MI8OS

LA GUIDA MI8OS · EDIZIONE MOBILE

Tutto sulla tua app e sulle tue carte.

Come creare, aprire e aggiornare una cassaforte, come prenderti cura della tua MI8OS Card gen 2 e come sono protetti i tuoi elementi, fino all'ultimo byte.

CREA · USA · CARTE · SICUREZZA



Scorri per iniziare · iPhone e Android · ottobre 2026

INDICE · TOCCA PER ANDARE

Cosa trovi in questa guida

01 **PRIMI PASSI**
Che cos'è MI8OS, le parole da conoscere, l'app in breve, come tenere una carta. →

02 **CREA UNA CASSAFORTE**
Aggiungi elementi, scegli una password della cassaforte, salva su una carta, scrivi le carte di backup. →

03 **USA LA TUA CASSAFORTE**
Apri una carta, leggi e copia elementi, codici 2FA, aggiungi ed elimina, aggiorna la carta. →

04 **GESTISCI LE TUE CARTE**
Le mie carte, rinomina, identifica, ripristina, blocca e sblocca con una password principale. →

05 **IMPOSTAZIONI**
Blocco dell'app, Face ID, gli appunti e l'aspetto. →

06 **COME SONO PROTETTI I TUOI ELEMENTI**
Due livelli di crittografia, un esempio reale con «12345678» e perché la password della cassaforte è importante. →

07 **CURA, ANDROID E AIUTO**
Tenere tre carte, le differenze su Android, risoluzione dei problemi. →

Leggi da computer o vuoi stampare? Esiste un'edizione A4 con lo stesso contenuto.

01

Primi passi

Cinque minuti per capire come funziona MI8OS, prima di toccare una carta.

01 Che cos'è MI8OS
02 Le parole da conoscere
03 L'app in breve
04 Come tenere la carta
05 Cosa mettere su una carta

CHE COS'È MI8OS

Una piccola cassaforte crittografata, su una carta che tieni tu.

MI8OS conserva i tuoi segreti più importanti, come codici di recupero, chiavi 2FA, frasi seed e PIN, in una cassaforte crittografata sul tuo telefono e salvata su una carta fisica. Nessun account, nessun cloud, nessun abbonamento.



Con te · quella che usi



Casa · al sicuro a casa



Altrove · in un altro luogo

CHE COS'È MI8OS

NEL TUO SET

Tre **MI8OS Cards, gen 2**. Ogni carta contiene fino a **20 elementi**. Scrivi la stessa cassaforte su tutte e tre e tienile in luoghi diversi.

COSA TI SERVE

Un iPhone o un telefono Android con NFC e l'app MI8OS dall'App Store o da Google Play (note su Android). E una password della cassaforte che riesci a ricordare: la cosa migliore è una lunga passphrase.

LE PAROLE DA CONOSCERE

Tre password, tre compiti diversi.

Questa è la pagina più importante della guida. Si somigliano, ma ognuna protegge qualcosa di diverso.

PASSWORD DELLA CASSAFORTE

Crittografa e apre gli elementi di una carta. Obbligatoria, almeno 12 caratteri.

Non viene mai salvata da nessuna parte. Nessuno può recuperarla, nemmeno MI8OS.

LE PAROLE DA CONOSCERE

PASSWORD PRINCIPALE

Facoltativa. Blocca la carta stessa, così nessuno può ripristinarla o cancellarla senza questa password.

Non apre nulla. Per leggere gli elementi serve sempre la password della cassaforte.

PIN DEL BLOCCO DELL'APP

Facoltativo. Sei cifre (o Face ID) per aprire l'app su questo telefono.

Non ha niente a che fare con le tue carte e non può decrittografare nulla.

LE PAROLE DA CONOSCERE

Cassaforte
Il tuo elenco di elementi. Esiste crittografato sulle tue carte, e decrittografato solo nella memoria dell'app mentre è aperta.

Elemento
Una voce: un nome (fino a 24 byte) e il segreto vero e proprio (fino a 96 byte), per esempio un PIN, un codice di recupero o una chiave 2FA.

Carta
La tua MI8OS Card gen 2. Conserva la cassaforte crittografata; puoi scrivere la stessa cassaforte su più carte.

Aggiorna la carta
Scrive le tue modifiche sulla carta. Fino ad allora, le modifiche esistono solo nella memoria dell'app.

L'APP IN BREVE

Tre schede. Un compito ciascuna.



Scansiona · apri una carta



Nuovo · crea una cassaforte



Altro · carte e impostazioni

L'APP IN BREVE

1 **SCANSIONA**

Tocca per scansionare una carta e avvicina la carta al telefono. La carta si apre in una finestra tutta sua, dove inserisci la sua password della cassaforte.

2 **NUOVO**

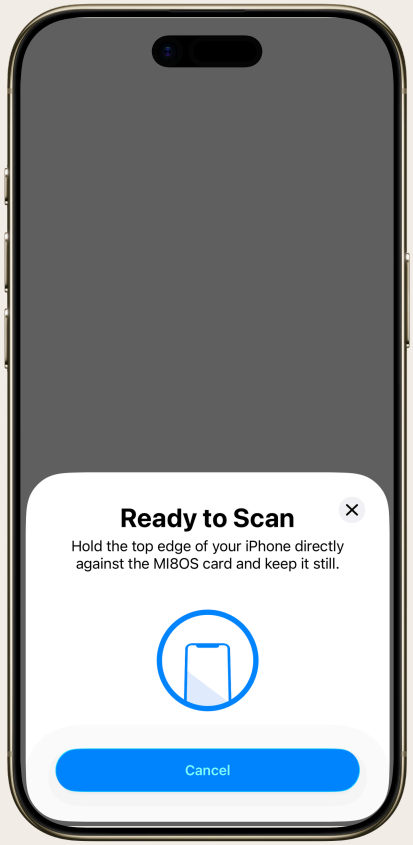
Tocca per creare una nuova cassaforte. Una procedura in quattro passaggi ti porta dal primo elemento a una carta che lo contiene.

3 **ALTRO**

Le tue carte, il Blocco dell'app, il timer degli appunti, l'aspetto e le pagine di aiuto integrate.

COME TENERE LA CARTA

Bordo superiore. Piatta. Ferma.



COME TENERE LA CARTA

Ogni volta che l'app comunica con una carta, l'iPhone mostra la propria finestra NFC. Poi:

1. **Tieni la carta piatta contro il bordo superiore** del retro dell'iPhone, dove si trova l'antenna NFC.
2. **Tienila ferma** finché l'app non conferma. La scrittura richiede qualche secondo; spostare la carta troppo presto è il motivo più comune per cui una scrittura va ripetuta.
3. Se non succede nulla, fai scorrere lentamente la carta un po' più in basso o più in alto, e togli le custodie spesse o di metallo.

> **Nessuna fretta.** Quando apri una carta, l'app prima prepara la tua chiave («Preparazione della chiave. Non serve ancora tenere la carta»). Avvicina la carta quando compare la finestra NFC.

> **Su Android**, l'app mostra una propria schermata di scansione e la carta va appoggiata sulla metà superiore del retro del telefono.

COSA METTERE SU UNA CARTA

Pochi elementi che contano molto.

MI8OS non vuole sostituire il tuo gestore di password. È il posto offline per quella manciata di cose che ti servirebbero se tutto il resto venisse a mancare.

IDEALI SU UNA CARTA

- ✓ Codici di recupero per l'email e per Apple / Google
- ✓ Chiavi di configurazione 2FA, così l'app può mostrarti i codici
- ✓ Frasi di recupero crypto (MI8OS non è un wallet e non custodisce fondi)
- ✓ La password principale del tuo gestore di password o i dati del suo kit di emergenza
- ✓ PIN importanti e note private

COSA METTERE SU UNA CARTA

BUONO A SAPERSI

- ✓ Fino a 20 elementi per carta
- ✓ Nome: fino a 24 byte · elemento: fino a 96 byte
- ✓ Lettere semplici, cifre e spazi occupano 1 byte; lettere accentate, greche o cirilliche 2; le emoji 4
- ✓ Le frasi seed lunghe possono richiedere due elementi (ad es. parole 1–12 e 13–24)

02

Crea una cassaforte

Quattro passaggi: Elementi, Password, Scrittura, Fine. Circa cinque minuti.

01 Passaggio 1 di 4 · Elementi
02 Passaggio 2 di 4 · Password
03 Passaggio 3 di 4 · Scrittura
04 Passaggio 4 di 4 · Fine
05 Una carta che contiene già una cassaforte

PASSAGGIO 1 DI 4 · ELEMENTI

Inizia dai tuoi elementi.



PASSAGGIO 1 DI 4 · ELEMENTI

1. Apri la scheda **Nuovo** e tocca il pulsante **Tocca per creare una nuova cassaforte**.
2. Tocca **Aggiungi elemento** per ogni cosa che vuoi conservare.
3. Scorri su un elemento per toglierlo di nuovo prima di continuare.
4. Tocca **Continua** quando l'elenco è pronto.

> **Non è ancora salvato nulla.** I tuoi elementi restano solo in questa procedura finché non salvi la cassaforte crittografata su una carta.

> **Hai già una cassaforte aperta?** L'app te lo chiede prima. Se hai modifiche che non sono ancora su una carta, ti propone di mantenerle.

AGGIUNGERE UN ELEMENTO

Un nome, e il segreto vero e proprio.



AGGIUNGERE UN ELEMENTO

Nome. Qualcosa che riconoscerai, come «Codici di recupero email». Fino a 24 byte; un contatore mostra quanto spazio resta.

Elemento. La password, il codice o il testo, fino a 96 byte. Tutto ciò che incolli o generi viene crittografato prima di arrivare su una carta.

Genera. Tocca il dado per creare una password casuale di 16, 32, 64 o 96 caratteri.

SALVARE UNA CHIAVE 2FA

Quando un servizio mostra la chiave di configurazione (o il link **otpauth://** dietro il suo codice QR), incollala come elemento. MI8OS la riconosce e poi mostra un pulsante **TOTP** che copia il codice attuale. Se il link supera i 96 byte, incolla solo la chiave di configurazione (la parte dopo **secret=**); MI8OS usa allora lo standard di 6 cifre ogni 30 secondi.

PASSAGGIO 2 DI 4 · PASSWORD

Scegli la password della cassaforte.



PASSAGGIO 2 DI 4 · PASSWORD

1. Digita la password della cassaforte, poi digitala di nuovo per confermarla.
2. Guarda la barra di robustezza: 12 caratteri sono il minimo, 20 o una frase con spazi danno «Lunghezza eccellente.»
3. Spunta la casella: *«Se perdo tutte le carte o dimentico questa password, MI8OS non può recuperare la cassaforte di questa carta.»*
4. Tocca **Crittografa la cassaforte**.

IL NOSTRO CONSIGLIO

Usa **cinque o sei parole casuali**, come *rame lanterna velluto orbita tundra* (ma non queste). Facili da ricordare, estremamente difficili da indovinare. **Ecco perché**.

PASSAGGIO 3 DI 4 · SCRITTURA

Prima crittografa. Poi avvicina la carta.



PASSAGGIO 3 DI 4 · SCRITTURA

La crittografia avviene sul tuo telefono, prima che parta l'NFC. Per un momento vedi «Rafforzamento della crittografia…» mentre l'app trasforma la tua password in chiavi. Quella pausa è voluta: rende lento indovinare la tua password per chiunque altro.

Quando compare **Crittografia pronta**:

1. Tocca **Salva sulla carta**.
2. Tieni la carta contro il bordo superiore dell'iPhone quando compare la finestra NFC.
3. Resta fermo. L'app scrive la cassaforte, poi **la rilegge per verificarla**.

> **Carta vuota?** L'app la prepara automaticamente nella stessa scansione.

PASSAGGIO 4 DI 4 · FINE

Ora scrivi le tue carte di backup.



PASSAGGIO 4 DI 4 · FINE

«Cassaforte salvata sulla carta» significa che la cassaforte è verificata su quella carta. **È l'unico momento in cui l'app può copiare l'intera cassaforte su altre carte**, quindi scrivile tutte adesso:

1. Tocca **Scrivi un'altra carta**.
2. Scegli **Usa la stessa password della cassaforte** (più semplice) oppure **Usa una password della cassaforte diversa** per questa carta.
3. Salva sulla carta successiva. Ripeti per la terza.

> **Stessa password, nuova crittografia.** Ogni carta riceve un proprio salt casuale, quindi anche con la stessa password i dati di ogni carta sono completamente diversi.

Rimuovi la cassaforte da questo iPhone chiude solo la cassaforte nella memoria dell'app. Non cancella mai una carta.

UNA CARTA CHE CONTIENE GIÀ UNA CASSAFORTE

MI8OS non sovrascrive mai una cassaforte di sorpresa.



UNA CARTA CHE CONTIENE GIÀ UNA CASSAFORTE

Se salvi una nuova cassaforte su una carta che ne contiene già una, non viene scritto nulla. L'app ti avvisa: **«Questa carta contiene già una cassaforte»**, e ti offre due scelte:

AGGIUNGI ELEMENTI

Aggiunge i nuovi elementi alla cassaforte della carta. Gli elementi già presenti vengono mantenuti. La tua password della cassaforte deve essere quella usata da questa carta, e avvicini la carta ancora una volta.

ANNULLA

Lascia la carta esattamente com'era.

> **Vuoi sostituire completamente la cassaforte?** Prima **ripristina la carta**, poi crea la nuova cassaforte sulla carta.

03

Usa la tua cassaforte

Apri, leggi, copia, modifica e riscrivi le modifiche sulla carta.

01 Aprire una carta
02 Dentro la cassaforte
03 Leggere e copiare
04 Codici 2FA
05 Modificare la cassaforte
06 Tieni aggiornata ogni copia

APRIRE UNA CARTA

Scansione, password, di nuovo la carta.



Scheda Scansiona



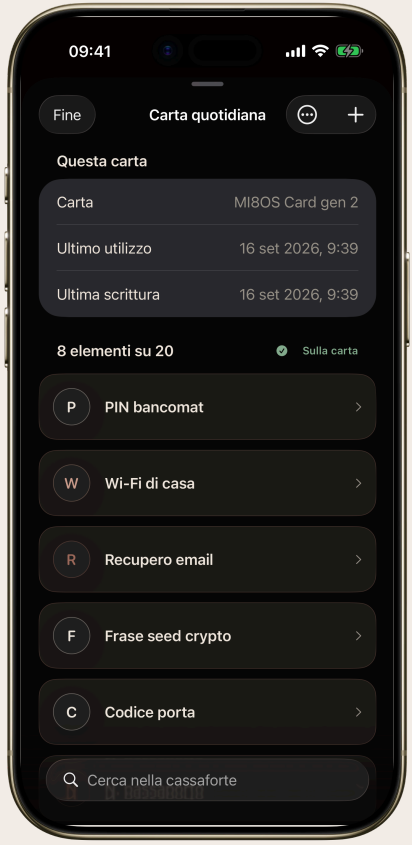
La finestra della carta

APRIRE UNA CARTA

1. In **Scansiona**, tocca il pulsante **Tocca per scansionare una carta** e avvicina la carta. La scansione legge solo le informazioni pubbliche della carta.
2. Inserisci la **Password della cassaforte** della carta e tocca **Apri la cassaforte**. L'app prepara la tua chiave, poi ti chiede la carta ancora una volta.

DENTRO LA CASSAFORTE

I tuoi elementi, per tutto il tempo che ti servono.



DENTRO LA CASSAFORTE

Questa carta mostra quale carta hai aperto, con ultimo utilizzo e ultima scrittura, e se ha una password principale.

«8 elementi su 20» indica quanto è piena la carta. **Sulla carta** significa che tutto ciò che vedi è salvato sulla carta.

Cerca nella cassaforte, in basso, trova un elemento per nome.

+ in alto aggiunge un elemento; ··· apre il **menu della carta**.

> **Decrittografati solo in memoria.** I tuoi elementi esistono in forma leggibile solo finché questa finestra è aperta. Tocca **Fine** e spariscono dal telefono.

LEGGERE E COPIARE

Nascosto finché non lo chiedi.



LEGGERE E COPIARE

Tocca un elemento per aprirlo. Il valore è nascosto dietro dei puntini.

Mostra lo visualizza; **Nascondi** lo nasconde di nuovo.

Copia lo mette negli appunti, e MI8OS **svuota di nuovo gli appunti** dopo 30 secondi (puoi cambiarlo in Altro: 15 sec, 30 sec o 1 min).

> **Incolla in fretta.** Allo scadere del timer gli appunti sono vuoti, così l'elemento non resta in giro in altre app. Il timer continua anche se chiudi la cassaforte prima della fine.

> **Registrazione o duplicazione dello schermo?** MI8OS copre lo schermo e chiude la cassaforte, così gli elementi non finiscono in una registrazione.

CODICI 2FA

Il tuo autenticatore, dalla carta.



CODICI 2FA

Se un elemento è una chiave di configurazione 2FA, la sua pagina mostra un pulsante **TOTP**. Toccalo e MI8OS calcola il codice attuale e lo copia, pronto da incollare.

La carta conserva solo la **chiave di configurazione crittografata**. Il codice viene calcolato nell'app dopo che hai aperto la cassaforte, a partire dalla chiave e dall'ora attuale, proprio come in qualsiasi app di autenticazione.

PERCHÉ È UTILE

Se i tuoi codici di autenticazione sono salvati solo sul telefono che perdi, se ne vanno con lui. Con le chiavi di configurazione sulle tue carte, puoi riavere i codici su qualsiasi nuovo telefono con l'app MI8OS.

MODIFICARE LA CASSAFORTE

Aggiungi, elimina, poi aggiorna la carta.



MODIFICARE LA CASSAFORTE

Aggiungere: tocca **+** e compila nome ed elemento.

Eliminare: scorri un elemento verso sinistra, oppure aprilo e tocca **Elimina elemento**. Resta nell'elenco, contrassegnato, finché non aggiorni la carta. Hai cambiato idea? Tocca **Mantieni**.

Modificare: di proposito non c'è un pulsante di modifica. Per cambiare un elemento, eliminalo e aggiungilo di nuovo.

Le modifiche sono contrassegnate come non ancora scritte. Tocca **Aggiorna la carta** e avvicina la carta per salvarle.

> **Chiudi con modifiche non scritte?** L'app ti avvisa: «Chiudere questa carta senza aggiornarla le farà perdere.»

TIENI AGGIORNATA OGNI COPIA

Ogni carta si aggiorna per conto suo.

Aggiorna la carta scrive sulla carta che hai aperto, e solo su quella. Le altre carte contengono ancora la versione precedente finché non aggiorni anche loro.

BUONA ABITUDINE

Una volta all’anno, apri ogni carta e controlla che tutte e tre mostrino lo stesso numero di elementi.

TIENI AGGIORNATA OGNI COPIA

1 MODIFICA UNA CARTA

Apri la carta Con te, aggiungi o elimina, tocca **Aggiorna la carta**.

2 RIPETI PER LE ALTRE

Apri le carte Casa e Altrove e fai la stessa modifica su ciascuna.

3 SCORCIATOIA PER I NUOVI ELEMENTI

Crea una «nuova cassaforte» con solo i nuovi elementi e salvala su una carta che contiene già la tua cassaforte. Scegli **Aggiungi elementi**, e vengono aggiunti a quelli presenti.

04

Gestisci le tue carte

I nomi, il menu della carta, il ripristino e la password principale facoltativa.

01 Le mie carte
02 Il menu della carta ···
03 Ripristinare una carta
04 Bloccare una carta · password principale
05 Sbloccare una carta · e un avvertimento

LE MIE CARTE

Dai un nome a ogni carta.



LE MIE CARTE

In **Altro** → **Le mie carte** vedi le carte che questo telefono conosce, con un'etichetta: il numero di elementi, **Vuota** o **Bloccata**.

Aggiungi una carta scansiona una carta e la memorizza. Legge solo ciò che è già pubblico sulla carta: nessuna password richiesta, nulla viene scritto.

Tocca una carta per aprirla, rinominarla o ripristinarla.

> **Apertura più rapida.** Una carta che questo telefono conosce già si apre con una sola scansione dopo che hai inserito la password.

> **Salvato solo su questo telefono:** i nomi che hai dato, quando le carte sono state usate l'ultima volta e le loro impostazioni pubbliche. Mai una password, mai un elemento.

IL MENU DELLA CARTA ···

Rinomina, identifica, rimuovi.



IL MENU DELLA CARTA ···

RINOMINA

Un nome che riconoscerai: «Con te», «Casa», «Cassaforte dei genitori».

IDENTIFICA

Non sai più quale carta è quale? Tocca Identifica e avvicina una carta. L'app ti dice se è quella che stai guardando, o quale altra carta è.

RIMUOVI

Toglie la carta dall'elenco di questo telefono. Sulla carta non cambia nulla, e puoi aggiungerla di nuovo in qualsiasi momento.

ALTRO

Ripristina la carta, Blocca la carta e Sblocca la carta. Vedi le pagine seguenti.

RIPRISTINARE UNA CARTA

Una carta pulita, pronta per una nuova cassaforte.



RIPRISTINARE UNA CARTA

··· → **Altro** → **Ripristina la carta** rimuove la cassaforte MI8OS e tutto il resto dalla carta, e libera tutta la sua memoria. **Non** chiede la password della cassaforte.

Usalo per:

- ✓ Sostituire completamente una cassaforte con una nuova
- ✓ Riutilizzare una carta dopo averne dimenticato la password della cassaforte (i suoi elementi vanno persi)
- ✓ Svuotare una carta prima di darla via

> **Le altre carte restano intatte.** Ripristinare una carta non tocca mai la cassaforte sulle altre carte.

> **Carta bloccata?** Rifiuta il ripristino finché non inserisci la sua password principale (pagina seguente).

BLOCCARE UNA CARTA · PASSWORD PRINCIPALE

Impedisci a chiunque di cancellare la tua carta.



BLOCCARE UNA CARTA · PASSWORD PRINCIPALE

Chiunque prenda una carta non bloccata può ripristinarla, anche senza la tua password della cassaforte. Non può comunque leggere nulla, ma potrebbe cancellarla.

Blocca la carta lo impedisce. Scegli una password principale, avvicina la carta, fatto. Da quel momento la carta non può essere ripristinata o cancellata senza di essa, né da MI8OS né da nient'altro.

1. ··· → **Altro** → **Blocca la carta**
2. Inserisci due volte una password principale e tocca **Blocca**.
3. Tieni la carta finché l'app non conferma «Carta bloccata».

> **Lettura e salvataggio non cambiano.** Usano sempre e solo la password della cassaforte.

SBLOCCARE UNA CARTA · E UN AVVERTIMENTO

Lo sblocco riporta la carta alla normalità.



SBLOCCARE UNA CARTA · E UN AVVERTIMENTO

··· → **Altro** → **Sblocca la carta**, inserisci la password principale e avvicina la carta. La carta torna a comportarsi come una carta non bloccata. La sua cassaforte e la sua password della cassaforte restano invariate.

Per ripristinare una carta bloccata, scegli Ripristina la carta: l'app chiede la password principale, poi formatta la carta.

NON DIMENTICARLA

Se dimentichi la password principale di una carta, quella carta non potrà **mai** essere ripristinata o riutilizzata. I suoi elementi restano leggibili con la password della cassaforte. L'app la chiede ogni volta e non la memorizza mai.

Puoi anche bloccare, sbloccare e ripristinare qualsiasi carta da **Altro** → **Avanzate**, scansionandola.

05

Impostazioni

Blocco dell’app, Face ID, gli appunti e l’aspetto dell’app.

01 Altro
02 Blocco dell’app

ALTRO

Tutto il resto, in un unico posto.



ALTRO

Aspetto dell’app
Sistema, Chiaro o Scuro.

Le mie carte
Le tue carte con nome.

Avanzate
Blocca, sblocca o ripristina qualsiasi carta scansionandola.

Blocco dell’app
Un PIN e Face ID per l’app (pagina seguente).

Svuota gli appunti dopo
15 sec, 30 sec o 1 min dopo che hai copiato un elemento.

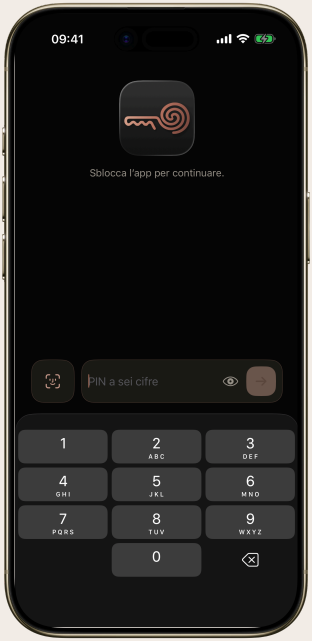
Carte e sicurezza
Aiuto integrato: Come funzionano le MI8OS Cards, Crittografia e password, Quanto è sicuro MI8OS?, Cura e recupero delle carte.

Supporto e note legali
Ordina MI8OS Cards, Informativa sulla privacy, Condizioni d’uso.

BLOCCO DELL’APP

Un blocco per l’app stessa.





BLOCCO DELL'APP

Attivalo in Altro → Blocco dell'app: scegli un PIN a sei cifre e, se vuoi, Face ID o Touch ID.

Blocca quando esco: Immediatamente, Dopo 1 minuto o Dopo 10 minuti. Se lasci l'app più a lungo, si chiude anche qualsiasi cassaforte aperta.

Il PIN apre solo l'app su questo telefono. Non può decrittografare una carta e non sostituisce una password della cassaforte. Scegli sei cifre che non aprano anche qualcos'altro.

06

Come sono protetti i tuoi elementi

Due livelli di crittografia, un esempio reale e la risposta onesta a «e se qualcuno mi ruba la carta?»

01 Il quadro generale
02 Dalla password alle chiavi
03 Esempio reale · 1 di 4 · Le chiavi
04 Se qualcuno ti ruba la carta
05 Perché la password della cassaforte è importante
06 Cosa MI8OS non fa mai

IL QUADRO GENERALE

Due livelli. Entrambi nascono dalla tua password.

1

NELL'APP: GLI ELEMENTI VENGONO SIGILLATI

Prima che qualsiasi cosa venga inviata alla carta, l'app crittografa ogni elemento sul tuo telefono con **ChaCha20-Poly1305** e una chiave a 256 bit ricavata dalla tua password della cassaforte.

Questa è la serratura principale. Anche chi ha in mano i dati grezzi vede solo byte dall'aspetto casuale, e qualsiasi modifica viene rilevata.

IL QUADRO GENERALE

2

SULLA CARTA: LA PORTA È CHIUSA A CHIAVE

Il chip sicuro della carta custodisce gli elementi crittografati dietro una propria chiave **AES-128**, anch'essa ricavata dalla tua password della cassaforte. Li consegna solo dopo che il telefono ha dimostrato di conoscere quella chiave.

Senza la password giusta, un lettore non ottiene altro che le impostazioni pubbliche della carta.

La tua password della cassaforte
mai salvata da nessuna parte

↓

Chiave dei contenuti
256 bit · sigilla gli elementi (livello 1)

Chiave della carta
128 bit · apre la porta della carta (livello 2)

Chiave di gestione
128 bit · gestisce la cassaforte sulla carta

DALLA PASSWORD ALLE CHIAVI

Perché «Rafforzamento della crittografia...» richiede un momento.

Password della cassaforte
+ un salt casuale di 16 byte, diverso per ogni carta

↓

Argon2id
64 MiB di memoria · 3 passaggi · 4 corsie (RFC 9106)

↓

Chiave radice a 256 bit
esiste solo in memoria, per poco

↓

HKDF-SHA256
divide la radice in chiavi indipendenti, ognuna con la propria etichetta

↓

Chiave dei contenuti
256 bit · per gli elementi

Chiave della carta
128 bit · per la porta della carta

Chiave di gestione
128 bit · per la configurazione della cassaforte

DALLA PASSWORD ALLE CHIAVI

ARGON2ID

Una funzione per password volutamente lenta e affamata di memoria. Ogni singolo tentativo costa 64 MiB di memoria e tempo reale, sul tuo telefono come sul computer di un attaccante.

IL SALT

Byte casuali salvati in chiaro sulla carta. Rendono uniche le chiavi di ogni carta, così nessuno può preparare in anticipo una tabella di tentativi.

ESEMPIO REALE · 1 DI 4 · LE CHIAVI

Crittografiamo «12345678».

Sono valori reali, prodotti con gli stessi algoritmi e le stesse impostazioni dell'app. La password serve solo per questo esempio.

PASSWORD DELLA CASSAFORTE

`copper-lantern-velvet-orbit`

NOME DELL'ELEMENTO

`Demo PIN`

ELEMENTO

`12345678`

SALT (CASUALE, SULLA CARTA)

`7a8dbeec53e1eb50c70ccd4674a0e624`

ESEMPIO REALE · 1 DI 4 · LE CHIAVI

CHIAVE RADICE (ARGON2ID)

84e743792af48790ce3ac4e2410ba1e9ef786851fa74467fc077208674905241

CHIAVE DEI CONTENUTI · 256 BIT

dcbe9b90a42a1c5e53f8bdaf07e3d763a61708ae3ad68fdfa7be72792fa6ab7c

CHIAVE DELLA CARTA · 128 BIT

266b550b4a87dd1029d53af4262244c1

CHIAVE DI GESTIONE · 128 BIT

d9715ed54fbc71325587258c440a8dc6

> **Nessuna di queste chiavi viene mai salvata.** L'app le calcola quando inserisci la password e le dimentica quando la cassaforte si chiude. Sulla carta c'è solo il salt.

ESEMPIO REALE · 2 DI 4 · LIVELLO 1 NELL'APP

Da «12345678» a byte dall'aspetto casuale.

1. L'elemento viene impacchettato in 20 byte: un campo nome e un campo elemento.

```
000  01 08 44 65 6d 6f 20 50 49 4e
010  02 08 31 32 33 34 35 36 37 38
```

tipo e lunghezza del campo · «Demo PIN» · "12345678"

ESEMPIO REALE · 2 DI 4 · LIVELLO 1 NELL'APP

2. ChaCha20-Poly1305 lo sigilla con la chiave dei contenuti, un nonce unico di 12 byte (ricavato dall'intestazione dello slot) e l'intestazione come dati autenticati.

NONCE

`be00fc197a76fb68b8f315fa`

TESTO CIFRATO · 20 BYTE

`5eda3e6b43d7aa61edf77ab4a26ae11e9b080c60`

TAG · 16 BYTE

`1b1b0dbbd23c5dffd6f4c462f9a449c4`

> **Il tag è un sigillo.** Se cambia anche un solo bit del testo cifrato o della sua intestazione, il tag non corrisponde più e l'app rifiuta i dati invece di mostrare qualcosa di sbagliato.

ESEMPIO REALE · 3 DI 4 · COSA C'È SULLA CARTA

Un elemento, uno slot da 192 byte.

Ecco esattamente ciò che la carta conserva per «Demo PIN». Cerca «12345678»: non c'è.

```
000  31 0d ce db 3c 00 01 00 01 00 01 14
012  5e da 3e 6b 43 d7 aa 61 ed f7 7a b4
024  a2 6a e1 1e 9b 08 0c 60 1b 1b 0d bb
036  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
060  00 00 00 00 00 00 00 00 00 00 00 00
072  00 00 00 00 00 00 00 00 00 00 00 00
084  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
108  00 00 00 00 00 00 00 00 00 00 00 00
120  00 00 00 00 00 00 00 00 00 00 00 00
132  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
156  00 00 00 00 00 00 00 00 00 00 00 00
168  00 00 00 00 00 00 00 00 00 00 00 00
180  00 00 00 00 00 00 00 00 00 00 00 00
```

intestazione: versione, elemento, posizione (12 byte)

testo cifrato (20 byte) tag (16 byte) spazio vuoto

ESEMPIO REALE · 3 DI 4 · COSA C'È SULLA CARTA

DIETRO LA PORTA DELLA CARTA

Questi slot si trovano nella parte protetta della carta. La carta li consegna solo dopo che il telefono ha superato la verifica con la chiave della carta (livello 2).

STESSO ELEMENTO, BYTE DIVERSI

Scrivi lo stesso elemento su un'altra carta e avrà un aspetto completamente diverso, perché ogni carta ha il proprio salt e le proprie chiavi.

ESEMPIO REALE · 4 DI 4 · LA PARTE PUBBLICA

Cosa può vedere chiunque abbia un lettore.

Ogni carta ha anche una piccola area pubblica (128 byte). È leggibile senza password, perché l'app ha bisogno del salt per creare le tue chiavi.

```
000  4d 49 38 4f 53 03 32 b3 fb 93 6e bf
012  4d 64 b7 6f 5e 90 f5 75 7f 6e 00 00
024  01 00 c0 00 27 10 7a 8d be ec 53 e1
036  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
060  00 00 00 00 00 00 00 00 00 00 00 00
072  00 00 00 00 00 00 00 00 00 00 00 00
084  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
108  00 00 00 00 00 00 00 00 00 00 00 00
120  00 00 00 00 00 00 00 00
```

- «MI8OS» e formato
- ID della cassaforte
- struttura della carta
- salt
- impostazioni Argon2id
- non usato

ESEMPIO REALE · 4 DI 4 · LA PARTE PUBBLICA

E CON UNA PASSWORD SBAGLIATA?

Cambia solo l'ultima lettera della password e la chiave della carta diventa:

`883e65196d88bc9f1aae79acf8fa7c74`

invece di `266b550b4a87dd1029d53af4262244c1`. Nessuna somiglianza. La carta rifiuta la verifica, non invia alcun elemento e non viene scritto nulla.

SE QUALCUNO TI RUBA LA CARTA

Ha una carta. Non i tuoi elementi.

Non esiste una backdoor né un passe-partout. L'unico modo per entrare è indovinare la tua password della cassaforte, ed entrambi i livelli rendono costoso ogni tentativo.

A

INDOVINARE PASSANDO DALLA CARTA

Ogni tentativo richiede la carta fisica. Il ladro esegue Argon2id per un tentativo, poi interroga la carta. La carta risponde a un tentativo alla volta tramite NFC. Secondo la nostra stima sono al massimo circa 20 tentativi al secondo.

SE QUALCUNO TI RUBA LA CARTA

B SMONTARE IL CHIP

La via costosa. Un laboratorio specializzato potrebbe provare a estrarre gli slot crittografati direttamente dal chip. A quel punto può tentare offline, su molti computer, ma ogni tentativo costa comunque un'esecuzione completa di Argon2id con 64 MiB di memoria.

IL BILANCIO ONESTO

Entrambe le strade portano alla stessa domanda: **quanto è difficile indovinare la tua password della cassaforte?** Con una password robusta, indovinarla è praticamente fuori portata. Con una debole, i due livelli fanno solo guadagnare tempo. La pagina seguente mostra quanto.

PERCHÉ LA PASSWORD DELLA CASSAFORTE È IMPORTANTE

Quanto ci vuole a provare ogni possibilità?

TRAMITE LA CARTA	LABORATORIO + ENORME
~20 tentativi / s	parco di computer 1.000.000 tentativi / s
Qualsiasi password presente in un elenco di 1 miliardo di password trapelate, ad es. «Estate2026!!»	
fino a circa 2 anni; quelle comuni molto prima	fino a circa 17 minuti; quelle comuni in pochi secondi
12 cifre casuali	
circa 1.600 anni	circa 12 giorni
4 parole casuali	
milioni di anni	circa 116 anni

PERCHÉ LA PASSWORD DELLA CASSAFORTE È IMPORTANTE

TRAMITE LA CARTA ~20 tentativi / s	LABORATORIO + ENORME parco di computer 1.000.000 tentativi / s
12 lettere minuscole casuali	
oltre 100 milioni di anni	circa 3.000 anni
5 parole casuali	
più a lungo di quanto esista l'universo	circa 900.000 anni
6 parole casuali	
più a lungo di quanto esista l'universo	circa 7 miliardi di anni

Il caso peggiore per te: il tempo per provare ogni possibilità. «Parole casuali» significa estratte con i dadi da un elenco di 7.776 parole. Le velocità di tentativo sono stime generose, a scopo illustrativo. Per avere un'idea: un tentativo ha richiesto circa 25 ms su un moderno computer Apple M4 con 4 core.

PERCHÉ LA PASSWORD DELLA CASSAFORTE È IMPORTANTE

RACCOMANDAZIONE

Cinque o sei parole casuali. Non riutilizzarla mai, non usare mai testi di canzoni, nomi o date.

E SCRIVILA

Conservane una copia in un posto sicuro e separato dalle tue carte. Una password della cassaforte dimenticata non si può recuperare.

COSA MI8OS NON FA MAI

Niente da violare nel cloud. Perché il cloud non c'è.

- ✓ **Nessun account, nessun server.** L'app non effettua alcuna connessione di rete.
- ✓ **Nessuna password salvata.** Le password della cassaforte e le password principali non vengono mai salvate, né sul telefono né sulla carta.
- ✓ **Nessuna copia sul telefono.** Gli elementi decrittografati esistono solo in memoria mentre una cassaforte è aperta.
  Un'eccezione: un elemento copiato resta negli appunti finché il timer non li svuota (da 15 sec a 1 min), anche se la cassaforte è stata chiusa.
- ✓ **Nessuna telemetria.** Niente tracciamento, niente analisi.

COSA MI8OS NON FA MAI

- ✓ **Si blocca quando esci.** Lasciare l'app chiude la cassaforte (subito o dopo il ritardo che hai scelto).
- ✓ **Copre lo schermo** nel selettore delle app, e durante la registrazione o la duplicazione dello schermo.
- ✓ **Rileva le manomissioni.** I dati modificati non superano il sigillo e vengono rifiutati.
- ✓ **Usa solo algoritmi pubblici e standard:** Argon2id, HKDF-SHA256, ChaCha20-Poly1305, AES-128.

L'ALTRA FACCIA DELL'ASSENZA DI BACKDOOR

Se perdi tutte le carte, o dimentichi la password della cassaforte, nessuno può recuperare i tuoi elementi. Né tu, né noi. Ecco perché hai tre carte e una password scritta su carta.

07

Cura, Android e aiuto

01 Cura e recupero delle carte
02 Su Android
03 Risoluzione dei problemi

CURA E RECUPERO DELLE CARTE

Tre carte, tre luoghi.

01 TIENILE SEPARATE

Una carta con te o a portata di mano, una a casa, una altrove: da un familiare, al lavoro o in una cassetta di sicurezza. Un solo incendio o furto non può portarsele via tutte e tre.

02 HAI PERSO UNA CARTA?

Chi la trova ha in mano dati crittografati. Crea una sostituta (vedi 03) per tornare a tre copie. Se temi che qualcuno conosca la password, crea allo stesso modo nuove casseforti con una nuova password della cassaforte, poi ripristina le vecchie carte.

CURA E RECUPERO DELLE CARTE

03 CREARE UNA SOSTITUTA

L'app può copiare una cassaforte su altre carte solo subito dopo averla creata. Per una sostituta in seguito, crea una nuova cassaforte su una carta vuota e inserisci di nuovo gli stessi elementi: apri una carta funzionante per leggerli, e se nel frattempo annoti qualcosa, distruggi poi quell'appunto. Fallo prima di arrivare all'ultima copia.

04 HAI DIMENTICATO LA PASSWORD DELLA CASSAFORTE?

Quegli elementi non si possono recuperare. Se un'altra carta usa una password che ricordi ancora, apri quella. Altrimenti ripristina le carte e crea una nuova cassaforte.

> **Abbi cura delle carte** come di una carta bancaria: niente pieghe, niente calore, niente spigoli taglienti. Tienile lontane dalle custodie di metallo quando scansioni.

SU ANDROID

Stessa app, qualche piccola differenza.



SU ANDROID

L’app Android è su **Google Play**. Funziona allo stesso modo e legge le stesse carte. Una cassaforte scritta su iPhone si apre su Android, e viceversa.

Scansione

Android non ha una finestra NFC di sistema, quindi MI8OS mostra una propria schermata di scansione con un pulsante per annullare.

Posizione della carta

Tieni la carta contro la metà superiore del retro del telefono. Il punto esatto varia da modello a modello.

NFC

L’NFC deve essere attivato nelle impostazioni del telefono.

Biometria

Il Blocco dell’app usa l’impronta digitale o lo sblocco con il volto del telefono.

RISOLUZIONE DEI PROBLEMI

Se qualcosa non funziona.

La carta non viene rilevata

Tienila piatta contro il bordo superiore dell'iPhone e tienila ferma. Togli una custodia spessa o di metallo. Prova un po' più in alto o più in basso.

La scrittura si è interrotta a metà

Tocca **Riprova** e tieni ferma la stessa carta. Ogni salvataggio riscrive l'intera carta, e le tue modifiche restano nell'app finché non riesce. Se l'app dice che il salvataggio non può essere completato, **ripristina la carta** e salva di nuovo, oppure usa una carta di backup e **sostituisci questa**.

Password errata

Controlla l'ortografia e gli spazi. Ricorda: ogni carta può avere la propria password della cassaforte.

RISOLUZIONE DEI PROBLEMI

«È una carta diversa»
Hai avvicinato una carta diversa da quella che hai aperto. Usa Identifica per trovare quella giusta.

La carta è piena
Una carta contiene 20 elementi. Eliminane uno che non ti serve più, oppure distribuisci gli elementi su più carte.

Una carta non si ripristina
È bloccata. Il ripristino chiede la sua password principale.

La cassaforte si è chiusa da sola
Hai lasciato l'app, oppure lo schermo veniva registrato. Apri di nuovo la carta.

La pausa «Preparazione della chiave»
Normale. È il rafforzamento voluto della password.

Altro aiuto · guide.mi8os.com

info@mi8os.com



MI8OS

La tua privacy appartiene a te.

MI8OS.COM

La guida MI8OS, edizione mobile, italiano, ottobre 2026. Descrive l'app MI8OS per iPhone e Android. Le schermate possono variare leggermente da una versione all'altra. Le chiavi e i byte di esempio del capitolo 06 sono stati generati per questa guida con una password dimostrativa; non usarla mai.
MI8OS · info@mi8os.com