MI8OS

MI8OS-ÚTMUTATÓ

Minden az appjáról és a kártyáiról.

Hogyan hozzon létre, nyisson meg és frissítsen egy széfet, hogyan gondozza MI8OS Card gen 2 kártyáját, és pontosan hogyan védjük a bejegyzéseit, egészen az utolsó bájtig.

LÉTREHOZÁS | HASZNÁLAT | KÁRTYÁK | BIZTONSÁG



A MI8OS apphoz iPhone-on és Androidon. 2026. október.

TARTALOM

Mit talál az útmutatóban

01 **ELSŐ LÉPÉSEK** p. 3
Mi a MI8OS, a fontos szavak, az app röviden, hogyan tartsa a kártyát.

02 **SZÉF LÉTREHOZÁSA** p. 9
Bejegyzések hozzáadása, széfjelszó választása, mentés kártyára, a tartalékkártyák felírása.

03 **A SZÉF HASZNÁLATA** p. 16
Kártya megnyitása, bejegyzések olvasása és másolása, 2FA-kódok, hozzáadás és törlés, a kártya frissítése.

04 **A KÁRTYÁK KEZELÉSE** p. 23
Kártyáim, átnevezés, azonosítás, visszaállítás, zárolás és feloldás mesterjelszóval.

05 **BEÁLLÍTÁSOK** p. 29
Appzár, Face ID, a vágólap és a megjelenés.

06 **HOGYAN VÉDJÜK A BEJEGYZÉSEIT** p. 32
Két titkosítási réteg, valós példa a „12345678” értékkel, és miért számít a széfjelszava.

07 **GONDOZÁS, ANDROID ÉS SÚGÓ** p. 42
Három kártya tartása, eltérések Androidon, hibaelhárítás.

01

Első lépések

Öt perc, hogy megértse, hogyan működik a MI8OS, mielőtt kártyához nyúlna.

MI A MI8OS

Kis, titkosított széf egy kártyán, amelyet Ön tart a kezében.

A MI8OS a legfontosabb titkait, például helyreállító kódokat, 2FA-kulcsokat, seed-kifejezéseket és PIN-kódokat egy olyan széfben őrzi, amelyet a telefonja titkosít, és egy fizikai kártyára ment. Nincs fiók, nincs felhő, nincs előfizetés.



Kéznél · amelyet használ



Otthon · biztonságban otthon



Máshol · egy másik helyen

A KÉSZLETÉBEN

Három **MI8OS Card, gen 2**. Minden kártya legfeljebb **20 bejegyzést** tárol. Írja fel ugyanazt a széfet mindhárom kártyára, és tartsa őket különböző helyeken.

AMIRE SZÜKSÉGE VAN

Egy NFC-képes iPhone vagy androidos telefon és a MI8OS app az App Store-ból vagy a Google Playről (Android-tudnivalók a 43. oldalon). És egy széfjelszó, amelyet meg tud jegyezni: a legjobb egy hosszú jelmondat.

A FONTOS SZAVAK

Három jelszó, három különböző feladat.

Ez az útmutató legfontosabb oldala. Hasonlóan hangzanak, de mindegyik mást véd.

SZÉFJELSZÓ

Titkosítja és megnyitja a kártya bejegyzéseit. Kötelező, legalább 12 karakter.

Sehol nem tárolódik. Senki sem tudja helyreállítani, még a MI8OS sem.

MESTERJELSZÓ

Opcionális. Magát a kártyát zárolja, így senki sem tudja visszaállítani vagy törölni e jelszó nélkül.

Semmit sem nyit meg. A bejegyzések olvasásához továbbra is a széfjelszó kell.

AZ APPZÁR PIN-KÓDJA

Opcionális. Hat számjegy (vagy Face ID) az app megnyitásához ezen a telefonon.

Semmi köze a kártyáihoz, és semmit sem tud visszafejteni.

SZÓ	JELENTÉS
Széf	A bejegyzései listája. Titkosítva létezik a kártyáin, visszafejtve pedig csak az app memóriájában, amíg nyitva van.
Bejegyzés	Egy tétel: egy név (legfeljebb 24 bájt) és maga a titok (legfeljebb 96 bájt), például egy PIN-kód, egy helyreállító kód vagy egy 2FA-kulcs.
Kártya	Az Ön MI8OS Card gen 2 kártyája. A titkosított széfet tárolja; ugyanazt a széfet több kártyára is felírhatja.
Kártya frissítése	A változtatásait a kártyára írja. Addig a változtatások csak az app memóriájában léteznek.

AZ APP RÖVIDEN

Három lap. Mindegyiknek egy feladata van.



Beolvasás · kártya megnyitása



Új · széf létrehozása



Továbbiak · kártyák és beállítások

1

BEOLVASÁS

Koppintson kártya beolvasásához, és tartsa a kártyát a telefonhoz. A kártya saját ablakban nyílik meg, ahol megadja a széfjelszavát.

2

ÚJ

Koppintson új széf létrehozásához. Egy négylépéses varázsló vezeti végig az első bejegyzéstől a kártyáig, amely tárolja.

3

TOVÁBBIAK

A kártyái, az appzár, a vágólap időzítője, a megjelenés és a beépített súgóoldalak.

A KÁRTYA TARTÁSA

Felső perem. Laposan. Mozdulatlanul.

Valahányszor az app egy kártyával kommunikál, az iPhone saját NFC-ablakot jelenít meg. Ezután:

1. **Tartsa a kártyát laposan a felső peremhez** az iPhone hátoldalán, ahol az NFC-antenna van.
2. **Tartsa mozdulatlanul**, amíg az app meg nem erősíti. A felírás néhány másodpercig tart; a kártya túl korai elmozdítása a leggyakoribb oka annak, hogy egy felírást meg kell ismételni.
3. Ha semmi sem történik, csúsztassa a kártyát lassan kicsit lejjebb vagy feljebb, és vegye le a vastag vagy fém tokot.

> **Nem kell sietni.** Amikor megnyit egy kártyát, az app először előkészíti a kulcsát („A kulcsa előkészítése folyamatban. Még nem kell odatartania a kártyát"). Akkor tartsa oda a kártyát, amikor megjelenik az NFC-ablak.

> **Androidon** az app saját beolvasási képernyőt mutat, és a kártyát a telefon hátoldalának felső feléhez kell tartani.



MI KERÜLJÖN A KÁRTYÁRA

Néhány bejegyzés, amely sokat számít.

A MI8OS nem a jelszókezelője helyett van. Ez az offline hely arra a maroknyi dologra, amelyre akkor lenne szüksége, ha minden más cserben hagyná.

KIVÁLÓ EGY KÁRTYÁRA

- ✓ Helyreállító kódok az e-mailhez és az Apple / Google fiókhoz
- ✓ 2FA-beállítókulcsok, hogy az app megjeleníthesse a kódjait
- ✓ Kriptovaluta-helyreállító kifejezések (a MI8OS nem tárca, és nem őriz pénzeszközt)
- ✓ A jelszókezelője mesterjelszava vagy a vészhelyzeti készlet adatai
- ✓ Fontos PIN-kódok és privát jegyzetek

JÓ TUDNI

- ✓ Legfeljebb 20 bejegyzés kártyánként
- ✓ Név: legfeljebb 24 bájt · bejegyzés: legfeljebb 96 bájt
- ✓ Az egyszerű betűk, számjegyek és szóközök 1 bájtot foglalnak; az ékezetes, görög vagy cirill betűk 2-t; az emojik 4-et
- ✓ A hosszú seed-kifejezésekhez két bejegyzés is kellhet (pl. az 1–12. és a 13–24. szó)

02

Széf létrehozása

Négy lépés: Bejegyzések, Jelszó, Felírás, Kész. Nagyjából öt perc.

1. LÉPÉS A 4-BŐL · BEJEGYZÉSEK

Kezdje a bejegyzéseivel.

1. Nyissa meg az **Új** lapot, és koppintson a **Koppintson új széf létrehozásához** gombra.
2. Koppintson a **Bejegyzés hozzáadása** gombra minden egyes dologhoz, amelyet meg szeretne őrizni.
3. Egy bejegyzést elhúzva még a továbblépés előtt eltávolíthat.
4. Koppintson a **Tovább** gombra, ha kész a lista.

> **Még semmi sincs mentve.** A bejegyzései csak ebben a varázslóban léteznek, amíg a titkosított széfet kártyára nem menti.

> **Már nyitva van egy széf?** Az app előbb rákérdez. Ha vannak még kártyára nem írt változtatásai, felajánlja a megtartásukat.



BEJEGYZÉS HOZZÁADÁSA

Egy név, és maga a titok.

Név. Valami, amire ráismer, például „E-mail helyreállító kódjai”. Legfeljebb 24 bájt; egy számláló mutatja, mennyi maradt.

Bejegyzés. A jelszó, a kód vagy a szöveg, legfeljebb 96 bájt. Mindent, amit beilleszt vagy generál, titkosítunk, mielőtt kártyára kerül.

Generálás. Koppintson a dobókockára egy 16, 32, 64 vagy 96 karakteres véletlen jelszó létrehozásához.



2FA-KULCS MENTÉSE

Amikor egy szolgáltatás megjeleníti a beállítókulcsot (vagy a QR-kódja mögötti otpauth:// linket), illessze be bejegyzésként. A MI8OS felismeri, és később megjelenít egy **TOTP** gombot, amely kimásolja az aktuális kódot. Ha a link 96 bájtnál hosszabb, csak magát a beállítókulcsot illessze be (a secret= utáni részt); a MI8OS ekkor a szabványos, 30 másodpercenként változó 6 számjegyet használja.

2. LÉPÉS A 4-BŐL · JELSZÓ

Válassza ki a széfjelszavát.

1. Írja be a széfjelszavát, majd a megerősítéshez írja be újra.
2. Figyelje az erősségjelzőt: 12 karakter a minimum, 20 vagy egy szóközös kifejezés a „Kiváló hossz." eredményt adja.
3. Jelölje be a négyzetet: *„Ha elvesztem az összes kártyát, vagy elfelejtem ezt a jelszót, a MI8OS nem tudja helyreállítani ennek a kártyának a széfjét."*
4. Koppintson a **Széf titkosítása** gombra.



TANÁCSUNK

Használjon **öt vagy hat véletlenszerű szót**, például *réz lámpás bársony pálya tundra* (de ne éppen ezeket). Könnyű megjegyezni, rendkívül nehéz kitalálni. A 40. oldal megmutatja, miért.

3. LÉPÉS A 4-BŐL · FELÍRÁS

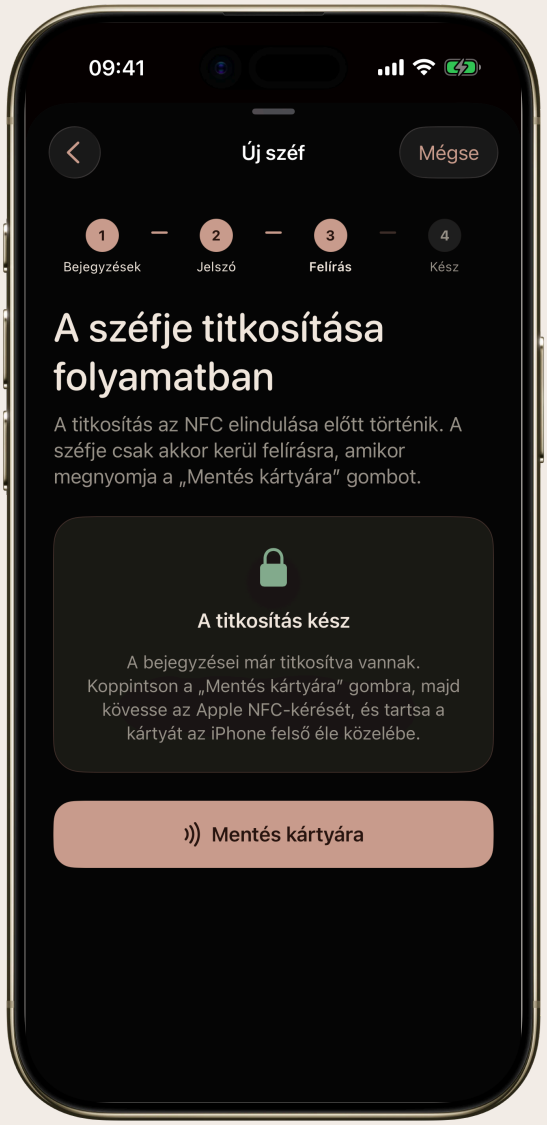
Előbb titkosítás. Aztán a kártya.

A titkosítás a telefonján történik, még mielőtt az NFC elindulna. Egy pillanatig „A titkosítás erősítése folyamatban…" feliratot lát, miközben az app kulcsokká alakítja a jelszavát. Ez a szünet szándékos: lassúvá teszi a jelszava kitalálását bárki más számára.

Amikor megjelenik **A titkosítás kész**:

1. Koppintson a **Mentés kártyára** gombra.
2. Tartsa a kártyát az iPhone felső pereméhez, amikor megjelenik az NFC-ablak.
3. Ne mozdítsa. Az app felírja a széfet, majd **visszaolvassa, hogy ellenőrizze**.

> **Üres kártya?** Az app ugyanazzal az odatartással automatikusan előkészíti.



4. LÉPÉS A 4-BŐL · KÉSZ

Most írja fel a tartalékkártyáit.

A „Széf mentve a kártyára” azt jelenti, hogy a széf ellenőrzötten azon a kártyán van. **Ez az egyetlen pillanat, amikor az app a teljes széfet más kártyákra másolhatja**, ezért most írja fel mindegyiket:

1. Koppintson a **Másik kártya felírása** gombra.
2. Válassza az **Ugyanannak a széfjelszónak a használata** (a legegyszerűbb) vagy a **Másik széfjelszó használata** lehetőséget ehhez a kártyához.
3. Mentsen a következő kártyára. Ismételje meg a harmadikkal.

> **Ugyanaz a jelszó, új titkosítás.** Minden kártya saját véletlen sót kap, így még ugyanazzal a jelszóval is teljesen máshogy néznek ki az egyes kártyák adatai.

A **Széf elvetése erről az iPhone-ról** csak az app memóriájában zárja be a széfet. Kártyát soha nem töröl.



KÁRTYA, AMELYEN MÁR VAN SZÉF

A MI8OS soha nem ír felül egy széfet váratlanul.

Ha új széfet ment egy olyan kártyára, amelyen már van egy, semmi sem íródik ki. Az app jelzi: **„Ezen a kártyán már van széf”**, és két lehetőséget kínál:

BEJEGYZÉSEK HOZZÁADÁSA

Hozzáadja az új bejegyzéseit a kártyán lévő széfhez. A már rajta lévő bejegyzések megmaradnak. A széfjelszavának annak kell lennie, amelyet ez a kártya használ, és még egyszer oda kell tartania a kártyát.

MÉGSE

A kártyát pontosan úgy hagyja, ahogy volt.

> **Teljesen le szeretné cserélni a széfet?** Előbb állítsa vissza a kártyát (26. oldal), majd hozza létre rajta az új széfet.



03

A széf használata

Megnyitás, olvasás, másolás, módosítás, és a változtatások visszaírása a kártyára.

KÁRTYA MEGNYITÁSA

Beolvasás, jelszó, újra odatartás.



A Beolvasás lap



A kártya ablaka

1. A **Beolvasás** lapon koppintson a **Koppintson kártya beolvasásához** gombra, és tartsa oda a kártyát. A beolvasás csak a kártya nyilvános adatait olvassa.
2. Adja meg a kártya **Széfjelszó** mezőjében a jelszót, és koppintson a **Széf megnyitása** gombra. Az app előkészíti a kulcsát, majd még egyszer kéri a kártyát.

A SZÉFBEN

A bejegyzései, ameddig szüksége van rájuk.

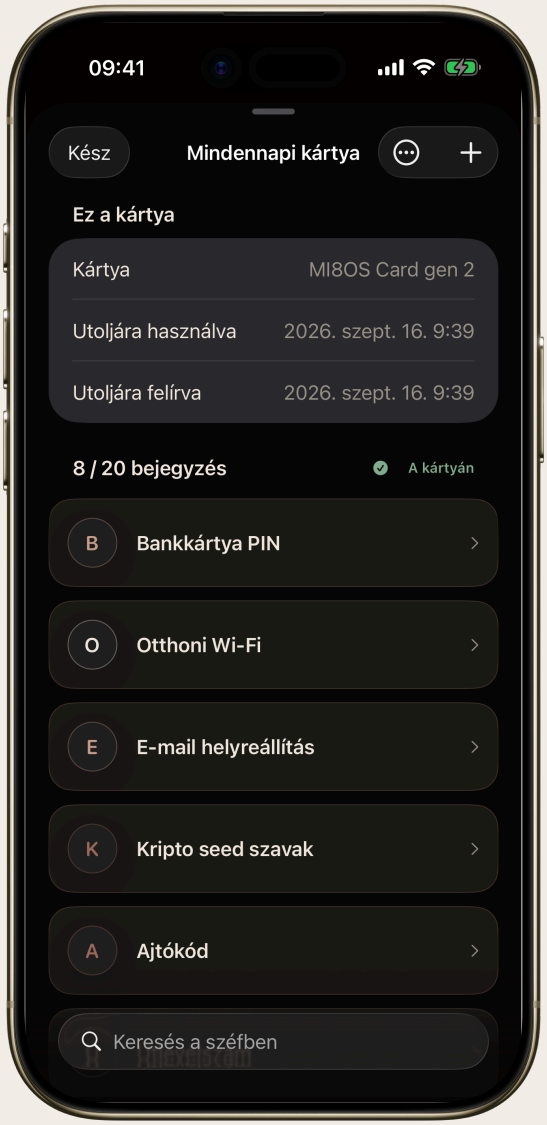
Az **Ez a kártya** mutatja, melyik kártya van megnyitva, az Utoljára használva és az Utoljára felírva adatot, valamint hogy van-e mesterjelszava.

A **„8 / 20 bejegyzés”** jelzi, mennyire telt meg a kártya. Az **A kártyán** azt jelenti, hogy minden, amit lát, a kártyára van mentve.

A lent található **Keresés a széfben** név alapján talál meg egy bejegyzést.

A fenti **+** bejegyzést ad hozzá; a **⋯** megnyitja a kártya menüjét (25. oldal).

> **Csak a memóriában visszafejtve.** A bejegyzései csak addig léteznek olvasható formában, amíg ez az ablak nyitva van. Koppintson a **Kész** gombra, és eltűnnek a telefonról.



OLVASÁS ÉS MÁSOLÁS

Rejtve, amíg nem kéri.

Koppintson egy bejegyzésre a megnyitásához. Az érték pontok mögé van rejtve.

A **Megjelenítés** megmutatja; az **Elrejtés** újra elrejti.

A **Másolás** a vágólapra teszi, és a MI8OS 30 másodperc után **újra törli a vágólapot** (ezt a Továbbiak alatt módosíthatja: 15 mp, 30 mp vagy 1 perc).

> **Illessze be gyorsan.** Az időzítő lejárta után a vágólap üres, így a bejegyzés nem marad más appokban. Az időzítő akkor is fut tovább, ha előbb bezárja a széfet.

> **Képernyőfelvétel vagy -tükrözés?** A MI8OS eltakarja a képernyőt és bezárja a széfet, hogy a bejegyzések ne kerüljenek felvételre.



2FA-KÓDOK

A hitelesítője, a kártyáról.

Ha egy bejegyzés 2FA-beállítókulcs, az oldalán **TOTP** gomb jelenik meg. Koppintson rá, és a MI8OS kiszámítja és kimásolja az aktuális kódot, beillesztésre készen.

A kártya csak a **titkosított beállítókulcsot** tárolja. A kódot az app számítja ki a széf megnyitása után, a kulcsból és az aktuális időből, pontosan úgy, mint bármely hitelesítő app.

MIÉRT SEGÍT EZ

Ha a hitelesítőkódjai csak azon a telefonon vannak, amelyet elveszít, azzal együtt elvesznek. Ha a beállítókulcsok a kártyáin vannak, bármely új telefonon visszakaphatja a kódjait a MI8OS appal.



A SZÉF MÓDOSÍTÁSA

Hozzáadás, törlés, majd a kártya frissítése.

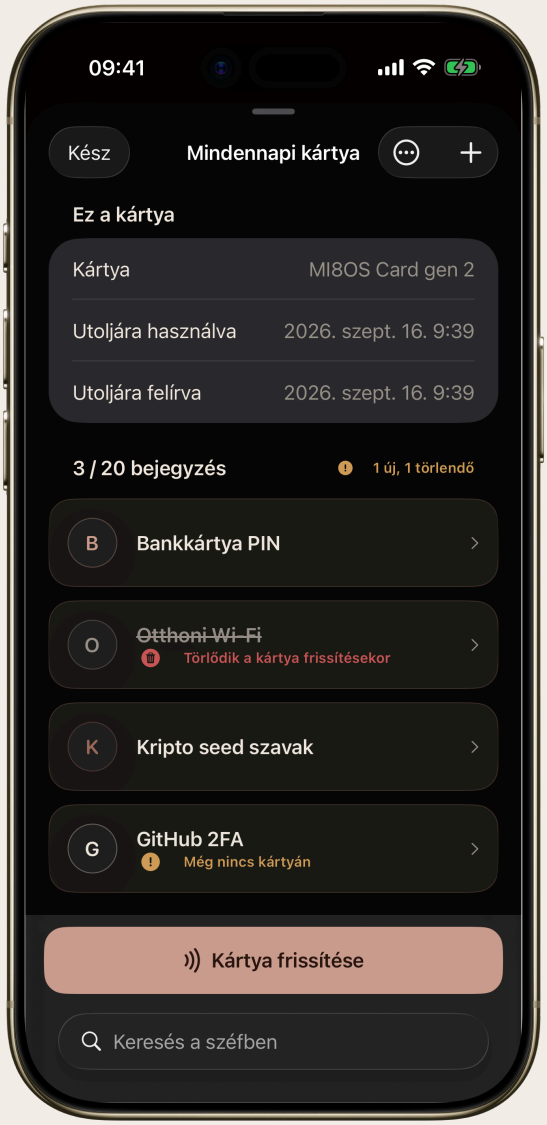
Hozzáadás: koppintson a **+** jelre, és töltse ki a nevet és a bejegyzést.

Törlés: húzza balra a bejegyzést, vagy nyissa meg, és koppintson a **Bejegyzés törlése** gombra. Megjelölve a listában marad, amíg nem frissíti a kártyát. Meggondolta magát? Koppintson a **Megtartás** gombra.

Szerkesztés: szándékosan nincs szerkesztés gomb. Egy bejegyzés módosításához törölje, majd adja hozzá újra.

A változtatások még fel nem írtként vannak jelölve. Koppintson a **Kártya frissítése** gombra, és tartsa oda a kártyát a mentésükhöz.

> **Fel nem írt változtatásokkal zárná be?** Az app figyelmezteti: „Ha frissítés nélkül zárja be ezt a kártyát, elvész."



MINDEN MÁSOLAT LEGYEN NAPRAKÉSZ

Minden kártya külön frissül.

A Kártya frissítése a megnyitott kártyára ír, és csak arra. A többi kártyáján az előző változat marad, amíg azokat is nem frissíti.

1

EGY KÁRTYA MÓDOSÍTÁSA

Nyissa meg a Kéznél kártyát, adjon hozzá vagy töröljön, majd koppintson a **Kártya frissítése** gombra.

2

ISMÉTELJE MEG A TÖBBINÉL

Nyissa meg az Otthon és a Máshol kártyát, és mindegyiken végezze el ugyanazt a módosítást.

3

GYORSABB ÚT AZ ÚJ BEJEGYZÉSEKHEZ

Hozzon létre egy „új széfet” csak az új bejegyzésekkel, és mentse egy olyan kártyára, amelyen már rajta van a széfje. Válassza a **Bejegyzések hozzáadása** lehetőséget, és a meglévőkhöz adódnak.

JÓ SZOKÁS

Évente egyszer nyisson meg minden kártyát, és ellenőrizze, hogy mindhárom ugyanannyi bejegyzést mutat-e.

04

A kártyák kezelése

Nevek, a kártya menüje, visszaállítás és az opcionális mesterjelszó.

KÁRTYÁIM

Adjon nevet minden kártyának.

A **Továbbiak** → **Kártyáim** alatt látja az ezen a telefonon ismert kártyákat egy címkével: a bejegyzések száma, **Üres** vagy **Zárolva**.

A **Kártya hozzáadása** beolvas egy kártyát, és megjegyzi. Csak azt olvassa, ami a kártyán már nyilvános: nem kell jelszó, és semmi sem íródik ki.

Koppintson egy kártyára a megnyitásához, átnevezéséhez vagy visszaállításához.

> **Gyorsabb megnyitás.** Egy olyan kártya, amelyet ez a telefon már ismer, a jelszó megadása után egyetlen beolvasással megnyílik.

> **Csak ezen a telefonon tárolódik:** az Ön által adott nevek, a kártyák utolsó használatának ideje és a nyilvános beállításaik. Soha nem jelszó, soha nem bejegyzés.



A KÁRTYA MENÜJE ···

Átnevezés, azonosítás, elfelejtés.

ÁTNEVEZÉS

Egy név, amelyre ráismer: „Kéznél”, „Otthon”, „A szülők széfje”.

AZONOSÍTÁS

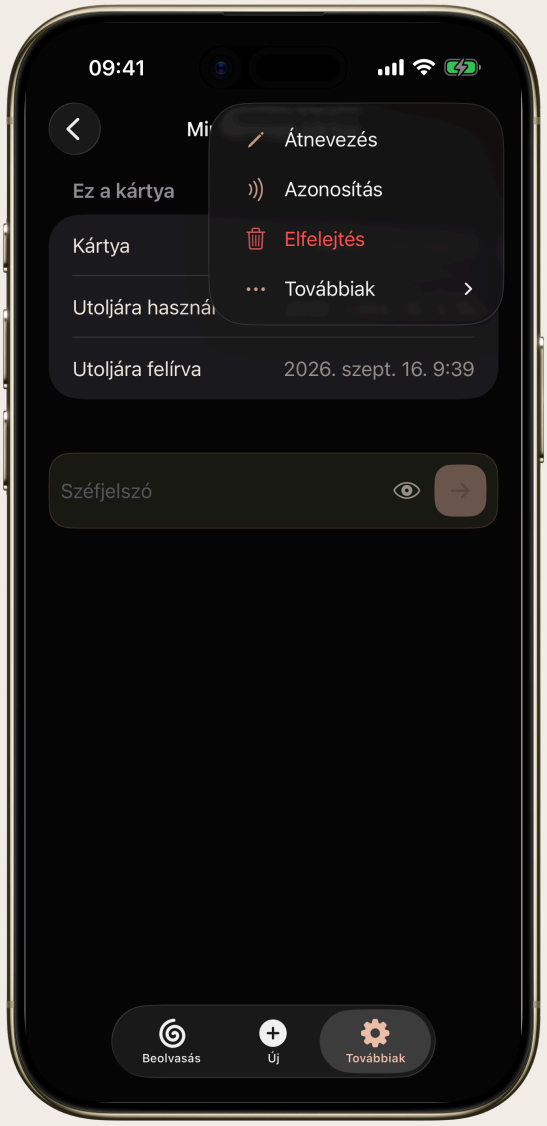
Nem biztos benne, melyik kártya melyik? Koppintson az Azonosítás lehetőségre, és tartson oda egy kártyát. Az app megmondja, hogy az-e, amelyiket éppen nézi, vagy melyik másik kártya.

ELFELEJTÉS

Eltávolítja a kártyát ennek a telefonnak a listájáról. A kártyán semmi sem változik, és bármikor újra hozzáadhatja.

TOVÁBBIAK

Kártya visszaállítása, Kártya zárolása és Kártya feloldása. Lásd a következő oldalakat.



KÁRTYA VISSZAÁLLÍTÁSA

Tiszta kártya, új széfre készen.

A ··· → **Továbbiak** → **Kártya visszaállítása** eltávolítja a MI8OS-széfet és minden mást a kártyáról, és felszabadítja a teljes tárhelyét. A széfjelszót **nem** kéri.

Arra használhatja, hogy:

- ✓ Egy széfet teljesen újra cseréljen
- ✓ Újra használjon egy kártyát, ha elfelejtette a széfjelszavát (a rajta lévő bejegyzések elvesznek)
- ✓ Kiürítsen egy kártyát, mielőtt odaadja

> **A többi kártya érintetlen marad.** Egy kártya visszaállítása soha nem érinti a többi kártyáján lévő széfet.

> **Zárolt kártya?** Megtagadja a visszaállítást, amíg meg nem adja a mesterjelszavát (következő oldal).



KÁRTYA ZÁROLÁSA · MESTERJELSZÓ

Akadályozza meg, hogy bárki letörölje a kártyáját.

Aki egy nem zárolt kártyát a kezébe vesz, visszaállíthatja, még az Ön széfjelszava nélkül is. Olvasni továbbra sem tud semmit, de törölni igen.

A **Kártya zárolása** ezt megakadályozza. Válasszon mesterjelszót, tartsa oda a kártyát, és kész. Ettől kezdve a kártyát nélküle nem lehet visszaállítani vagy törölni, sem a MI8OS-szel, sem semmi mással.

1. ··· → **Továbbiak** → **Kártya zárolása**
2. Adja meg kétszer a mesterjelszót, és koppintson a **Zárolás** gombra.
3. Tartsa oda a kártyát, amíg az app meg nem erősíti: „Kártya zárolva”.

> **Az olvasás és a mentés nem változik.** Ezekhez továbbra is csak a széfjelszó kell.



KÁRTYA FELOLDÁSA · ÉS EGY FIGYELMEZTETÉS

A feloldás visszaállítja a kártya normál állapotát.

··· → **Továbbiak** → **Kártya feloldása**, adja meg a mesterjelszót, és tartsa oda a kártyát. A kártya ismét nem zárolt kártyaként viselkedik. A széfje és a széfjelszava változatlan.

Zárolt kártya visszaállításához válassza a Kártya visszaállítása lehetőséget: az app kéri a mesterjelszót, majd formázza a kártyát.

NE FELEJTSE EL

Ha elfelejti egy kártya mesterjelszavát, azt a kártyát **soha** többé nem lehet visszaállítani vagy újra használni. A bejegyzései a széfjelszóval továbbra is olvashatók. Az app minden alkalommal kéri, és soha nem jegyzi meg.

Bármely kártyát zárolhat, feloldhat és visszaállíthat a **Továbbiak** → **Speciális** menüben is, a kártya beolvasásával.



05

Beállítások

Appzár, Face ID, a vágólap és az app megjelenése.

TOVÁBBIAK

Minden más, egy helyen.

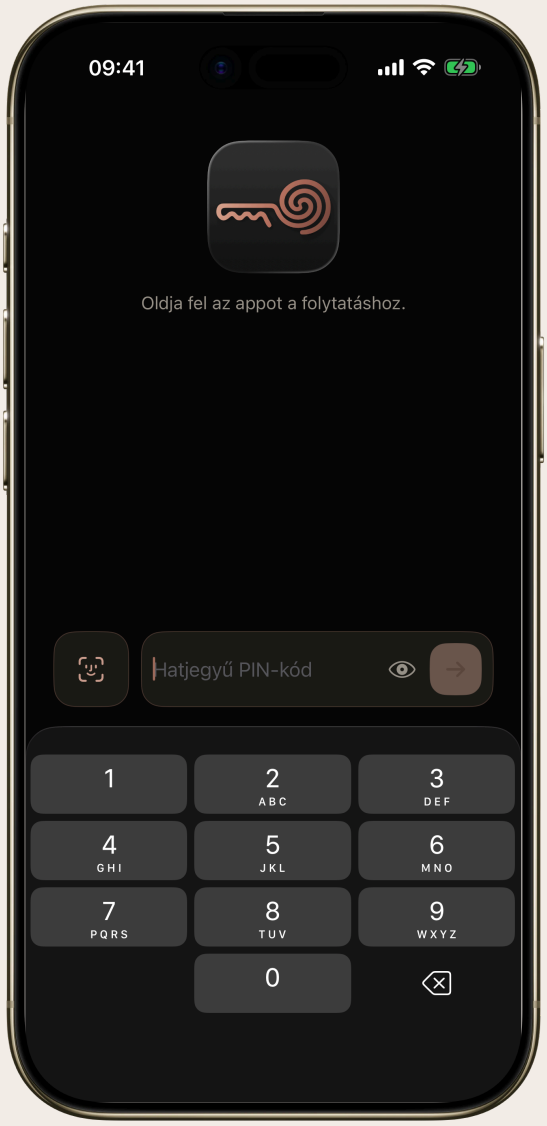
BEÁLLÍTÁS	MIT CSINÁL
Az app megjelenése	Rendszer, Világos vagy Sötét.
Kártyáim	A névvel ellátott kártyái (24. oldal).
Speciális	Bármely kártya zárolása, feloldása vagy visszaállítása beolvasással.
Appzár	PIN-kód és Face ID az apphoz (következő oldal).
Vágólap törlése ennyi után	15 mp, 30 mp vagy 1 perc egy bejegyzés kimásolása után.
Kártyák és biztonság	Beépített súgó: Így működik a MI8OS Card, Titkosítás és jelszavak, Mennyire biztonságos a MI8OS?, Kártyagondozás és helyreállítás.
Támogatás és jogi tudnivalók	MI8OS Card rendelése, Adatvédelmi irányelvek, Használati feltételek.



APPZÁR

Zár magának az appnak.





Kapcsolja be a Továbbiak → Appzár alatt: válasszon hatjegyű PIN-kódot, és ha szeretné, Face ID-t vagy Touch ID-t.

Zárolás, amikor kilépek: Azonnal, 1 perc után vagy 10 perc után. Ha hosszabb időre kilép az appból, a nyitott széf is bezárul.

A PIN-kód csak az appot nyitja meg ezen a telefonon. Nem fejt vissza kártyát, és nem helyettesíti a széfjelszót. Olyan hat számjegyet válasszon, amely mást nem nyit.

06

Hogyan védjük a bejegyzéseit

Két titkosítási réteg, egy valós példa és őszinte válasz arra, hogy „mi van, ha valaki ellopja a kártyámat?”

A NAGY KÉP

Két réteg. Mindkettő a jelszavából ered.

1

AZ APPBAN: A BEJEGYZÉSEK LEPECSÉTELŐDNEK

Mielőtt bármi a kártyára kerülne, az app a telefonján titkosít minden bejegyzést **ChaCha20-Poly1305** algoritmussal és egy, a széfjelszavából előállított 256 bites kulccsal.

Ez a fő zár. Aki a nyers adatokat birtokolja, az is csak véletlenszerűnek tűnő bájtokat lát, és minden módosításuk lebukik.

2

A KÁRTYÁN: AZ AJTÓ ZÁRVA

A kártya biztonságos chipje a titkosított bejegyzéseket saját **AES-128** kulcsa mögött tartja, amelyet szintén a széfjelszavából állítunk elő. Csak akkor adja ki őket, ha a telefon bizonyította, hogy ismeri ezt a kulcsot.

A helyes jelszó nélkül egy olvasó csak a kártya nyilvános beállításait kapja meg.

Az Ön széfjelszava

soha, sehol nem tárolódik

↓

Tartalomkulcs

256 bites · lepecsételi a bejegyzéseket (1. réteg)

Kártyakulcs

128 bites · kinyitja a kártya ajtaját (2. réteg)

Kezelőkulcs

128 bites · kezeli a kártyán lévő széfet

A JELSZÓTÓL A KULCSOKIG

Miért tart egy pillanatig „A titkosítás erősítése folyamatban…”.

Széfjelszó
+ egy véletlen, 16 bájtos só, minden kártyánál más

↓

Argon2id
64 MiB memória · 3 menet · 4 sáv (RFC 9106)

↓

256 bites gyökérkulcs
csak a memóriában létezik, rövid ideig

↓

HKDF-SHA256
független kulcsokra bontja a gyökeret, mindegyiket saját címkével

↓

Tartalomkulcs
256 bites · a bejegyzésekhez

Kártyakulcs
128 bites · a kártya ajtajához

Kezelőkulcs
128 bites · a széf beállításához

ARGON2ID

Szándékosan lassú, memóriaigényes jelszófüggvény. Minden egyes próbálkozás 64 MiB memóriába és valódi időbe kerül, a telefonján éppúgy, mint egy támadó számítógépén.

A SÓ

Véletlen bájtok, nyíltan tárolva a kártyán. Egyedivé teszik minden kártya kulcsait, így senki sem készíthet előre próbálkozási táblázatot.

VALÓS PÉLDA · 1/4 · A KULCSOK

Titkosítsuk a „12345678” értéket.

Ezek valós értékek, ugyanazokkal az algoritmusokkal és beállításokkal előállítva, mint az appban. A jelszó csak ehhez a példához készült.

Széfjelszó	`copper-lantern-velvet-orbit`
Bejegyzés neve	`Demo PIN`
Bejegyzés	`12345678`
Só (véletlen, a kártyán)	`7a8dbeec53e1eb50c70ccd4674a0e624`
Gyökérkulcs (Argon2id)	`84e743792af48790ce3ac4e2410ba1e9ef786851fa74467fc077208674905241`
Tartalomkulcs · 256 bites	`dcbe9b90a42a1c5e53f8bdaf07e3d763a61708ae3ad68fdfa7be72792fa6ab7c`
Kártyakulcs · 128 bites	`266b550b4a87dd1029d53af4262244c1`
Kezelőkulcs · 128 bites	`d9715ed54fbc71325587258c440a8dc6`

> **Ezek közül egyik kulcs sem tárolódik soha.** Az app akkor számítja ki őket, amikor megadja a jelszavát, és elfelejti, amikor a széf bezárul. A kártyán csak a só van.

VALÓS PÉLDA · 2/4 · 1. RÉTEG AZ APPBAN

A „12345678” értéktől a véletlenszerűnek tűnő bájtokig.

1. A bejegyzés becsomagolódik 20 bájtba: egy névmezőbe és egy bejegyzésmezőbe.

```
000  01 08 44 65 6d 6f 20 50 49 4e 02 08 31 32 33 34 35 36 37 38
```

mezőtípus és hossz · „Demo PIN” · "12345678"

2. A ChaCha20-Poly1305 lepecsételi a tartalomkulccsal, egy egyedi, 12 bájtos nonce-szal (a slot fejlécéből származtatva) és a fejléccel mint hitelesített adattal.

Nonce	`be00fc197a76fb68b8f315fa`
Rejtjeles szöveg · 20 bájt	`5eda3e6b43d7aa61edf77ab4a26ae11e9b080c60`
Címke · 16 bájt	`1b1b0dbbd23c5dffd6f4c462f9a449c4`

> **A címke pecsét.** Ha a rejtjeles szöveg vagy a fejléce akár egyetlen bitje megváltozik, a címke már nem egyezik, és az app elutasítja az adatot, ahelyett hogy valami hibásat mutatna.

VALÓS PÉLDA · 3/4 · AMI A KÁRTYÁN VAN

Egy bejegyzés, egy 192 bájtos slot.

Pontosan ezt tárolja a kártya a „Demo PIN” bejegyzéshez. Keresse meg benne a „12345678” értéket: nincs ott.

```
000  31 0d ce db 3c 00 01 00 01 00 01 14 5e da 3e 6b
016  43 d7 aa 61 ed f7 7a b4 a2 6a e1 1e 9b 08 0c 60
032  1b 1b 0d bb d2 3c 5d ff d6 f4 c4 62 f9 a4 49 c4
048  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
064  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
096  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
112  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
128  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
144  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
176  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

fejléc: verzió, bejegyzés, pozíció (12 bájt) · rejtjeles szöveg (20 bájt) · címke (16 bájt) · üres hely

A KÁRTYA AJTAJA MÖGÖTT

Ezek a slotok a kártya védett részén vannak. A kártya csak azután adja ki őket, hogy a telefon a kártyakulccsal átment az ellenőrzésen (2. réteg).

UGYANAZ A BEJEGYZÉS, MÁS BÁJTOK

Írja ugyanazt a bejegyzést egy másik kártyára, és teljesen máshogy fog kinézni, mert minden kártyának saját sója és saját kulcsai vannak.

VALÓS PÉLDA · 4/4 · A NYILVÁNOS RÉSZ

Amit bárki láthat, akinek olvasója van.

Minden kártyának van egy kis nyilvános területe is (128 bájt). Jelszó nélkül olvasható, mert az appnak szüksége van a sóra a kulcsai előállításához.

```
000  4d 49 38 4f 53 03 32 b3 fb 93 6e bf 4d 64 b7 6f
016  5e 90 f5 75 7f 6e 00 00 01 00 c0 00 27 10 7a 8d
032  be ec 53 e1 eb 50 c7 0c cd 46 74 a0 e6 24 00 01
048  00 00 00 00 00 03 04 00 20 00 00 00 00 00 00 00
064  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
096  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
112  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

„MI8OS" és formátum · széfazonosító · kártyaelrendezés · só · Argon2id-beállítások · nem használt

ÉS ROSSZ JELSZÓVAL?

Változtassa meg csak a jelszó utolsó betűjét, és a kártyakulcs ez lesz:

`883e65196d88bc9f1aae79acf8fa7c74`

e helyett: `266b550b4a87dd1029d53af4262244c1`. Semmi hasonlóság. A kártya elutasítja az ellenőrzést, nem küld bejegyzést, és semmi sem íródik ki.

HA VALAKI ELLOPJA A KÁRTYÁJÁT

Egy kártyája van. Nem a bejegyzései.

Nincs hátsó ajtó, és nincs álkulcs. Az egyetlen út befelé a széfjelszava kitalálása, és mindkét réteg drágává tesz minden próbálkozást.

A

TALÁLGATÁS A KÁRTYÁN KERESZTÜL

Minden próbálkozáshoz kell a fizikai kártya. A tolvaj lefuttatja az Argon2id-t egy próbálkozáshoz, majd megkérdezi a kártyát. A kártya NFC-n egyszerre egy kísérletre válaszol. Becslésünk szerint ez legfeljebb körülbelül 20 kísérlet másodpercenként.

B

A CHIP SZÉTSZEDÉSE

A drága út. Egy szakosodott labor megpróbálhatja közvetlenül a chipből kinyerni a titkosított slotokat. Ezután offline, sok számítógépen találgathat, de minden próbálkozás továbbra is egy teljes, 64 MiB memóriát használó Argon2id-futásba kerül.

AZ ŐSZINTE ÖSSZEGZÉS

Mindkét út ugyanoda vezet: **mennyire nehéz kitalálni a széfjelszavát?** Egy erős jelszó kitalálása gyakorlatilag elérhetetlen. Egy gyengénél a két réteg csak időt nyer. A következő oldal megmutatja, mennyit.

MIÉRT SZÁMÍT A SZÉFJELSZAVA

Mennyi idő kipróbálni minden lehetőséget?

A SZÉFJELSZÓ TÍPUSA	A KÁRTYÁN KERESZTÜL ~20 PRÓBÁLKOZÁS / MP	LABOR + HATALMAS SZÁMÍTÓGÉPPARK 1 000 000 PRÓBÁLKOZÁS / MP
Bármely jelszó egy 1 milliárd kiszivárgott jelszót tartalmazó listáról, pl. „Nyár2026!!”	legfeljebb kb. 2 év; a gyakoriak sokkal hamarabb	legfeljebb kb. 17 perc; a gyakoriak másodpercek alatt
12 véletlen számjegy	kb. 1600 év	kb. 12 nap
4 véletlen szó	évmilliók	kb. 116 év
12 véletlen kisbetű	több mint 100 millió év	kb. 3000 év
5 véletlen szó	hosszabb, mint amióta a világegyetem létezik	kb. 900 000 év
6 véletlen szó	hosszabb, mint amióta a világegyetem létezik	kb. 7 milliárd év

Az Ön számára legrosszabb eset: minden lehetőség kipróbálásának ideje. A „véletlen szavak” egy 7776 szavas listáról dobókockával kiválasztott szavakat jelentenek. A találgatási sebességek szemléltető, bőkezű becslések. Viszonyításként: egy próbálkozás kb. 25 ms-ig tartott egy modern, 4 magot használó Apple M4 számítógépen.

AJÁNLÁS

Öt vagy hat véletlen szó. Soha ne használja újra, és soha ne használjon dalszöveget, nevet vagy dátumot.

ÉS ÍRJA LE

Tartson egy példányt biztonságos helyen, a kártyáitól elkülönítve. Az elfelejtett széfjelszó nem állítható helyre.

AMIT A MI8OS SOHA NEM TESZ

Nincs mit feltörni a felhőben. Mert nincs felhő.

- ✓ **Nincs fiók, nincs szerver.** Az app egyáltalán nem létesít hálózati kapcsolatot.
- ✓ **Nincsenek tárolt jelszavak.** A széfjelszavakat és a mesterjelszavakat soha nem menti, sem a telefonra, sem a kártyára.
- ✓ **Nincs másolat a telefonon.** A visszafejtett bejegyzések csak a memóriában léteznek, amíg egy széf nyitva van. Egy kivétel: egy kimásolt bejegyzés a vágólapon marad, amíg az időzítő nem törli (15 mp és 1 perc között), akkor is, ha a széf már bezárult.
- ✓ **Nincs telemetria.** Nincs nyomkövetés, nincs analitika.
- ✓ **Zárol, amikor kilép.** Az appból kilépve a széf bezárul (azonnal vagy a választott késleltetés után).
- ✓ **Eltakarja a képernyőt** az appváltóban, valamint képernyőfelvétel vagy -tükrözés közben.
- ✓ **Észleli a manipulációt.** A módosított adat nem megy át a pecséten, és elutasításra kerül.
- ✓ **Csak nyilvános, szabványos algoritmusokat használ:** Argon2id, HKDF-SHA256, ChaCha20-Poly1305, AES-128.

A HÁTSÓ AJTÓ HIÁNYÁNAK MÁSIK OLDALA

Ha elveszíti az összes kártyát, vagy elfelejti a széfjelszót, senki sem tudja visszaszerezni a bejegyzéseit. Sem Ön, sem mi. Ezért van három kártyája és egy leírt jelszava.

KÁRTYAGONDOZÁS ÉS HELYREÁLLÍTÁS

Három kártya, három hely.

01

TARTSA ŐKET KÜLÖN

Egy kártya Önnél vagy a közelben, egy otthon, egy valahol máshol: a családnál, a munkahelyen vagy egy széfben. Egyetlen tűz vagy betörés nem viheti el mindhármat.

02

ELVESZETT EGY KÁRTYA?

A megtaláló csak titkosított adatot kap. Készítsen pótkártyát (lásd 03), hogy újra három másolata legyen. Ha attól tart, hogy valaki ismeri a jelszót, ugyanígy hozzon létre új széfeket új széfjelszóval, majd állítsa vissza a régi kártyáit.

03

PÓTKÁRTYA KÉSZÍTÉSE

Az app csak közvetlenül a létrehozás után tud egy széfet más kártyákra másolni. Későbbi pótkártyához hozzon létre egy új széfet egy üres kártyán, és adja meg újra ugyanazokat a bejegyzéseket: nyisson meg egy működő kártyát, hogy kiolvassa őket, és ha közben bármit leír, azt a jegyzetet utána semmisítse meg. Tegye ezt meg, mielőtt csak az utolsó másolata marad.

04

ELFELEJTETTE A SZÉFJELSZÓT?

Ezeket a bejegyzéseket nem lehet helyreállítani. Ha egy másik kártya olyan jelszót használ, amelyre még emlékszik, azt nyissa meg. Ellenkező esetben állítsa vissza a kártyákat, és kezdjen új széfet.

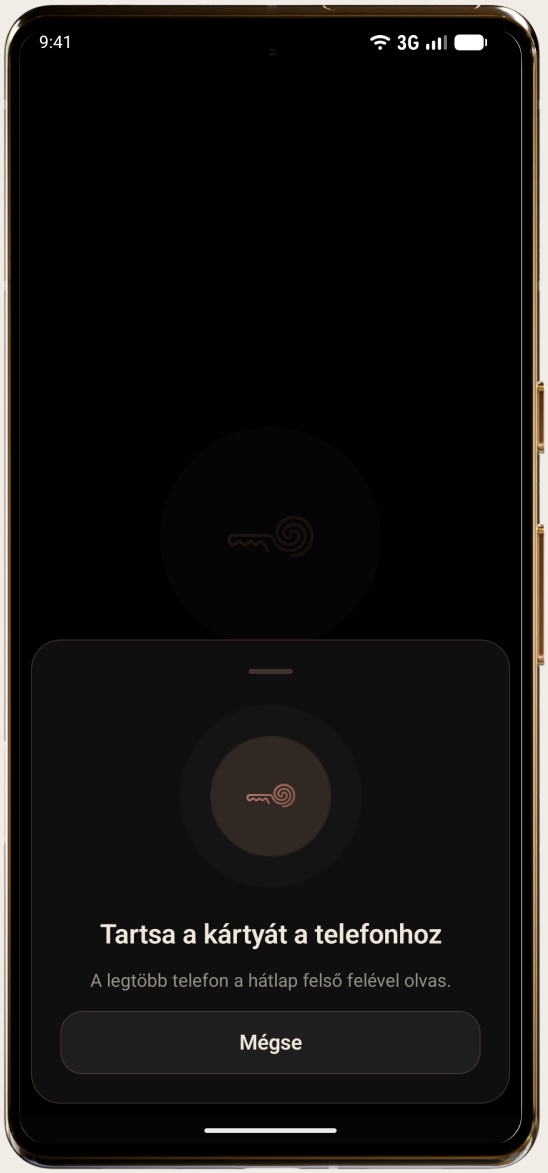
> **Vigyázzon a kártyákra**, mint egy bankkártyára: ne hajlítsa meg, ne érje hő, ne érjen éles élekhez. Beolvasáskor tartsa távol őket a fém tokoktól.

ANDROIDON

Ugyanaz az app, néhány apró különbséggel.

Az androidos app a **Google Playen** érhető el. Ugyanúgy működik, és ugyanazokat a kártyákat olvassa. Az iPhone-on felírt széf Androidon is megnyílik, és fordítva.

ANDROIDON	MI MÁS
Beolvasás	Az Androidnak nincs rendszerszintű NFC-ablaka, ezért a MI8OS saját beolvasási képernyőt mutat egy mégse gombbal.
A kártya helye	Tartsa a kártyát a telefon hátoldalának felső feléhez. A pontos hely típusonként eltér.
NFC	Az NFC-nek bekapcsolva kell lennie a telefon beállításaiban.
Biometria	Az appzár a telefon ujjlenyomat- vagy arcfelismerését használja.



HIBAELHÁRÍTÁS

Ha valami nem működik.

AMIT LÁT	TEENDŐ
A kártyát nem érzékeli	Tartsa laposan az iPhone felső pereméhez, és ne mozdítsa. Vegye le a vastag vagy fém tokot. Próbálja kicsit feljebb vagy lejjebb.
A felírás félúton megszakadt	Koppintson az **Újrapróbálkozás** gombra, és tartsa mozdulatlanul ugyanazt a kártyát. Minden mentés a teljes kártyát újraírja, a változtatásai pedig az appban maradnak, amíg sikerül. Ha az app jelzi, hogy a mentés nem fejezhető be, állítsa vissza a kártyát (26. oldal), és mentsen újra, vagy használjon tartalékkártyát, és cserélje le ezt (42. oldal).
Hibás jelszó	Ellenőrizze a helyesírást és a szóközöket. Ne feledje: minden kártyának lehet saját széfjelszava.
„Ez egy másik kártya”	A felhelyezett kártya nem az, amelyik meg van nyitva. A megfelelőt az Azonosítás funkcióval találja meg.
A kártya megtelt	Egy kártya 20 bejegyzést tárol. Töröljön egyet, amelyre már nincs szüksége, vagy ossza el a bejegyzéseit több kártya között.
Egy kártya nem állítható vissza	Zárolva van. A visszaállítás kéri a mesterjelszavát.
A széf magától bezárult	Kilépett az appból, vagy a képernyőt felvették. Nyissa meg újra a kártyát.
„A kulcsa előkészítése folyamatban” szünet	Ez normális. A 34. oldalon leírt szándékos jelszóerősítésről van szó.

További segítség: guide.mi8os.com · info@mi8os.com

MI8OS

A magánszférája az Öné.

MI8OS.COM

MI8OS-útmutató, magyar nyelvű, 2026. október. A MI8OS appot írja le iPhone-ra és Androidra. A képernyők verziónként kissé eltérhetnek. A 06. fejezet példakulcsai és -bájtjai ehhez az útmutatóhoz, egy bemutató jelszóval készültek; soha ne használja. MI8OS · info@mi8os.com