

UniCredit mBanking mobilalkalmazás ügyféltájékoztató

hatályos 2025. december 15-től

Az UniCredit mBanking mobilalkalmazás Android, iOS vagy EMUI/HarmonyOS rendszerű, internetkapcsolattal rendelkező okostelefonra vagy tabletre tölthető le az Apple App Storeból, a Google Play Storeból és a Huawei AppGalleryből. Az alkalmazás bejelentkezést igénylő funkcióit csak a szolgáltatások (mBanking és mToken) aktiválását követően lehet használni. (A nagy kezdőbetűs kifejezések a Bank Általános Üzleti Feltételeiben meghatározott tartalommal bírnak.)

UniCredit mBanking mobilalkalmazás

Az UniCredit Bank Hungary Zrt. mobilalkalmazásának segítségével a hét bármely napján, a nap 24 órájában tájékozódhat bankszámláinak, megtakarításainak és hiteleinek aktuális egyenlegéről, átutalásokat, saját számlák közötti átvezetéseket vagy betétlekötéseket kezdeményezhet, és bankkártya nélkül vehet fel készpénzt.

Az alkalmazáson keresztül két szolgáltatás érhető el: mobilalkalmazási szolgáltatásunk az [UniCredit mBanking] és az mToken kódgeneráló.

Az alkalmazásban a szolgáltatások aktiválása nélkül az alábbi funkciók érhetőek el:

- online számlanyitás (EMUI/HarmonyOS rendszeren nem érhető el)
- online hiteligénylés (EMUI/HarmonyOS rendszeren nem érhető el)
- árfolyamok lekérdezése;
- kiterjesztett ATM- és fiókkereső – a címadatok az összes UniCredit országból megjelennek az ATM és fiókkeresőben; (EMUI/HarmonyOS rendszeren nem érhető el)
- ügyfélszolgálati és közösségi média elérhetőségek.

Az UniCredit mBanking mobilalkalmazást egy felhasználó több készüléken is használhatja. Külön, tabletre optimalizált verzió 2018. június 26-tól már nem elérhető, de a mobilverzió tableten is használható, aktiválást követően. A szolgáltatás részletes szabályait az Általános Üzleti Feltételek tartalmazza.

Szeretné igénybe venni szolgáltatásainkat?

Mindkét szolgáltatás használatához azok aktiválása szükséges. A szolgáltatásokat az internetbanki szolgáltatásban eBanking meglévő felhasználói azonosítójával bankfiók meglátogatása nélkül is aktiválhatja amennyiben megbízásaihoz SMS- vagy mToken-hitelesítést használ.

Ha nem rendelkezik eBanking-azonosítóval, de szeretné használni az mBanking szolgáltatást, erre vonatkozó igényét jelezheti nyitvatartási időben bármelyik bankfiókunkban, vagy minden nap 8:00 és 18:00 óra között, azonosítást követően a Telefonbankon keresztül.

Az mBanking szolgáltatás jelenleg az UniCredit magánszemély ügyfelei részére érhető el, és a szolgáltatást kizárólag a fizetési számla, vagy a hitelkártya elszámolási számla számlatulajdonosa igényelheti saját részére.

Az mBanking szolgáltatás aktiválása

Aktiválás eBanking felhasználó azonosítóval

1. **Aktiválás elindítása:** töltse le és indítsa el az alkalmazást, majd klikkeljen az „mBanking aktiválása” gombra. Az első oldalon válassza az „eBanking felhasználói azonosítóval,” opciót, az azonosítás képernyőn pedig adja meg eBanking felhasználó-nevét és jelszavát.
2. **Aktiváló-kód fogadása:** ha érvényesek a megadott adatok, és ön az eBanking szolgáltatást SMS- vagy mToken-hitelesítéssel használja, egyedi aktiváló kódját SMS-ben küldjük el az ön által megadott belföldi mobilszámra. A kódra kattintva az alkalmazás automatikusan beilleszti azt a megfelelő mezőbe.
3. **PIN-kód és biometrikus azonosító megadása:** az ön adatainak biztonsága érdekében szükséges rögzítenie egy legalább 6, legfeljebb 16 számjegyből álló PIN-kódot, de emellett arra alkalmas készülékeken beállíthat biometrikus azonosítót is. A továbbiakban csak ezen azonosítók egyikét (PIN-kód, ujjlenyomat, arcfelismerés) használva tud majd belépni a szolgáltatásba, vagy tudja jóváhagyni tranzakcióit. A PIN-kód nem állhat

egymást követő, növekvő sorrendbe helyezett számjegyekből (pl.: 123456), egymást követő azonos számjegypárokból (pl.: 112233), és nem lehet benne 4 azonos számjegy egymás után (pl.: 111123).

Aktiválás digitális userID-val (eBanking felhasználói azonosító nélkül)

1. **Digitális user ID** -ját a fiókban történt szerződéskötéskor kapja meg, de a későbbiekben a Telefonbankon keresztül is tud ezzel kapcsolatos segítséget kérni a +36 (1/20/30/70) 325 3200-ás telefonszámon, a hét minden napján 8:00 és 18:00 óra között, a megfelelő azonosítás után.
2. **Aktiválás elindítása:** töltse le, telepítse és indítsa el az UniCredit mBanking mobilalkalmazást, majd klikkeljen az „mBanking aktiválása” gombra. Ha ismeri a Digitális user ID-ját, de nincs érvényes aktiváló kódja, akkor is fel kell keresnie egy bankfiókot vagy a Telefonbankot, hogy létrehozzanak az ön számára egy új aktiváló kódot.
3. **Aktiváló-kód fogadása:** a Digitális user ID-val való aktiválás opció elindítása utáni első lépésnél adja meg Digitális userID-ját. Ha felvette a kapcsolatot valamelyik kollégánkkal és ezáltal létrehoztak önnek egy aktiváló kódot, akkor az oldalról való továbblépés után SMS-ben fogja megkapni azt. Androidos készüléknél az alkalmazás automatikusan be fogja olvasni az aktiváló kódot, ha az SMS megérkezésének pillanatában még a Visszaszámláló oldalon tartózkodik. iOS operációs rendszerű készülékeken, az aktiváló kód kattintható az SMS-ben, így nincs szüksége annak manuális beírására. Az SMS-ben elküldött aktiváló kódok a küldéstől számított 3 napig érvényesek. Ha az aktiválás 3 napon belül nem történik meg, új kód igénylése szükséges, de a Bank az első aktiváló kód megküldését követően legfeljebb 3 alkalommal a Felhasználó kérése nélkül is újraküldi az aktiváló kódot.
4. **PIN-kód és biometrikus azonosító megadása:** az ön adatainak biztonsága érdekében szükséges rögzítenie egy legalább 6, legfeljebb 16 számjegyből álló PIN-kódot, de emellett arra alkalmas készülékeken beállíthat biometrikus azonosítót is. A továbbiakban csak ezen azonosítók egyikét (PIN-kód, ujjlenyomat, arcfelismerés) használva tud majd belépni a szolgáltatásba, vagy tudja jóváhagyni tranzakcióit. A PIN-kód nem állhat egymást követő, növekvő sorrendbe helyezett számjegyekből (pl.: 123456), egymást követő azonos számjegypárokból (pl.: 112233), és nem lehet benne 4 azonos számjegy egymás után (pl.: 111123).

Felhívjuk a figyelmét, hogy az eBanking felhasználói azonosítóval történő aktiválás a 8:00 és 18:00 óra közötti időszakon kívül lassabb lehet.

Ha több saját eszközön is szeretné használni az alkalmazást, akkor mindegyiken külön kell aktiválnia, a fentebb leírt módszerek valamelyikével.

Felhívjuk figyelmét, hogy az SMS-ben küldött aktiváló kódot kizárólag az alkalmazásban, a szolgáltatások aktiválása során adhatja meg. Az aktiváló kód harmadik fél részére történő továbbítása, vagy bármely más felületen (pl. weboldalon) történő megadása illetéktelen hozzáférést eredményezhet!

Az mBanking szolgáltatáson keresztül a következő szolgáltatások vehetők igénybe

- Számlainformációk
 - Bankszámlák, megtakarítások, hitelek egyenlege és a számlák részletes adatainak lekérdezése
 - Számlatörténet és a tranzakciók részleteinek lekérdezése
 - Költsékekkel és bevételekkel kapcsolatos hasznos információk megjelenítése a számlatörténetben
 - Számlaadatok megosztása
 - Másodlagos azonosítók beállítása
 - Hitelvisszafizetési ütemterv emailben való kiküldése
- mCash

Ezzel a funkcióval bankkártya nélkül, egy egyedi azonosító kód létrehozásával vehet fel készpénzt UniCredit ATM-ből.
- Kategorizálás
 - Kiadások és bevételek kategorizálása
 - egyéb forrásból történt pénzmozgás feltöltése és kategorizálása (pl.: készpénzes vásárlások)
 - analitika és riportok a bevételek és kiadások alapján
- Online értékpapírszámla-nyitás
- Befektetés modul (EMUI/HarmonyOS rendszeren nem érhető el)

Értékpapírszámlával rendelkező ügyfeleink számára érhető el. Egyenleg ellenőrzésére, utolsó ismert árfolyamok és hozaminformációk megtekintésére, lakossági állampapír vételére, befektetési alap és BÉT részvény vételére és eladására van benne lehetőség.

- Átutalások
 - Eseti forintátutalás bankon kívül
 - Eseti forintátutalás bankon belül
 - Saját számlák közötti átvezetés forintban
 - Saját forint- és devizaszámla közötti átvezetés konverzióval, forintban vagy devizában megadva
 - SEPA átutalás
 - Állandó átutalási megbízások rögzítése, meglévő állandó átutalási megbízások módosítása, törlése
 - Állandó átutalási megbízás létrehozása könyvelt, kimenő tranzakcióból
 - Csoportos beszedési megbízások rögzítése, meglévő megbízások módosítása, törlése

Az mBanking szolgáltatásban létrehozott átutalásokhoz és átvezetésekhez, bankfiókban vagy megfelelő azonosítást követően Telefonbankon keresztül való szerződéskötéskor Felhasználó szintű napi limitet, Felhasználó szintű tranzakciós limitet és Számla szintű napi limitet lehet beállítani. A Felhasználó szintű tranzakciós limit és a Számla szintű napi limit az Általános Üzleti Feltételekben meghatározott alapértelmezett értékekkel lép életbe. A Felhasználó szintű napi limitnek nincs alapértelmezett értéke, de ha be van állítva, akkor a felhasználóhoz tartozó összes számlára együttesen érvényes és a Számla szintű napi limitek felett áll. Beállítása nélkül a Számla szintű napi limitek a mérvadók az egyes számlákra vonatkozóan.

Az átutalásra vonatkozó limitek biztonsági okokból nem módosíthatóak az mBanking szolgáltatásban csak bankfiókban vagy Telefonbankon keresztül.

- Fizetési kérelem küldése, fogadása és a kérelmek kezelése (a funkcióhoz push üzenetküldés is kapcsolódik, ami alapértelmezetten nincs bekapcsolva. Ezt az ügyfél tudja megtenni az Egyéb/Beállítások/Push értesítések/Számlaértesítések oldalon) (EMUI/HarmonyOS rendszeren nem érhető el)
- Sablonok és kedvezményezettek kezelése
 - Létrehozott megbízások mentése sablonként
 - Kedvezményezett adatainak automatikus mentése
 - Megbízás létrehozása mentett adatokkal vagy sablonnal
 - Sablonok és kedvezményezettek törlése
- Beolvasás és fizetés
 - Csekkbeolvasás

Az alkalmazásban található "Csekkbeolvasás" funkció, okostelefonja kamerájának segítségével beolvassa a befizetni kívánt postai csekk adatait, majd a beolvasott adatok alapján egy automatikusan kitöltött átutalási megbízást készít. A csekk sikeres beolvasásához fontos, hogy a képernyőn megjelenő utasításoknak megfelelően használja a szolgáltatást!

A funkció nem alkalmas kézzel kitöltött csekkek és QR-kódok beolvasására.
 - Részletek beolvasása

Az alkalmazás, az okostelefonja kamerájának segítségével mezőnként beolvassa a befizetni kívánt számla adatait, majd egy ez alapján automatikusan kitöltött átutalási megbízást készít. A számla adatainak sikeres beolvasásához fontos, hogy a számlának az adott információt tartalmazó része teljes terjedelmében a képernyőn látható keretbe illeszkedjen.

A funkció nem alkalmas kézzel kitöltött számlaadatok és QR-kódok beolvasására.

FONTOS: Az automatikusan kitöltött átutalási megbízáson minden esetben ellenőrizze a kedvezményezett számlaszámát, összeget és a közlemény mezőbe kerülő „Megbízóazonosító”-t, hogy megfelelő összeg kerüljön befizetésre, illetve egyértelműen beazonosítható legyen a befizető fél. A "Kedvezményezett neve" mező beolvasása során előfordulhatnak karakterhibák, ez azonban nem befolyásolja a fizetés teljesülését. Betéti kártya aktiválása
 - Átutalás QR-kód beolvasásával (EMUI/HarmonyOS rendszeren nem érhető el)

Egységes adatbeviteli megoldással kezdeményezett azonnali átutalás (qvik). A funkció egyben tartalmazza az érintéses fizetést biztosító NFC alapú, valamint az úgynevezett deeplink alapú fizetési megoldásokat is.
- Bankkártya aktiválása
- Bankkártya információk
 - Kártya áttekintő és a kártya részletes adatainak lekérdezése
 - Tranzakciótörténet és az egyes tranzakciók részletes adatainak lekérdezése
 - Online vásárlást hitelesítő push üzenet fogadása (EMUI/HarmonyOS rendszeren nem érhető el)

- PIN-kód megtekintés
- Bankkártya aktiválása az ApplePay és GooglePay szolgáltatásokba (EMUI/HarmonyOS rendszeren nem érhető el)
- Betéti kártya felfüggesztése és annak feloldása
Nem egyenértékű a Telefonbankon keresztül vagy fiókban intézett kártya lezárással, így új kártya igénylés nélkül, gyorsan felfüggesztheti kártyáját, ezzel korlátozva használatának lehetőségét, ha azt gyanítja, hogy elhagyta vagy eltulajdonították annak adatait. Kizárólag az mBanking szolgáltatásban felfüggesztett kártyákat lehet ugyanígy feloldani.
- Kártya-limitek módosítása
 - Bankkártyás készpénzfelvételi limit
 - Kártyás vásárlási limit
 - Internetes vásárlási limit(A limitek abban az esetben nem módosíthatóak mBankingben, ha a három közül valamelyiknél a mBankingben beállíthatónál magasabb limit lett beállítva bankfiókban vagy Telefonbankon keresztül.)
- Hitelkártya törlesztés (túlfizetési lehetőséggel)
- Kártya+ Kedvezményprogram
Lakossági betéti- és hitelkártyához kapcsolódó kedvezményprogram.
- Lekötött betétek kezelése
 - Lekötött betétek lekérdezése
 - Betétlekötés meglévő betétszámlára
- Termékeink listája
- Profilom oldal
Tartalmazza a személyes adatokat illetve lehetőséget ad a kapcsolattartási email cím és telefonszám módosítására, valamint a kivonatok kézbesítési módjának kezelésére.
- Banki üzenetek fogadása
- Bemutató videók az alkalmazás funkcióiról (EMUI/HarmonyOS rendszeren nem érhető el)
- Dokumentumok
 - Elektronikusan aláírt dokumentumok
 - Havi számlakivonatok
 - Hitelkártya számlakivonatok
 - Éves díjkimutatások
- Azonnali blokkolás funkció (EMUI/HarmonyOS rendszeren nem érhető el)
Az ügyfélnek lehetősége van azonnali hatállyal blokkolni a digitális szolgáltatásait és bankkártyáit. A funkció tipikus alkalmazási esete, ha az ügyfél azt észlelte vagy azt gyanítja, hogy csalók vagy bármely illetéktelen harmadik személy férhetett hozzá digitális azonosítóihoz vagy bankkártyáihoz, hitelesítő adataihoz és fennáll a veszélye annak, hogy illetéktelenek használják a bankszámláját. A blokkolást követően az ügyfelet azonnal kizárjuk a digitális szolgáltatásokból és minden aktivált eszközt inaktíválunk, valamint letiltjuk a bankkártyáit.
- A feltört (jailbreakelt, rootolt) eszközök felismerése
Az aktiválás során az alkalmazás figyelmezteti Önt, ha a mobilkészítő gyártói korlátozása korábban fel lett törve. Tekintettel arra, hogy ilyen esetben az UniCredit mBanking mobilalkalmazás működése nem garantált, az aktiválás csak ezen kockázatok tudomásul vételét és elfogadását követően folytatódhat.
- Ujjlenyomattal vagy arcfelismeréssel való bejelentkezés és tranzakció aláírás
Arra alkalmas, megfelelő tanúsítványokkal rendelkező hardverrel ellátott készülékeken a Felhasználó saját felelősségére engedélyezheti, hogy a Felhasználó azonosítása bejelentkezéskor a mobilkészítő által elvégzett ujjlenyomat-azonosítással vagy arcfelismeréssel történjen.

Androidos készülékeken a legalább CLASS3 szintű tanúsítvánnyal rendelkező eszközök felelnek meg a biztonsági követelményeknek. Az Android operációs rendszerhez kapcsolódó tanúsítványokról az Android weboldalon* olvashat részletesebben. Az iOS-es készülékeken a Secure Enclave környezetben tárolt biometrikus adatok felelnek meg a biztonsági követelményeknek. Az iOS operációs rendszerhez kapcsolódó tanúsítványokról az Apple weboldalon** olvashat részletesebben. A továbbiakban csak a beállított azonosítási módok egyikét (PIN-kód, ujjlenyomat, arcfelismerés) használva tud majd belépni a szolgáltatásba, vagy tudja tudja jövőbeli tranzakcióit.

*https://source.android.com/compatibility/12/android-12-cdd#7_3_10_biometric_sensors

******<https://developer.apple.com/design/human-interface-guidelines/ios/user-interaction/accounts/>

FONTOS: Az ujjlenyomat és az arcfelismerés ebben az esetben a Számlatulajdonos, illetve a Számlatulajdonos által bejelentett rendelkezésre jogosult által a Bank részére megadott és a Bank által elfogadott aláírás minta szerinti aláírással egyenértékű. Ujjlenyomattal vagy arcfelismeréssel történő azonosítás használata esetén a Felhasználó köteles gondoskodni arról, hogy a készüléken kizárólag a Felhasználó ujjlenyomatai és arca kerüljön rögzítésre, tárolásra.

A Felhasználó köteles kellő gondossággal eljárni, hogy ujjlenyomat-azonosítást és arcfelismerést a mobil eszközön a Felhasználón kívül más személy ne alkalmazhasson! A Felhasználónak a funkció bekapcsolásakor nyilatkoznia kell arról, hogy a készülék ujjlenyomat-azonosító és arcfelismerő funkcióját kizárólagosan alkalmazza. A még biztonságosabb használat érdekében ajánlatos a mobilkészítőt zárolni és az eszközbe való belépéshez azonosítót alkalmazni!

- mBanking beállításai
 - nyelv kiválasztása
 - widget ki-be kapcsolása
 - PIN-kód módosítása
 - biometrikus azonosítók ki-be kapcsolása
 - push értesítések kezelése (EMUI/HarmonyOS rendszeren nem érhető el)
 - jóváírásokról szóló push értesítések és az azokhoz tartozó limitek beállítása
 - visszautasított tranzakciókról szóló értesítések
 - fizetési kérelemmel kapcsolatos értesítések (küldésről, fogadásról, kifizetésről, elutasításról és közlő lejáratáról – FONTOS, hogy ezek az értesítések alapértelmezetten nincsenek bekapcsolva)
 - lekötött betét lejáratáról szóló értesítések
 - kártyatranzakciós értesítések
 - kiegészítő információk be-ki kapcsolása
 - harmadik feles felhatalmazások beállítása (TPP)

A harmadik feles szolgáltatók azon (átutaláskezdemenyezési illetve számlainformációs szolgáltatásokat kínáló) piaci szereplők, akik – a megfelelő engedélyek és felhatalmazások megszerzését követően – jogosultak a banki adatok lekérdezésére, illetve átutaláskezdemenyezésre szolgáló nyílt interfész (open API) használatára, hogy szolgáltatásokat nyújthassanak az online is hozzáférhető számlával rendelkező ügyfelek számára. Ebben a menüpontban lehetőség van ezen harmadik feles szolgáltatókkal kapcsolatos engedélyek kezelésére, és az ilyen szolgáltatókon keresztül végzett lekérdezések, tranzakciók listázására, szűrésére.

mToken (mobil token) hitelesítés

Az mToken az UniCredit mBanking mobilalkalmazáson keresztül elérhető szoftver alapú, PIN-kóddal védett kódgeneráló szolgáltatás. A szolgáltatás használatával az eBanking rendszerbe való belépéshez szükséges belépési kódot, az ott készített megbízásokhoz használható e-Sign aláíró kódot készítheti el, amely maximum 3.5 percig érvényes.

Az mToken igénybe vételéhez az UniCredit mBanking mobilalkalmazás letöltése és az mToken szolgáltatása aktiválása szükséges. Az mToken szolgáltatás az mBanking szolgáltatástól függetlenül aktiválható.

Az mToken aktiválása

Aktiválás eBanking felhasználó azonosítóval

1. **Aktiválás elindítása:** töltse le és indítsa el az alkalmazást, majd klikkeljen az „mToken aktiválása” opcióra. Az első oldalon válassza az „eBanking felhasználói azonosítóval,” opciót, az azonosítás képernyőn pedig adja meg eBanking felhasználó-nevét és jelszavát.
2. **Aktiváló-kód fogadása:** ha érvényesek a megadott adatok, és Ön az eBanking szolgáltatást SMS- vagy mToken-hitelesítéssel használja, egyedi aktiváló kódját SMS-ben küldjük el az Ön által megadott belföldi mobilszámra. A kódra kattintva az alkalmazás automatikusan beilleszti azt a megfelelő mezőbe.
3. **PIN-kód és biometrikus azonosító megadása:** az Ön adatainak biztonsága érdekében szükséges rögzítenie egy legalább 6, legfeljebb 16 számjegyből álló PIN-kódot, de emellett arra alkalmas készülékeken beállíthat biometrikus azonosítót is. A továbbiakban csak ezen azonosítók egyikét (PIN-kód, ujjlenyomat, arcfelismerés) használva tud majd belépni a szolgáltatásba, vagy tudja jóváhagyni tranzakcióit. A PIN-kód nem állhat

egymást követő, növekvő sorrendbe helyezett számjegyekből (pl.: 123456), egymást követő azonos számjegypárokból (pl.: 112233), és nem lehet benne 4 azonos számjegy egymás után (pl.: 111123).

4. **PIN-ellenőrző zászló:** mToken aktiválásakor, a PIN-kód megadása után megjelenik majd egy PIN-ellenőrző zászló, amivel a későbbiekben ellenőrizheti, hogy helyes PIN-kódot adott-e meg a belépésnél.

Aktiválás digitális userID-val

1. **Digitális user ID-ját** a fiókban történt szerződéskötéskor kapja meg, de a későbbiekben a Telefonbankon keresztül is tud ezzel kapcsolatos segítséget kérni a +36 (1/20/30/70) 325 3200-ás telefonszámon, a hét minden napján 8:00 és 18:00 óra között, a megfelelő azonosítás után.
2. **Aktiválás elindítása:** töltse le, telepítse és indítsa el az UniCredit mBanking mobilalkalmazást, majd klikkeljen az „mToken aktiválása” opcióra. Ha ismeri a Digitális userID-ját, de nincs érvényes aktiváló kódja, akkor is fel kell keresnie egy bankfiókot vagy a Telefonbankot, hogy létrehozzanak az ön számára egy új aktiváló kódot.
3. **Aktiváló-kód fogadása:** a Digitális userID-val való aktiválás opció elindítása utáni első lépésnél adja meg Digitális userID-ját. Ha felvette a kapcsolatot valamelyik kollégánkkal és ezáltal létrehoztak önnek egy aktiváló kódot, akkor az oldalról való továbblépés után SMS-ben fogja megkapni azt. Androidos készüléknél az alkalmazás automatikusan be fogja olvasni az aktiváló kódot, ha az SMS megérkezésének pillanatában még a Visszaszámláló oldalon tartózkodik. iOS operációs rendszerű készülékeken, az aktiváló kód kattintható az SMS-ben, így nincs szüksége annak manuális beírására. Az SMS-ben elküldött aktiváló kódok a küldéstől számított 3 napig érvényesek. Ha az aktiválás 3 napon belül nem történik meg, új kód igénylése szükséges, de a Bank az első aktiváló kód megküldését követően legfeljebb 3 alkalommal a felhasználó kérése nélkül is újraküldi az aktiváló kódot.
4. **PIN-kód és biometrikus azonosító megadása:** az Ön adatainak biztonsága érdekében szükséges rögzítenie egy legalább 6, legfeljebb 16 számjegyből álló PIN-kódot, de emellett arra alkalmas készülékeken beállíthat biometrikus azonosítót is. A továbbiakban csak ezen azonosítók egyikét (PIN-kód, ujjlenyomat, arcfelismerés) használva tud majd belépni a szolgáltatásba, vagy tudja jóváhagyni tranzakcióit. A PIN-kód nem állhat egymást követő, növekvő sorrendbe helyezett számjegyekből (pl.: 123456), egymást követő azonos számjegypárokból (pl.: 112233), és nem lehet benne 4 azonos számjegy egymás után (pl.: 111123).
5. **PIN-ellenőrző zászló:** mToken aktiválásakor a PIN-kód megadása után megjelenik majd egy PIN-ellenőrző zászló, amivel a későbbiekben ellenőrizheti, hogy helyes PIN-kódot adott-e meg a belépésnél.

FONTOS: Egy Felhasználói azonosítóhoz kapcsolódóan egy időben csak egy mToken lehet aktiválva, ennek következtében az adott Felhasználói azonosítóhoz kapcsolódóan végrehajtott új aktiválás a korábban aktivált mToken deaktiválását eredményezi.

Ha az mToken generálását megelőzően helytelen PIN-kódot adott meg, az eBanking vissza fogja utasítani a generált kódot. A PIN-ellenőrző zászló lehetőséget biztosít a megadott PIN-kód helyességének előzetes ellenőrzésére, mivel hibás PIN-kód esetén nem a kezdeti beállításkor bemutatott zászlót jeleníti meg. Ha a megjelenített zászló nem az Ön biztonsági ellenőrző zászlója, akkor az Ön által megadott PIN-kód érvénytelen. A helyes PIN-kód megadására a Vissza gomb megnyomásával van lehetőség.

Az mToken szolgáltatáson keresztül a következő funkciók érhetőek el:

- token-kód generálás
Fizikai tokent nem használó Felhasználóink az eBanking szolgáltatásba való bejelentkezéskor a felhasználói azonosító és a jelszó megadása után szükséges azonosító kódot tudják a szolgáltatás segítségével előállítani legenerálni, valamint nem fizetési tranzakciókat (pl.: ingyenes készpénzfelvétel) írhatnak alá a szolgáltatás segítségével előállított kódok használatával.
- e-Sign-kód generálás
Az eBanking rendszerben, az adott megbízások hitelesítéséhez szükséges e-Sign-kód állítható elő a szolgáltatás segítségével, egy 6 számjegyből álló kód és az utalandó összegnek a megadásával.
- Push üzenetek fogadása eBankingben létrehozott tranzakciók aláírásához
Amennyiben engedélyezte a Push üzeneteket az mToken beállításában, lehetősége van kódgenerálás nélkül, a kapott Push üzenet jóváhagyásával aláírni a tranzakcióit. (EMUI/HarmonyOS rendszeren nem érhető el)
FONTOS: a folyamat ebben az esetben is az eBanking felületen ér véget, mert a Push üzenet jóváhagyása után az eBankingban még szükséges a tranzakció véglegesítése. Ha ez elmarad, a tranzakcióit nem küldi be a bankba, hanem azok függő tételként az aláírandó tételek között maradnak.
- Ujjlenyomattal vagy arcfelismeréssel való bejelentkezés és tranzakció aláírás

Arra alkalmas, megfelelő tanúsítványokkal rendelkező hardverrel ellátott készülékeken a Felhasználó saját felelősségére engedélyezheti, hogy a Felhasználó azonosítása bejelentkezéskor a mobilkészítők által elvégzett ujjlenyomat-azonosítással vagy arcfelismeréssel történjen.

Androidos készülékeken a legalább CLASS3 szintű tanúsítvánnyal rendelkező eszközök felelnek meg a biztonsági követelményeknek. Az Android operációs rendszerhez kapcsolódó tanúsítványokról az Android weboldalon* olvashat részletesebben. Az iOS-es készülékeken a Secure Enclave környezetben tárolt biometrikus adatok felelnek meg a biztonsági követelményeknek. Az iOS operációs rendszerhez kapcsolódó tanúsítványokról az Apple weboldalon** olvashat részletesebben. A továbbiakban csak a beállított azonosítási módok egyikét (PIN-kód, ujjlenyomat, arcfelismerés) használva tud majd belépni a szolgáltatásba, vagy tudja jóváhagyni tranzakcióit.

*https://source.android.com/compatibility/12/android-12-cdd#7_3_10_biometric_sensors

**<https://developer.apple.com/design/human-interface-guidelines/ios/user-interaction/accounts/>

Biometrikus azonosítás esetén az alkalmazás nem jeleníti meg a biztonsági ellenőrző zászlót.

FONTOS: Az ujjlenyomat és az arcfelismerés ebben az esetben a Számlatulajdonos, illetve a Számlatulajdonos által bejelentett rendelkezésre jogosult által a Bank részére megadott és a Bank által elfogadott aláírás minta szerinti aláírással egyenértékű. Ujjlenyomattal vagy arcfelismeréssel történő azonosítás használata esetén a Felhasználó köteles gondoskodni arról, hogy a készüléken kizárólag a Felhasználó ujjlenyomatai és arca kerüljön rögzítésre, tárolásra.

A Felhasználó köteles kellő gondossággal eljárni, hogy ujjlenyomat-azonosítást és arcfelismerést mobil eszközön a Felhasználón kívül más személy ne alkalmazzon! A Felhasználónak a funkció bekapcsolásakor nyilatkoznia kell arról, hogy a készülék ujjlenyomat-azonosító és arcfelismerő funkcióját kizárólagosan alkalmazza. A még biztonságosabb használat érdekében ajánlatos a mobilkészítők zárolni és az eszközbe való belépéshez azonosítót alkalmazni!

Általános információk

A szolgáltatások igénybe vételéhez szükséges technikai feltételek:

UniCredit mBanking mobilalkalmazás letöltése, internetkapcsolat a szolgáltatások aktiválásához és az mBanking használatához (mobilhálózati vagy WiFi); (az mToken használatához nem szükséges internetkapcsolat, mivel az mToken offline, azaz internetkapcsolat nélküli módban is használható).

Minimális technikai feltételek a telepítéshez és frissítéshez:

Okostelefonokhoz:

- legalább iOS 13 vagy annál újabb verziójú operációs rendszer, vagy
- legalább Android 7 vagy annál újabb verziójú operációs rendszer,
- legalább EMUI 10 vagy annál újabb verziójú operációs rendszer,
- legalább HarmonyOS 2.0 vagy annál újabb verziójú operációs rendszer,
- a kijelző minimum felbontása 480x800 képpont, képpontsűrűsége minimum 225 képpont per hüvelyk (ppi = pixel per inch),

tablet esetén:

- legalább iOS 13 vagy annál újabb verziójú operációs rendszerrel rendelkező, legalább iPad 2 készülék, vagy
- legalább Android 7 vagy annál újabb verziójú operációs rendszer,
- minimum 7" kijelzőméret.

Csak olyan eszközök esetében garantált a szolgáltatás működése, amelyeken nincs feloldva a hivatalos gyártói korlátozás. Jailbreak (iOS) és rootolás (Android).

Az iOS 25.3.28-as és az Android 25.3.26-os számú verzióktól kezdve alkalmazásaink nem tölthetők le iOS 13-as vagy Android 7-es operációs rendszernél régebbi verzióval rendelkező készülékekre. Azon ügyfeleink, akik alkalmazásunk iOS 25.3.28-asnál vagy Android 25.3.26-osnál régebbi verzióját használják olyan készüléken, amely iOS 13-as vagy Android 7-es operációs rendszernél régebbi verzióval rendelkeznek, 2025. június 6-át követően nem

tudják frissíteni az alkalmazásainkat, így nem férnek hozzá azokhoz a funkciókhoz sem, amelyek az újabb alkalmazásverziókban érhetők el.

Funkciók bevezetésének listája

Az egyes új funkciók frissítésekkel érkeznek az alkalmazásba, így a korábbi verziószámmal jelölt alkalmazást használó Felhasználók csak akkor vehetik használatba az új funkciókat, ha frissítik az UniCredit mBanking mobilalkalmazást. A frissítés kihagyása esetén a Felhasználók az új funkció nélkül használhatják tovább a mobilalkalmazás szolgáltatásait. Frissítéssel vagy letöltéssel csak a legmagasabb verziószámmal jelölt UniCredit mBanking mobilalkalmazás vehető használatba, alacsonyabb verziószámra történő visszalépésre nincs lehetőség.

Funkciók	UniCredit mBanking mobilalkalmazás verziószám		
	Android	iOS	EMUI/HarmonyOS
Árfolyamok lekérdezése, ATM- és fiókkereső, Ügyfélszolgálat és közösségi média elérhetőség, Számlainformációk, Bankkártya információk, Lekötött betétek kezelése, Átutalások, Sablonok és gyorsfizetés (FastPay), Alkalmazás beállításai (PIN módosítás, nyelv kiválasztása, hangjelzések), Alkalmazás beállításai (PIN módosítás, nyelv kiválasztása, hangjelzések)	v1.10.	v2.4.	-
Saját forint- és devizaszámla közötti átvétel konverzióval, forintban vagy devizában megadva	2.0.14.	2.10.	-
mTokenes hitelesítés	2.7.21.1.	3.2.14.	-
Kártya limitmódosítás	2.11.16.	3.4.17.	-
Csoportos beszédési megbízások nyomkövetése	3.0.65.	4.0.48.	-
Állandó átutalási megbízások létrehozása, szerkesztése	3.1.61.0.	4.1.121.	-
Betéti kártya aktiválás	3.1.61.0.	4.1.121.	-
Hitelkártya törlesztés	3.1.61.0.	4.1.121.	-
Jóváírásokról szóló push értesítések	3.3.37.	4.2.127.	-
mCash	3.7.12.	4.5.0.	-
Arcfelismeréssel való bejelentkezés	3.10.34.	4.8.2.	-
Kétfaktoros azonosítás	3.11.66.	4.9.0.	-
Tranzakció aláírások push üzenettel	3.11.66.	4.9.0.	-
Belépés és tranzaktálás ujjlenyomat azonosítással	3.13.34.	4.10.0.	-
Belépés és tranzaktálás arcfelismeréssel	3.13.34.	4.10.0.	-
Kártyatranzakciós push értesítések	3.15.31.	4.12.0.	-
Azonnali utalás	3.15.36.	4.12.1.	-
Másodlagos azonosító regisztráció	3.15.36.	4.12.1.	-
Az Unión belüli, határokon átnyúló, Európában történő fizetések egyes díjainak és a pénznemek közti átváltási díjak megjelenítése	3.17.14.	4.14.0.117.	-

Funkciók	UniCredit mBanking mobilalkalmazás verziószám		
	Android	iOS	EMUI/HarmonyOS
Új alkalmazás (megújult külső, kategorizálás, elemzés, widget)	4.6.59.	5.5.63.	-
TBSZ számlák kezelése	4.15.4.2.	5.14.4.	-
SEPA átutalás	4.18.12.0.	5.17.20.	-
Csoportos beszédési megbízások létrehozása	4.18.12.0.	5.17.20.	-
Számlák oldal frissítése	4.18.12.0.	5.17.20.	-
Profilom oldal	4.20.64.	5.19.76.	-
Kapcsolattartási adatok módosítása	4.20.64.	5.19.76.	-
Számlakivonatok és díjkimutatások	4.20.64.	5.19.76.	-
Bankkártya PIN-kód megtekintése	4.24.15.0.	5.23.12.	-
Push üzenet a törölt megbízásokról	4.24.15.0.	5.23.12.	-
Push üzenet a lejártó lekötött betétekről	4.24.15.0.	5.23.12.	-
Megújult nyitó- és számlák oldal	4.25.9.0.	5.24.4.	-
Online személyi kölcsön igénylés	4.25.61.0.	5.24.82.	-
ApplePay – kártya regisztráció az Apple Walletben	-	5.25.30.	-
Kedvezményezett törlésének lehetősége a Sablonok és kedvezményezett listáról	4.28.11.0.	5.27.9.	-
Kategorizálás beállítása múltbeli és kategorizálás megjegyzése a jövőbeni tranzakciókhoz	4.28.11.0.	5.27.9.	-
GooglePay – kártya regisztráció a GPay Walletben	4.29.13.1.	-	-
Állandó átutalási megbízás létrehozása kimenő tranzakcióból	4.29.13.1.	5.28.17.	-
GooglePay – kártya regisztráció az mBanking használatával	4.29.13.1.	-	-
ApplePay – kártya regisztráció az mBanking használatával	-	5.28.87.	-
Hitelkártyákhoz kapcsolódó limitek módosítása	4.31.12.0.	5.30.15.	-
Számlainformációk másolása	4.31.12.0.	5.30.15.	-
Számlatörténetben megjelenő hasznos információk (be-/kikapcsolható)	4.31.12.0.	5.30.15.	-
Huawei alkalmazás bevezetése	-	-	4.33.27.0.
Betétikártya felfüggesztés/feloldás	4.38.32.0.	5.37.30.	4.38.32.0.
Módosítások a felhasználói felületen	4.45.20.	5.43.20.	4.45.20.
Kártya+ Kedvezményprogram	4.45.20.	5.43.20.	4.45.20.
Fizetési kérelem	4.46.11.	5.44.10.	-
Online számlanyitás és hiteligénylés indítása az alkalmazás nyitóoldaláról	4.48.10.1	5.46.13	-
QVIK azonnali fizetés	4.49.10.0	5.47.12.	-
Befektetés modul	4.50.12.0.	5.48.16.	-
Azonnali blokkolás	4.51.17.0.	5.49.23.	-

Funkciók	UniCredit mBanking mobilalkalmazás verziószám		
	Android	iOS	EMUI/HarmonyOS
Hitelkártya túlfizetés	4.51.17.0.	5.49.23.	-
Bemutató videók	4.51.17.0.	5.49.23.	-
Digitális akadálymentesítés	25.2.96.	25.3.28.	-
Elektronikusan elérhető hitelkártya számlakivonat	25.3.26.	25.3.28.	-
Hitelvisszafizetési ütemterv küldés	25.8.40.	25.8.35.	-
Online értékpapírszámla-nyitás	25.8.40.	25.8.35.	-