EncryptFire Whitepaper

Secure, Offline Continuity for the Self-Custody of Digital Assets

1. Introduction

The rise of self-custody in digital assets presents both freedom and fragility. While wallets give users full control, most backup methods rely on risky, outdated habits: writing seed phrases on paper, storing credentials in cloud services, in password managers, or in hardware that may not survive a decade.

EncryptFire was created to solve a modern problem:
> *How do you protect a crypto wallet across time — without relying on trust, centralization, or fragile backups?*

2. Purpose of EncryptFire

EncryptFire is a browser-based tool for securely backing up and passing on wallet credentials **without exposing the seed phrase**, relying on online storage, or involving third-party custodians. It helps users preserve control today — and prepare for structured continuity tomorrow.

- No installations
- No accounts
- No telemetry
- Just encrypted, printable files — and complete user control

3. Design Philosophy

EncryptFire was designed around four principles:

- **Offline-first**: All logic and encryption happen in-browser with no connection to the outside world.
- **Zero trust**: The tool stores nothing and transmits nothing.
- **Layered security**: Wallet words are transformed using a cipher map and stored separately from both the map and password.
- **Continuity of access**: Built not just for secure storage, but for intentional, structured control.

4. System Overview

- **Seed Map**: A randomized cipher layer that transforms wallet words into obfuscated numeric seed codes.
- **Seed Codes**: These numbers are stored separately and are meaningless without the seed map.
- **Master Password**: A 32-character complex string used to encrypt and protect all sensitive files.
- **Cloud Password** (optional): Used to encrypt the master password for time-delayed delivery. The encrypted master password can be stored in the cloud, while the cloud password remains offline. Upon handoff, the user or trustee gains access to the encrypted password file, unlocking the entire archive.

These elements are encrypted independently and distributed according to the user's own preference — typically across USB drives, offline storage, and legal or personal

custodianship. Files can also be exported in printable form, offering physical backup options for long-term resilience.

5. Institutional Workflow Summary

For estate planners, financial advisors, and their clientele, EncryptFire offers a streamlined version of its original app. Multiple steps are securely bundled into a **single click**, generating all required files in one encrypted package — ready for conversion into hardened cold storage seed codes.

- Seed maps, encrypted password files, and printable assets are auto-generated and zipped for download
- Users retain full control while benefiting from the speed, safety, and structure of a centralized custody experience — **without the third-party risk**
- Files can be stored across physical and digital media, providing multi-layered recovery paths

This workflow preserves the transparency and inspectability of the original tool, while delivering institutional-grade usability.

6. Use Cases

- **Crypto holders** who want secure, long-term protection for their wallets — without relying on fragile storage methods
- **Financial advisors** who support self-custody clients and want to offer an alternative to custodial solutions

- **Estate planners** who need a digital asset management continuity tool to reference in their planning process
- **Privacy-focused users** who want to eliminate traditional risks of holding and securing digital wallets

EncryptFire allows for the optional use of cloud services to hold **encrypted password files** only. This is fundamentally different from storing seed phrases in the cloud or within browser-based password managers. The sensitive material remains offline — cloud delivery only acts as a delayed handoff mechanism.

7. Continuity Through Trusteeship

EncryptFire is designed to enable secure **continuity of control**, not ownership. In estate and planning scenarios, this often involves a **trusted party** — a spouse, legal representative, or informal trustee — who is granted access only when needed, and only with the proper components.

Rather than embedding sensitive data in legal documents or cloud accounts, EncryptFire allows users to:

- Split the critical elements of wallet recovery
- Distribute those elements across separate physical and digital locations
- Enable retrieval only by the designated party when access is granted according to pre-defined protocols

"Control can be passed without exposure. Responsibility without risk. Trusteeship without compromise."

8. Security Model

- Uses AES-128 bit encryption for password protection and AES-256 bit encryption for content via industry-standard JavaScript libraries
- Files are generated offline and stored airgapped
- Nothing is ever stored in the browser — including cookies, session data, local files, or indexed data
- Users can verify all behavior transparently using browser developer tools
- Encryption keys are never transmitted or logged — all actions occur client-side

9. Limitations and Considerations

- Password security is entirely user-driven — EncryptFire only uses 32-character complex random strings to support the highest level of encryption
- If the user loses their password(s), no recovery mechanism exists
  > *With redundant, multi-location backups, this becomes a feature — not a bug*
- Wallet seed phrases can be backed up without entering them into the app
- EncryptFire is not a wallet and does not generate seed phrases
- Legal arrangements such as wills, trusts, and custody agreements should be handled separately, with EncryptFire serving as a digital continuity layer

10. Vision and Future Work

EncryptFire is the first in a planned suite of decentralized security tools. Future developments include:

- **FreezeKeys**: A cold storage tool for encrypted private keys
- **FreezeAuth**: Offline recovery and backup of identity and login credentials

11. Conclusion

EncryptFire empowers users to maintain digital sovereignty over their assets — not just today, but for the long term. It achieves this by creating a secure, layered, private multi-backup method with automated access control. The EncryptFire hardened cold storage system delivers continuity without compromise and control without dependency.

Crypto Security Tools
8 The Green, Ste B
Dover, DE 19901

CryptoSecurityTools.com