ChatGPT Memory Key

External User-Controlled Memory Architecture (BIO-DISK Concept)

Author: Dr. Evgeny Feldman

Date: May 11, 2025

Abstract

This proposal outlines an architecture for external, encrypted memory storage for ChatGPT and other LLM-based systems. It introduces a modular, user-controlled system where personal memory is stored locally on physical or logical drives, ensuring full privacy, data sovereignty, and clear legal boundaries. Inspired by crypto wallets, secure USB drives, and zero-knowledge systems, it combines practical usability with robust privacy and security.

1. Goal

Enable ChatGPT to store and access personal memory outside of OpenAI servers via encrypted, user-controlled devices. The system ensures total user autonomy, maximum privacy, and no dependency on centralized storage.

2. Architecture Overview

Hardware Option:

- USB device with onboard E2E encryption

- User-owned master key, no OpenAI access

- Emergency wipe button

- 'Plug to enable, unplug to disable'

Software Option:

- Format any drive/partition via app

- Secure containers for BIO, HISTORY, TASKS

- Optional cloud sync

Hybrid Option:

- Store low-risk segments server-side (BIO), keep sensitive data local

3. Segmented Memory Structure

- BIO: User facts

- HISTORY: Context

- TASKS: Goals

- MARKED: Pinned content

Segments loaded on demand by relevance to reduce token usage.

4. BYOB Model (Bring Your Own Backup)

- No central backup or data access by OpenAI

- User must manage device, backups, and keys

- Mirrors Ledger, Trezor, IronKey: 'Loss of key = loss of data, no liability'.

5. Emergency Wipe

- Hardware/software trigger

- Delete encryption key or overwrite sectors

- Non-recoverable by design

6. Interface & Access Control

- Show active/inactive memory

- Allow toggling

- Logs of memory usage and timestamps

7. Key Management

- Generate master key locally

- User-backed via seed phrase/QR/export

- No recovery by OpenAI

8. Format & Storage

- Includes embeddings, metadata, memory graph

- Optimized for transformer access

9. Technical Integration

- API: memory.get(), memory.query()

- Read/write encrypted containers

- Low-latency embedding fetch

10. Transparency & Logs

- View audit logs

- Download transparency reports

11. Optional Hardware Features

- Secure chip, USB-C, NFC, biometric unlock

- Offline mode

- Driver-based ChatGPT connection

Conclusion

BIO-DISK enables ChatGPT to scale memory with user ownership, privacy, and engineering feasibility.

License

This proposal is shared openly by Dr. Evgeny Feldman without claim to compensation or ownership. Attribution is welcome if used.