

Internetes bankkártyás vásárlások (erős ügyfél-hitelesítés) GYIK

ÁLTALÁNOS INFORMÁCIÓK

1. Milyen módon változnak az internetes bankkártyás vásárlások?

Az EU vonatkozó rendeletének¹ megfelelően az **internetes bankkártyás² fizetések túlnyomó többségéhez 2021. január 1-jét követően szükség lesz** majd:

- egy SMS-ben kapott egyszer használható kód és
- egy állandó 4 jegyű Internetes PIN / iPIN jelszó megadására.

Ezek megadása nélkül **biztosan nem fog tudni internetes bankkártyás tranzakciót végrehajtani az ügyfél**, amennyiben az elfogadó Európai Unión belüli.

2. Mi lesz az internetes vásárlások új menete?

1. Az internetes kártyás vásárlások folyamata a megszokott módon kezdődik: az elfogadó hely (pl.: webáruház) először az idáig is használt kártyaadatok megadását kéri: kártyaszámot, lejáratot, CVV kódot, adott esetben a kártyabirtokos nevét vagy e-mail címét.

The screenshot shows a payment form with the following fields and buttons:

- Bankkártyás fizetés** (orange button)
- Bankkártya száma**: input field with placeholder "0000 0000 0000 0000"
- Lejárat dátum**: input field with placeholder "00/00"
- CVC kód**: input field with placeholder "000"
- E-mail cím**: input field with placeholder "a@b.c"
- Fizetés** (blue button)

¹ (EU) 2015/2366 európai parlamenti és tanácsi irányelvnek az erős ügyfél-hitelesítésre, valamint a közös és biztonságos nyílt kommunikációs standardokra vonatkozó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló 2017. november 27-i (EU) 2018/389 felhatalmazáson alapuló bizottsági rendelete.

² A Takarékbank Zrt-nél vezetett bankszámlákhoz kapcsolódó bankkártyákat az MTB Magyar Takarékszövetkezeti Bank Zrt. bocsátja ki, továbbá a Takarékbank logóval ellátott ATM-eket az MTB Zrt. üzemelteti.

2. A fenti adatok megadása után a vásárló automatikusan továbbításra kerül a hitelesítési oldalra, ahol egy egyszer használatos, a bank által SMS-ben a telefonszámára kiküldött 6 számjegyű kódot kell megadnia, ez a kód minden egyes kiküldött SMS-ben más.

Mégse

MTB
Magyar Takarékszövetkezeti Bank

mastercard
ID Check

Tranzakció hitelesítése

A tranzakció teljesítése érdekében, a hitelesítés végrehajtásához, kérjük, adja meg a mobiltelefonjára, SMS-ben kapott egyszer használatos jelszavát. Telefonszám utolsó 4 számjegye: 1629.

Tranzakció helye: 3DS2 Shop, Összege: 2312.00 EUR, Időpontja: 2020.12.12, Kártyaszám: 5457 **** * 0739

Adja meg egyszer használatos jelszavát:

407025

Jóváhagyás

Kód újraküldése

Segítség ↓

Ha nem kap SMS-t, ellenőriznie kell, hogy a feltüntetett számok megegyeznek-e telefonszámának utolsó négy számjegyével. Amennyiben a képernyőn 9999 szerepel a telefonszám utolsó 4 számjegyeként, akkor nyilvántartásunkban nem szerepel az ügyfél bankkártyához érvényes telefonszám, ebben az esetben az ügyfél vegye fel a kapcsolatot a számlavezető bankjával a 3. pont szerint.

Kiküldött SMS:

MTB Zrt. ellenorzo kod: 407025 internetes
vasarlashoz.Összeg: 2312.00 EUR
Kereskedo: "3DS2 Shop" Kartyaszam: 5457
**** * 0739 2020.12.12

3. A következő képernyőn internetes PIN kódját kell megadnia, ami alapértelmezetten az ügyfél bankkártyájához tartozó bankszámlaszámának 13-16. karaktere:

Mégse

MTB
Magyar Takarékszövetkezeti Bank

mastercard
ID Check

Tranzakció hitelesítése

Kérjük, adja meg internetes PIN-kódját:

Tranzakció helye: 3DS2 Shop, Összege: 2312.00 EUR, Időpontja: 2020.12.12, Kártyaszám: 5457 **** * 0739

Adja meg internetes PIN-kódját:

Jóváhagyás

Segítség ↓

4. Amennyiben a megadott adatok helyesek, a bank rendszereiben elvégzi a tranzakció engedélyezéséhez szükséges további műveleteket (pl.: státusz ellenőrzés, fedezet ellenőrzés stb.), az ügyfél pedig visszairányításra kerül az elfogadóhely oldalára, ahol tájékoztatást kap a vásárlás sikerességéről.

TELEFONSZÁM ÉS INTERNETES PIN KÓD

3. Hol lehet módosítani a telefonszámot, amire az egyszer használatos kód kiküldése történik?

Az SMS fogadására megjelölt **mobiltelefonszámot** megadhatja / módosíthatja:

- a Takaréék Csoport által üzemeltetett ATM berendezések többségén készpénzfelvételi tranzakció közben⁴ vagy
- a számlavezető bankfiókban.

4. Mi a kártyához tartozó iPIN kód?

Az Internetes PIN kód (továbbiakban: iPIN) netes vásárlások jóváhagyásához szükséges 4 számjegyű kizárólag számokból álló kód, amely nem egyezik meg a személyesen, POS terminálnál vagy ATM-nél használt PIN kóddal.

Az iPIN jelszó alapértelmezetten a bankkártyához tartozó bankszámlaszám 13-16. karaktere lesz.
Pl: Számlaszám: 12345678–98765432–00112233, iPIN: 5432.

Ezt a kezdeti jelszót 2021. március 31-ig meg kell változtatnia az ügyfélnek a Takaréék Csoport által üzemeltetett ATM-ek bármelyikén! ATM kereső: <https://www.takarekbank.hu/atm-fiook> oldalon.

5. Hol lehet módosítani az iPIN kódot?

A bankkártya segítségével bármely Takaréék Csoport által üzemeltetett ATM-en³ keresztül, „Internetes PIN megadás” menüpontot választva 2020. december 30-ától lehet módosítani az iPIN kódot.

6. Hogyan lehet módosítani az Internetes PIN kódot ATM-en³ keresztül?

1. A bankkártya behelyezését, a nyelv kiválasztását és a bankkártyájához tartozó fizikai PIN kód megadását követően **ki kell választani az „Internetes PIN megadás” funkciót.**

2. Itt **megadható az új**, ügyfél általa választott **4 számjegyből álló iPIN kód**, majd a következő képernyőn **meg kell erősítenie** újra.

3. Ezt követően eldöntheti, hogy kér-e bizonylatot a módosításról.

4. **Az iPIN kód azonnal módosul**, az erős ügyfél-hitelesítéssel jóváhagyandó tranzakciók során már ezt az új kódot kell használni.

Amennyiben több bankkártyája is van az ügyfélnek, akkor az iPIN módosítás műveletét minden kártyájával külön el kell végezni ahhoz, hogy az általa kiválasztott iPIN kóddal tudja használni. Bankkártyánként más és más iPIN beállítása lehetséges.

7. Mi történik, ha a kártyát tiltás, megújítás vagy egyéb csere miatt újra gyártják?

Amennyiben egy élő bankkártya szerződésen belül új bankkártyát bocsátunk a rendelkezésére, akkor az előző, lecserélt kártyához beállított SMS küldési telefonszám és aktuális iPIN kód ugyanaz lesz az újonnan kézhez kapott kártyánál. Azaz amennyiben az ügyfél módosította az alapértelmezett iPIN kódját, majd később például megújult a bankkártyája, vagy egyéb okból pótlásra, cserére kerül sor, akkor az új, megújított bankkártyáját is az általa megadott iPIN kóddal tudja használni.

8. Mi történik, ha a vásárlás során az ügyfél többször elrontja az SMS kódot és/vagy iPIN jelszót?

Amennyiben 5-ször sikertelenül próbálkozik (egy próbálkozásnak számít az SMS kód és az iPIN megadása), a rendszer 60 percre blokkolja az erős ügyfél-hitelesítéssel történő azonosítást. Ez a blokkolás csak az online kártyás fizetésekre vonatkozik, az ATM-nél vagy POS terminálnál személyesen végrehajtott tranzakciókat nem érinti. 60 perc lejáta után a blokkolás feloldódik.

³ A Takaréékbank Zrt-nél vezetett bankszámlákhoz kapcsolódó bankkártyákat az MTB Magyar Takarékszövetkezeti Bank Zrt. bocsátja ki, továbbá a Takaréékbank Zrt logóval ellátott ATM-eket az MTB Magyar Takarékszövetkezeti Bank Zrt. üzemelteti.

⁴ Azon hitelintézetek ügyfelei számára érhető el a szolgáltatás, akik ezt megrendelték és az élesítésről visszaigazolást kaptak.

9. Mi történik, ha az ügyfél félbe hagyja a hitelesítési folyamatot. Tudja-e még folytatni a megkezdett tranzakciót?

Ha az SMS kódot vagy iPIN kódját nem adja meg 10 percen belül, akkor a hitelesítési folyamat sikertelenül fog végződni, a vásárlás nem fog megtörténni. Ilyenkor javasoljuk, hogy kezdje előlről a vásárlást a kereskedő online felületén.

BIZTONSÁG

10. Vannak rendszerkövetelményei az erős ügyfél-hitelesítés végrehajtásának?

A számítógépek, laptopok, mobiltelefonok internetes böngészőinek legnagyobb többsége alkalmas arra, hogy végrehajtsa rajta az erős-ügyfélhitelesítést. Felhívjuk figyelmét, hogy az előugró ablakokat gátló szoftverek zavarhatják az erős ügyfél-hitelesítés használatát.

11. Mi az, amire az erős ügyfél-hitelesítés használatakor is figyelni kell?

Az erős ügyfél-hitelesítés biztonsági lépései nem helyettesíthetik az ügyfél számítógépes rendszerének védelmét biztosító intézkedések (tűzfal, jelszó, vírusvédelem, belépési kód, titkosítás, titoktartás, egyéb rendszervédelmi intézkedések) megtételét. Győződjön meg továbbá minden esetben arról is, hogy az adott webáruház, illetve egyéb online szolgáltató, amelynél internetes tranzakciót végez, rendelkezik a szükséges biztonsági protokollokkal, valamint a megadott adatainak biztonsága érdekében a szükséges lépéseket megtette.

Arról, hogy egy kereskedő megfelelő hitelesítési rendszert használ-e, a Mastercard és a VISA elnevezései (Visa Secure, Verified by Visa, Mastercard ID Check, Mastercard Secure Code és az ezeket tartalmazó logók) nyújtanak előzetes információt. Amennyiben ezek az oldalon megtalálhatóak, a kereskedő várhatóan támogatja technikailag a hitelesítést.

12. Minden online kereskedőre vonatkozik az erős ügyfél-hitelesítés irányelve?

2021. január 1-től minden olyan internetes kereskedőre vonatkozik az erős ügyfél-hitelesítés irányelve, melynek székhelye az Európai Unió tagállamaiban, továbbá Norvégiában, Liechtensteinben és Izlandon van. Az említett országokon kívüli, például ázsiai vagy amerikai online kereskedők azonban nem feltétlenül követelik meg.

Szintén 2021. január 1-től azon internetes bankkártyás vásárlásokat, ahol nincs erős ügyfél-hitelesítés, mert az EU-n belüli elfogadó nem hitelesített rendszert használ, a jogszabály által a kis összegű műveletek esetében alkalmazható kivétel szerint

- 9.000 Ft-ig egy összegben és
- 30.000 Ft-ig egymást követően engedélyezzük maximum.

Ezen összegek elérése esetén az online vásárlási tranzakciók elutasításra kerülnek.

A hitelesítés kapcsán a Bank fenntartja a jogot, hogy a jogszabály adta kereteken belül további kivételeket alkalmazzon.

Folyamatosan aktualizált információ az erős-ügyfélhitelesítésről a <https://takarekbank.hu/fontos-internetes-bankkartyas-fizetes-valtozasa> oldalon található.