# STADIUM KEYS : Zero-Knowledge Security Blueprint

PBKDF2 SHA-256 key derivation, dual-wrapped DEK/KEK architecture, and AES-256-GCM per-record encryption.

https://stadium-keys.lovable.app

## Why Stadium Keys Exists

Commercial password managers rent you a locker in their warehouse. If their servers go dark, or they decide they don't like you, your digital life is held hostage. And if the cloud gets wiped by ransomware, your data is gone.

Stadium Keys is a zero-knowledge architecture that blinds the cloud and lets you keep your own encrypted backup — all without enterprise data center fees.

**The cloud is blind**

The database, backend and host hold zero keys and cannot read your credentials.

**You hold the backup**

Encrypted .cube.json snapshots can live anywhere you control and restore offline.

## Cryptographic Lifecycle

Everything left of the boundary happens on your device. Nothing right of it can be read without your keys.

**01 // Master Passphrase**

Typed into this browser tab only. Never stored, logged or transmitted. Exists in memory only for the milliseconds required during key derivation.

**02 // PBKDF2 SHA-256 Derivation**

The passphrase is stretched on-device into a Key Encryption Key (KEK).

**03 // Dual-Wrapped Vault Key**

A random AES-256 Data Encryption Key is generated on-device and wrapped twice: once by your passphrase KEK, and once by your Sovereign Recovery Key. Either can unlock it offline; neither unencrypted key ever touches storage.

**04 // AES-256-GCM Per Record**

Every credential is encrypted individually with its own fresh 96-bit IV. GCM authentication tags guarantee any tampering is immediately detected.

**05 // Sealed Sync**

Encrypted vault payloads sync to an owner-only cloud vault through revision-checked saves, so one device can never silently overwrite another.

## Security Posture

**Account is not the vault**

Signing in (email, Google, Apple, Microsoft or Lovable) only unlocks the mailbox, not the safe. The master passphrase still does.

**Sovereign Recovery Key**

An offline recovery key wraps the vault key independently, so a forgotten passphrase is not a lost vault.

**One-time share links**

Each shared item is encrypted with its own key kept only in the link's # part; the server deletes the drop the moment it is opened.

**Faraday Cube backups**

Export an encrypted .cube.json snapshot any time. It's already scrambled, so it's safe anywhere.