MI8OS

MI8OS-OPAS

Kaikki apistasi ja korteistasi.

Miten luot, avaat ja päivität holvin, miten huolehdit MI8OS Card gen 2:sta ja miten kohteesi on suojattu, viimeistä tavua myöten.

LUO | KÄYTÄ | KORTIT | TURVALLISUUS



MI8OS-apille iPhonessa ja Androidissa. Lokakuu 2026.

SISÄLTÖ

Mitä oppaasta löytyy

01 **ALOITUS** p. 3
Mikä MI8OS on, sanat joihin törmäät, appi lyhyesti, miten korttia pidetään.

02 **LUO HOLVI** p. 9
Lisää kohteita, valitse holvin salasana, tallenna kortille, kirjoita varakorttisi.

03 **KÄYTÄ HOLVIASI** p. 16
Avaa kortti, lue ja kopioi kohteita, 2FA-koodit, lisää ja poista, päivitä kortti.

04 **HALLITSE KORTTEJASI** p. 23
Korttini, nimen vaihto, tunnistus, nollaus, lukitseminen ja lukituksen avaaminen pääsalasanalla.

05 **ASETUKSET** p. 29
Apin lukitus, Face ID, leikepöytä ja ulkoasu.

06 **MITEN KOHTEESI ON SUOJATTU** p. 32
Kaksi salauskerrosta, todellinen esimerkki luvulla ”12345678” ja miksi holvin salasanallasi on merkitystä.

07 **HOITO, ANDROID JA APU** p. 42
Kolmen kortin pitäminen, erot Androidissa, vianmääritys.

01

Aloitus

Viisi minuuttia siihen, että ymmärrät miten MI8OS toimii, ennen kuin kosket korttiin.

MIKÄ MI8OS ON

Pieni, salattu holvi kortilla, jota pidät itse hallussasi.

MI8OS säilyttää tärkeimmät salaisuutesi, kuten palautuskoodit, 2FA-avaimet, seed-lauseet ja PIN-koodit, holvissa, joka salataan puhelimessasi ja tallennetaan fyysiselle kortille. Ei tiliä, ei pilveä, ei tilausta.



Mukana · se, jota käytät



Koti · turvassa kotona



Muualla · jossain muualla

PAKKAUKSESSASI

Kolme **MI8OS Card gen 2 -korttia**. Jokaiselle kortille mahtuu enintään **20 kohdetta**. Kirjoita sama holvi kaikille kolmelle ja säilytä niitä eri paikoissa.

MITÄ TARVITSET

iPhonen tai Android-puhelimen, jossa on NFC, sekä MI8OS-apin App Storesta tai Google Playsta (Android-huomiot sivulla 43). Ja holvin salasanan, jonka muistat: pitkä salalause on paras.

SANAT, JOIHIN TÖRMÄÄT

Kolme salasanaa, kolme eri tehtävää.

Tämä on oppaan tärkein sivu. Ne kuulostavat samalta, mutta jokainen suojaa eri asiaa.

HOLVIN SALASANA

Salaa ja avaa kortin kohteet. Pakollinen, vähintään 12 merkkiä.

Ei tallennu mihinkään. Kukaan ei voi palauttaa sitä, ei edes MI8OS.

PÄÄSALASANA

Valinnainen. Lukitsee itse kortin, niin ettei kukaan voi nollata tai tyhjentää sitä ilman tätä salasanaa.

Ei avaa mitään. Kohteiden lukemiseen tarvitaan edelleen holvin salasana.

APIN LUKITUKSEN PIN-KOODI

Valinnainen. Kuusi numeroa (tai Face ID), joilla appi avataan tässä puhelimessa.

Ei liity kortteihisi mitenkään eikä voi purkaa salausta.

SANA	MERKITYS
Holvi	Kohteidesi luettelo. Se on salattuna korteillasi ja salaamattomana vain apin muistissa, kun se on auki.
Kohde	Yksi merkintä: nimi (enintään 24 tavua) ja itse salaisuus (enintään 96 tavua), esimerkiksi PIN-koodi, palautuskoodi tai 2FA-avain.
Kortti	MI8OS Card gen 2 -korttisi. Se tallentaa salatun holvin; voit kirjoittaa saman holvin useille korteille.
Päivitä kortti	Kirjoittaa muutoksesi kortille. Siihen asti muutokset ovat vain apin muistissa.

APPI LYHYESTI

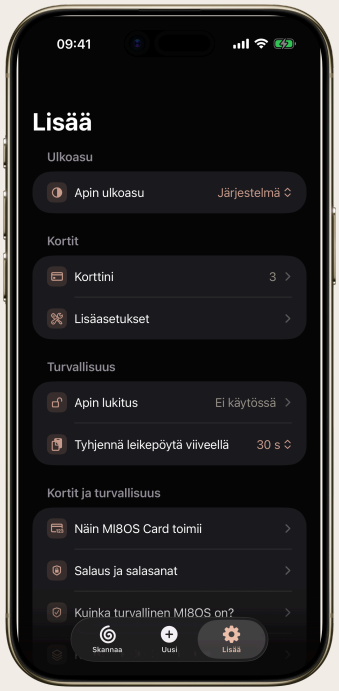
Kolme välilehteä. Kullakin yksi tehtävä.



Skannaa · avaa kortti



Uusi · luo holvi



Lisää · kortit ja asetukset

1

SKANNAA

Skannaa kortti napauttamalla ja pidä korttia puhelinta vasten. Kortti aukeaa omaan ikkunaansa, jossa annat sen holvin salasanan.

2

UUSI

Luo uusi holvi napauttamalla. Nelivaiheinen ohjattu toiminto vie sinut ensimmäisestä kohteesta kortille, joka sisältää sen.

3

LISÄÄ

Korttisi, Apin lukitus, leikepöydän ajastin, ulkoasu ja sisäänrakennetut ohjesivut.

KORTIN PITÄMINEN

Yläreuna. Tasaisesti. Paikallaan.

Aina kun appi viestii kortin kanssa, iPhone näyttää oman NFC-ikkunansa. Sitten:

1. **Pidä korttia tasaisesti yläreunaa vasten** iPhonen takapuolella, jossa NFC-antenni on.
2. **Pidä se paikallaan**, kunnes appi vahvistaa. Kirjoittaminen kestää muutaman sekunnin; kortin siirtäminen liian aikaisin on yleisin syy siihen, että kirjoitus pitää toistaa.
3. Jos mitään ei tapahdu, liu'uta korttia hitaasti hieman alemmas tai ylemmäs ja poista paksut tai metalliset kuoret.

> **Ei kiirettä.** Kun avaat kortin, appi valmistelee ensin avaimesi ("Valmistellaan avaintasi. Korttia ei tarvitse vielä pitää esillä"). Pidä korttia esillä, kun NFC-ikkuna tulee näkyviin.

> **Androidissa** appi näyttää oman skannausnäkymänsä, ja korttia pidetään puhelimen takapuolen yläpuoliskoa vasten.



MITÄ KORTILLE KUULUU

Muutama kohde, joilla on paljon merkitystä.

MI8OS ei ole tarkoitettu korvaamaan salasanojen hallintaohjelmaasi. Se on offline-paikka sille kourallisille asioita, joita tarvitsisit, jos kaikki muu pettäisi.

ERINOMAISTA KORTILLE

- ✓ Sähköpostin sekä Applen / Googlen palautuskoodit
- ✓ 2FA-määritysavaimet, jotta appi voi näyttää koodisi
- ✓ Kryptovaluuttojen palautuslauseet (MI8OS ei ole lompakko eikä säilytä varoja)
- ✓ Salasanojen hallintaohjelmasi pääsalasana tai hätäpaketin tiedot
- ✓ Tärkeät PIN-koodit ja yksityiset muistiinpanot

HYVÄ TIETÄÄ

- ✓ Enintään 20 kohdetta kortilla
- ✓ Nimi: enintään 24 tavua · kohde: enintään 96 tavua
- ✓ Tavalliset kirjaimet, numerot ja välilyönnit vievät 1 tavun; tarkkeelliset, kreikkalaiset tai kyrilliset kirjaimet 2; emojit 4
- ✓ Pitkät seed-lauseet voivat vaatia kaksi kohdetta (esim. sanat 1–12 ja 13–24)

02

Luo holvi

Neljä vaihetta: Kohteet, Salasana, Kirjoitus, Valmis. Noin viisi minuuttia.

VAIHE 1/4 · KOHTEET

Aloita kohteistasi.

1. Avaa **Uusi**-välilehti ja napauta painiketta **Luo uusi holvi napauttamalla**.
2. Napauta **Lisää kohde** jokaiselle asialle, jonka haluat säilyttää.
3. Pyyhkäise kohdetta poistaaksesi sen ennen kuin jatkat.
4. Napauta **Jatka**, kun luettelosi on valmis.

> **Mitään ei ole vielä tallennettu.** Kohteesi ovat vain tässä ohjatussa toiminnossa, kunnes tallennat salatun holvin kortille.

> **Onko sinulla jo holvi auki?** Appi kysyy ensin. Jos sinulla on muutoksia, jotka eivät vielä ole kortilla, se tarjoutuu säilyttämään ne.



KOHTEEN LISÄÄMINEN

Nimi ja itse salaisuus.

Nimi. Jotain, minkä tunnistat, kuten ”Sähköpostin palautuskoodit”. Enintään 24 tavua; laskuri näyttää, paljonko on jäljellä.

Kohde. Salasana, koodi tai teksti, enintään 96 tavua. Kaikki, mitä liität tai luot, salataan ennen kuin se päätyy kortille.

Luonti. Napauta noppaa luodaksesi satunnaisen 16, 32, 64 tai 96 merkin salasanan.

2FA-AVAIMEN TALLENTAMINEN

Kun palvelu näyttää määritysavaimen (tai QR-koodin takana olevan otpauth://-linkin), liitä se kohteeksi. MI8OS tunnistaa sen ja näyttää myöhemmin **TOTP**-painikkeen, joka kopioi voimassa olevan koodin. Jos linkki on yli 96 tavua, liitä vain itse määritysavain (osa kohdan secret= jälkeen); MI8OS käyttää silloin vakiota, 6 numeroa 30 sekunnin välein.



VAIHE 2/4 · SALASANA

Valitse holvin salasana.

1. Kirjoita holvin salasana ja vahvista se kirjoittamalla se uudelleen.
2. Seuraa vahvuuspalkkia: 12 merkkiä on vähimmäismäärä, 20 tai välilyönneillä erotettu lause antaa tuloksen "Erinomainen pituus."
3. Rastita ruutu: *"Jos menetän kaikki kortit tai unohdan tämän salasanan, MI8OS ei voi palauttaa tämän kortin holvia."*
4. Napauta **Salaa holvi**.



NEUVOMME

Käytä **viittä tai kuutta satunnaista sanaa**, kuten *kupari lyhty sametti kiertorata tundra* (mutta älä juuri näitä). Helppo muistaa, äärimmäisen vaikea arvata. Sivu 40 näyttää miksi.

VAIHE 3/4 · KIRJOITUS

Ensin salaus. Sitten kortti esille.

Salaus tapahtuu puhelimessasi ennen kuin NFC käynnistyy. Näet hetken tekstin ”Vahvistetaan salaustasi…”, kun appi muuttaa salasanasi avaimiksi. Tauko on tarkoituksellinen: se tekee salasanasi arvaamisesta hidasta kaikille muille.

Kun näkyvissä on **Salaus valmis**:

1. Napauta **Tallenna kortille**.
2. Pidä korttia iPhonen yläreunaa vasten, kun NFC-ikkuna tulee näkyviin.
3. Pysy paikallasi. Appi kirjoittaa holvin ja **lukee sen sitten takaisin tarkistaakseen sen**.

> **Tyhjä kortti?** Appi valmistelee sen automaattisesti samalla skannauksella.



VAIHE 4/4 · VALMIS

Kirjoita nyt varakorttisi.

”Holvi tallennettu kortille” tarkoittaa, että holvi on tarkistettu kyseisellä kortilla. **Tämä on ainoa hetki, jolloin appi voi kopioida koko holvisi muille korteille**, joten kirjoita ne kaikki nyt:

1. Napauta **Kirjoita toinen kortti**.
2. Valitse tälle kortille **Käytä samaa holvin salasanaa** (helpoin) tai **Käytä eri holvin salasanaa**.
3. Tallenna seuraavalle kortille. Toista kolmannelle.

> **Sama salasana, uusi salaus.** Jokainen kortti saa oman satunnaisen suolan, joten samallakin salasanalla jokaisen kortin tiedot näyttävät täysin erilaisilta.

Hylkää holvi tästä iPhonesta sulkee vain holvin apin muistissa. Se ei koskaan tyhjennä korttia.



KORTTI, JOLLA ON JO HOLVI

MI8OS ei koskaan korvaa holvia yllättäen.

Jos tallennat uuden holvin kortille, jolla on jo holvi, mitään ei kirjoiteta. Appi ilmoittaa: **”Tällä kortilla on jo holvi”** ja antaa sinulle kaksi vaihtoehtoa:

LISÄÄ KOHTEITA

Lisää uudet kohteesi kortin holviin. Kortilla jo olevat kohteet säilyvät. Holvin salasanasi on oltava se, jota tämä kortti käyttää, ja pidät korttia esillä vielä kerran.

PERUUTA

Jättää kortin täsmälleen ennalleen.

> **Haluatko korvata holvin kokonaan?** Nollaa kortti ensin (sivu 26) ja luo sitten uusi holvi sille.



03

Käytä holviasi

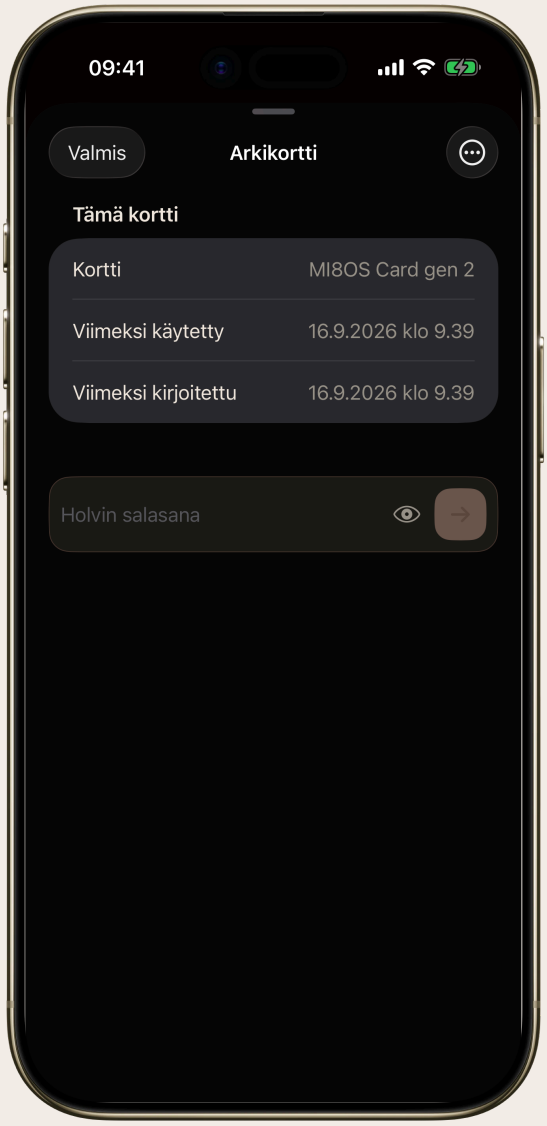
Avaa, lue, kopioi, muuta ja kirjoita muutokset takaisin kortille.

KORTIN AVAAMINEN

Skannaus, salasana, kortti uudelleen esille.



Skannaa-välilehti



Kortin ikkuna

1. Napauta **Skannaa**-välilehdellä painiketta **Skannaa kortti napauttamalla** ja pidä korttia esillä. Skannaus lukee vain kortin julkiset tiedot.
2. Anna kortin **Holvin salasana** ja napauta **Avaa holvi**. Appi valmistelee avaimesi ja pyytää sitten korttia vielä kerran.

HOLVIN SISÄLLÄ

Kohteesi, niin kauan kuin tarvitset niitä.

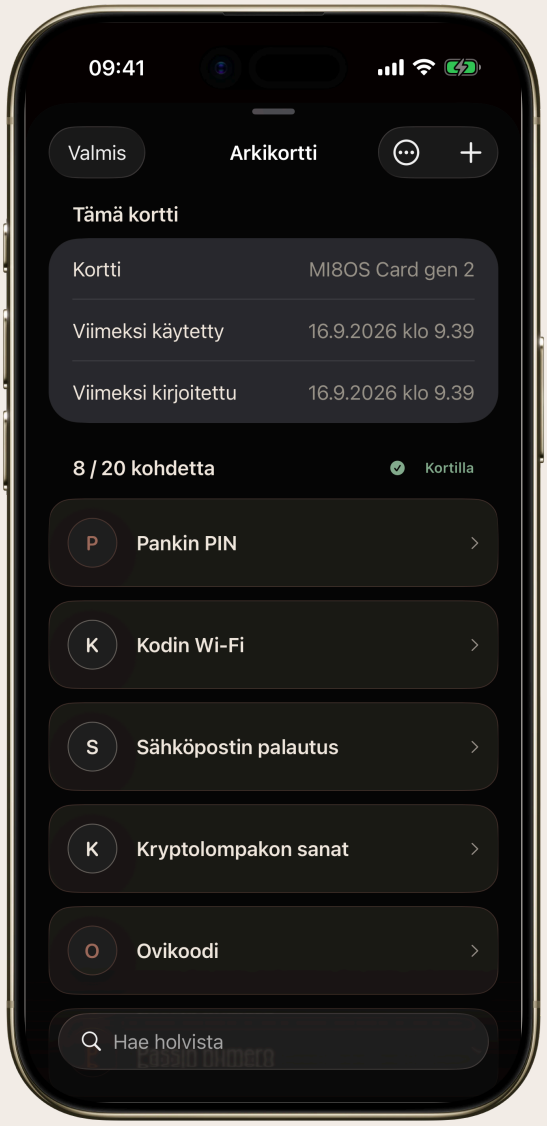
Tämä kortti näyttää, minkä kortin avasit, tiedot Viimeksi käytetty ja Viimeksi kirjoitettu sekä sen, onko kortilla pääsalasana.

”8 / 20 kohdetta” kertoo, kuinka täynnä kortti on. **Kortilla** tarkoittaa, että kaikki näkemäsi on tallennettu kortille.

Hae holvista alareunassa löytää kohteen nimen perusteella.

+ yläreunassa lisää kohteen; **⋯** avaa korttivalikon (sivu 25).

> **Salaus purettuna vain muistissa.** Kohteesi ovat luettavassa muodossa vain, kun tämä ikkuna on auki. Napauta **Valmis**, niin ne katoavat puhelimesta.



LUKEMINEN JA KOPIOINTI

Piilossa, kunnes pyydät.

Avaa kohde napauttamalla sitä. Arvo on piilossa pisteiden takana.

Näytä näyttää sen; **Kätke** piilottaa sen taas.

Kopioi vie sen leikepöydälle, ja MI8OS **tyhjentää leikepöydän taas** 30 sekunnin kuluttua (muuta kohdassa Lisää: 15 s, 30 s tai 1 min).

> **Liitä nopeasti.** Ajastimen jälkeen leikepöytä on tyhjä, joten kohde ei jää lojumaan muihin appeihin. Ajastin jatkaa, vaikka sulkisit holvin ennen sen päättymistä.

> **Näytön tallennus tai peilaus?** MI8OS peittää näytön ja sulkee holvin, jotta kohteet eivät päädy tallenteeseen.



2FA-KOODIT

Todennussovelluksesi, kortilta.

Jos kohde on 2FA-määritysavain, sen sivulla näkyy **TOTP**-painike. Napauta sitä, niin MI8OS laskee voimassa olevan koodin ja kopioi sen valmiiksi liitettäväksi.

Kortti tallentaa vain **salatun määritysavaimen**. Koodi lasketaan apissa holvin avaamisen jälkeen avaimen ja nykyisen ajan perusteella, aivan kuten missä tahansa todennussovelluksessa.

MIKSI TÄSTÄ ON APUA

Jos todennuskoodisi ovat vain puhelimessa, jonka kadotat, ne katoavat sen mukana. Kun määritysavaimet ovat korteillasi, saat koodisi mihin tahansa uuteen puhelimeen, jossa on MI8OS-appi.



HOLVIN MUUTTAMINEN

Lisää, poista ja päivitä sitten kortti.

Lisääminen: napauta **+** ja täytä nimi ja kohde.

Poistaminen: pyyhkäise kohdetta vasemmalle tai avaa se ja napauta **Poista kohde**. Se jää luetteloon merkittynä, kunnes päivität kortin. Muutitko mielesi? Napauta **Säilytä**.

Muokkaaminen: muokkauspainiketta ei ole tarkoituksella. Jos haluat muuttaa kohdetta, poista se ja lisää se uudelleen.

Muutokset on merkitty vielä kirjoittamattomiksi. Napauta **Päivitä kortti** ja pidä korttia esillä tallentaaksesi ne.

> **Suljetko kirjoittamattomien muutosten kanssa?** Appi varoittaa: ”Jos suljet tämän kortin päivittämättä sitä, muutokset katoavat.”



PIDÄ JOKAINEN KOPIO AJAN TASALLA

Jokainen kortti päivitetään erikseen.

Päivitä kortti kirjoittaa avaamallesi kortille, ja vain sille. Muilla korteillasi on edelleen edellinen versio, kunnes päivität nekin.

1

MUUTA YHTÄ KORTTIA

Avaa Mukana-korttisi, lisää tai poista, napauta **Päivitä kortti**.

2

TOISTA MUILLE

Avaa Koti- ja Muualla-korttisi ja tee sama muutos kumpaankin.

3

OIKOTIE UUSILLE KOHTEILLE

Luo ”uusi holvi”, jossa on vain uudet kohteet, ja tallenna se kortille, jolla holvisi jo on. Valitse **Lisää kohteita**, niin ne lisätään olemassa oleviin.

HYVÄ TAPA

Kerran vuodessa: avaa jokainen kortti ja tarkista, että kaikissa kolmessa näkyy sama määrä kohteita.

04

Hallitse korttejasi

Nimet, korttivalikko, nollaus ja valinnainen pääsalasana.

KORTTINI

Anna jokaiselle kortille nimi.

Kohdassa **Lisää** → **Korttini** näet kortit, jotka tämä puhelin tuntee, merkinnän kera: kohteiden määrä, **Tyhjä** tai **Lukittu**.

Lisää kortti skannaa kortin ja muistaa sen. Se lukee vain sen, mikä kortilla on jo julkista: salasanaa ei tarvita, mitään ei kirjoiteta.

Napauta korttia avataksesi sen, vaihtaaksesi sen nimen tai nollataksesi sen.

> **Nopeampi avaus.** Kortti, jonka tämä puhelin jo tuntee, aukeaa yhdellä skannauksella salasanan antamisen jälkeen.

> **Tallennetaan vain tähän puhelimeen:** antamasi nimet, milloin kortteja on viimeksi käytetty, ja niiden julkiset asetukset. Ei koskaan salasanaa, ei koskaan kohdetta.



KORTTIVALIKKO ···

Vaihda nimi, tunnista, unohda.

VAIHDA NIMI

Nimi, jonka tunnistat: ”Mukana”, ”Koti”, ”Vanhempien kassakaappi”.

TUNNISTA

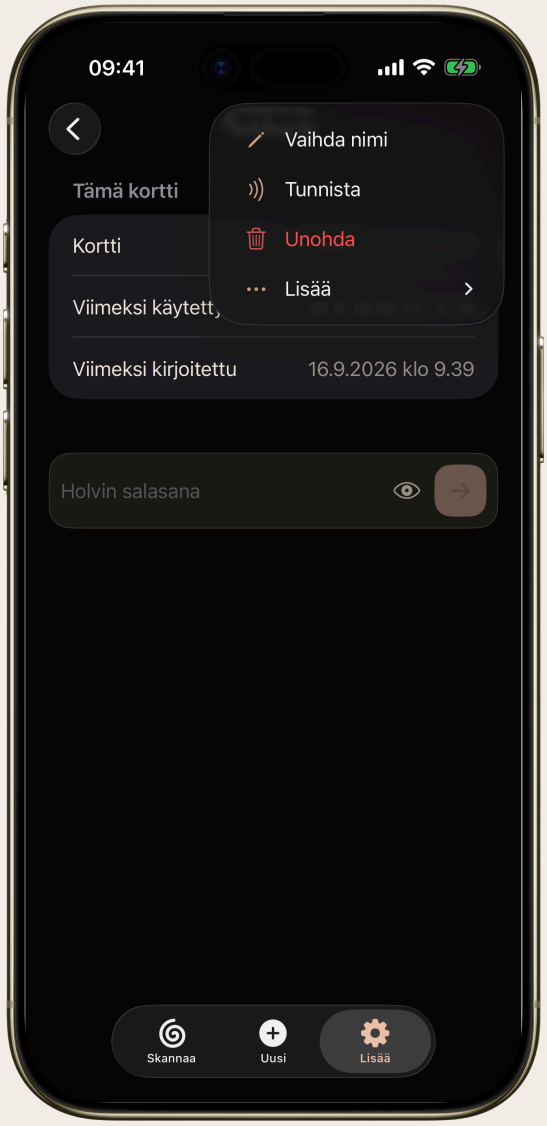
Etkö ole varma, mikä kortti on mikä? Napauta Tunnista ja pidä korttia esillä. Appi kertoo, onko se katsomasi kortti vai mikä muu kortti se on.

UNOHDA

Poistaa kortin tämän puhelimen luettelosta. Kortilla mikään ei muutu, ja voit lisätä sen uudelleen milloin tahansa.

LISÄÄ

Nollaa kortti, Lukitse kortti ja Avaa kortin lukitus. Katso seuraavat sivut.



KORTIN NOLLAAMINEN

Puhdas kortti, valmis uudelle holville.

··· → **Lisää** → **Nollaa kortti** poistaa MI8OS-holvin ja kaiken muun kortilta ja vapauttaa koko sen tallennustilan. Se **ei** kysy holvin salasanaa.

Käytä sitä, kun haluat:

- ✓ Korvata holvin kokonaan uudella
- ✓ Käyttää korttia uudelleen, kun olet unohtanut sen holvin salasanan (sen kohteet menetetään)
- ✓ Tyhjentää kortin ennen kuin annat sen pois

> **Muihin kortteihin ei kosketa.** Yhden kortin nollaaminen ei koskaan vaikuta muiden korttiesi holviin.

> **Lukittu kortti?** Se kieltäytyy nollauksesta, kunnes annat sen pääsalasanan (seuraava sivu).



KORTIN LUKITSEMINEN · PÄÄSALASANA

Estä ketä tahansa tyhjentämästä korttiasi.

Kuka tahansa, joka saa käsiinsä lukitsemattoman kortin, voi nollata sen jopa ilman holvin salasanaasi. Hän ei silti pysty lukemaan mitään, mutta voi tyhjentää sen.

Lukitse kortti estää sen. Valitse pääsalasana, pidä korttia esillä, valmista. Sen jälkeen korttia ei voi nollata tai tyhjentää ilman sitä, ei MI8OS eikä mikään muukaan.

1. ··· → **Lisää** → **Lukitse kortti**
2. Anna pääsalasana kahdesti ja napauta **Lukitse**.
3. Pidä korttia esillä, kunnes appi vahvistaa ”Kortti lukittu”.

> **Lukeminen ja tallentaminen eivät muutu.** Niihin käytetään edelleen vain holvin salasanaa.



KORTIN LUKITUKSEN AVAAMINEN · JA VAROITUS

Lukituksen avaaminen palauttaa kortin normaaliksi.

··· → **Lisää** → **Avaa kortin lukitus**, anna pääsalasana ja pidä korttia esillä. Kortti toimii taas kuin lukitsematon kortti. Sen holvi ja holvin salasana pysyvät ennallaan.

Jos haluat nollata lukitun kortin, valitse Nollaa kortti: appi pyytää pääsalasanaa ja alustaa sitten kortin.

ÄLÄ UNOHDA SITÄ

Jos unohdat kortin pääsalasanan, korttia ei voi **koskaan** nollata tai käyttää uudelleen. Sen kohteet ovat yhä luettavissa holvin salasanalla. Appi kysyy sitä joka kerta eikä koskaan muista sitä.

Voit myös lukita, avata ja nollata minkä tahansa kortin kohdassa **Lisää** → **Lisäasetukset** skannaamalla sen.



05

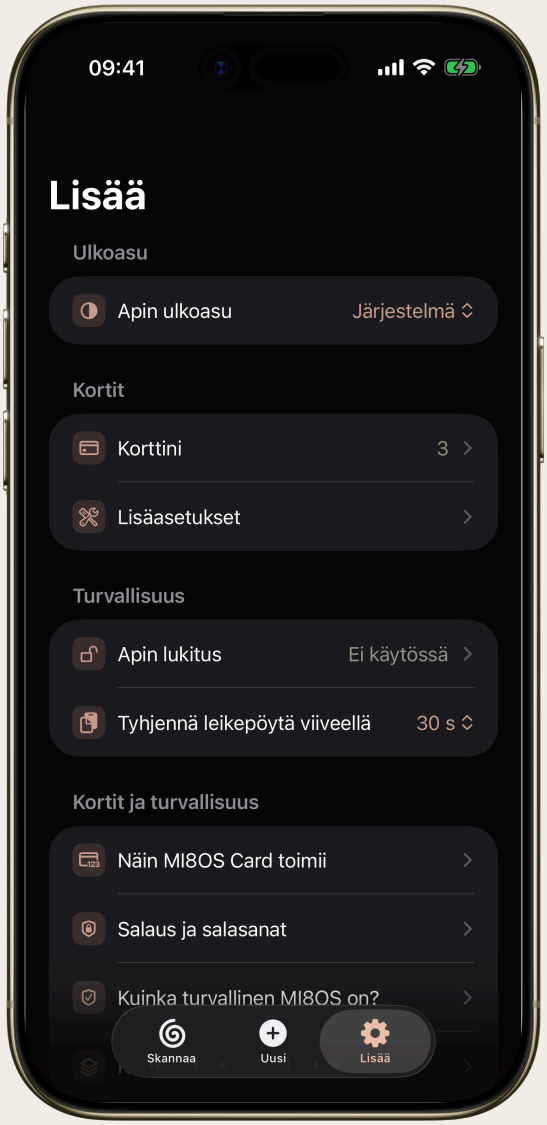
Asetukset

Apin lukitus, Face ID, leikepöytä ja apin ulkoasu.

LISÄÄ

Kaikki muu, yhdessä paikassa.

ASETUS	MITÄ SE TEKEE
Apin ulkoasu	Järjestelmä, Vaalea tai Tumma.
Korttini	Nimetyt korttisi (sivu 24).
Lisäasetukset	Lukitse, avaa tai nollaa mikä tahansa kortti skannaamalla se.
Apin lukitus	PIN-koodi ja Face ID apille (seuraava sivu).
Tyhjennä leikepöytä viiveellä	15 s, 30 s tai 1 min sen jälkeen, kun olet kopioinut kohteen.
Kortit ja turvallisuus	Sisäänrakennettu ohje: Näin MI8OS Card toimii, Salaus ja salasanat, Kuinka turvallinen MI8OS on?, Korttien hoito ja palautus.
Tuki ja juridiikka	Tilaa MI8OS Card, Tietosuojakäytäntö, Käyttöehdot.



APIN LUKITUS

Lukko itse apille.





Ota se käyttöön kohdassa Lisää → Apin lukitus: valitse kuusinumeroinen PIN-koodi ja halutessasi Face ID tai Touch ID.

Lukitse, kun poistun apista: Heti, 1 minuutin kuluttua tai 10 minuutin kuluttua. Jos poistut apista pidemmäksi aikaa, myös avoinna oleva holvi sulkeutuu.

PIN-koodi avaa vain apin tässä puhelimessa. Se ei voi purkaa kortin salausta eikä korvaa holvin salasanaa. Valitse kuusi numeroa, jotka eivät avaa myös jotain muuta.

06

Miten kohteesi on suojattu

Kaksi salauskerrosta, yksi todellinen esimerkki ja rehellinen vastaus kysymykseen ”entä jos joku varastaa korttini?”

KOKONAISKUVA

Kaksi kerrosta. Molemmat syntyvät salasanastasi.

1

APISSA: KOHTEET SINETÖIDÄÄN

Ennen kuin mitään lähetetään kortille, appi salaa jokaisen kohteen puhelimessasi **ChaCha20-Poly1305**-algoritmilla ja 256-bittisellä avaimella, joka muodostetaan holvin salasanastasi.

Tämä on päälukko. Raakadatankin haltija näkee vain satunnaiselta näyttäviä tavuja, ja kaikki niihin tehdyt muutokset havaitaan.

2

KORTILLA: OVI ON LUKOSSA

Kortin suojattu siru pitää salatut kohteet oman **AES-128**-avaimensa takana, joka sekin muodostetaan holvin salasanastasi. Se luovuttaa ne vasta, kun puhelin on todistanut tuntevansa avaimen.

Ilman oikeaa salasanaa lukija ei saa muuta kuin kortin julkiset asetukset.

Holvin salasanasi

ei tallennu mihinkään

↓

Sisältöavain

256-bittinen · sinetöi kohteet (kerros 1)

Korttiavain

128-bittinen · avaa kortin oven (kerros 2)

Hallinta-avain

128-bittinen · hallitsee kortin holvia

SALASANASTA AVAIMIKSI

Miksi ”Vahvistetaan salaustasi…” kestää hetken.



ARGON2ID

Tarkoituksella hidas ja paljon muistia vaativa salasanafunktio. Jokainen yksittäinen arvaus vie 64 MiB muistia ja todellista aikaa, niin puhelimessasi kuin hyökkääjän tietokoneella.

SUOLA

Satunnaisia tavuja, jotka on tallennettu kortille avoimesti. Ne tekevät jokaisen kortin avaimista ainutlaatuisia, joten kukaan ei voi valmistella arvaustaulukkoa etukäteen.

TODELLINEN ESIMERKKI · 1/4 · AVAIMET

Salataan ”12345678”.

Nämä ovat todellisia arvoja, jotka on tuotettu samoilla algoritmeilla ja asetuksilla kuin apissa. Salasana on vain tätä esimerkkiä varten.

Holvin salasana	`copper-lantern-velvet-orbit`
Kohteen nimi	`Demo PIN`
Kohde	`12345678`
Suola (satunnainen, kortilla)	`7a8dbeec53e1eb50c70ccd4674a0e624`
Juuriavain (Argon2id)	`84e743792af48790ce3ac4e2410ba1e9ef786851fa74467fc077208674905241`
Sisältöavain · 256-bittinen	`dcbe9b90a42a1c5e53f8bdaf07e3d763a61708ae3ad68fdfa7be72792fa6ab7c`
Korttiavain · 128-bittinen	`266b550b4a87dd1029d53af4262244c1`
Hallinta-avain · 128-bittinen	`d9715ed54fbc71325587258c440a8dc6`

> **Mitään näistä avaimista ei koskaan tallenneta.** Appi laskee ne, kun annat salasanasi, ja unohtaa ne, kun holvi sulkeutuu. Kortilla on vain suola.

TODELLINEN ESIMERKKI · 2/4 · KERROS 1 APISSA

Luvusta ”12345678” satunnaiselta näyttäviksi tavuiksi.

1. Kohde pakataan 20 tavuun: nimikenttään ja kohdekenttään.

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

kentän tyyppi ja pituus ”Demo PIN” "12345678"

2. ChaCha20-Poly1305 sinetöi sen sisältöavaimella, ainutkertaisella 12 tavun noncella (johdettu paikan otsakkeesta) ja otsakkeella todennettuna datana.

Nonce	`be00fc197a76fb68b8f315fa`
Salateksti · 20 tavua	`5eda3e6b43d7aa61edf77ab4a26ae11e9b080c60`
Tunniste · 16 tavua	`1b1b0dbbd23c5dffd6f4c462f9a449c4`

> **Tunniste on sinetti.** Jos salatekstistä tai sen otsakkeesta muuttuu yksikin bitti, tunniste ei enää täsmää, ja appi hylkää datan sen sijaan, että näyttäisi jotain väärää.

TODELLINEN ESIMERKKI · 3/4 · MITÄ KORTILLA ON

Yksi kohde, yksi 192 tavun paikka.

Tämä on täsmälleen se, mitä kortti tallentaa kohteelle ”Demo PIN”. Etsi ”12345678”: sitä ei ole siellä.

```
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
```

otsake: versio, kohde, sijainti (12 tavua) · salateksti (20 tavua) · tunniste (16 tavua) · tyhjä tila

KORTIN OVEN TAKANA

Nämä paikat ovat kortin suojatussa osassa. Kortti luovuttaa ne vasta, kun puhelin on läpäissyt tarkistuksen korttiavaimella (kerros 2).

SAMA KOHDE, ERI TAVUT

Kirjoita sama kohde toiselle kortille, niin se näyttää täysin erilaiselta, koska jokaisella kortilla on oma suolansa ja omat avaimensa.

TODELLINEN ESIMERKKI · 4/4 · JULKINEN OSA

Mitä kuka tahansa lukijan haltija näkee.

Jokaisella kortilla on myös pieni julkinen alue (128 tavua). Sen voi lukea ilman salasanaa, koska appi tarvitsee suolan avaintesi muodostamiseen.

```
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 muoto · holvin tunnus · kortin rakenne · suola · Argon2id-asetukset · käyttämätön

ENTÄ VÄÄRÄLLÄ SALASANALLA?

Muuta vain salasanan viimeistä kirjainta, niin korttiavaimeksi tulee:

`883e65196d88bc9f1aae79acf8fa7c74`

eikä `266b550b4a87dd1029d53af4262244c1`. Ei mitään yhteistä. Kortti hylkää tarkistuksen, ei lähetä yhtään kohdetta, eikä mitään kirjoiteta.

JOS JOKU VARASTAA KORTTISI

Hänellä on kortti. Ei kohteitasi.

Takaovea tai yleisavainta ei ole. Ainoa tie sisään on arvata holvin salasanasi, ja molemmat kerrokset tekevät jokaisesta arvauksesta kallista.

A

ARVAAMINEN KORTIN KAUTTA

Jokainen arvaus vaatii fyysisen kortin. Varas ajaa Argon2id:n yhtä arvausta varten ja kysyy sitten kortilta. Kortti vastaa NFC:n kautta yhteen yritykseen kerrallaan. Arviomme mukaan se tekee enintään noin 20 yritystä sekunnissa.

B

SIRUN PURKAMINEN

Kallis reitti. Erikoistunut laboratorio voisi yrittää irrottaa salatut paikat suoraan sirulta. Sen jälkeen se voi arvata offline-tilassa monella tietokoneella, mutta jokainen arvaus vaatii silti täyden Argon2id-ajon 64 MiB:n muistilla.

REHELLINEN JOHTOPÄÄTÖS

Molemmat reitit päättyvät samaan kysymykseen: **kuinka vaikea holvin salasanasi on arvata?** Vahvan salasanan arvaaminen on käytännössä mahdotonta. Heikon kanssa kerrokset vain ostavat aikaa. Seuraava sivu näyttää, kuinka paljon.

MIKSI HOLVIN SALASANALLASI ON MERKITYSTÄ

Kuinka kauan kaikkien vaihtoehtojen kokeileminen kestää?

HOLVIN SALASANAN TYYPPI	KORTIN KAUTTA ~20 ARVAUSTA / S	LABORATORIO + VALTAVA TIETOKONEJOUKKO 1 000 000 ARVAUSTA / S
Mikä tahansa salasana miljardin vuotaneen salasanan listalta, esim. ”Kesä2026!!”	enintään noin 2 vuotta; yleiset paljon nopeammin	enintään noin 17 minuuttia; yleiset sekunneissa
12 satunnaista numeroa	noin 1 600 vuotta	noin 12 päivää
4 satunnaista sanaa	miljoonia vuosia	noin 116 vuotta
12 satunnaista pientä kirjainta	yli 100 miljoonaa vuotta	noin 3 000 vuotta
5 satunnaista sanaa	kauemmin kuin maailmankaikkeus on ollut olemassa	noin 900 000 vuotta
6 satunnaista sanaa	kauemmin kuin maailmankaikkeus on ollut olemassa	noin 7 miljardia vuotta

Pahin tapaus sinulle: aika, joka kuluu kaikkien vaihtoehtojen kokeilemiseen. ”Satunnaiset sanat” tarkoittaa nopilla valittuja sanoja 7 776 sanan listalta. Arvausnopeudet ovat havainnollistavia, avokätisiä arvioita. Mittakaavaksi: yksi arvaus kesti noin 25 ms nykyaikaisella Apple M4 -tietokoneella 4 ytimellä.

SUOSITUS

Viisi tai kuusi satunnaista sanaa. Älä koskaan käytä sitä uudelleen, äläkä koskaan käytä laulujen sanoja, nimiä tai päivämääriä.

JA KIRJOITA SE MUISTIIN

Säilytä kopiota turvallisessa paikassa erillään korteistasi. Unohdettua holvin salasanaa ei voi palauttaa.

MITÄ MI8OS EI KOSKAAN TEE

Pilvessä ei ole mitään murrettavaa. Koska pilveä ei ole.

- ✓ **Ei tiliä, ei palvelinta.** Appi ei muodosta lainkaan verkkoyhteyksiä.
- ✓ **Ei tallennettuja salasanoja.** Holvin salasanoja ja pääsalasanoja ei koskaan tallenneta, ei puhelimeen eikä kortille.
- ✓ **Ei kopiota puhelimessa.** Puretut kohteet ovat olemassa vain muistissa, kun holvi on auki. Yksi poikkeus: kopioimasi kohde pysyy leikepöydällä, kunnes ajastin tyhjentää sen (15 sekunnista 1 minuuttiin), vaikka holvi olisi jo suljettu.
- ✓ **Ei telemetriaa.** Ei seurantaa, ei analytiikkaa.
- ✓ **Lukittuu, kun poistut.** Apista poistuminen sulkee holvin (heti tai valitsemasi viiveen jälkeen).
- ✓ **Peittää näyttönsä** sovelluksen vaihtajassa sekä näytön tallennuksen ja peilauksen aikana.
- ✓ **Havaitsee peukaloinnin.** Muutettu data ei läpäise sinettiä, ja se hylätään.
- ✓ **Käyttää vain julkisia vakioalgoritmeja:** Argon2id, HKDF-SHA256, ChaCha20-Poly1305, AES-128.

TAKAOVEN PUUTTUMISEN TOINEN PUOLI

Jos menetät kaikki kortit tai unohdat holvin salasanan, kukaan ei saa kohteitasi takaisin. Et sinä, emmekä me. Siksi sinulla on kolme korttia ja muistiin kirjoitettu salasana.

KORTTIEN HOITO JA PALAUTUS

Kolme korttia, kolme paikkaa.

01

PIDÄ NE ERILLÄÄN

Yksi kortti mukanasi tai lähellä, yksi kotona, yksi jossain muualla: perheen luona, töissä tai kassakaapissa. Yksi tulipalo tai murto ei voi viedä kaikkia kolmea.

02

KADOTITKO KORTIN?

Löytäjällä on vain salattua dataa. Tee korvaava kortti (katso 03), jotta sinulla on taas kolme kopiota. Jos pelkäät, että joku tietää salasanan, luo samalla tavalla uudet holvit uudella holvin salasanalla ja nollaa sitten vanhat korttisi.

03

KORVAAVAN KORTIN TEKEMINEN

Appi voi kopioida holvin muille korteille vain heti sen luomisen jälkeen. Myöhempää korvaavaa korttia varten luo tyhjälle kortille uusi holvi ja syötä samat kohteet uudelleen: avaa toimiva kortti lukeaksesi ne, ja jos kirjoitat jotain muistiin välillä, tuhoa muistiinpano jälkeenpäin. Tee se ennen kuin sinulla on jäljellä enää viimeinen kopio.

04

UNOHDITKO HOLVIN SALASANAN?

Niitä kohteita ei voi palauttaa. Jos toinen kortti käyttää salasanaa, jonka vielä muistat, avaa se. Muuten nollaa kortit ja aloita uusi holvi.

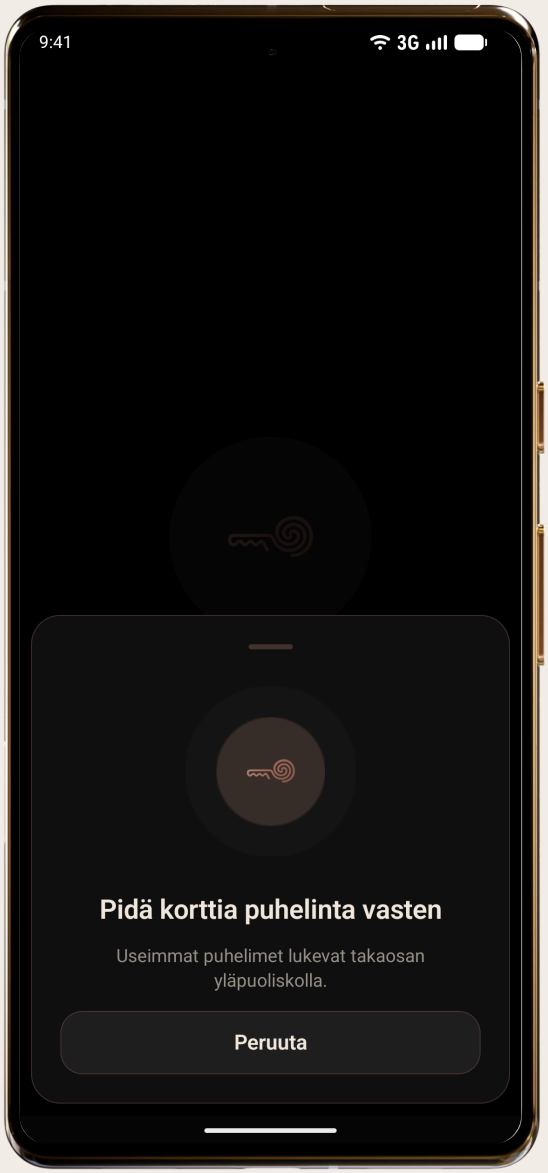
> **Pidä korteista huolta** kuin pankkikortista: ei taivuttelua, ei kuumuutta, ei teräviä reunoja. Pidä ne skannatessa poissa metallisten kuorten läheltä.

ANDROIDISSA

Sama appi, muutama pieni ero.

Android-appi on **Google Playssa**. Se toimii samalla tavalla ja lukee samoja kortteja. iPhonella kirjoitettu holvi aukeaa Androidissa ja päinvastoin.

ANDROIDISSA	MIKÄ ON TOISIN
Skannaus	Androidissa ei ole järjestelmän NFC-ikkunaa, joten MI8OS näyttää oman skannausnäkymänsä ja peruutuspainikkeen.
Kortin paikka	Pidä korttia puhelimen takapuolen yläpuoliskoa vasten. Tarkka kohta vaihtelee malleittain.
NFC	NFC:n on oltava päällä puhelimen asetuksissa.
Biometriikka	Apin lukitus käyttää puhelimesi sormenjälkeä tai kasvojentunnistusta.



VIANMÄÄRITYS

Jos jokin ei toimi.

MITÄ NÄET	MITÄ TEET
Korttia ei tunnisteta	Pidä sitä tasaisesti iPhonen yläreunaa vasten ja pidä se paikallaan. Poista paksu tai metallinen kuori. Kokeile hieman ylempää tai alempaa.
Kirjoitus pysähtyi kesken	Napauta **Yritä uudelleen** ja pidä samaa korttia paikallaan. Jokainen tallennus kirjoittaa koko kortin uudelleen, ja muutoksesi pysyvät apissa, kunnes se onnistuu. Jos appi ilmoittaa, ettei tallennusta voi viedä loppuun, nollaa kortti (sivu 26) ja tallenna uudelleen tai käytä varakorttia ja korvaa tämä kortti (sivu 42).
Väärä salasana	Tarkista kirjoitusasu ja välilyönnit. Muista: jokaisella kortilla voi olla oma holvin salasanansa.
”Se on eri kortti”	Pidit esillä eri korttia kuin avasit. Etsi oikea kortti Tunnista-toiminnolla.
Kortti on täynnä	Kortille mahtuu 20 kohdetta. Poista yksi, jota et enää tarvitse, tai jaa kohteesi useammalle kortille.
Kortti ei nollaudu	Se on lukittu. Nollaus pyytää sen pääsalasanaa.
Holvi sulkeutui itsestään	Poistuit apista, tai näyttöä tallennettiin. Avaa kortti uudelleen.
Tauko ”Valmistellaan avaintasi”	Normaalia. Se on sivulla 34 kuvattu tarkoituksellinen salasanan vahvistus.

Lisää apua: guide.mi8os.com · info@mi8os.com

MI8OS

Yksityisyytesi kuuluu sinulle.

MI8OS.COM

MI8OS-opas, suomi, lokakuu 2026. Kuvaa MI8OS-appia iPhonelle ja Androidille. Näkymät voivat vaihdella hieman versioittain. Luvun 06 esimerkkiavaimet ja -tavut luotiin tätä opasta varten demosalasanalla; älä koskaan käytä sitä. MI8OS · info@mi8os.com