MI8OS

PRŮVODCE MI8OS

Vše o vaší aplikaci a vašich kartách.

Jak vytvořit, otevřít a aktualizovat trezor, jak pečovat o MI8OS Card gen 2 a jak přesně jsou vaše položky chráněny, až do posledního bajtu.

VYTVOŘIT · POUŽÍVAT · KARTY · ZABEZPEČENÍ



Pro aplikaci MI8OS na iPhonu a Androidu. Říjen 2026.

OBSAH

Co v průvodci najdete

01 **ZAČÍNÁME** p. 3
Co je MI8OS, slova, se kterými se setkáte, aplikace v kostce, jak držet kartu.

02 **VYTVOŘENÍ TREZORU** p. 9
Přidejte položky, zvolte heslo trezoru, uložte na kartu, zapište záložní karty.

03 **POUŽÍVÁNÍ TREZORU** p. 16
Otevření karty, čtení a kopírování položek, kódy 2FA, přidávání a mazání, aktualizace karty.

04 **SPRÁVA KARET** p. 23
Moje karty, přejmenování, identifikace, reset, zamknutí a odemknutí hlavním heslem.

05 **NASTAVENÍ** p. 29
Zámek aplikace, Face ID, schránka a vzhled.

06 **JAK JSOU VAŠE POLOŽKY CHRÁNĚNY** p. 32
Dvě vrstvy šifrování, skutečný příklad s „12345678“ a proč na vašem hesle trezoru záleží.

07 **PÉČE, ANDROID A NÁPOVĚDA** p. 42
Tři karty, rozdíly na Androidu, řešení potíží.

01

Začínáme

Pět minut na to, abyste pochopili, jak MI8OS funguje, než se dotknete karty.

CO JE MI8OS

Malý šifrovaný trezor na kartě, kterou máte v ruce.

MI8OS uchovává vaše nejdůležitější tajemství, jako jsou obnovovací kódy, klíče 2FA, seed fráze a PIN kódy, v trezoru, který se šifruje ve vašem telefonu a ukládá na fyzickou kartu. Žádný účet, žádný cloud, žádné předplatné.



S sebou · ta, kterou používáte



Doma · v bezpečí doma



Jinde · na jiném místě

VE VAŠÍ SADĚ

Tři **MI8OS Card, gen 2**. Každá karta pojme až **20 položek**. Zapište stejný trezor na všechny tři a uložte je na různá místa.

CO POTŘEBUJETE

iPhone nebo telefon s Androidem s NFC a aplikaci MI8OS z App Storu nebo Google Play (poznámky k Androidu na straně 43). A heslo trezoru, které si zapamatujete: nejlepší je dlouhá heslová fráze.

SLOVA, SE KTERÝMI SE SETKÁTE

Tři hesla, tři různé úkoly.

Toto je nejdůležitější strana průvodce. Zní podobně, ale každé chrání něco jiného.

HESLO TREZORU

Šifruje a otevírá položky na kartě. Povinné, alespoň 12 znaků.

Nikde se neukládá. Nikdo ho nemůže obnovit, ani MI8OS.

HLAVNÍ HESLO

Volitelné. Zamyká samotnou kartu, aby ji nikdo nemohl resetovat ani vymazat bez tohoto hesla.

Nic neotevírá. Ke čtení položek je stále potřeba heslo trezoru.

PIN ZÁMKU APLIKACE

Volitelný. Šest číslic (nebo Face ID) k otevření aplikace v tomto telefonu.

Nemá nic společného s vašimi kartami a nic nedešifruje.

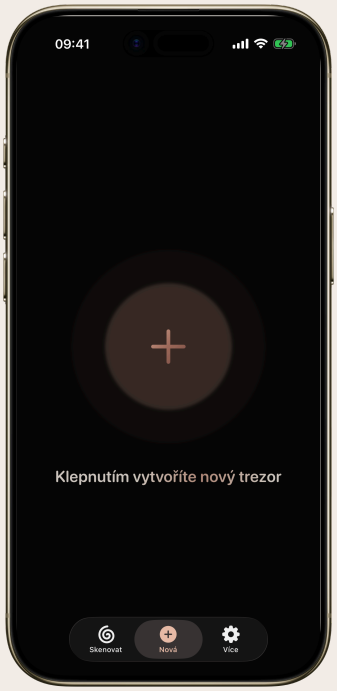
SLOVO	VÝZNAM
Trezor	Váš seznam položek. Existuje zašifrovaný na vašich kartách a dešifrovaný jen v paměti aplikace, dokud je otevřený.
Položka	Jeden záznam: název (až 24 bajtů) a samotné tajemství (až 96 bajtů), například PIN, obnovovací kód nebo klíč 2FA.
Karta	Vaše MI8OS Card gen 2. Ukládá šifrovaný trezor; stejný trezor můžete zapsat na více karet.
Aktualizovat kartu	Zapíše vaše změny na kartu. Do té doby existují změny jen v paměti aplikace.

APLIKACE V KOSTCE

Tři záložky. Každá má jeden úkol.



Skenovat · otevřít kartu



Nová · vytvořit trezor



Více · karty a nastavení

1

SKENOVAT

Klepnutím naskenujete kartu a přiložte kartu k telefonu. Karta se otevře ve vlastním okně, kde zadáte její heslo trezoru.

2

NOVÁ

Klepnutím vytvoříte nový trezor. Průvodce o čtyřech krocích vás provede od první položky až ke kartě, která ji obsahuje.

3

VÍCE

Vaše karty, zámek aplikace, časovač schránky, vzhled a vestavěné stránky nápovědy.

DRŽENÍ KARTY

Horní okraj. Naplocho. V klidu.

Pokaždé, když aplikace komunikuje s kartou, zobrazí iPhone vlastní okno NFC. Potom:

1. **Přiložte kartu naplocho k hornímu okraji** zadní strany iPhonu, kde je anténa NFC.
2. **Držte ji v klidu**, dokud aplikace nepotvrdí. Zápis trvá několik sekund; předčasné oddálení karty je nejčastější důvod, proč je nutné zápis opakovat.
3. Pokud se nic neděje, posuňte kartu pomalu o kousek níž nebo výš a sundejte silné nebo kovové pouzdro.



> **Není kam spěchat.** Když otevíráte kartu, aplikace nejprve připraví váš klíč („Připravuje se váš klíč. Kartu zatím není třeba přikládat“). Kartu přiložte, až se objeví okno NFC.

> **Na Androidu** aplikace zobrazí vlastní obrazovku skenování a karta se přikládá k horní polovině zadní strany telefonu.

CO PATŘÍ NA KARTU

Pár položek, na kterých hodně záleží.

MI8OS nemá nahradit váš správce hesel. Je to offline místo pro hrstku věcí, které byste potřebovali, kdyby všechno ostatní selhalo.

IDEÁLNÍ NA KARTU

- ✓ Obnovovací kódy pro e-mail a Apple / Google
- ✓ Instalační klíče 2FA, aby aplikace mohla zobrazit vaše kódy
- ✓ Obnovovací fráze pro kryptoměny (MI8OS není peněženka a nedrží žádné prostředky)
- ✓ Hlavní heslo vašeho správce hesel nebo údaje z jeho nouzové sady
- ✓ Důležité PIN kódy a soukromé poznámky

DOBRÉ VĚDĚT

- ✓ Až 20 položek na kartu
- ✓ Název: až 24 bajtů · položka: až 96 bajtů
- ✓ Běžná písmena, číslice a mezery zabírají 1 bajt; písmena s diakritikou, řecká nebo cyrilice 2; emoji 4
- ✓ Dlouhé seed fráze mohou potřebovat dvě položky (např. slova 1–12 a 13–24)

02

Vytvoření trezoru

Čtyři kroky: Položky, Heslo, Zápis, Hotovo. Asi pět minut.

KROK 1 ZE 4 · POLOŽKY

Začněte svými položkami.

1. Otevřete záložku **Nová** a klepněte na tlačítko **Klepnutím vytvoříte nový trezor**.
2. Klepněte na **Přidat položku** pro každou věc, kterou chcete uchovat.
3. Přejetím po položce ji před pokračováním zase odeberete.
4. Až bude seznam hotový, klepněte na **Pokračovat**.

> **Zatím se nic neuložilo.** Vaše položky zůstávají jen v tomto průvodci, dokud šifrovaný trezor neuložíte na kartu.

> **Máte už otevřený trezor?** Aplikace se nejprve zeptá. Pokud máte změny, které ještě nejsou na žádné kartě, nabídne jejich ponechání.



PŘIDÁNÍ POLOŽKY

Název a samotné tajemství.

Název. Něco, co poznáte, třeba „Obnovovací kódy e-mailu“. Až 24 bajtů; počítadlo ukazuje, kolik zbývá.

Položka. Heslo, kód nebo text, až 96 bajtů. Vše, co vložíte nebo vygenerujete, se zašifruje dřív, než se dostane na kartu.

Generování. Klepnutím na kostku vytvoříte náhodné heslo o 16, 32, 64 nebo 96 znacích.

ULOŽENÍ KLÍČE 2FA

Když služba zobrazí instalační klíč (nebo odkaz otpauth:// za svým QR kódem), vložte ho jako položku. MI8OS ho rozpozná a později zobrazí tlačítko **TOTP**, které zkopíruje aktuální kód. Pokud je odkaz delší než 96 bajtů, vložte jen samotný instalační klíč (část za secret=); MI8OS pak použije standardních 6 číslic každých 30 sekund.



KROK 2 ZE 4 · HESLO

Zvolte heslo trezoru.

1. Zadejte heslo trezoru a pro potvrzení ho zadejte znovu.
2. Sledujte ukazatel síly: 12 znaků je minimum, 20 nebo fráze s mezerami dá „Vynikající délka.“
3. Zaškrtněte políčko: *„Pokud ztratím všechny karty nebo zapomenu toto heslo, MI8OS trezor z této karty neobnoví.“*
4. Klepněte na **Zašifrovat trezor**.



NAŠE RADA

Použijte **pět nebo šest náhodných slov**, například *měď lucerna samet oběžnice tundra* (ale ne právě tato). Snadno se pamatují, extrémně těžko se hádají. Strana 40 ukazuje proč.

KROK 3 ZE 4 · ZÁPIS

Nejdřív šifrování. Pak přiložení.

Šifrování probíhá ve vašem telefonu, ještě než se spustí NFC. Na chvíli uvidíte „Posiluje se vaše šifrování…“, zatímco aplikace mění vaše heslo na klíče. Ta pauza je záměrná: komukoli jinému hádání vašeho hesla zpomalí.

Když se zobrazí **Šifrování připraveno**:

1. Klepněte na **Uložit na kartu**.
2. Až se objeví okno NFC, přiložte kartu k hornímu okraji iPhonu.
3. Nehýbejte s ní. Aplikace zapíše trezor a pak **ho znovu přečte, aby ho zkontrolovala**.

> **Prázdná karta?** Aplikace ji automaticky připraví v rámci stejného přiložení.



KROK 4 ZE 4 · HOTOVO

Teď zapište záložní karty.

„Trezor uložen na kartu“ znamená, že je trezor na té kartě ověřený. **Je to jediný okamžik, kdy aplikace může zkopírovat celý váš trezor na další karty**, proto je teď zapište všechny:

1. Klepněte na **Zapsat další kartu**.
2. Zvolte **Použít stejné heslo trezoru** (nejjednodušší) nebo **Použít jiné heslo trezoru** pro tuto kartu.
3. Uložte na další kartu. Zopakujte pro třetí.

> **Stejné heslo, nové šifrování.** Každá karta dostane vlastní náhodnou sůl, takže i se stejným heslem vypadají data na každé kartě úplně jinak.

Zahodit trezor z tohoto iPhonu jen zavře trezor v paměti aplikace. Kartu nikdy nevymaže.



KARTA, KTERÁ UŽ TREZOR MÁ

MI8OS nikdy nepřepíše trezor bez varování.

Pokud uložíte nový trezor na kartu, která už nějaký má, nic se nezapíše. Aplikace vám řekne: **„Tato karta už trezor má“** a nabídne dvě možnosti:

PŘIDAT POLOŽKY

Přidá vaše nové položky do trezoru na kartě. Položky, které na ní už jsou, zůstanou. Vaše heslo trezoru musí být to, které tato karta používá, a kartu přiložíte ještě jednou.

ZRUŠIT

Ponechá kartu přesně tak, jak byla.

> **Chcete trezor úplně nahradit?** Nejprve kartu resetujte (strana 26) a pak na ní vytvořte nový trezor.



03

Používání trezoru

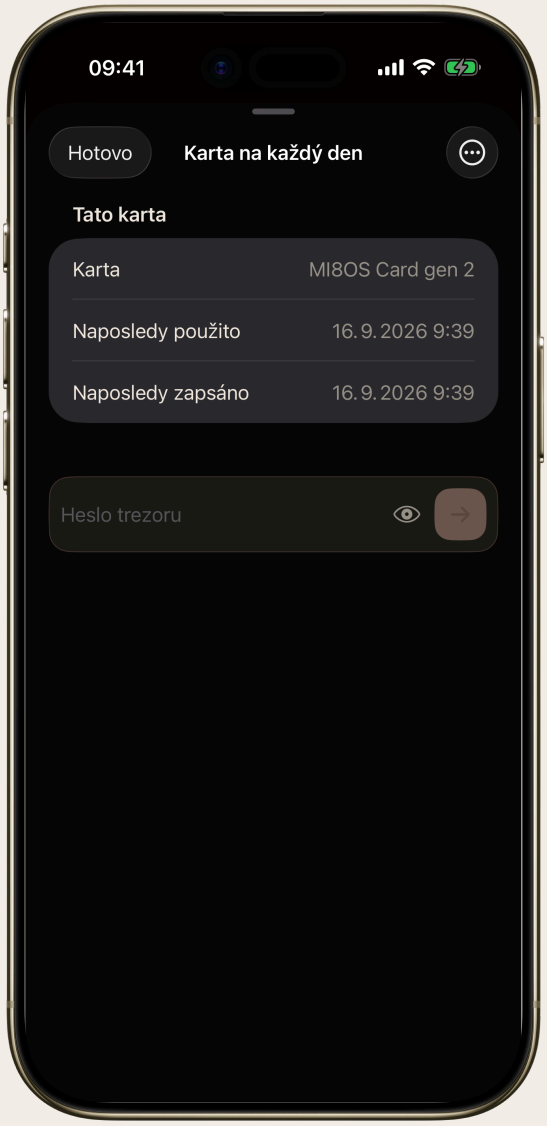
Otevřít, číst, kopírovat, měnit a zapsat změny zpět na kartu.

OTEVŘENÍ KARTY

Skenování, heslo, znovu přiložit.



Záložka Skenovat



Okno karty

1. V záložce **Skenovat** klepněte na tlačítko **Klepnutím naskenujete kartu** a přiložte kartu. Skenování čte jen veřejné informace karty.
2. Zadejte **Heslo trezoru** karty a klepněte na **Otevřít trezor**. Aplikace připraví váš klíč a pak si kartu vyžádá ještě jednou.

UVNITŘ TREZORU

Vaše položky, tak dlouho, jak je potřebujete.

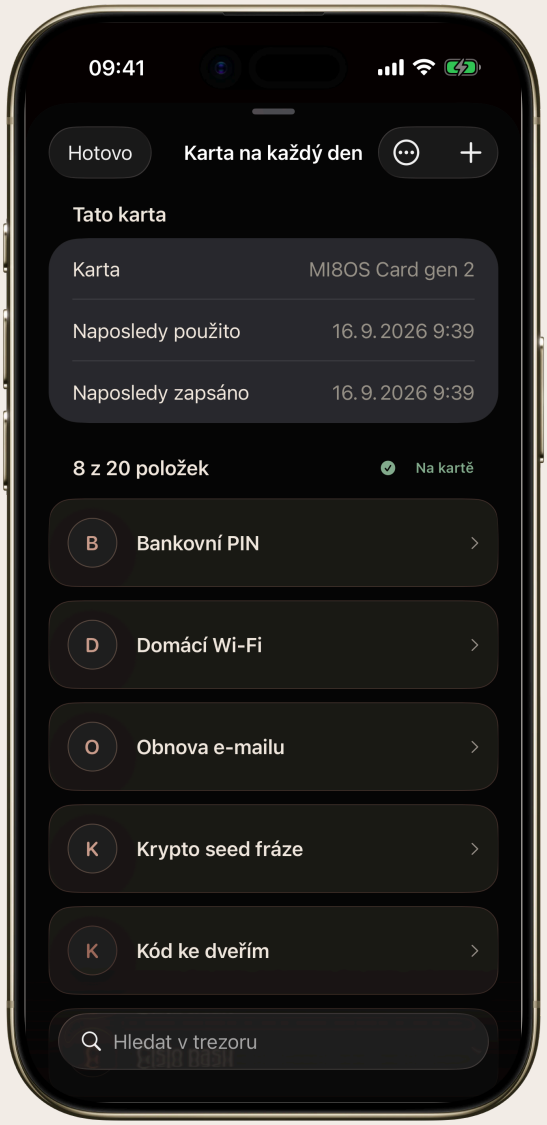
Tato karta ukazuje, která karta je otevřená, údaje Naposledy použito a Naposledy zapsáno a zda má hlavní heslo.

„8 z 20 položek“ říká, jak je karta plná. **Na kartě** znamená, že vše, co vidíte, je uložené na kartě.

Hledat v trezoru dole najde položku podle názvu.

+ nahoře přidá položku; **⋯** otevře nabídku karty (strana 25).

> **Dešifrováno jen v paměti.** Vaše položky existují v čitelné podobě jen, dokud je toto okno otevřené. Klepněte na **Hotovo** a z telefonu zmizí.



ČTENÍ A KOPÍROVÁNÍ

Skryté, dokud o to nepožádáte.

Klepnutím položku otevřete. Hodnota je skrytá za tečkami.

Zobrazit ji ukáže; **Skrýt** ji znovu skryje.

Kopírovat ji vloží do schránky a MI8OS **schránku zase vymaže** po 30 sekundách (změníte ve Více: 15 s, 30 s nebo 1 min).

> **Vkládejte rychle.** Po uplynutí časovače je schránka prázdná, takže položka nezůstane v jiných aplikacích. Časovač běží dál, i když trezor zavřete dřív.

> **Nahrávání nebo zrcadlení obrazovky?** MI8OS zakryje obrazovku a zavře trezor, aby se položky nedostaly do záznamu.



KÓDY 2FA

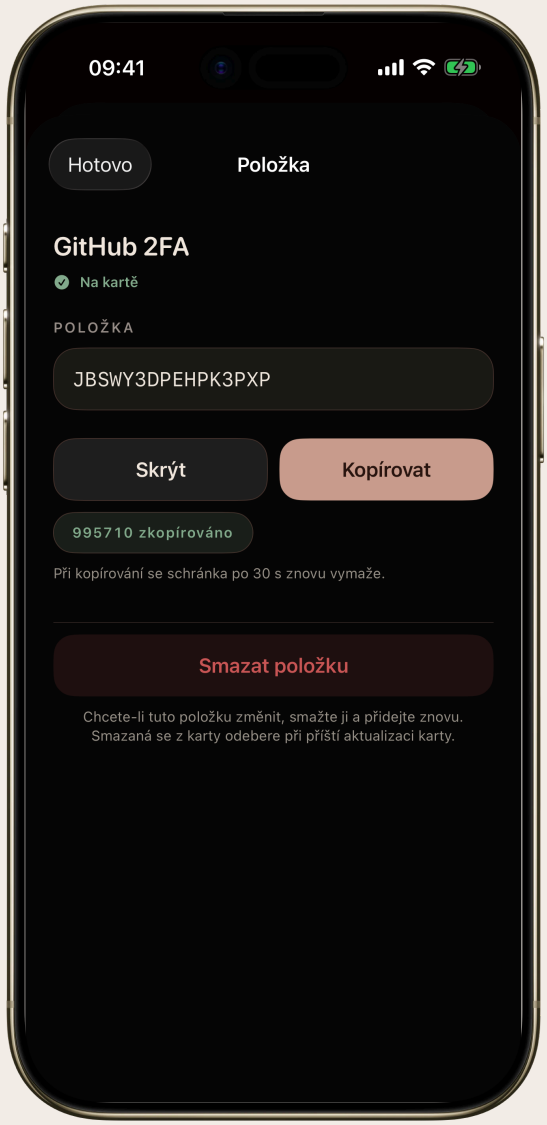
Váš ověřovač, z karty.

Pokud je položka instalačním klíčem 2FA, její stránka zobrazí tlačítko **TOTP**. Klepněte na něj a MI8OS vypočítá aktuální kód a zkopíruje ho, připravený k vložení.

Karta ukládá jen **šifrovaný instalační klíč**. Kód se počítá v aplikaci po otevření trezoru, z klíče a aktuálního času, stejně jako v každé ověřovací aplikaci.

PROČ TO POMÁHÁ

Pokud jsou vaše ověřovací kódy uložené jen v telefonu, který ztratíte, zmizí s ním. S instalačními klíči na kartách získáte kódy na jakémkoli novém telefonu s aplikací MI8OS.



ZMĚNA TREZORU

Přidat, smazat, pak aktualizovat kartu.

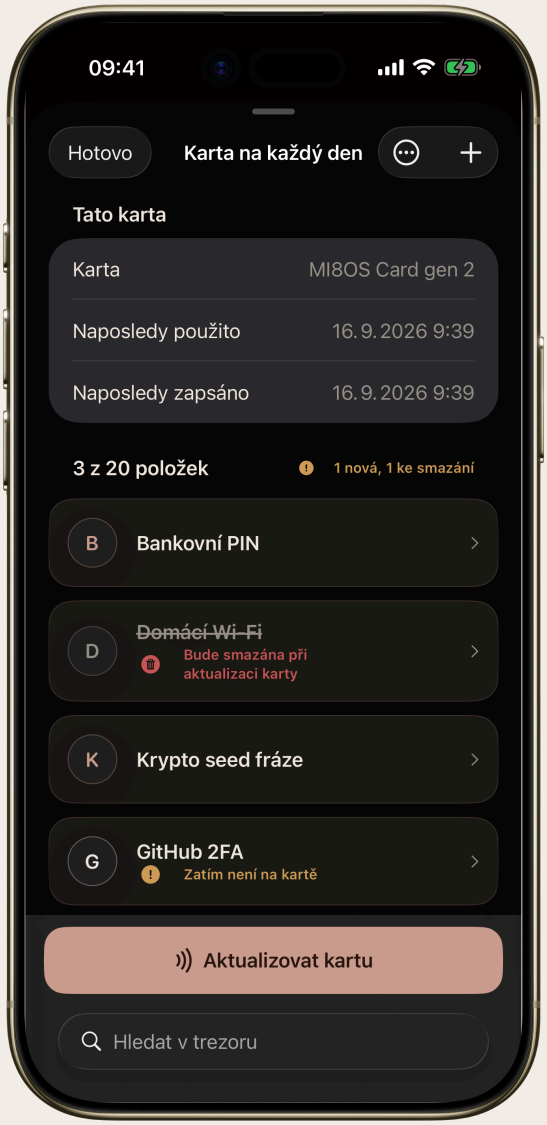
Přidání: klepněte na **+** a vyplňte název a položku.

Smazání: přejeďte položkou doleva, nebo ji otevřete a klepněte na **Smazat položku**. Zůstane v seznamu, označená, dokud kartu neaktualizujete. Rozmysleli jste si to? Klepněte na **Ponechat**.

Úpravy: tlačítko pro úpravy záměrně chybí. Chcete-li položku změnit, smažte ji a přidejte znovu.

Změny jsou označené jako dosud nezapsané. Klepněte na **Aktualizovat kartu** a přiložte kartu, abyste je uložili.

> **Zavíráte s nezapsanými změnami?** Aplikace vás upozorní: „Pokud tuto kartu zavřete bez aktualizace, přijdete o ně.“



KAŽDOU KOPII UDRŽUJTE AKTUÁLNÍ

Každá karta se aktualizuje zvlášť.

Aktualizovat kartu zapisuje na otevřenou kartu, a jen na ni. Ostatní karty mají předchozí verzi, dokud neaktualizujete i je.

1

ZMĚŇTE JEDNU KARTU

Otevřete kartu S sebou, přidejte nebo smažte, klepněte na **Aktualizovat kartu**.

2

ZOPAKUJTE U OSTATNÍCH

Otevřete karty Doma a Jinde a proveďte na každé stejnou změnu.

3

ZKRATKA PRO NOVÉ POLOŽKY

Vytvořte „nový trezor“ jen s novými položkami a uložte ho na kartu, která už váš trezor má. Zvolte **Přidat položky** a přidají se k tomu, co tam už je.

DOBRÝ ZVYK

Jednou ročně otevřete každou kartu a zkontrolujte, že všechny tři ukazují stejný počet položek.

04

Správa karet

Názvy, nabídka karty, reset a volitelné hlavní heslo.

MOJE KARTY

Pojmenujte každou kartu.

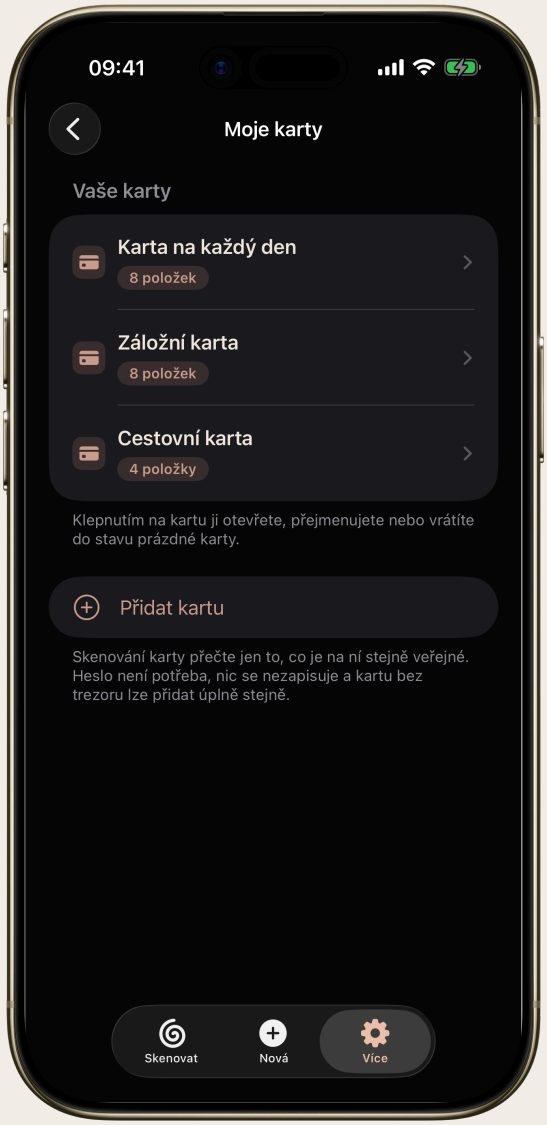
V **Více** → **Moje karty** vidíte karty, které tento telefon zná, se štítkem: počet položek, **Prázdná** nebo **Zamčená**.

Přidat kartu kartu naskenuje a zapamatuje si ji. Čte jen to, co je na kartě už veřejné: žádné heslo, nic se nezapisuje.

Klepnutím na kartu ji otevřete, přejmenujete nebo resetujete.

> **Rychlejší otevírání.** Karta, kterou tento telefon už zná, se po zadání hesla otevře jediným skenováním.

> **Uloženo jen v tomto telefonu:** názvy, které jste zadali, kdy byly karty naposledy použity, a jejich veřejná nastavení. Nikdy heslo, nikdy položka.



NABÍDKA KARTY ···

Přejmenovat, identifikovat, zapomenout.

PŘEJMENOVAT

Název, který poznáte: „S sebou“, „Doma“, „Trezor rodičů“.

IDENTIFIKOVAT

Nevíte, která karta je která? Klepněte na Identifikovat a přiložte kartu. Aplikace řekne, zda je to ta, na kterou se díváte, nebo která jiná.

ZAPOMENOUT

Odebere kartu ze seznamu tohoto telefonu. Na kartě se nic nemění a kdykoli ji můžete přidat znovu.

VÍCE

Resetovat kartu, Zamknout kartu a Odemknout kartu. Viz další strany.



RESET KARTY

Čistá karta, připravená na nový trezor.

··· → **Více** → **Resetovat kartu** odstraní trezor MI8OS a vše ostatní z karty a uvolní celé její úložiště. Heslo trezoru **nevyžaduje**.

Použijte ho, když chcete:

- ✓ Úplně nahradit trezor novým
- ✓ Znovu použít kartu po zapomenutí jejího hesla trezoru (položky na ní se ztratí)
- ✓ Vyčistit kartu, než ji někomu dáte

> **Ostatních karet se to nedotkne.** Reset jedné karty nikdy neovlivní trezor na vašich ostatních kartách.

> **Zamčená karta?** Reset odmítne, dokud nezadáte její hlavní heslo (další strana).



ZAMKNUTÍ KARTY · HLAVNÍ HESLO

Zabraňte komukoli vymazat vaši kartu.

Kdokoli, kdo vezme nezamčenou kartu, ji může resetovat, i bez vašeho hesla trezoru. Nic z ní nepřečte, ale může ji vymazat.

Zamknout kartu tomu zabrání. Zvolte hlavní heslo, přiložte kartu, hotovo. Od té chvíle kartu bez něj nelze resetovat ani vymazat, ani přes MI8OS, ani ničím jiným.

1. ··· → **Více** → **Zamknout kartu**
2. Zadejte dvakrát hlavní heslo a klepněte na **Zamknout**.
3. Držte kartu, dokud aplikace nepotvrdí „Karta zamčena“.

> **Čtení a ukládání se nemění.** Stále používají jen heslo trezoru.



ODEMKNUTÍ KARTY · A VAROVÁNÍ

Odemknutím se karta vrátí do normálu.

··· → **Více** → **Odemknout kartu**, zadejte hlavní heslo a přiložte kartu. Karta se znovu chová jako nezamčená. Její trezor i heslo trezoru zůstávají beze změny.

Chcete-li resetovat zamčenou kartu, zvolte Resetovat kartu: aplikace požádá o hlavní heslo a pak kartu naformátuje.

NEZAPOMEŇTE HO

Pokud zapomenete hlavní heslo karty, tuto kartu už **nikdy** nepůjde resetovat ani znovu použít. Její položky zůstanou čitelné s heslem trezoru. Aplikace se na něj ptá pokaždé a nikdy si ho nepamatuje.

Zamknout, odemknout a resetovat libovolnou kartu můžete i ve **Více** → **Pokročilé**, a to jejím naskenováním.



05

Nastavení

Zámek aplikace, Face ID, schránka a vzhled aplikace.

VÍCE

Všechno ostatní, na jednom místě.

NASTAVENÍ	CO DĚLÁ
Vzhled aplikace	Systém, Světlý nebo Tmavý.
Moje karty	Vaše pojmenované karty (strana 24).
Pokročilé	Zamknout, odemknout nebo resetovat libovolnou kartu jejím naskenováním.
Zámek aplikace	PIN a Face ID pro aplikaci (další strana).
Vymazat schránku po	15 s, 30 s nebo 1 min po zkopírování položky.
Karty a zabezpečení	Vestavěná nápověda: Jak MI8OS Card funguje, Šifrování a hesla, Jak bezpečný je MI8OS?, Péče o karty a obnova.
Podpora a právní informace	Objednat MI8OS Card, Zásady ochrany soukromí, Podmínky užívání.



ZÁMEK APLIKACE

Zámek pro samotnou aplikaci.





Zapněte ho ve Více → Zámek aplikace: zvolte šestimístný PIN a podle potřeby Face ID nebo Touch ID.

Zamknout, když odejdu: Okamžitě, Po 1 minutě nebo Po 10 minutách. Delší opuštění aplikace zavře i otevřený trezor.

PIN otevírá jen aplikaci v tomto telefonu. Nedešifruje kartu a nenahrazuje heslo trezoru. Zvolte šest číslic, které neotevírají nic jiného.

06

Jak jsou vaše položky chráněny

Dvě vrstvy šifrování, jeden skutečný příklad a upřímná odpověď na otázku „co když mi někdo kartu ukradne?“

CELKOVÝ OBRAZ

Dvě vrstvy. Obě vycházejí z vašeho hesla.

1

V APLIKACI: POLOŽKY SE ZAPEČETÍ

Než se cokoli odešle na kartu, aplikace zašifruje každou položku ve vašem telefonu pomocí **ChaCha20-Poly1305** a 256bitového klíče odvozeného z vašeho hesla trezoru.

Toto je hlavní zámek. I ten, kdo má surová data, vidí jen náhodně vypadající bajty a každá jejich změna se odhalí.

2

NA KARTĚ: DVEŘE JSOU ZAMČENÉ

Bezpečný čip karty drží šifrované položky za vlastním klíčem **AES-128**, rovněž odvozeným z vašeho hesla trezoru. Vydá je, až telefon prokáže, že tento klíč zná.

Bez správného hesla čtečka nezíská nic kromě veřejných nastavení karty.

Vaše heslo trezoru

nikde se neukládá

↓

Klíč obsahu

256 bitů · pečetí položky (vrstva 1)

Klíč karty

128 bitů · otevírá dveře karty (vrstva 2)

Správcovský klíč

128 bitů · spravuje trezor na kartě

OD HESLA KE KLÍČŮM

Proč „Posiluje se vaše šifrování…“ chvíli trvá.



ARGON2ID

Záměrně pomalá funkce pro hesla, náročná na paměť. Každý jednotlivý pokus stojí 64 MiB paměti a skutečný čas, ve vašem telefonu stejně jako v počítači útočníka.

SŮL

Náhodné bajty uložené na kartě otevřeně. Díky nim jsou klíče každé karty jedinečné, takže nikdo nemůže předem připravit tabulku pokusů.

SKUTEČNÝ PŘÍKLAD · 1 ZE 4 · KLÍČE

Zašifrujme „12345678“.

Jsou to skutečné hodnoty, vytvořené stejnými algoritmy a nastaveními jako v aplikaci. Heslo slouží jen pro tento příklad.

Heslo trezoru	`copper-lantern-velvet-orbit`
Název položky	`Demo PIN`
Položka	`12345678`
Sůl (náhodná, na kartě)	`7a8dbeec53e1eb50c70ccd4674a0e624`
Kořenový klíč (Argon2id)	`84e743792af48790ce3ac4e2410ba1e9ef786851fa74467fc077208674905241`
Klíč obsahu · 256 bitů	`dcbe9b90a42a1c5e53f8bdaf07e3d763a61708ae3ad68fdfa7be72792fa6ab7c`
Klíč karty · 128 bitů	`266b550b4a87dd1029d53af4262244c1`
Správcovský klíč · 128 bitů	`d9715ed54fbc71325587258c440a8dc6`

> **Žádný z těchto klíčů se nikdy neukládá.** Aplikace je vypočítá, když zadáte heslo, a zapomene je, když se trezor zavře. Na kartě je jen sůl.

SKUTEČNÝ PŘÍKLAD · 2 ZE 4 · VRSTVA 1 V APLIKACI

Od „12345678“ k náhodně vypadajícím bajtům.

1. Položka se zabalí do 20 bajtů: pole názvu a pole položky.

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

typ a délka pole · „Demo PIN“ · "12345678"

2. ChaCha20-Poly1305 ji zapečetí klíčem obsahu, jedinečnou 12bajtovou hodnotou nonce (odvozenou z hlavičky slotu) a hlavičkou jako ověřenými daty.

Nonce	`be00fc197a76fb68b8f315fa`
Šifrový text · 20 bajtů	`5eda3e6b43d7aa61edf77ab4a26ae11e9b080c60`
Tag · 16 bajtů	`1b1b0dbbd23c5dffd6f4c462f9a449c4`

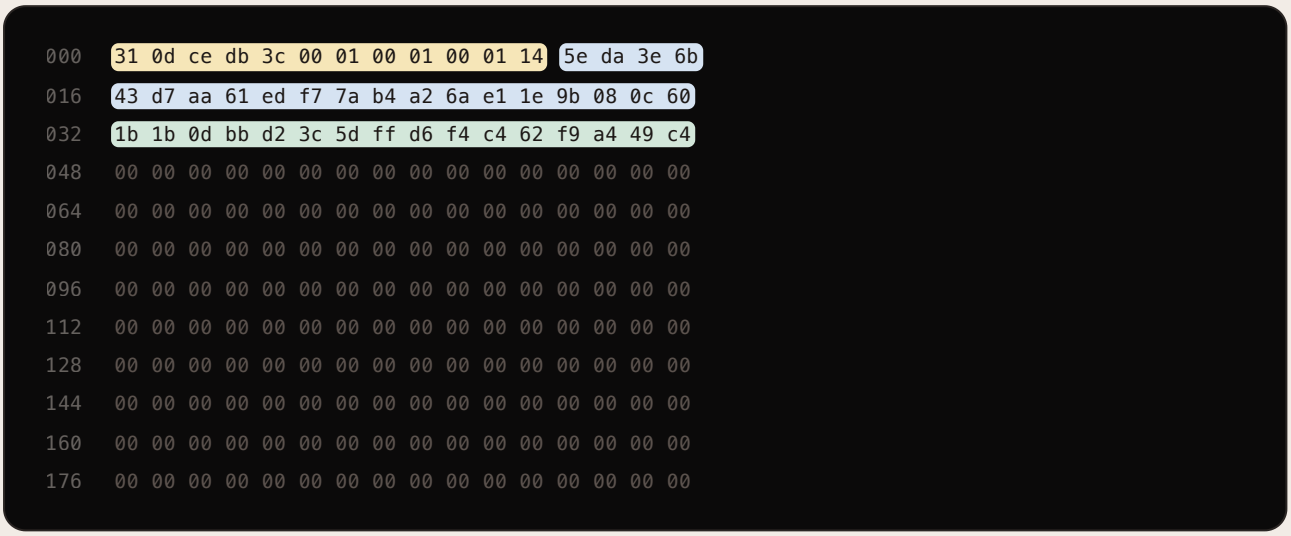
> **Tag je pečeť.** Pokud se změní byť jediný bit šifrového textu nebo jeho hlavičky, tag přestane sedět a aplikace data odmítne, místo aby ukázala něco špatně.

SKUTEČNÝ PŘÍKLAD · 3 ZE 4 · CO JE NA KARTĚ

Jedna položka, jeden slot o 192 bajtech.

Přesně toto karta ukládá pro „Demo PIN“. Hledejte „12345678“: není tam.

```
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
```



hlavička: verze, položka, pozice (12 bajtů) · šifrový text (20 bajtů) · tag (16 bajtů) · volné místo

ZA DVEŘMI KARTY

Tyto sloty leží v chráněné části karty. Karta je vydá teprve poté, co telefon projde kontrolou s klíčem karty (vrstva 2).

STEJNÁ POLOŽKA, JINÉ BAJTY

Zapište stejnou položku na jinou kartu a bude vypadat úplně jinak, protože každá karta má vlastní sůl a vlastní klíče.

SKUTEČNÝ PŘÍKLAD · 4 ZE 4 · VEŘEJNÁ ČÁST

Co vidí kdokoli se čtečkou.

Každá karta má také malou veřejnou oblast (128 bajtů). Lze ji přečíst bez hesla, protože aplikace potřebuje sůl k vytvoření vašich klíčů.

```
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“ a formát · ID trezoru · rozložení karty · sůl · nastavení Argon2id · nevyužito

A SE ŠPATNÝM HESLEM?

Změňte jen poslední písmeno hesla a klíč karty bude:

`883e65196d88bc9f1aae79acf8fa7c74`

místo `266b550b4a87dd1029d53af4262244c1`. Žádná podobnost. Karta kontrolu odmítne, nepošle žádné položky a nic se nezapíše.

KDYŽ VÁM NĚKDO UKRADNE KARTU

Má kartu. Ne vaše položky.

Neexistují žádná zadní vrátka ani univerzální klíč. Jediná cesta dovnitř je uhodnout vaše heslo trezoru a obě vrstvy dělají každý pokus drahým.

A

HÁDÁNÍ PŘES KARTU

Každý pokus vyžaduje fyzickou kartu. Zloděj spustí Argon2id pro jeden pokus a pak se zeptá karty. Karta odpovídá přes NFC na jeden pokus po druhém. Podle našeho odhadu je to nejvýš asi 20 pokusů za sekundu.

B

ROZEBRÁNÍ ČIPU

Drahá cesta. Specializovaná laboratoř by se mohla pokusit vytáhnout šifrované sloty přímo z čipu. Pak může hádat offline, na mnoha počítačích, ale každý pokus stále stojí celý běh Argon2id se 64 MiB paměti.

UPŘÍMNÝ ZÁVĚR

Obě cesty končí stejnou otázkou: **jak těžké je uhodnout vaše heslo trezoru?** Se silným heslem je uhodnutí prakticky mimo dosah. Se slabým obě vrstvy jen získají čas. Další strana ukazuje kolik.

PROČ NA VAŠEM HESLE TREZORU ZÁLEŽÍ

Jak dlouho trvá vyzkoušet všechny možnosti?

TYP HESLA TREZORU	PŘES KARTU ~20 POKUSŮ / S	LABORATOŘ + OBŘÍ VÝPOČETNÍ FARMA 1 000 000 POKUSŮ / S
Jakékoli heslo ze seznamu 1 miliardy uniklých hesel, např. „Leto2026!!“	až asi 2 roky; běžná mnohem dřív	až asi 17 minut; běžná během sekund
12 náhodných číslic	asi 1600 let	asi 12 dní
4 náhodná slova	miliony let	asi 116 let
12 náhodných malých písmen	přes 100 milionů let	asi 3 000 let
5 náhodných slov	déle, než existuje vesmír	asi 900 000 let
6 náhodných slov	déle, než existuje vesmír	asi 7 miliard let

Nejhorší případ pro vás: doba potřebná k vyzkoušení všech možností. „Náhodná slova“ znamená vybraná kostkou ze seznamu 7 776 slov. Rychlosti hádání jsou velkorysé odhady pro ilustraci. Pro představu: jeden pokus trval asi 25 ms na moderním počítači Apple M4 se 4 jádry.

DOPORUČENÍ

Pět nebo šest náhodných slov. Nikdy ho nepoužívejte znovu a nikdy nepoužívejte texty písní, jména ani data.

A ZAPIŠTE SI HO

Uložte si kopii na bezpečné místo, odděleně od karet. Zapomenuté heslo trezoru nelze obnovit.

CO MI8OS NIKDY NEDĚLÁ

V cloudu není co hacknout. Protože žádný cloud není.

- ✓ **Žádný účet, žádný server.** Aplikace nenavazuje vůbec žádná síťová spojení.
- ✓ **Žádná uložená hesla.** Hesla trezoru ani hlavní hesla se nikdy neukládají, ani v telefonu, ani na kartě.
- ✓ **Žádná kopie v telefonu.** Dešifrované položky existují jen v paměti, dokud je trezor otevřený. Jedna výjimka: zkopírovaná položka zůstává ve schránce, dokud ji časovač nevymaže (15 s až 1 min), i když se trezor mezitím zavřel.
- ✓ **Žádná telemetrie.** Žádné sledování, žádná analytika.
- ✓ **Zamkne se, když odejdete.** Opuštění aplikace zavře trezor (okamžitě nebo po zvolené prodlevě).
- ✓ **Zakryje obrazovku** v přepínači aplikací a při nahrávání nebo zrcadlení obrazovky.
- ✓ **Odhalí manipulaci.** Změněná data neprojdou pečetí a jsou odmítnuta.
- ✓ **Používá jen veřejné standardní algoritmy:** Argon2id, HKDF-SHA256, ChaCha20-Poly1305, AES-128.

DRUHÁ STRANA NEEXISTENCE ZADNÍCH VRÁTEK

Pokud ztratíte všechny karty nebo zapomenete heslo trezoru, nikdo vaše položky nezíská zpět. Ani vy, ani my. Proto máte tři karty a zapsané heslo.

PÉČE O KARTY A OBNOVA

Tři karty, tři místa.

01

MĚJTE JE ODDĚLENĚ

Jednu kartu u sebe nebo poblíž, jednu doma, jednu jinde: u rodiny, v práci nebo v trezoru. Jeden požár ani vloupání nevezme všechny tři.

02

ZTRACENÁ KARTA?

Nálezce má jen šifrovaná data. Vytvořte náhradní kartu (viz 03), abyste měli znovu tři kopie. Pokud se obáváte, že někdo zná heslo, vytvořte stejným způsobem nové trezory s novým heslem trezoru a pak staré karty resetujte.

03

VYTVOŘENÍ NÁHRADNÍ KARTY

Aplikace může zkopírovat trezor na další karty jen hned po jeho vytvoření. Pro pozdější náhradu vytvořte nový trezor na prázdné kartě a zadejte stejné položky znovu: otevřete funkční kartu, abyste je mohli přečíst, a pokud si mezitím něco zapíšete, poznámku pak zničte. Udělejte to dřív, než vám zbude poslední kopie.

04

ZAPOMENUTÉ HESLO TREZORU?

Tyto položky nelze obnovit. Pokud jiná karta používá heslo, které si ještě pamatujete, otevřete ji. Jinak karty resetujte a začněte nový trezor.

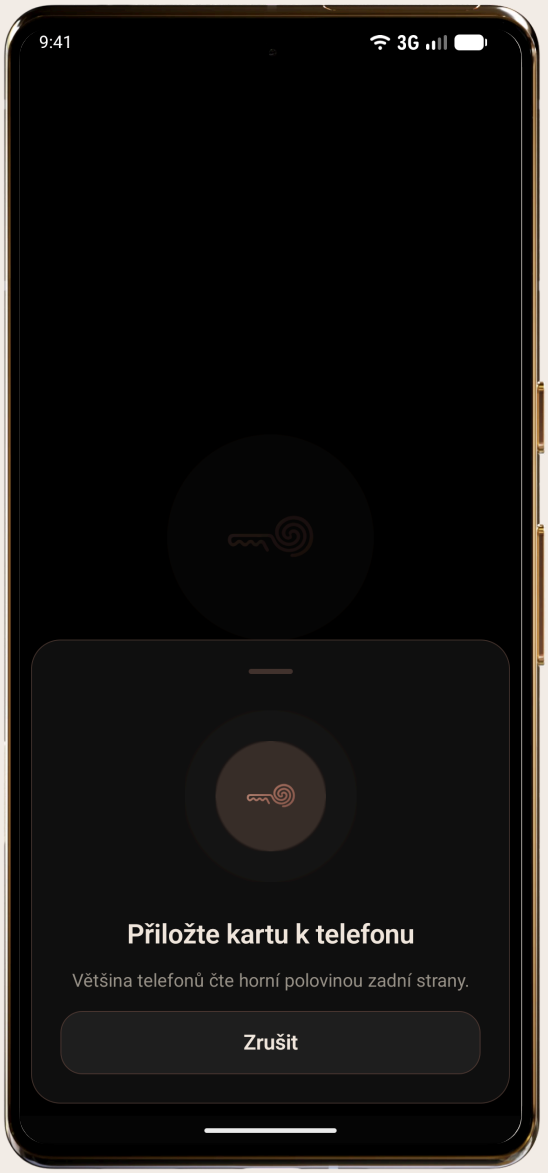
> **Pečujte o karty** jako o platební kartu: neohýbat, žádné horko, žádné ostré hrany. Při skenování je držte dál od kovových pouzder.

NA ANDROIDU

Stejná aplikace, pár drobných rozdílů.

Aplikace pro Android je na **Google Play**. Funguje stejně a čte stejné karty. Trezor zapsaný na iPhonu se otevře na Androidu a naopak.

NA ANDROIDU	CO JE JINAK
Skenování	Android nemá systémové okno NFC, a tak MI8OS zobrazuje vlastní obrazovku skenování s tlačítkem pro zrušení.
Poloha karty	Přiložte kartu k horní polovině zadní strany telefonu. Přesné místo se liší podle modelu.
NFC	NFC musí být zapnuté v nastavení telefonu.
Biometrie	Zámek aplikace používá otisk prstu nebo odemykání obličejem vašeho telefonu.



ŘEŠENÍ POTÍŽÍ

Když něco nefunguje.

CO VIDÍTE	CO DĚLAT
Karta není rozpoznána	Přiložte ji naplocho k hornímu okraji iPhonu a držte ji v klidu. Sundejte silné nebo kovové pouzdro. Zkuste o kousek výš nebo níž.
Zápis se zastavil v polovině	Klepněte na **Zkusit znovu** a držte stejnou kartu v klidu. Každé uložení přepíše celou kartu a vaše změny zůstávají v aplikaci, dokud se to nepodaří. Pokud aplikace hlásí, že uložení nelze dokončit, resetujte kartu (strana 26) a uložte znovu, nebo použijte záložní kartu a tuto nahraďte (strana 42).
Špatné heslo	Zkontrolujte pravopis a mezery. Pamatujte: každá karta může mít vlastní heslo trezoru.
„To je jiná karta“	Přiložená karta není ta, která je otevřená. Správnou najdete funkcí Identifikovat.
Karta je plná	Karta pojme 20 položek. Smažte jednu, kterou už nepotřebujete, nebo rozdělte položky na více karet.
Kartu nelze resetovat	Je zamčená. Reset vyžaduje její hlavní heslo.
Trezor se zavřel sám	Aplikace byla opuštěna nebo se nahrávala obrazovka. Otevřete kartu znovu.
Pauza „Připravuje se váš klíč“	Normální. Je to záměrné posílení hesla ze strany 34.

Další nápověda: guide.mi8os.com · info@mi8os.com

MI8OS

Vaše soukromí patří vám.

MI8OS.COM

Průvodce MI8OS, česky, říjen 2026. Popisuje aplikaci MI8OS pro iPhone a Android. Obrazovky se mohou mezi verzemi mírně lišit. Ukázkové klíče a bajty v kapitole 06 byly pro tohoto průvodce vytvořeny s ukázkovým heslem; nikdy ho nepoužívejte. MI8OS · info@mi8os.com