MI8OS

MI8OS-I JUHEND

Kõik sinu rakendusest ja kaartidest.

Kuidas luua, avada ja uuendada seifi, kuidas hoolitseda oma MI8OS Card gen 2 eest ja kuidas täpselt sinu kirjeid kaitstakse, viimase baidini.

LOO | KASUTA | KAARDID | TURVALISUS



MI8OS-i rakendusele iPhone'is ja Androidis. Oktoober 2026.

SISUKORD

Mida juhendist leiad

01 **ALUSTAMINE** p. 3
Mis on MI8OS, sõnad, millega kokku puutud, rakendus lühidalt, kuidas kaarti hoida.

02 **LOO SEIF** p. 9
Lisa kirjeid, vali seifi parool, salvesta kaardile, kirjuta oma varukaardid.

03 **KASUTA OMA SEIFI** p. 16
Ava kaart, loe ja kopeeri kirjeid, 2FA-koodid, lisa ja kustuta, uuenda kaarti.

04 **HALDA OMA KAARTE** p. 23
Minu kaardid, nime muutmine, tuvastamine, lähtestamine, lukustamine ja avamine põhiparooliga.

05 **SEADED** p. 29
Rakenduse lukk, Face ID, lõikelaud ja välimus.

06 **KUIDAS SINU KIRJEID KAITSTAKSE** p. 32
Kaks krüptimiskihti, päris näide väärtusega „12345678“ ja miks sinu seifi parool loeb.

07 **HOOLDUS, ANDROID JA ABI** p. 42
Kolm kaarti, erinevused Androidis, tõrkeotsing.

01

Alustamine

Viis minutit, et mõista, kuidas MI8OS töötab, enne kui kaarti puudutad.

MIS ON MI8OS

Väike krüptitud seif kaardil, mida hoiad ise käes.

MI8OS hoiab sinu kõige olulisemaid saladusi, nagu taastekoodid, 2FA-võtmed, seed-fraasid ja PIN-koodid, seifis, mis krüptitakse sinu telefonis ja salvestatakse füüsilisele kaardile. Ei kontot, ei pilve, ei tellimust.



Kaasas · see, mida kasutad



Kodus · turvaliselt kodus



Mujal · kusagil mujal

SINU KOMPLEKTIS

Kolm **MI8OS Card, gen 2**. Igale kaardile mahub kuni **20 kirjet**. Kirjuta sama seif kõigile kolmele ja hoia neid eri kohtades.

MIDA SUL VAJA ON

NFC-ga iPhone või Android-telefon ja MI8OS-i rakendus App Store'ist või Google Playst (Androidi märkused lehel 43). Ja seifi parool, mida suudad meeles pidada: parim on pikk paroolifraas.

SÕNAD, MILLEGA KOKKU PUUTUD

Kolm parooli, kolm eri ülesannet.

See on juhendi kõige tähtsam leht. Need kõlavad sarnaselt, kuid igaüks kaitseb eri asja.

SEIFI PAROOL

Krüptib ja avab kaardi kirjed. Kohustuslik, vähemalt 12 märki.

Seda ei salvestata kuhugi. Keegi ei saa seda taastada, isegi mitte MI8OS.

PÕHIPAROOL

Valikuline. Lukustab kaardi enda, et keegi ei saaks seda ilma selle paroolita lähtestada ega kustutada.

Ei ava midagi. Kirjete lugemiseks on ikka vaja seifi parooli.

RAKENDUSE LUKU PIN

Valikuline. Kuus numbrit (või Face ID) rakenduse avamiseks selles telefonis.

Sel pole sinu kaartidega mingit pistmist ja see ei suuda midagi dekrüptida.

SÕNA	TÄHENDUS
Seif	Sinu kirjete loend. See on sinu kaartidel krüptituna ja dekrüptituna ainult rakenduse mälus, kuni see on avatud.
Kirje	Üks sissekanne: nimi (kuni 24 baiti) ja saladus ise (kuni 96 baiti), näiteks PIN, taastekood või 2FA-võti.
Kaart	Sinu MI8OS Card gen 2. See talletab krüptitud seifi; sama seifi saad kirjutada mitmele kaardile.
Uuenda kaarti	Kirjutab sinu muudatused kaardile. Seni on muudatused ainult rakenduse mälus.

RAKENDUS LÜHIDALT

Kolm vahekaarti. Igal üks ülesanne.



Skanni · ava kaart



Uus · loo seif



Rohkem · kaardid ja seaded

1

SKANNI

Puuduta, et kaarti skannida ja hoia kaarti vastu telefoni. Kaart avaneb omaette aknas, kuhu sisestad selle seifi parooli.

2

UUS

Puuduta, et luua uus seif. Neljasammuline viisard viib sind esimesest kirjest kaardini, mis seda hoiab.

3

ROHKEM

Sinu kaardid, rakenduse lukk, lõikelaua taimer, välimus ja sisseehitatud abilehed.

KAARDI HOIDMINE

Ülemine serv. Lamedalt. Paigal.

Iga kord, kui rakendus kaardiga suhtleb, näitab iPhone oma NFC-akent. Seejärel:

1. **Hoia kaarti lamedalt vastu ülemist serva** iPhone'i tagaküljel, kus asub NFC-antenn.
2. **Hoia seda paigal**, kuni rakendus kinnitab. Kirjutamine võtab mõne sekundi; kaardi liiga varajane liigutamine on kõige sagedasem põhjus, miks kirjutamist tuleb korrata.
3. Kui midagi ei juhtu, libista kaarti aeglaselt veidi allapoole või ülespoole ja eemalda paks või metallist ümbris.



> **Kiiret pole.** Kui avad kaardi, valmistab rakendus esmalt sinu võtme ette („Valmistame sinu võtit ette. Kaarti ei ole veel vaja hoida"). Hoia kaarti vastu, kui ilmub NFC-aken.

> **Androidis** näitab rakendus oma skannimisekraani ja kaart käib vastu telefoni tagakülje ülemist poolt.

MIS KAARDILE KUULUB

Mõni kirje, mis loeb väga palju.

MI8OS ei ole mõeldud sinu paroolihaldurit asendama. See on võrguväline koht peotäiele asjadele, mida vajaksid, kui kõik muu üles ütleks.

SUUREPÄRANE KAARDIL

- ✓ E-posti ning Apple'i / Google'i taastekoodid
- ✓ 2FA seadistusvõtmed, et rakendus saaks sinu koode näidata
- ✓ Krüptovarade taastefraasid (MI8OS ei ole rahakott ega hoia raha)
- ✓ Sinu paroolihalduri põhiparool või selle hädaolukorra komplekti andmed
- ✓ Olulised PIN-koodid ja privaatsed märkmed

HEA TEADA

- ✓ Kuni 20 kirjet kaardi kohta
- ✓ Nimi: kuni 24 baiti · kirje: kuni 96 baiti
- ✓ Lihtsad tähed, numbrid ja tühikud võtavad 1 baidi; diakriitikuga, kreeka või kirillitsa tähed 2; emojid 4
- ✓ Pikad seed-fraasid võivad vajada kahte kirjet (nt sõnad 1–12 ja 13–24)

02

Loo seif

Neli sammu: Kirjed, Parool, Kirjutamine, Valmis. Umbes viis minutit.

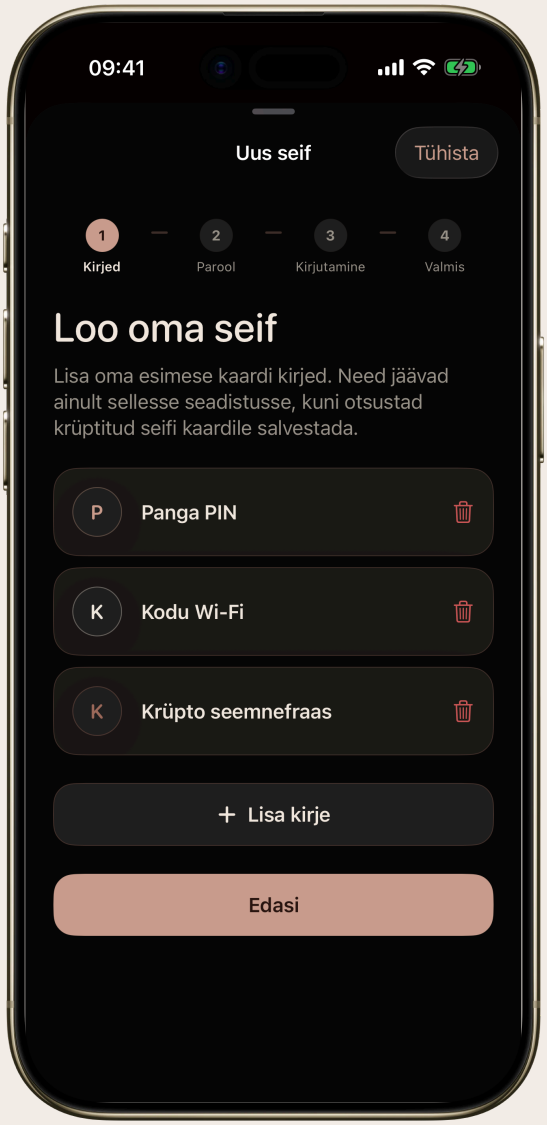
SAMM 1/4 · KIRJED

Alusta oma kirjetest.

1. Ava vahekaart **Uus** ja puuduta nuppu **Puuduta, et luua uus seif**.
2. Puuduta **Lisa kirje** iga asja jaoks, mida tahad hoida.
3. Pühi kirjet, et see enne jätkamist uuesti eemaldada.
4. Kui loend on valmis, puuduta **Edasi**.

> **Midagi pole veel salvestatud.** Sinu kirjed on ainult selles viisardis, kuni salvestad krüptitud seifi kaardile.

> **Sul on seif juba avatud?** Rakendus küsib kõigepealt. Kui sul on muudatusi, mis pole veel ühelgi kaardil, pakub see nende säilitamist.



KIRJE LISAMINE

Nimi ja saladus ise.

Nimi. Midagi, mille ära tunned, näiteks „E-posti taastekoodid“. Kuni 24 baiti; loendur näitab, palju on alles.

Kirje. Parool, kood või tekst, kuni 96 baiti. Kõik, mida kleebid või genereerid, krüptitakse enne, kui see kaardile jõuab.

Genereerimine. Puuduta täringut, et luua juhuslik 16, 32, 64 või 96 märgi pikkune parool.

2FA-VÕTME SALVESTAMINE

Kui teenus näitab seadistusvõtit (või QR-koodi taga olevat otpauth://-linki), kleebi see kirjeks. MI8OS tunneb selle ära ja näitab hiljem nuppu **TOTP**, mis kopeerib kehtiva koodi. Kui link on pikem kui 96 baiti, kleebi ainult seadistusvõti ise (osa pärast secret=); MI8OS kasutab siis standardset 6 numbrit iga 30 sekundi järel.



SAMM 2/4 · PAROOL

Vali oma seifi parool.

1. Sisesta seifi parool ja kinnitamiseks sisesta see uuesti.
2. Jälgi tugevusriba: 12 märki on miinimum, 20 või tühikutega fraas annab tulemuse „Suurepärane pikkus.“
3. Märgi ruut: *„Kui ma kaotan kõik kaardid või unustan selle parooli, ei suuda MI8OS selle kaardi seifi taastada.“*
4. Puuduta **Krüpti seif**.

MEIE NÕUANNE

Kasuta **viit või kuut juhuslikku sõna**, näiteks *vask latern samet orbiit tundra* (aga mitte just neid). Lihtne meeles pidada, äärmiselt raske ära arvata. Leht 40 näitab, miks.



SAMM 3/4 · KIRJUTAMINE

Kõigepealt krüptimine. Siis kaart.

Krüptimine toimub sinu telefonis enne, kui NFC käivitub. Hetkeks näed teksti „Tugevdame sinu krüptimist…“, kui rakendus muudab sinu parooli võtmeteks. See paus on tahtlik: see teeb sinu parooli äraarvamise kõigile teistele aeglaseks.

Kui kuvatakse **Krüptimine valmis**:

1. Puuduta **Salvesta kaardile**.
2. Hoia kaarti vastu iPhone’i ülemist serva, kui ilmub NFC-aken.
3. Hoia paigal. Rakendus kirjutab seifi ja **loeb selle siis kontrolliks uuesti**.

> **Tühi kaart?** Rakendus valmistab selle sama puudutusega automaatselt ette.



SAMM 4/4 · VALMIS

Nüüd kirjuta oma varukaardid.

„Seif salvestatud kaardile“ tähendab, et seif on sellel kaardil kontrollitud. **See on ainus hetk, mil rakendus saab kogu sinu seifi teistele kaartidele kopeerida**, nii et kirjuta need kõik kohe:

1. Puuduta **Kirjuta veel üks kaart**.
2. Vali selle kaardi jaoks **Kasuta sama seifi parooli** (lihtsaim) või **Kasuta teist seifi parooli**.
3. Salvesta järgmisele kaardile. Korda kolmanda puhul.

> **Sama parool, uus krüptimine.** Iga kaart saab oma juhusliku soola, nii et isegi sama parooliga näevad iga kaardi andmed täiesti erinevad välja.

Loobu seifist selles iPhone'is sulgeb seifi ainult rakenduse mälus. See ei kustuta kunagi kaarti.



KAART, MILLEL ON JUBA SEIF

MI8OS ei kirjuta seifi kunagi ootamatult üle.

Kui salvestad uue seifi kaardile, millel see juba on, ei kirjutata midagi. Rakendus ütleb sulle: **„Sellel kaardil on juba seif“** ja annab kaks valikut:

LISA KIRJEID

Lisab sinu uued kirjed kaardil olevasse seifi. Juba olemasolevad kirjed säilivad. Sinu seifi parool peab olema see, mida see kaart kasutab, ja hoiad kaarti veel korra vastu.

TÜHISTA

Jätab kaardi täpselt selliseks, nagu see oli.

> **Tahad seifi täielikult asendada?** Lähtesta kõigepealt kaart (leht 26) ja loo siis sellele uus seif.



03

Kasuta oma seifi

Ava, loe, kopeeri, muuda ja kirjuta muudatused kaardile tagasi.

KAARDI AVAMINE

Skanni, parool, kaart uuesti vastu.



Vahekaart Skanni



Kaardi aken

1. Vahekaardil **Skanni** puuduta nuppu **Puuduta, et kaarti skannida** ja hoia kaarti vastu. Skannimine loeb ainult kaardi avalikku teavet.
2. Sisesta kaardi **Seifi parool** ja puuduta **Ava seif**. Rakendus valmistab sinu võtme ette ja küsib siis kaarti veel korra.

SEIFI SEES

Sinu kirjed, nii kauaks, kui neid vajad.

See kaart näitab, milline kaart on avatud, välju Viimati kasutatud ja Viimati kirjutatud ning seda, kas kaardil on põhiparool.

„8 / 20 kirjest“ näitab, kui täis kaart on. **Kaardil** tähendab, et kõik, mida näed, on kaardile salvestatud.

Otsi seifist allservas leiab kirje nime järgi.

+ üleval lisab kirje; **⋯** avab kaardimenüü (leht 25).

> **Dekrüptitud ainult mälus.** Sinu kirjed on loetaval kujul olemas ainult siis, kui see aken on avatud. Puuduta **Valmis** ja need kaovad telefonist.



LUGEMINE JA KOPEERIMINE

Peidus, kuni küsid.

Puuduta kirjet, et see avada. Väärtus on peidetud punktide taha.

Näita kuvab selle; **Peida** peidab selle uuesti.

Kopeeri paneb selle lõikelauale ja MI8OS **tühjendab lõikelaua uuesti** 30 sekundi pärast (muuda vahekaardil Rohkem: 15 s, 30 s või 1 min).

> **Kleebi kiiresti.** Pärast taimerit on lõikelaud tühi, nii et kirje ei jää teistesse rakendustesse. Taimer jookseb edasi ka siis, kui sulged seifi enne selle lõppu.

> **Ekraanisalvestus või -peegeldus?** MI8OS katab ekraani ja sulgeb seifi, et kirjed ei satuks salvestisse.



2FA-KOODID

Sinu autentija, kaardilt.

Kui kirje on 2FA seadistusvõti, näitab selle leht nuppu **TOTP**. Puuduta seda ja MI8OS arvutab kehtiva koodi ning kopeerib selle, kleepimiseks valmis.

Kaart talletab ainult **krüptitud seadistusvõtme**. Kood arvutatakse rakenduses pärast seifi avamist, võtmest ja kellaajast, täpselt nagu igas autentimisrakenduses.

MIKS SEE AITAB

Kui sinu autentimiskoodid on ainult telefonis, mille kaotad, kaovad need koos sellega. Kui seadistusvõtmed on sinu kaartidel, saad oma koodid igas uues telefonis, kus on MI8OS-i rakendus.



SEIFI MUUTMINE

Lisa, kustuta, seejärel uuenda kaarti.

Lisamine: puuduta **+** ning täida nimi ja kirje.

Kustutamine: pühi kirjet vasakule või ava see ja puuduta **Kustuta kirje**. See jääb märgituna loendisse, kuni uuendad kaarti. Mõtlesid ümber? Puuduta **Säilita**.

Muutmine: muutmisnuppu meelega ei ole. Kirje muutmiseks kustuta see ja lisa uuesti.

Muudatused on märgitud veel kirjutamata. Puuduta **Uuenda kaarti** ja hoia kaarti vastu, et need salvestada.

> **Sulged kirjutamata muudatustega?** Rakendus hoiatab: „Kui sulged selle kaardi ilma seda uuendamata, lähevad need kaotsi.“



HOIA IGA KOOPIA AJAKOHANE

Iga kaarti uuendatakse eraldi.

Uuenda kaarti kirjutab avatud kaardile ja ainult sellele. Sinu teistel kaartidel on endiselt eelmine versioon, kuni uuendad ka neid.

1

MUUDA ÜHT KAARTI

Ava oma kaart Kaasas, lisa või kustuta, puuduta **Uuenda kaarti**.

2

KORDA TEISTEGA

Ava kaardid Kodus ja Mujal ning tee igaühel sama muudatus.

3

OTSETEE UUTELE KIRJETELE

Loo „uus seif“ ainult uute kirjetega ja salvesta see kaardile, millel on juba sinu seif. Vali **Lisa kirjeid** ja need lisatakse olemasolevatele.

HEA HARJUMUS

Kord aastas ava iga kaart ja kontrolli, et kõik kolm näitaksid sama arvu kirjeid.

04

Halda oma kaarte

Nimed, kaardimenüü, lähtestamine ja valikuline põhiparool.

MINU KAARDID

Anna igale kaardile nimi.

Jaotises **Rohkem** → **Minu kaardid** näed kaarte, mida see telefon tunneb, koos sildiga: kirjete arv, **Tühi** või **Lukustatud**.

Lisa kaart skannib kaardi ja jätab selle meelde. See loeb ainult seda, mis on kaardil juba avalik: parooli pole vaja, midagi ei kirjutata.

Puuduta kaarti, et see avada, ümber nimetada või lähtestada.

> **Kiirem avamine.** Kaart, mida see telefon juba tunneb, avaneb pärast parooli sisestamist ühe skannimisega.

> **Salvestatakse ainult selles telefonis:** sinu antud nimed, millal kaarte viimati kasutati, ja nende avalikud seaded. Mitte kunagi parooli, mitte kunagi kirjet.



KAARDIMENÜÜ ···

Muuda nime, tuvasta, unusta.

MUUDA NIME

Nimi, mille ära tunned: „Kaasas“, „Kodus“, „Vanemate seif“.

TUVASTA

Pole kindel, milline kaart on milline? Puuduta Tuvasta ja hoia kaarti vastu. Rakendus ütleb, kas see on see, mida vaatad, või milline teine kaart see on.

UNUSTA

Eemaldab kaardi selle telefoni loendist. Kaardil ei muutu midagi ja saad selle igal ajal uuesti lisada.

ROHKEM

Lähtesta kaart, Lukusta kaart ja Ava kaardi lukustus. Vaata järgmisi lehti.



KAARDI LÄHTESTAMINE

Puhas kaart, valmis uueks seifiks.

··· → **Rohkem** → **Lähtesta kaart** eemaldab MI8OS-i seifi ja kõik muu kaardilt ning vabastab kogu selle salvestusruumi. See **ei** küsi seifi parooli.

Kasuta seda, et:

- ✓ Asendada seif täielikult uuega
- ✓ Kasutada kaarti uuesti pärast seda, kui oled selle seifi parooli unustanud (selle kirjed lähevad kaotsi)
- ✓ Tühjendada kaart enne selle ära andmist

> **Teised kaardid jäävad puutumata.** Ühe kaardi lähtestamine ei mõjuta kunagi teiste kaartide seifi.

> **Lukustatud kaart?** See keeldub lähtestamisest, kuni sisestad selle põhiparooli (järgmine leht).



KAARDI LUKUSTAMINE · PÕHIPAROOL

Takista kellelgi oma kaarti tühjendamast.

Igaüks, kes lukustamata kaardi kätte saab, võib selle lähtestada, isegi ilma sinu seifi paroolita. Ta ei saa ikka midagi lugeda, aga ta võiks selle tühjendada.

Lukusta kaart takistab seda. Vali põhiparool, hoia kaarti vastu, valmis. Edaspidi ei saa kaarti ilma selleta lähtestada ega tühjendada, ei MI8OS-iga ega millegi muuga.

1. ··· → **Rohkem** → **Lukusta kaart**
2. Sisesta põhiparool kaks korda ja puuduta **Lukusta**.
3. Hoia kaarti, kuni rakendus kinnitab „Kaart lukustatud“.

> **Lugemine ja salvestamine ei muutu.** Need kasutavad endiselt ainult seifi parooli.



KAARDI LUKUSTUSE AVAMINE · JA HOIATUS

Lukustuse avamine teeb kaardi jälle tavaliseks.

··· → **Rohkem** → **Ava kaardi lukustus**, sisesta põhiparool ja hoia kaarti vastu. Kaart käitub jälle lukustamata kaardina. Selle seif ja seifi parool jäävad samaks.

Lukustatud kaardi lähtestamiseks vali Lähtesta kaart: rakendus küsib põhiparooli ja vormindab seejärel kaardi.

ÄRA UNUSTA SEDA

Kui unustad kaardi põhiparooli, ei saa seda kaarti **kunagi** lähtestada ega uuesti kasutada. Selle kirjed jäävad seifi parooliga loetavaks. Rakendus küsib seda iga kord ega jäta seda kunagi meelde.

Saad ka lukustada, avada ja lähtestada mis tahes kaarti jaotises **Rohkem** → **Täpsemalt**, seda skannides.



05

Seaded

Rakenduse lukk, Face ID, lõikelaud ja rakenduse välimus.

ROHKEM

Kõik muu, ühes kohas.

SEADE	MIDA SEE TEEB
Rakenduse välimus	Süsteem, Hele või Tume.
Minu kaardid	Sinu nimega kaardid (leht 24).
Täpsemalt	Lukusta, ava või lähtesta mis tahes kaart seda skannides.
Rakenduse lukk	PIN ja Face ID rakenduse jaoks (järgmine leht).
Tühjenda lõikelaud pärast	15 s, 30 s või 1 min pärast kirje kopeerimist.
Kaardid ja turvalisus	Sisseehitatud abi: Kuidas MI8OS Card töötab, Krüptimine ja paroolid, Kui turvaline on MI8OS?, Kaartide hooldus ja taaste.
Tugi ja õigusteave	Telli MI8OS Card, Privaatsuspoliitika, Kasutustingimused.



RAKENDUSE LUKK

Lukk rakendusele endale.





Lülita see sisse jaotises Rohkem → Rakenduse lukk: vali kuuekohaline PIN-kood ja soovi korral Face ID või Touch ID.

Lukusta, kui lahkun: Kohe, 1 minuti pärast või 10 minuti pärast. Kui lahkud rakendusest kauemaks, sulgub ka avatud seif.

PIN avab ainult rakenduse selles telefonis. See ei suuda kaarti dekrüptida ega asenda seifi parooli. Vali kuus numbrit, mis ei ava ka midagi muud.

06

Kuidas sinu kirjeid kaitstakse

Kaks krüptimiskihti, üks päris näide ja aus vastus küsimusele „mis siis, kui keegi mu kaardi varastab?“

SUUR PILT

Kaks kihti. Mõlemad pärinevad sinu paroolist.

1

RAKENDUSES: KIRJED SULETAKSE PITSERIGA

Enne kui midagi kaardile saadetakse, krüptib rakendus sinu telefonis iga kirje algoritmiga **ChaCha20-Poly1305** ja 256-bitise võtmega, mis tehakse sinu seifi paroolist.

See on peamine lukk. Isegi toorandmete valdaja näeb ainult juhuslikuna näivaid baite ning iga muudatus neis avastatakse.

2

KAARDIL: UKS ON LUKUS

Kaardi turvakiip hoiab krüptitud kirjeid oma **AES-128**-võtme taga, mis on samuti tehtud sinu seifi paroolist. See annab need välja alles siis, kui telefon on tõestanud, et teab seda võtit.

Ilma õige paroolita ei saa lugeja midagi peale kaardi avalike seadete.



PAROOLIST VÕTMETENI

Miks „Tugevdame sinu krüptimist…“ võtab hetke.



ARGON2ID

Tahtlikult aeglane ja mälunõudlik paroolifunktsioon. Iga üksik katse maksab 64 MiB mälu ja päris aega, nii sinu telefonis kui ka ründaja arvutis.

SOOL

Juhuslikud baidid, mis on kaardile avalikult salvestatud. Need teevad iga kaardi võtmed ainulaadseks, nii et keegi ei saa katsete tabelit ette valmistada.

PÄRIS NÄIDE · 1/4 · VÕTMED

Krüptime väärtuse „12345678“.

Need on päris väärtused, mis on loodud samade algoritmide ja seadetega nagu rakenduses. Parool on ainult selle näite jaoks.

Seifi parool	`copper-lantern-velvet-orbit`
Kirje nimi	`Demo PIN`
Kirje	`12345678`
Sool (juhuslik, kaardil)	`7a8dbeec53e1eb50c70ccd4674a0e624`
Juurvõti (Argon2id)	`84e743792af48790ce3ac4e2410ba1e9ef786851fa74467fc077208674905241`
Sisuvõti · 256-bitine	`dcbe9b90a42a1c5e53f8bdaf07e3d763a61708ae3ad68fdfa7be72792fa6ab7c`
Kaardivõti · 128-bitine	`266b550b4a87dd1029d53af4262244c1`
Haldusvõti · 128-bitine	`d9715ed54fbc71325587258c440a8dc6`

> **Ühtki neist võtmetest ei salvestata kunagi.** Rakendus arvutab need, kui sisestad parooli, ja unustab need, kui seif sulgub. Kaardil on ainult sool.

PÄRIS NÄIDE · 2/4 · KIHT 1 RAKENDUSES

Väärtusest „12345678“ juhuslikuna näivate baitideni.

1. Kirje pakitakse 20 baiti: nimeväli ja kirjeväli.

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

välja tüüp ja pikkus „Demo PIN“ "12345678"

2. ChaCha20-Poly1305 pitseerib selle sisuvõtme, unikaalse 12-baidise nonce’i (tuletatud pesa päisest) ja päisega kui autenditud andmetega.

Nonce	`be00fc197a76fb68b8f315fa`
Šifreeritud tekst · 20 baiti	`5eda3e6b43d7aa61edf77ab4a26ae11e9b080c60`
Tag · 16 baiti	`1b1b0dbbd23c5dffd6f4c462f9a449c4`

> **Tag on pitser.** Kui šifreeritud tekstis või selle päises muutub kasvõi üks bitt, ei klapi tag enam ja rakendus lükkab andmed tagasi, selle asemel et midagi valesti näidata.

PÄRIS NÄIDE · 3/4 · MIS ON KAARDIL

Üks kirje, üks 192-baidine pesa.

Täpselt seda talletab kaart kirje „Demo PIN“ jaoks. Otsi „12345678“: seda seal pole.

```
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
```

päis: versioon, kirje, asukoht (12 baiti) · šifreeritud tekst (20 baiti) · tag (16 baiti) · tühi ruum

KAARDI UKSE TAGA

Need pesad asuvad kaardi kaitstud osas. Kaart annab need välja alles pärast seda, kui telefon on kaardivõtmega kontrolli läbinud (kiht 2).

SAMA KIRJE, TEISED BAIDID

Kirjuta sama kirje teisele kaardile ja see näeb välja täiesti teistsugune, sest igal kaardil on oma sool ja oma võtmed.

PÄRIS NÄIDE · 4/4 · AVALIK OSA

Mida igaüks lugejaga näha saab.

Igal kaardil on ka väike avalik ala (128 baiti). Seda saab lugeda ilma paroolita, sest rakendus vajab sinu võtmete loomiseks soola.

```
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“ ja vorming · seifi ID · kaardi paigutus · sool · Argon2id seaded · kasutamata

JA VALE PAROOLIGA?

Muuda ainult parooli viimast tähte ja kaardivõti muutub selliseks:

`883e65196d88bc9f1aae79acf8fa7c74`

selle asemel: `266b550b4a87dd1029d53af4262244c1`. Mitte mingit sarnasust. Kaart lükkab kontrolli tagasi, ei saada ühtegi kirjet ja midagi ei kirjutata.

KUI KEEGI SU KAARDI VARASTAB

Tal on kaart. Mitte sinu kirjed.

Tagaust ega peavõtit ei ole. Ainus tee sisse on sinu seifi parool ära arvata ning mõlemad kihid teevad iga katse kalliks.

A

ARVAMINE KAARDI KAUDU

Iga katse vajab füüsilist kaarti. Varas käivitab ühe katse jaoks Argon2id ja küsib siis kaardilt. Kaart vastab NFC kaudu ühele katsele korraga. Meie hinnangul on see kõige rohkem umbes 20 katset sekundis.

B

KIIBI LAHTIVÕTMINE

Kallis tee. Spetsialiseeritud labor võiks proovida krüptitud pesad otse kiibist välja võtta. Siis saab see arvata võrguväliselt, paljudel arvutitel, kuid iga katse maksab ikka terve Argon2id käivituse 64 MiB mäluga.

AUS KOKKUVÕTE

Mõlemad teed lõpevad sama küsimusega: **kui raske on sinu seifi parooli ära arvata?** Tugeva parooli puhul on äraarvamine praktiliselt võimatu. Nõrga puhul võidavad mõlemad kihid ainult aega. Järgmine leht näitab, kui palju.

MIKS SINU SEIFI PAROOL LOEB

Kui kaua võtab kõigi võimaluste proovimine?

SEIFI PAROOLI TÜÜP	KAARDI KAUDU ~20 KATSET / S	LABOR + HIIGLASLIK ARVUTIPARK 1 000 000 KATSET / S
Mis tahes parool 1 miljardi lekkinud parooli loendist, nt „Suvi2026!!“	kuni umbes 2 aastat; levinud palju varem	kuni umbes 17 minutit; levinud sekunditega
12 juhuslikku numbrit	umbes 1600 aastat	umbes 12 päeva
4 juhuslikku sõna	miljoneid aastaid	umbes 116 aastat
12 juhuslikku väiketähte	üle 100 miljoni aasta	umbes 3000 aastat
5 juhuslikku sõna	kauem, kui universum on olemas olnud	umbes 900 000 aastat
6 juhuslikku sõna	kauem, kui universum on olemas olnud	umbes 7 miljardit aastat

Halvim juhtum sinu jaoks: aeg kõigi võimaluste proovimiseks. „Juhuslikud sõnad“ tähendab täringuga valitud sõnu 7776-sõnalisest loendist. Arvamiskiirused on illustreerivad, heldelt arvestatud hinnangud. Võrdluseks: üks katse võttis umbes 25 ms tänapäevasel 4 tuumaga Apple M4 arvutil.

SOOVITUS

Viis või kuus juhuslikku sõna. Ära kasuta seda kunagi uuesti ega kasuta kunagi laulusõnu, nimesid ega kuupäevi.

JA KIRJUTA SEE ÜLES

Hoia koopiat turvalises kohas, oma kaartidest eraldi. Unustatud seifi parooli ei saa taastada.

MIDA MI8OS KUNAGI EI TEE

Pilves pole midagi häkkida. Sest pilve pole.

- ✓ **Ei kontot, ei serverit.** Rakendus ei loo üldse võrguühendusi.
- ✓ **Ei salvestatud paroole.** Seifi paroole ja põhiparoole ei salvestata kunagi, ei telefoni ega kaardile.
- ✓ **Ei koopiat telefonis.** Dekrüptitud kirjed on olemas ainult mälus, kuni seif on avatud. Üks erand: kopeeritud kirje jääb lõikelauale, kuni taimer selle tühjendab (15 s kuni 1 min), isegi kui seif on suletud.
- ✓ **Ei telemeetriat.** Ei jälgimist, ei analüütikat.
- ✓ **Lukustub, kui lahkud.** Rakendusest lahkumine sulgeb seifi (kohe või valitud viivituse järel).
- ✓ **Katab oma ekraani** rakenduste vahetajas ning ekraani salvestamise või peegeldamise ajal.
- ✓ **Avastab võltsimise.** Muudetud andmed ei läbi pitserit ja lükatakse tagasi.
- ✓ **Kasutab ainult avalikke standardseid algoritme:** Argon2id, HKDF-SHA256, ChaCha20-Poly1305, AES-128.

TAGAUKSE PUUDUMISE TEINE POOL

Kui kaotad kõik kaardid või unustad seifi parooli, ei saa keegi sinu kirjeid tagasi. Mitte sina, mitte meie. Seepärast on sul kolm kaarti ja üles kirjutatud parool.

KAARTIDE HOOLDUS JA TAASTE

Kolm kaarti, kolm kohta.

01

HOIA NEID LAHUS

Üks kaart sinuga või lähedal, üks kodus, üks kusagil mujal: pere juures, tööl või seifis. Üks tulekahju või sissemurdmine ei saa viia kõiki kolme.

02

KAOTASID KAARDI?

Leidjal on ainult krüptitud andmed. Tee asenduskaart (vt 03), et sul oleks jälle kolm koopiat. Kui kardad, et keegi teab parooli, loo samal viisil uued seifid uue seifi parooliga ja lähtesta seejärel vanad kaardid.

03

ASENDUSKAARDI TEGEMINE

Rakendus saab seifi teistele kaartidele kopeerida ainult kohe pärast selle loomist. Hilisema asenduse jaoks loo tühjale kaardile uus seif ja sisesta samad kirjed uuesti: ava töötav kaart, et neid lugeda, ja kui vahepeal midagi üles kirjutad, hävita see märkus pärast. Tee seda enne, kui sul on alles ainult viimane koopia.

04

UNUSTASID SEIFI PAROOLI?

Neid kirjeid ei saa taastada. Kui mõni teine kaart kasutab parooli, mida veel mäletad, ava see. Muul juhul lähtesta kaardid ja alusta uut seifi.

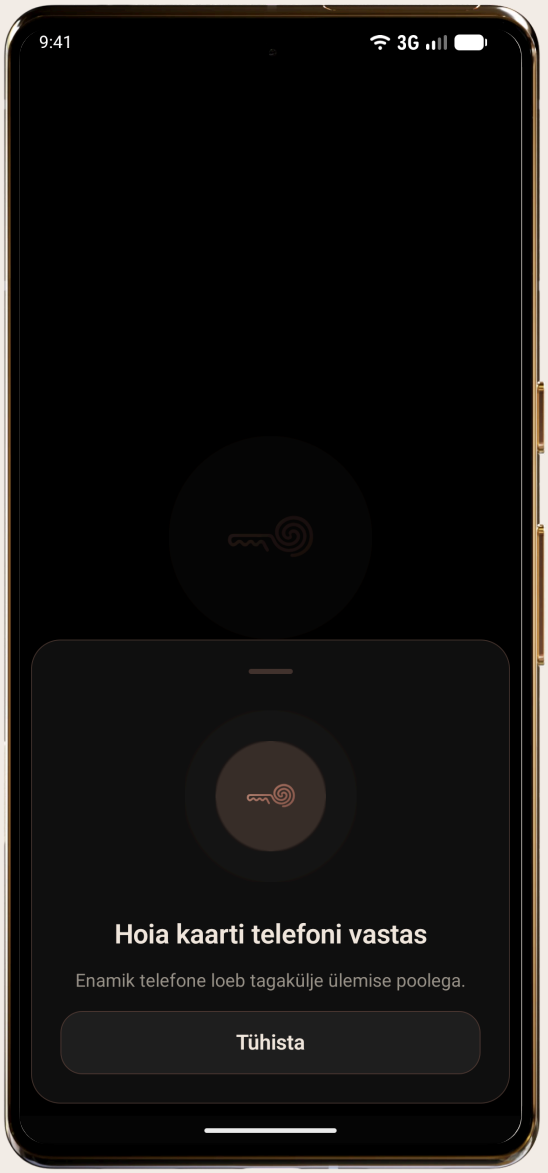
> **Hoolitse kaartide eest** nagu pangakaardi eest: ei painutamist, ei kuumust, ei teravaid servi. Hoia neid skannimisel metallümbristest eemal.

ANDROIDIS

Sama rakendus, mõned väikesed erinevused.

Androidi rakendus on **Google Plays**. See töötab samamoodi ja loeb samu kaarte. iPhone'is kirjutatud seif avaneb Androidis ja vastupidi.

ANDROIDIS	MIS ON TEISITI
Skannimine	Androidil ei ole süsteemset NFC-akent, seega näitab MI8OS oma skannimisekraani koos tühistamisnupuga.
Kaardi asukoht	Hoia kaarti vastu telefoni tagakülje ülemist poolt. Täpne koht oleneb mudelist.
NFC	NFC peab telefoni seadetes sisse lülitatud olema.
Biomeetria	Rakenduse lukk kasutab sinu telefoni sõrmejälge või näotuvastust.



TÕRKEOTSING

Kui miski ei tööta.

MIDA NÄED	MIDA TEHA
Kaarti ei tuvastata	Hoia seda lamedalt vastu iPhone'i ülemist serva ja paigal. Eemalda paks või metallist ümbris. Proovi veidi kõrgemal või madalamal.
Kirjutamine katkes poole peal	Puuduta **Proovi uuesti** ja hoia sama kaarti paigal. Iga salvestamine kirjutab kogu kaardi uuesti ja sinu muudatused jäävad rakendusse, kuni see õnnestub. Kui rakendus ütleb, et salvestamist ei saa lõpetada, lähtesta kaart (leht 26) ja salvesta uuesti või kasuta varukaarti ja asenda see kaart (leht 42).
Vale parool	Kontrolli õigekirja ja tühikuid. Pea meeles: igal kaardil võib olla oma seifi parool.
„See on teine kaart"	Vastu hoitud kaart pole see, mis on avatud. Õige leidmiseks kasuta funktsiooni Tuvasta.
Kaart on täis	Kaardile mahub 20 kirjet. Kustuta üks, mida enam ei vaja, või jaga kirjed mitme kaardi vahel.
Kaart ei lähtestu	See on lukustatud. Lähtestamine küsib selle põhiparooli.
Seif sulgus iseenesest	Lahkusid rakendusest või ekraani salvestati. Ava kaart uuesti.
Paus „Valmistame sinu võtit ette"	Normaalne. See on lehel 34 kirjeldatud tahtlik parooli tugevdamine.

Rohkem abi: guide.mi8os.com · info@mi8os.com

MI8OS

Sinu privaatsus kuulub sulle.

MI8OS.COM

MI8OS-i juhend, eesti keeles, oktoober 2026. Kirjeldab MI8OS-i rakendust iPhone'ile ja Androidile. Ekraanid võivad versiooniti veidi erineda. Peatüki 06 näidisvõtmed ja -baidid loodi selle juhendi jaoks demoparooliga; ära kasuta seda kunagi. MI8OS · info@mi8os.com