EverPass: A Zero-Trust Vault for Timed, Trusted Information Delivery

1. Project Overview

EverPass is a zero-trust, decentralized tool designed to securely store and deliver encrypted messages, files, instructions, or personal data to trusted recipients—only when specific conditions are met, such as prolonged silence, predefined dates, or multi-party confirmations.

Built on local encryption and transparent logic, EverPass enables users to plan how their most important digital messages are transmitted, without compromising privacy or security.

The tool serves a wide range of high-sensitivity use cases—ranging from inheritance instructions to multi-phase disclosures or life planning messages.

2. Core Philosophy

EverPass is designed for:

- People who need absolute control over their digital messages
- Situations where timing matters more than immediacy
- Users who prioritize zero trust and privacy by design

We believe final words, keys, and life instructions deserve the same protection as assets. Our system ensures they are delivered only when intended, to only the people chosen.

3. Key Features

- Local AES-256 encryption (zero platform access)
- Trigger-based delivery: time delay, inactivity, witness verification

- Multi-stage messaging (deliver messages in phases)
- File and text content support
- Multi-recipient vaults
- Optional decentralized storage (IPFS integration planned)
- Minimal, human-friendly interface

4. Example Use Cases

- **Life transition messages**: Prewritten advice or personal letters to children or partners, sent upon life-changing events
- **Crypto inheritance**: Securely transmit wallet keys or access instructions upon death or confirmed loss
- **Delayed confessions or truths**: Send letters after a fixed time period or a period of silence
- **Multi-phase document release**: Gradually release documents (e.g., startup plans, family letters, creative drafts)
- **Emergency backups**: Provide information to legal/medical contacts when silent or missing

Note on Legal Validity:

While EverPass can be used to deliver personal, financial, or inheritance-related messages, it does **not currently constitute a legally binding will** in any jurisdiction. However, in the future, we hope it may serve as a recognized complement in regions where digital-first estate planning frameworks are adopted.

5. Target Users

- Web3 and crypto holders
- Privacy-first individuals

- Digital nomads, frequent travelers, long-term planners
- Estate lawyers, family planners, and legacy writers
- Anyone with a message to protect and a moment to wait for

6. Trust & Security Model

EverPass follows a strict zero-trust model:

- All encryption happens on the user's device
- We never see, store, or transmit plaintext
- Only ciphertext is stored—optionally off-chain or via IPFS
- All triggering logic is open source and auditable
- No recovery is possible without user-chosen keys

7. Monetization Plan (Future)

- Optional storage plans (vault size, file types)
- Custom trigger modules (e.g., lawyer-verified delivery)
- High net-worth or enterprise plans
- Possible DAO-based inheritance or multi-signature workflows

8. Project Status & Collaboration

- Concept, flow, and zero-trust model fully defined
- Prototypes in planning
- GitHub public: https://github.com/liu192932380/everpass
- Looking for frontend/backend developers, cryptography experts, and privacy-minded partners
- Contact: everpass.project@protonmail.com