or authorizing transactions.

Activation with [UniCredit eBanking] credentials:

1. **Starting the activation process:** download and start the application, then click on the "Activate mBanking" option. On the next screen choose„with eBanking credentials" option and enter your eBanking username and password on the next screen.
2. **Receiving your activation code:** if the data provided are valid and you use [UniCredit eBanking] service with SMS or mToken authorization, we will send you your personal activation code in a text message (SMS) to your domestic mobile phone number. Clicking on the code will automatically paste the code into the appropriate field.
3. **Setting the PIN code and biometrical identifier:** in order to ensure the safety of your personal data please set a PIN code for later use. Furthermore, you can also set a biometrical identifier on suitable devices. From now on you will have to sign in with one of these identification methods (PIN code, fingerprint and face recognition on iPhone X or later iOS devices) when login the service or authorizing transactions.

Please note that activation with [UniCredit 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 one of the activation methods 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 digits and may not contain 6 sequential numbers in increasing order (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 [UniCredit mBanking] service

- Account history
  - Balance and detailed account informations of bank account, savings and loans
  - Account history and transaction details
  - Sharing of account informations
  - Setting of secondary identifiers
- Categorization
  - Categorization of the expenses and incomes
  - Upload and categorize money transactions from other source
  - Analytics and reports based on the expenses and incomes
- Bank card information
  - Card overview and detailed information
  - Transaction history and transaction details
  - Receiving push messages confirming your online purchases
- 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
- Push notifications of incoming transactions
- Push Notifications for card transactions (for debit and credit cards as well)
- Managing term deposits
  - Term deposit query
  - Deposit order for existing deposit account
- Transfers
  - Ad-hoc bank-to-bank HUF transferAd-hoc in-bank HUF transfer
  - HUF transfers between own accounts

H-1054 Budapest
Szabadság tér 5-6.
Telefon: +36 1 325 3200
Mobiltelefon: +36 20/30/70 325 3200
Telefax: +36 1 353 49 59
www.unicreditbank.hu

- Transfer between own different currency accounts with currency exchange, calculated in HUF or foreign currency
- SEPA payment
- Creating new standing orders, editing and deleting existing standing orders
- Creating direct debit orders, editing and deleting existing direct debit orders

- Managing forms
  - Saving templates from created transactions
  - Automatic savings of the beneficiary datas
  - Creating a payment from template or saved beneficiary datas
  - Deletion of templates
- 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
- Login and signing orders with fingerprint or face recognition
  The user can allow a suitable device to identify the user by recognising the fingerprint or face recognition on iPhone X or later iOS devices 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.
- Scan & Pay
  - 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. To scan the check properly, please follow the instructions appearing on the screen of the application!
    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 that the entire segment content has to 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.
- [UniCredit mBanking] settings
  - Choosing language
  - Turn on-off the widget
  - Changing PIN code
  - Turn on-off the biometrical identifications
  - 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

H-1054 Budapest
Szabadság tér 5-6.
Telefon: +36 1 325 3200
Mobiltelefon: +36 20/30/70 325 3200
Telefax: +36 1 353 49 59
www.unicreditbank.hu

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.

When applying for the activation code through the UniCredit branch or [UniCredit Telephone Banking] , unique daily and transaction limits can be rendered to the service; while if you activate with [UniCredit 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 mBanking mobile application 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 mBanking mobile application. With mToken you can generate login codes for [UniCredit eBanking] system and e-Sign code for the transactions made there which are valid for a maximum of 3,5 minutes.
In order to use the mToken, Users will need to download the UniCredit mBanking mobile application and activate the mToken function. The mToken function may be activated independently of the [UniCredit mBanking].

Activation of mToken

Activation without [UniCredit eBanking] user ID:

1. **Digital user ID:** if you **do not own** a [UniCredit eBanking] identification number please visit one of our branches or call the [UniCredit 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 digital user ID which you can use to activate the services.
2. **Initiating activation:** download and open the UniCredit mBanking mobile application, then click on the "Activate mToken" option. Choose the „with digital user ID" option on the first screen, and enter your digital user ID on the next screen.
3. **Receiving your activation code:** we will send you your personal activation code in a text message (SMS) to your domestic mobile phone number. Clicking on the code will automatically paste the code into the appropriate field. 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 but the bank will automatically send new activation codes up to 3 times after the sending of the first code.
4. **Setting the PIN code and the biometrical identifier:** in order to ensure the safety of your personal data please set a PIN code for later use. Furthermore, you can also set a biometrical identifier on suitable devices. From now on you will have to sign in with one of these identification methods (PIN code, fingerprint and face recognition on iPhone X or later iOS devices) when login the service or authorizing transactions.
5. **Security flag:** After entering your PIN code, a security flag appears on the screen. This feature is to check whether the right PIN code has been entered before.

Activation with [UniCredit eBanking] credentials:

1. **Starting the activation process:** download and start the application, then click on the "Activate mToken" option. On the next screenchoose„with eBanking credentials" option and enter your eBanking username and password on the next screen.
2. **Receiving your activation code:** if the data provided are valid and you use [UniCredit eBanking] with SMS authorization, we will send you your personal activation code in a text message (SMS) to your domestic mobile phone number. Clicking on the code will automatically paste the code into the appropriate field.
3. **Setting the PIN code and biometrical identifier:** in order to ensure the safety of your personal data please set a PIN code for later use. Furthermore, you can also set a biometrical identifier on suitable devices. From now on you will have to sign in with one of these identification methods (PIN code, fingerprint and face recognition on iPhone X or later iOS devices) when login the service or authorizing transactions
4. **Security flag:** After entering your PIN code, a security flag appears on the screen. This feature is to check whether the right PIN code has been entered before.

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 [UniCredit eBanking]. The PIN verification flag helps you to check if your PIN code was correct. In case of incorrect PIN another flag will be

H-1054 Budapest
Szabadság tér 5-6.
Telefon: +36 1 325 3200
Mobiltelefon: +36 20/30/70 325 3200
Telefax: +36 1 353 49 59
www.unicreditbank.hu

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.

The following functions are available through the mToken service:

- 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 [UniCredit eBanking] service. Furthermore, they can sign non-payment transactions (e.g. free cash withdrawal) using the codes generated via this service.
- Generating e-Sign code
  You can generate the e-Sign code required to sign payment orders in the [UniCredit eBanking] system by entering a 6-digit code and the transferable amount.
- Receiving Push notifications for signing transactions in [UniCredit 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 [UniCredit eBanking] platform, because it is necessary to click the "Finalize" button in [UniCredit eBanking], 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.
- Login and transaction signing with fingerprint or face recognition on iPhone X or later iOS devices
  The user can enable for own responsibility the biometric identify for login and transaction signing on the suitable mobile devices. When using biometric identification, the system will not display the security flag.
  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.

If multiple private/company accounts are assigned to one [UniCredit eBanking] user, the changing of the way of signing will affect all accounts. In the case of two or more [UniCredit eBanking] users (private + company/private + private), SMS + mToken or two mToken codes can be used as signature. Two or more [UniCredit 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

Minimal technical requirements for using the services:
For download the UniCredit mBanking mobile application, using the free functions and the [UniCredit mBanking]: internet access (mobile network or WiFi) required; 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,

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	UniCredit mBanking mobile application version number (Android)	UniCredit mBanking mobile application version number (iOS)
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.
Managing forms and FastPay	v1.10.	v2.4.
App settings (PIN change, select language, sounds)	v1.10.	v2.4.
Transfer between own different currency accounts with currency exchange	2.0.14.	2.10.
Authentication with mToken	2.7.21.1.	3.2.14.
Card limit change	2.11.16.	3.4.17.
Direct debits	3.0.65.	4.0.48.
Debitcard activation	3.1.64.2.	4.1.132.
Creditcard repayment	3.1.64.2.	4.1.132.
Push notifications of incoming transactions	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.
Log in and transaction signing with fingerprint	3.13.34.0	4.10.0.150
Log in and transaction signing with face recognition	-	4.10.0.150
Push notifications for card transactions	3.15.31.0	4.12.0.149
Instant payment and Secondary identifier	3.15.36.	4.12.1.
Display of certain fees and cross-currency conversion fees for cross-border payments in euro within the Union	3.17.14.	4.14.0.117.
New design, Categorization, Analytics, Widget	4.6.59.	5.5.63.
Handling of saving accounts	4.15.4.2.	5.14.4.
SEPA payment, Direct debit orders, Refresh the Accounts page	4.18.12.0.	5.17.20.

UniCredit Bank Hungary Zrt.
H-1054 Budapest
Szabadság tér 5-6.
Telefon: +36 1 325 3200
Mobiltelefon: +36 20/30/70 325 3200
Telefax: +36 1 353 49 59
www.unicreditbank.hu