MI8OS

MI8OS-GUIDEN

# Alt om appen og kortene dine.

Hvordan du oppretter, åpner og oppdaterer et hvelv, hvordan du tar vare på MI8OS Card gen 2, og nøyaktig hvordan elementene dine er beskyttet, helt ned til siste byte.

OPPRETT BRUK KORT SIKKERHET



For MI8OS-appen på iPhone og Android. Oktober 2026.

INNHOLD

# Dette finner du i guiden

01 **KOM I GANG** p. 3
Hva MI8OS er, ordene du møter, appen i korte trekk, hvordan du holder et kort.

02 **OPPRETT ET HVELV** p. 9
Legg til elementer, velg et hvelvpassord, lagre på et kort, skriv reservekortene dine.

03 **BRUK HVELVET DITT** p. 16
Åpne et kort, les og kopier elementer, 2FA-koder, legg til og slett, oppdater kortet.

04 **ADMINISTRER KORTENE DINE** p. 23
Kortene mine, endre navn, identifiser, nullstill, lås og lås opp med et hovedpassord.

05 **INNSTILLINGER** p. 29
Applås, Face ID, utklippstavlen og utseendet.

06 **SLIK ER ELEMENTENE DINE BESKYTTET** p. 32
To lag med kryptering, et ekte eksempel med «12345678», og hvorfor hvelvpassordet ditt betyr noe.

07 **STELL, ANDROID OG HJELP** p. 42
Å ha tre kort, forskjeller på Android, feilsøking.

# 01

# Kom i gang

Fem minutter for å forstå hvordan MI8OS fungerer, før du tar i et kort.

HVA MI8OS ER

# Et lite, kryptert hvelv på et kort du holder i hånden.

MI8OS oppbevarer de viktigste hemmelighetene dine, som gjenopprettingskoder, 2FA-nøkler, seed-fraser og PIN-koder, i et hvelv som krypteres på telefonen din og lagres på et fysisk kort. Ingen konto, ingen sky, ikke noe abonnement.



**Med deg** · det du bruker



**Hjemme** · trygt hjemme



**Et annet sted** · et annet sted

## I SETTET DITT

Tre **MI8OS Cards, gen 2**. Hvert kort rommer opptil **20 elementer**. Skriv det samme hvelvet til alle tre og oppbevar dem på forskjellige steder.

## DETTE TRENGER DU

En iPhone eller Android-telefon med NFC og MI8OS-appen fra App Store eller Google Play (Android-merknader på side 43). Og et hvelvpassord du husker: en lang passordfrase er best.

ORD DU MØTER

# Tre passord, tre forskjellige oppgaver.

Dette er den viktigste siden i guiden. De høres like ut, men hvert av dem beskytter noe forskjellig.

### HVELVPASSORD

Krypterer og åpner elementene på et kort. Påkrevd, minst 12 tegn.

Lagres aldri noe sted. Ingen kan gjenopprette det, ikke engang MI8OS.

### HOVEDPASSORD

Valgfritt. Låser selve kortet, slik at ingen kan nullstille eller slette det uten dette passordet.

Åpner ingenting. For å lese elementene trengs fortsatt hvelvpassordet.

### PIN-KODE FOR APPLÅSEN

Valgfritt. Seks sifre (eller Face ID) for å åpne appen på denne telefonen.

Har ingenting med kortene dine å gjøre og kan ikke dekryptere noe.

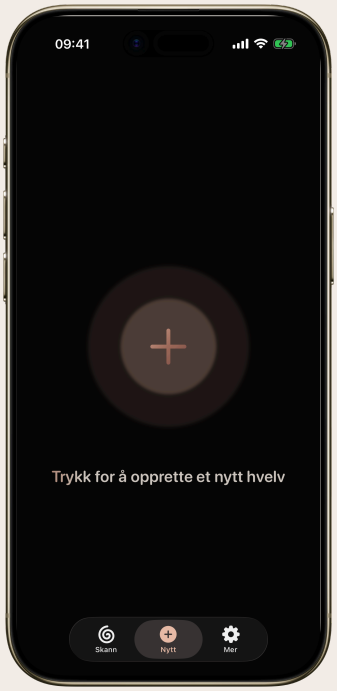
| ORD | BETYDNING |
|---|---|
| **Hvelv** | Listen din med elementer. Den finnes kryptert på kortene dine, og dekryptert bare i appens minne mens den er åpen. |
| **Element** | Én oppføring: et navn (opptil 24 byte) og selve hemmeligheten (opptil 96 byte), for eksempel en PIN-kode, en gjenopprettingskode eller en 2FA-nøkkel. |
| **Kort** | Ditt MI8OS Card gen 2. Det lagrer det krypterte hvelvet; du kan skrive det samme hvelvet til flere kort. |
| **Oppdater kort** | Skriver endringene dine til kortet. Inntil da finnes endringene bare i appens minne. |

APPEN I KORTE TREKK

# Tre faner. Én oppgave hver.




**Skann** · åpne et kort




**Nytt** · opprett et hvelv




**Mer** · kort og innstillinger

1

SKANN

**Trykk for å skanne et kort** og hold kortet mot telefonen. Kortet åpnes i et eget vindu, der du skriver inn hvelvpassordet for kortet.

2

NYTT

**Trykk for å opprette et nytt hvelv.** En veiviser i fire trinn tar deg fra det første elementet til et kort som inneholder det.

3

MER

Kortene dine, applåsen, tidsuret for utklippstavlen, utseendet og de innebygde hjelpesidene.

SLIK HOLDER DU KORTET

# Øverste kant. Flatt. Stille.

Hver gang appen snakker med et kort, viser iPhone sin egen NFC-melding. Deretter:

1. **Hold kortet flatt mot øverste kant** på baksiden av iPhone, der NFC-antennen sitter.
2. **Hold det stille** til appen bekrefter. Skrivingen tar noen sekunder; å flytte kortet for tidlig er den vanligste grunnen til at en skriving må gjentas.
3. Hvis ingenting skjer, flytt kortet sakte litt lavere eller høyere, og ta av tykke deksler eller metalldeksler.

> **Ingen hast.** Når du åpner et kort, klargjør appen først nøkkelen din («Klargjør nøkkelen din. Du trenger ikke å holde kortet ennå»). Hold frem kortet når NFC-meldingen vises.

> **På Android** viser appen sin egen skanneskjerm, og kortet holdes mot øvre halvdel av baksiden på telefonen.



HVA SOM HØRER HJEMME PÅ ET KORT

# Noen få elementer som betyr mye.

MI8OS er ikke ment å erstatte passordbehandleren din. Det er det frakoblede stedet for den håndfullen ting du ville trenge hvis alt annet sviktet.

### PERFEKT PÅ ET KORT

- ✓ Gjenopprettingskoder for e-post og Apple / Google
- ✓ 2FA-oppsettnøkler, slik at appen kan vise kodene dine
- ✓ Gjenopprettingsfraser for krypto (MI8OS er ingen lommebok og har ingen midler)
- ✓ Hovedpassordet til passordbehandleren din eller detaljene i nødsettet
- ✓ Viktige PIN-koder og private notater

### GREIT Å VITE

- ✓ Opptil 20 elementer per kort
- ✓ Navn: opptil 24 byte · element: opptil 96 byte
- ✓ Vanlige bokstaver, sifre og mellomrom bruker 1 byte; bokstaver med aksent, greske eller kyrilliske bokstaver 2; emoji 4
- ✓ Lange seed-fraser kan trenge to elementer (f.eks. ord 1–12 og 13–24)

02

# Opprett et hvelv

Fire trinn: Elementer, Passord, Skriv, Ferdig. Omtrent fem minutter.

TRINN 1 AV 4 · ELEMENTER

# Begynn med elementene dine.

1. Åpne fanen **Nytt** og trykk på knappen **Trykk for å opprette et nytt hvelv**.
2. Trykk på **Legg til element** for hver ting du vil ta vare på.
3. Sveip over et element for å fjerne det igjen før du fortsetter.
4. Trykk på **Fortsett** når listen er klar.

> **Ingenting er lagret ennå.** Elementene dine finnes bare i denne veiviseren til du lagrer det krypterte hvelvet på et kort.

> **Har du allerede et hvelv åpent?** Appen spør først. Hvis du har endringer som ikke er på et kort ennå, tilbyr den å beholde dem.



LEGGE TIL ET ELEMENT

# Et navn, og selve hemmeligheten.

**Navn.** Noe du kjenner igjen, som «Gjenopprettingskoder e-post». Opptil 24 byte; en teller viser hvor mye som er igjen.

**Element.** Passordet, koden eller teksten, opptil 96 byte. Alt du limer inn eller genererer, krypteres før det når et kort.

**Generer.** Trykk på terningen for å lage et tilfeldig passord på 16, 32, 64 eller 96 tegn.




### LAGRE EN 2FA-NØKKEL

Når en tjeneste viser oppsettnøkkelen (eller otpauth://-lenken bak QR-koden), limer du den inn som et element. MI8OS gjenkjenner den og viser senere en **TOTP**-knapp som kopierer gjeldende kode. Hvis lenken er lengre enn 96 byte, limer du bare inn selve oppsettnøkkelen (delen etter secret=); MI8OS bruker da standarden med 6 sifre hvert 30. sekund.

TRINN 2 AV 4 · PASSORD

# Velg hvelvpassordet ditt.

1. Skriv inn hvelvpassordet, og skriv det inn en gang til for å bekrefte.
2. Følg med på styrkemåleren: 12 tegn er minimum, 20 eller en frase med mellomrom gir «Utmerket lengde.»
3. Kryss av i boksen: *«Hvis jeg mister alle kortene eller glemmer dette passordet, kan ikke MI8OS gjenopprette hvelvet på dette kortet.»*
4. Trykk på **Krypter hvelvet**.




## VÅRT RÅD

Bruk **fem eller seks tilfeldige ord**, som *kobber lykt fløyel bane tundra* (men ikke akkurat disse). Lette å huske, ekstremt vanskelige å gjette. Side 40 viser hvorfor.

TRINN 3 AV 4 · SKRIV

# Krypter først. Hold så frem kortet.

**Krypteringen skjer på telefonen, før NFC starter.** Du ser «Forsterker krypteringen din…» et øyeblikk mens appen gjør passordet om til nøkler. Pausen er med vilje: Den gjør det tregt for alle andre å gjette passordet ditt.

Når det står **Kryptering klar**:

1. Trykk på **Lagre på kort**.
2. Hold kortet mot øverste kant av iPhone når NFC-meldingen vises.
3. Hold stille. Appen skriver hvelvet og **leser det deretter tilbake for å kontrollere det**.

> **Tomt kort?** Appen klargjør det automatisk i samme skanning.



TRINN 4 AV 4 · FERDIG

# Skriv nå reservekortene dine.

«Hvelvet er lagret på kortet» betyr at hvelvet er bekreftet på det kortet. **Dette er det eneste øyeblikket appen kan kopiere hele hvelvet ditt til andre kort**, så skriv alle nå:

1. Trykk på **Skriv et kort til**.
2. Velg **Bruk det samme hvelvpassordet** (enklest) eller **Bruk et annet hvelvpassord** for dette kortet.
3. Lagre på neste kort. Gjenta for det tredje.

> **Samme passord, ny kryptering.** Hvert kort får sitt eget tilfeldige salt, så selv med samme passord ser dataene på hvert kort helt forskjellige ut.

**Forkast hvelvet fra denne iPhone-en** lukker bare hvelvet i appens minne. Det sletter aldri et kort.



ET KORT SOM ALLEREDE HAR ET HVELV

# MI8OS overskriver aldri et hvelv uten forvarsel.

Hvis du lagrer et nytt hvelv på et kort som allerede har ett, skrives ingenting. Appen sier: **«Dette kortet har allerede et hvelv»**, og gir deg to valg:

### LEGG TIL ELEMENTER

Legger de nye elementene til i hvelvet på kortet. Elementene som allerede er der, beholdes. Hvelvpassordet ditt må være det dette kortet bruker, og du holder frem kortet en gang til.

### AVBRYT

Lar kortet være nøyaktig som det var.

> **Vil du erstatte hvelvet helt?** Nullstill kortet først (side 26), og opprett deretter det nye hvelvet på det.



# 03

## Bruk hvelvet ditt

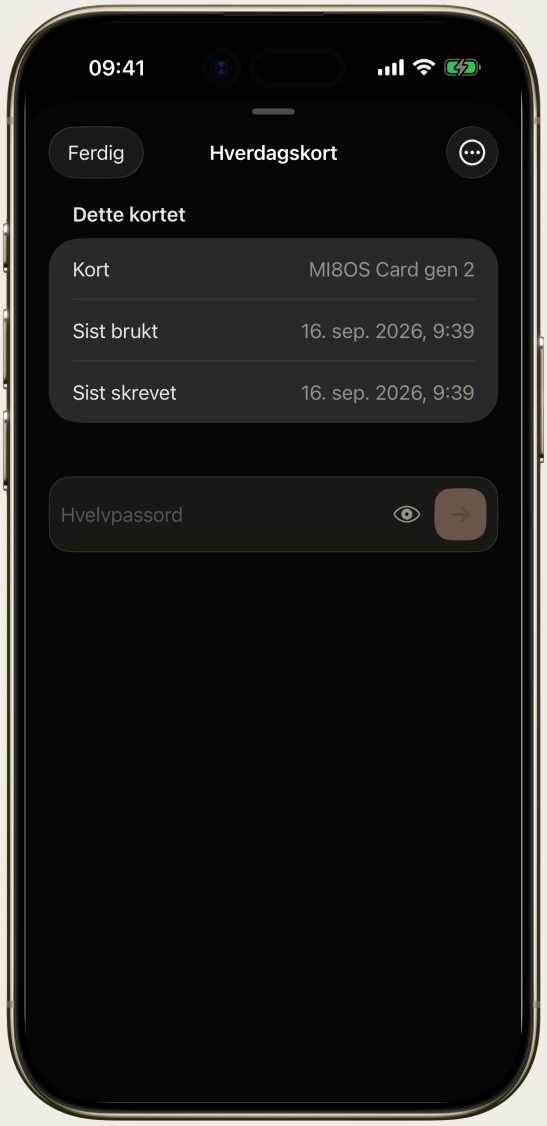
Åpne, lese, kopiere, endre og skrive endringene tilbake til kortet.

ÅPNE ET KORT

# Skann, passord, hold frem igjen.




Fanen Skann




Kortets vindu

1. I **Skann** trykker du på knappen **Trykk for å skanne et kort** og holder frem kortet. Skanningen leser bare kortets offentlige informasjon.
2. Skriv inn kortets **Hvelvpassord** og trykk på **Åpne hvelvet**. Appen klargjør nøkkelen din og ber deretter om kortet en gang til.

INNE I HVELVET

# Elementene dine, så lenge du trenger dem.

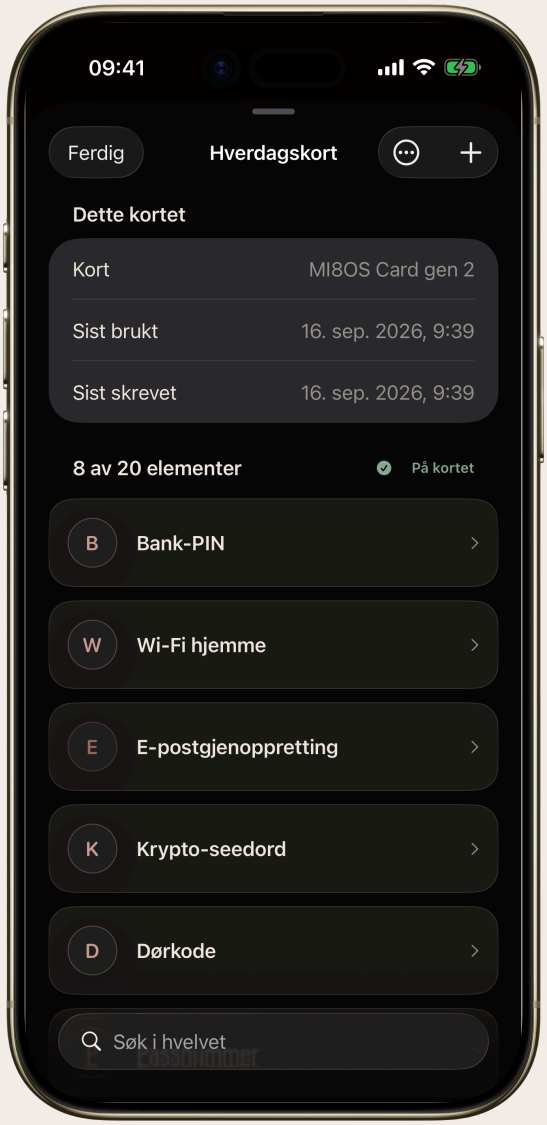
**Dette kortet** viser hvilket kort du åpnet, med Sist brukt og Sist skrevet, og om det har et hovedpassord.

**«8 av 20 elementer»** forteller hvor fullt kortet er. **På kortet** betyr at alt du ser, er lagret på kortet.

**Søk i hvelvet** nederst finner et element etter navn.

**+** øverst legger til et element; **⋯** åpner kortmenyen (side 25).

> **Dekryptert bare i minnet.** Elementene dine finnes i lesbar form bare mens dette vinduet er åpent. Trykk på **Ferdig**, så er de borte fra telefonen.



LES OG KOPIER

# Skjult til du ber om det.

Trykk på et element for å åpne det. Verdien er skjult bak prikker.

**Vis** viser den; **Skjul** skjuler den igjen.

**Kopier** legger den på utklippstavlen, og MI8OS **tømmer utklippstavlen igjen** etter 30 sekunder (endre dette under Mer: 15 sek, 30 sek eller 1 min).

> **Lim inn raskt.** Etter tidsuret er utklippstavlen tom, så elementet blir ikke liggende i andre apper. Tidsuret fortsetter selv om du lukker hvelvet før det er ferdig.

> **Skjermopptak eller skjermspeiling?** MI8OS dekker skjermen og lukker hvelvet, så elementene ikke havner i et opptak.



2FA-KODER

# Autentiseringsappen din, fra kortet.

Hvis et element er en 2FA-oppsettnøkkel, viser siden en **TOTP**-knapp. Trykk på den, så beregner MI8OS gjeldende kode og kopierer den, klar til å limes inn.

Kortet lagrer bare den **krypterte oppsettnøkkelen**. Koden beregnes i appen etter at du har åpnet hvelvet, ut fra nøkkelen og klokkeslettet, akkurat som i en hvilken som helst autentiseringsapp.

### DERFOR HJELPER DET

Hvis autentiseringskodene dine bare ligger på telefonen du mister, forsvinner de med den. Med oppsettnøklene på kortene dine kan du få kodene tilbake på en hvilken som helst ny telefon med MI8OS-appen.



ENDRE HVELVET

# Legg til, slett, og oppdater deretter kortet.

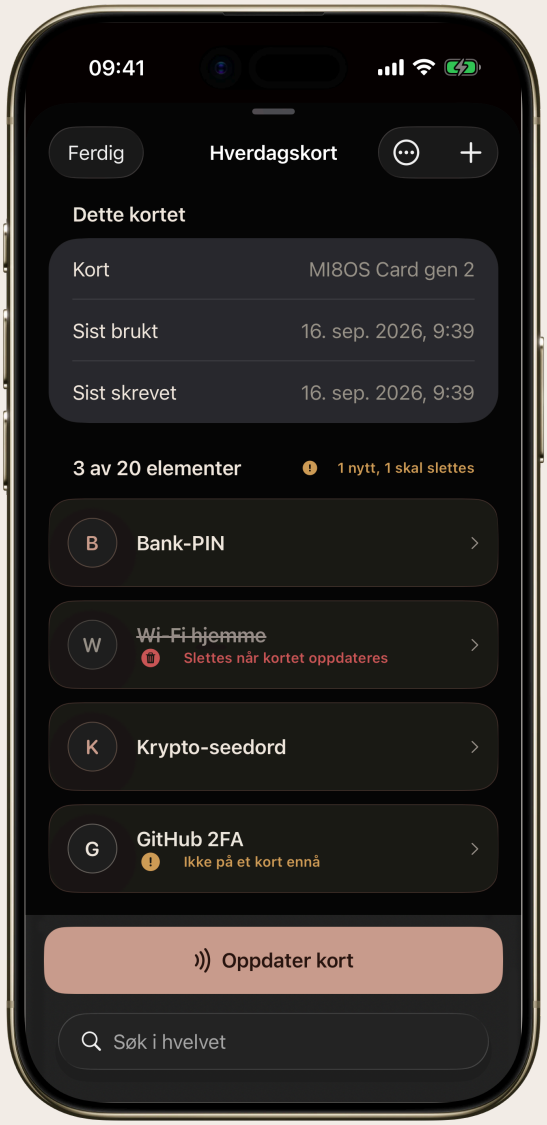
**Legge til:** trykk på **+** og fyll inn navn og element.

**Slette:** sveip et element mot venstre, eller åpne det og trykk på **Slett element**. Det blir stående i listen, merket, til du oppdaterer kortet. Ombestemt deg? Trykk på **Behold**.

**Redigere:** det finnes med vilje ingen redigeringsknapp. For å endre et element sletter du det og legger det til igjen.

Endringer merkes som ikke skrevet ennå. Trykk på **Oppdater kort** og hold frem kortet for å lagre dem.

> **Lukker du med endringer som ikke er skrevet?** Appen advarer deg: «Lukker du dette kortet uten å oppdatere det, går de tapt.»



HOLD HVER KOPI OPPDATERT

# Hvert kort oppdateres for seg.

Oppdater kort skriver til kortet du åpnet, og bare til det. De andre kortene dine har fortsatt forrige versjon til du oppdaterer dem også.

1

ENDRE ETT KORT

Åpne kortet Med deg, legg til eller slett, trykk på **Oppdater kort**.

2

GJENTA FOR DE ANDRE

Åpne kortene Hjemme og Et annet sted og gjør den samme endringen på hvert av dem.

3

SNARVEI FOR NYE ELEMENTER

Opprett et «nytt hvelv» med bare de nye elementene og lagre det på et kort som allerede har hvelvet ditt. Velg **Legg til elementer**, så legges de til det som allerede er der.

GOD VANE

Én gang i året: Åpne hvert kort og kontroller at alle tre viser like mange elementer.

# 04

## Administrer kortene dine

Navn, kortmenyen, nullstilling og det valgfrie hovedpassordet.

KORTENE MINE

# Gi hvert kort et navn.

Under **Mer** → **Kortene mine** ser du kortene denne telefonen kjenner, med en merkelapp: antall elementer, **Tomt** eller **Låst**.

**Legg til kort** skanner et kort og husker det. Det leser bare det som allerede er offentlig på kortet: Du trenger ikke passord, og ingenting skrives.

Trykk på et kort for å åpne det, endre navnet eller nullstille det.

> **Raskere åpning.** Et kort denne telefonen allerede kjenner, åpnes med én enkelt skanning etter at du har skrevet inn passordet.

> **Lagres bare på denne telefonen:** navnene du har gitt, når kortene sist ble brukt, og de offentlige innstillingene deres. Aldri et passord, aldri et element.



KORTMENYEN ···

# Endre navn, identifiser, glem.

### ENDRE NAVN

Et navn du kjenner igjen: «Med deg», «Hjemme», «Foreldrenes safe».

### IDENTIFISER

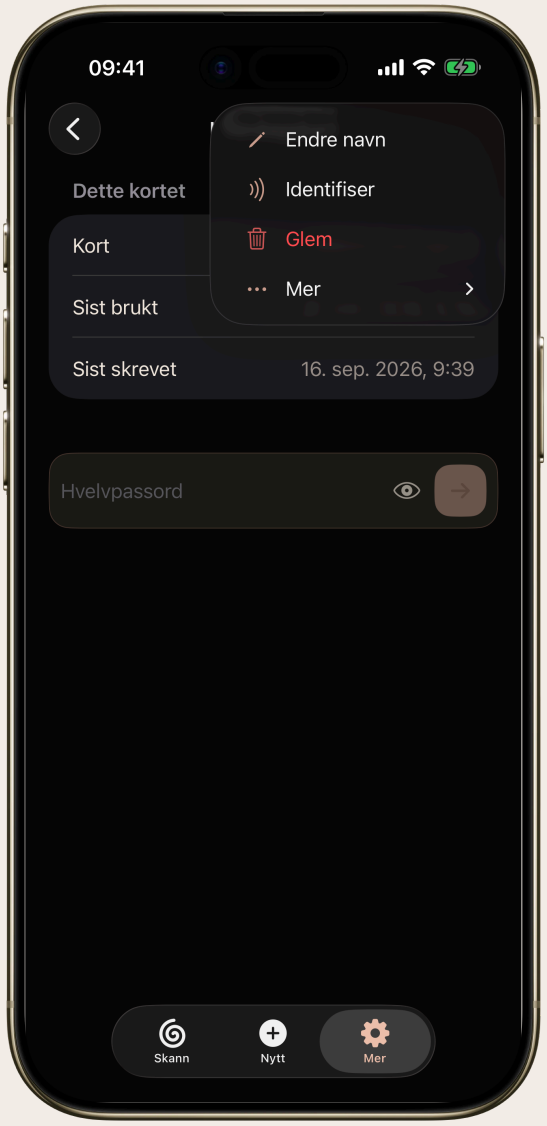
Usikker på hvilket kort som er hvilket? Trykk på Identifiser og hold frem et kort. Appen forteller om det er kortet du ser på, eller hvilket annet kort det er.

### GLEM

Fjerner kortet fra listen på denne telefonen. Ingenting endres på kortet, og du kan legge det til igjen når som helst.

### MER

Nullstill kortet, Lås kortet og Lås opp kortet. Se de neste sidene.



NULLSTILL ET KORT

# Et rent kort, klart for et nytt hvelv.

··· → **Mer** → **Nullstill kortet** fjerner MI8OS-hvelvet og alt annet på kortet, og frigjør all lagringsplassen. Det ber **ikke** om hvelvpassordet.

Bruk det til å:

- ✓ Erstatte et hvelv helt med et nytt
- ✓ Bruke et kort på nytt etter at du har glemt hvelvpassordet (elementene på det går tapt)
- ✓ Tømme et kort før du gir det bort

> **Andre kort berøres ikke.** Å nullstille ett kort påvirker aldri hvelvet på de andre kortene dine.

> **Låst kort?** Det nekter å bli nullstilt til du skriver inn hovedpassordet (neste side).



LÅS ET KORT · HOVEDPASSORD

# Hindre at noen sletter kortet ditt.

Alle som får tak i et ulåst kort, kan nullstille det, selv uten hvelvpassordet ditt. De kan fortsatt ikke lese noe, men de kan slette det.

**Lås kortet** hindrer det. Velg et hovedpassord, hold frem kortet, ferdig. Fra da av kan kortet ikke nullstilles eller slettes uten det, verken av MI8OS eller av noe annet.

1. ··· → **Mer** → **Lås kortet**
2. Skriv inn et hovedpassord to ganger og trykk på **Lås**.
3. Hold kortet til appen bekrefter «Kort låst».

> **Lesing og lagring endres ikke.** Der brukes fortsatt bare hvelvpassordet.



LÅS OPP ET KORT · OG EN ADVARSEL

# Opplåsing gjør kortet normalt igjen.

··· → **Mer** → **Lås opp kortet**, skriv inn hovedpassordet og hold frem kortet. Kortet oppfører seg som et ulåst kort igjen. Hvelvet og hvelvpassordet er uendret.

For å nullstille et låst kort velger du Nullstill kortet: Appen ber om hovedpassordet og formaterer deretter kortet.




### IKKE GLEM DET

Hvis du glemmer hovedpassordet til et kort, kan det kortet **aldri** nullstilles eller brukes på nytt. Elementene kan fortsatt leses med hvelvpassordet. Appen spør etter det hver gang og husker det aldri.

Du kan også låse, låse opp og nullstille et hvilket som helst kort under **Mer** → **Avansert**, ved å skanne det.

# 05

# Innstillinger

Applås, Face ID, utklippstavlen og hvordan appen ser ut.

MER

# Alt annet, på ett sted.

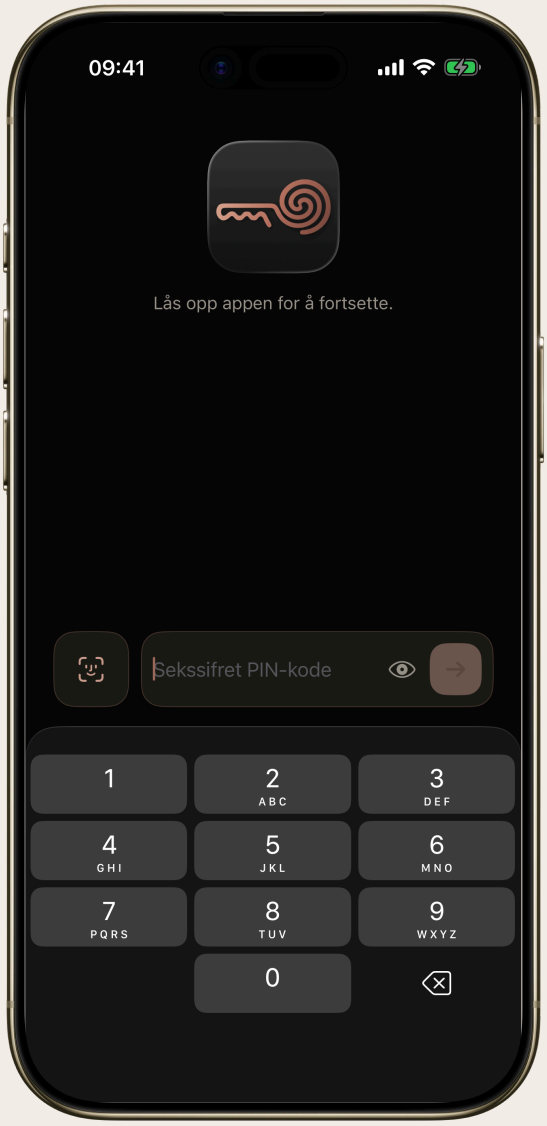
| INNSTILLING | HVA DEN GJØR |
|---|---|
| **Utseende for appen** | System, Lys eller Mørk. |
| **Kortene mine** | Kortene dine med navn (side 24). |
| **Avansert** | Lås, lås opp eller nullstill et hvilket som helst kort ved å skanne det. |
| **Applås** | En PIN-kode og Face ID for appen (neste side). |
| **Tøm utklippstavlen etter** | 15 sek, 30 sek eller 1 min etter at du har kopiert et element. |
| **Kort og sikkerhet** | Innebygd hjelp: Slik fungerer MI8OS Cards, Kryptering og passord, Hvor trygt er MI8OS?, Stell og gjenoppretting av kort. |
| **Støtte og juridisk** | Bestill MI8OS Cards, Personvernerklæring, Bruksvilkår. |



APPLÅS

# En lås for selve appen.




**Slå den på** under Mer → Applås: Velg en sekssifret PIN-kode og, om du vil, Face ID eller Touch ID.

**Lås når jeg går ut av appen:** Umiddelbart, Etter 1 minutt eller Etter 10 minutter. Går du ut av appen lenger, lukkes også et åpent hvelv.

PIN-koden åpner bare appen på denne telefonen. Den kan ikke dekryptere et kort og erstatter ikke et hvelvpassord. Velg seks sifre som ikke også åpner noe annet.

06

# Slik er elementene dine beskyttet

To lag med kryptering, ett ekte eksempel og det ærlige svaret på «hva om noen stjeler kortet mitt?»

HELHETEN

# To lag. Begge kommer fra passordet ditt.

1

### I APPEN: ELEMENTENE FORSEGLES

Før noe sendes til kortet, krypterer appen hvert element på telefonen din med **ChaCha20-Poly1305** og en 256-biters nøkkel laget av hvelvpassordet ditt.

Dette er hovedlåsen. Selv den som har rådataene, ser bare tilfeldig utseende byte, og enhver endring i dem oppdages.

2

### PÅ KORTET: DØREN ER LÅST

Kortets sikre brikke holder de krypterte elementene bak sin egen **AES-128**-nøkkel, også laget av hvelvpassordet ditt. Den gir dem bare fra seg når telefonen har bevist at den kjenner nøkkelen.

Uten riktig passord får en leser ikke annet enn kortets offentlige innstillinger.

**Hvelvpassordet ditt**

lagres aldri noe sted

↓

**Innholdsnøkkel**

256 bit · forsegler elementene (lag 1)

**Kortnøkkel**

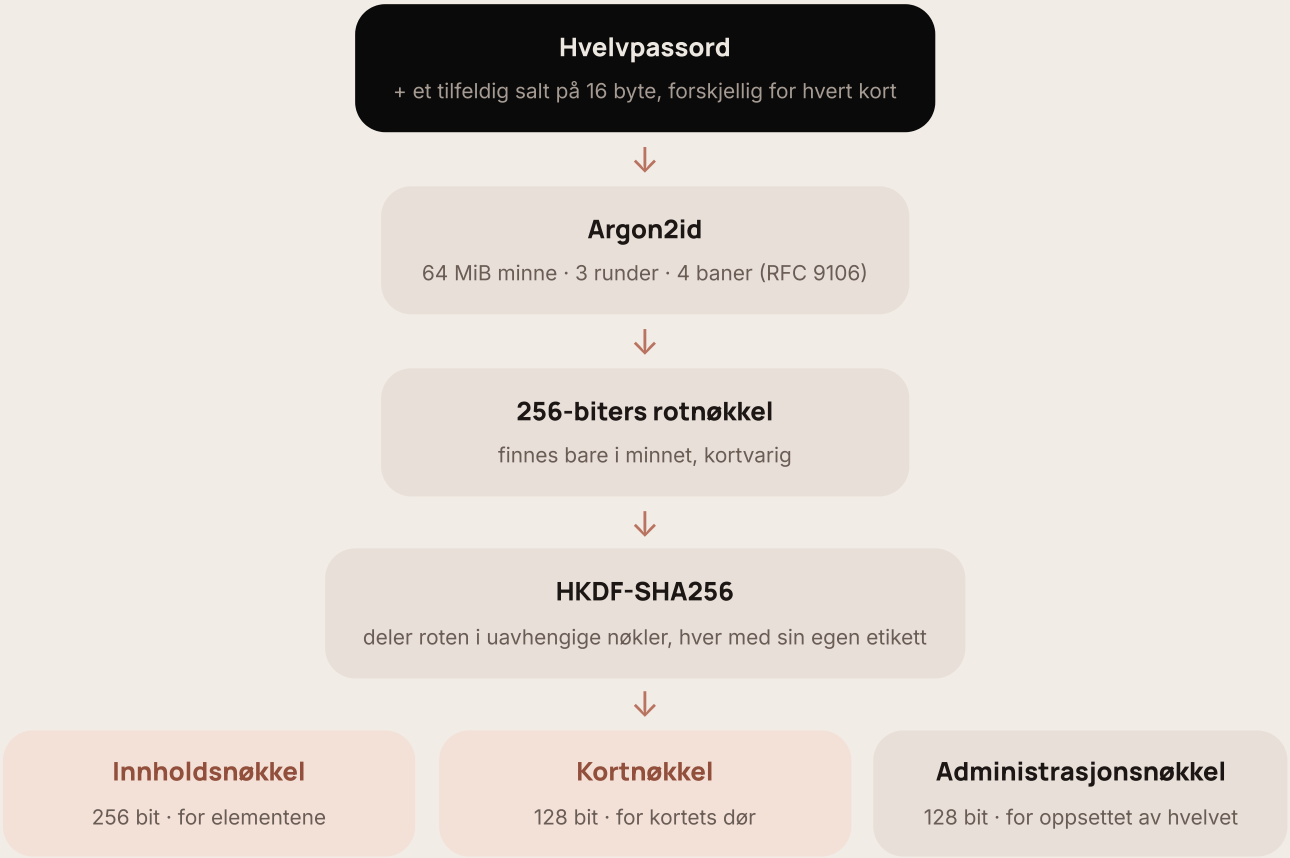
128 bit · åpner kortets dør (lag 2)

**Administrasjonsnøkkel**

128 bit · administrerer hvelvet på kortet

FRA PASSORD TIL NØKLER

# Hvorfor «Forsterker krypteringen din…» tar et øyeblikk.




### ARGON2ID

En bevisst treg og minnekrevende passordfunksjon. Hver eneste gjetning koster 64 MiB minne og reell tid, både på telefonen din og på datamaskinen til en angriper.

### SALTET

Tilfeldige byte som lagres åpent på kortet. De gjør nøklene på hvert kort unike, slik at ingen kan lage en tabell med gjetninger på forhånd.

EKTE EKSEMPEL · 1 AV 4 · NØKLENE

# La oss kryptere «12345678».

Dette er ekte verdier, laget med de samme algoritmene og innstillingene som appen. Passordet er bare for dette eksemplet.

| | |
|---|---|
| **Hvelvpassord** | `copper-lantern-velvet-orbit` |
| **Navn på element** | `Demo PIN` |
| **Element** | `12345678` |
| **Salt (tilfeldig, på kortet)** | `7a8dbeec53e1eb50c70ccd4674a0e624` |
| **Rotnøkkel (Argon2id)** | `84e743792af48790ce3ac4e2410ba1e9ef786851fa74467fc077208674905241` |
| **Innholdsnøkkel · 256 bit** | `dcbe9b90a42a1c5e53f8bdaf07e3d763a61708ae3ad68fdfa7be72792fa6ab7c` |
| **Kortnøkkel · 128 bit** | `266b550b4a87dd1029d53af4262244c1` |
| **Administrasjonsnøkkel · 128 bit** | `d9715ed54fbc71325587258c440a8dc6` |

> **Ingen av disse nøklene lagres noen gang.** Appen beregner dem når du skriver inn passordet, og glemmer dem når hvelvet lukkes. Bare saltet ligger på kortet.

EKTE EKSEMPEL · 2 AV 4 · LAG 1 I APPEN

# Fra «12345678» til tilfeldig utseende byte.

**1. Elementet pakkes** i 20 byte: et navnefelt og et elementfelt.

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

felttype og lengde · «Demo PIN» · "12345678"

**2. ChaCha20-Poly1305 forsegler det** med innholdsnøkkelen, en unik nonce på 12 byte (avledet fra plassens header) og headeren som autentiserte data.

| | |
|---|---|
| **Nonce** | `be00fc197a76fb68b8f315fa` |
| **Chiffertekst · 20 byte** | `5eda3e6b43d7aa61edf77ab4a26ae11e9b080c60` |
| **Tag · 16 byte** | `1b1b0dbbd23c5dffd6f4c462f9a449c4` |

> **Taggen er et segl.** Hvis så mye som én bit i chiffferteksten eller headeren endres, stemmer ikke taggen lenger, og appen avviser dataene i stedet for å vise noe feil.

EKTE EKSEMPEL · 3 AV 4 · HVA SOM LIGGER PÅ KORTET

# Ett element, én plass på 192 byte.

Dette er nøyaktig hva kortet lagrer for «Demo PIN». Se etter «12345678»: Det er ikke der.

```
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
```

header: versjon, element, posisjon (12 byte) · chiffertekst (20 byte) · tag (16 byte) · ledig plass

### BAK KORTETS DØR

Disse plassene ligger i den beskyttede delen av kortet. Kortet gir dem bare fra seg etter at telefonen har bestått kontrollen med kortnøkkelen (lag 2).

### SAMME ELEMENT, ANDRE BYTE

Skriv det samme elementet til et annet kort, så ser det helt annerledes ut, fordi hvert kort har sitt eget salt og sine egne nøkler.

EKTE EKSEMPEL · 4 AV 4 · DEN OFFENTLIGE DELEN

# Dette kan alle med en leser se.

Hvert kort har også et lite offentlig område (128 byte). Det kan leses uten passord, fordi appen trenger saltet for å lage nøklene dine.

```
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» og format · hvelv-ID · kortets oppsett · salt · Argon2id-innstillinger · ubrukt

### OG MED FEIL PASSORD?

Endre bare den siste bokstaven i passordet, så blir kortnøkkelen:

`883e65196d88bc9f1aae79acf8fa7c74`

i stedet for `266b550b4a87dd1029d53af4262244c1`. Ingen likhet. Kortet avviser kontrollen, sender ingen elementer, og ingenting skrives.

HVIS NOEN STJELER KORTET DITT

# De har et kort. Ikke elementene dine.

Det finnes ingen bakdør og ingen hovednøkkel. Den eneste veien inn er å gjette hvelvpassordet ditt, og begge lagene gjør hver gjetning dyr.

**A**

GJETTE VIA KORTET

**Hver gjetning krever det fysiske kortet.** Tyven kjører Argon2id for én gjetning og spør deretter kortet. Kortet svarer på ett forsøk om gangen via NFC. Etter vårt anslag blir det høyst rundt 20 forsøk per sekund.

**B**

TA BRIKKEN FRA HVERANDRE

**Den dyre veien.** Et spesialisert laboratorium kan prøve å hente ut de krypterte plassene direkte fra brikken. Da kan de gjette frakoblet, på mange datamaskiner, men hver gjetning koster fortsatt en full Argon2id-kjøring med 64 MiB minne.

DEN ÆRLIGE KONKLUSJONEN

Begge veiene ender i samme spørsmål: **hvor vanskelig er hvelvpassordet ditt å gjette?** Med et sterkt passord er det praktisk talt utenfor rekkevidde. Med et svakt kjøper de to lagene bare tid. Neste side viser hvor mye.

HVORFOR HVELVPASSORDET DITT BETYR NOE

# Hvor lang tid tar det å prøve alle muligheter?

| TYPE HVELVPASSORD | VIA KORTET ~20 GJETNINGER / S | LABORATORIUM + ENORM DATAPARK 1 000 000 GJETNINGER / S |
|---|---|---|
| **Et hvilket som helst passord i en liste med 1 milliard lekkede passord, f.eks. «Sommer2026!!»** | opptil rundt 2 år; vanlige mye før | opptil rundt 17 minutter; vanlige på sekunder |
| **12 tilfeldige sifre** | rundt 1600 år | rundt 12 dager |
| **4 tilfeldige ord** | millioner av år | rundt 116 år |
| **12 tilfeldige små bokstaver** | over 100 millioner år | rundt 3 000 år |
| **5 tilfeldige ord** | lenger enn universet har eksistert | rundt 900 000 år |
| **6 tilfeldige ord** | lenger enn universet har eksistert | rundt 7 milliarder år |

Verste tilfelle for deg: tiden det tar å prøve alle muligheter. «Tilfeldige ord» betyr valgt med terninger fra en liste på 7 776 ord. Gjettehastighetene er rause anslag til illustrasjon. Til sammenligning: Én gjetning tok rundt 25 ms på en moderne Apple M4-datamaskin med 4 kjerner.

ANBEFALING

**Fem eller seks tilfeldige ord.** Bruk det aldri på nytt, og bruk aldri sangtekster, navn eller datoer.

OG SKRIV DET NED

Oppbevar en kopi på et trygt sted, atskilt fra kortene dine. Et glemt hvelvpassord kan ikke gjenopprettes.

DETTE GJØR MI8OS ALDRI

# Ingenting å hacke i skyen. For det finnes ingen sky.

- ✓ **Ingen konto, ingen server.** Appen oppretter ingen nettverkstilkoblinger i det hele tatt.
- ✓ **Ingen lagrede passord.** Hvelvpassord og hovedpassord lagres aldri, verken på telefonen eller på kortet.
- ✓ **Ingen kopi på telefonen.** Dekrypterte elementer finnes bare i minnet mens et hvelv er åpent. Ett unntak: Et element du har kopiert, blir liggende på utklippstavlen til tidsuret tømmer den (15 sek til 1 min), selv om hvelvet er lukket.
- ✓ **Ingen telemetri.** Ingen sporing, ingen analyse.
- ✓ **Låser når du går ut.** Når du går ut av appen, lukkes hvelvet (umiddelbart eller etter forsinkelsen du har valgt).
- ✓ **Dekker skjermen** i appveksleren og under skjermopptak eller skjermspeiling.
- ✓ **Oppdager manipulering.** Endrede data består ikke seglet og avvises.
- ✓ **Bruker bare åpne standardalgoritmer:** Argon2id, HKDF-SHA256, ChaCha20-Poly1305, AES-128.

BAKSIDEN AV INGEN BAKDØR

Hvis du mister alle kortene, eller glemmer hvelvpassordet, kan ingen få tilbake elementene dine. Ikke du, ikke vi. Derfor har du tre kort og et nedskrevet passord.

STELL OG GJENOPPRETTING AV KORT

# Tre kort, tre steder.

**01**

HOLD DEM ATSKILT

Ett kort hos deg eller i nærheten, ett hjemme, ett et annet sted: hos familie, på jobb eller i en safe. Én brann eller ett innbrudd kan ikke ta alle tre.

**02**

MISTET ET KORT?

Den som finner det, har bare krypterte data. Lag et erstatningskort (se 03) for å komme tilbake til tre kopier. Er du redd for at noen kjenner passordet, oppretter du nye hvelv med et nytt hvelvpassord på samme måte og nullstiller deretter de gamle kortene.

**03**

LAGE ET ERSTATNINGSKORT

Appen kan bare kopiere et hvelv til andre kort rett etter at det er opprettet. For et erstatningskort senere oppretter du et nytt hvelv på et tomt kort og skriver inn de samme elementene igjen: Åpne et kort som fungerer for å lese dem, og hvis du skriver ned noe underveis, makulerer du notatet etterpå. Gjør det før du bare har den siste kopien igjen.

**04**

GLEMT HVELVPASSORDET?

Disse elementene kan ikke gjenopprettes. Hvis et annet kort bruker et passord du fortsatt husker, åpner du det. Ellers nullstiller du kortene og starter et nytt hvelv.

> **Ta vare på kortene** som et bankkort: ingen bøying, ingen varme, ingen skarpe kanter. Hold dem unna metalldeksler når du skanner.

PÅ ANDROID

# Samme app, noen små forskjeller.

Android-appen finnes på **Google Play**. Den fungerer på samme måte og leser de samme kortene. Et hvelv skrevet på iPhone åpnes på Android, og omvendt.

| PÅ ANDROID | DETTE ER FORSKJELLIG |
|---|---|
| **Skanning** | Android har ingen NFC-melding i systemet, så MI8OS viser sin egen skanneskjerm med en avbryt-knapp. |
| **Kortets plassering** | Hold kortet mot øvre halvdel av baksiden på telefonen. Det nøyaktige stedet varierer fra modell til modell. |
| **NFC** | NFC må være slått på i telefonens innstillinger. |
| **Biometri** | Applåsen bruker telefonens fingeravtrykk eller ansiktsopplåsing. |



FEILSØKING

# Hvis noe ikke fungerer.

| DETTE SER DU | DETTE GJØR DU |
|---|---|
| **Kortet blir ikke funnet** | Hold det flatt mot øverste kant av iPhone og hold det stille. Ta av et tykt deksel eller et metalldeksel. Prøv litt høyere eller lavere. |
| **Skrivingen stoppet halvveis** | Trykk på **Prøv på nytt** og hold det samme kortet stille. Hver lagring skriver hele kortet på nytt, og endringene dine blir i appen til det lykkes. Hvis appen sier at lagringen ikke kan fullføres, nullstiller du kortet (side 26) og lagrer på nytt, eller bruker et reservekort og erstatter dette (side 42). |
| **Feil passord** | Kontroller stavemåte og mellomrom. Husk: Hvert kort kan ha sitt eget hvelvpassord. |
| **«Det er et annet kort»** | Du holdt frem et annet kort enn det du åpnet. Bruk Identifiser for å finne det riktige. |
| **Kortet er fullt** | Et kort rommer 20 elementer. Slett ett du ikke lenger trenger, eller fordel elementene på flere kort. |
| **Et kort lar seg ikke nullstille** | Det er låst. Nullstillingen ber om hovedpassordet. |
| **Hvelvet lukket seg selv** | Du gikk ut av appen, eller skjermen ble tatt opp. Åpne kortet igjen. |
| **Pausen «Klargjør nøkkelen din»** | Normalt. Det er den tilsiktede passordforsterkningen fra side 34. |

Mer hjelp: guide.mi8os.com · info@mi8os.com

# MI8OS

Personvernet ditt hører hjemme hos deg.

MI8OS.COM

MI8OS-guiden, norsk bokmål, oktober 2026. Beskriver MI8OS-appen for iPhone og Android. Skjermbildene kan variere noe mellom versjoner. Eksempelnøklene og -bytene i kapittel 06 ble laget for denne guiden med et demopassord; bruk det aldri. MI8OS · info@mi8os.com