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

Author: Dr. Evgeny Feldman

Date: May 11, 2025

Role: Anesthesiologist, advanced ChatGPT user, architecture-level thinker from outside the tech industry.

Core Proposal:
A secure, modular, user-controlled memory system for ChatGPT - allowing encrypted memory to be stored outside OpenAI servers (e.g., on USB/Bluetooth/NFC devices), with segment-based access (BIO, HISTORY, TASKS), offline security, and user-owned key control.

Inspired by crypto hardware wallets, secure enclave architectures, and the "context window" bottleneck in LLMs.

This is not a UX fix. This is a memory architecture.

What makes it valuable:
- Architecturally complete: memory segmentation, format design, key lifecycle, API integration, user toggles, fail-safes.
- User-centric: aligns with BYOB (Bring Your Own Backup), GDPR privacy, and enterprise zero-knowledge models.
- Technically grounded: compatible with current transformer logic (precomputed embeddings, secure containers, minimal token footprint).
- Legally safe: shifts memory responsibility to the user while protecting OpenAI from liability.

Use Cases Enabled:
- Offline memory mode (plug-in, plug-out)
- Enterprise-controlled memory (no cloud)
- Audit trails for medical, legal, and military users
- High-trust user interactions over long time spans

Documentation:
Full whitepaper available (PDF):

"ChatGPT Memory Key - BIO-DISK Architecture" by Dr. Evgeny Feldman

Includes system overview, memory structure, security logic, API commands, legal frame, and hardware spec ideas.

Purpose of this message:

I am not seeking compensation or credit. I care that the idea - which solves a deep structural problem - is seen by someone who can recognize and refine it.

If this resonates with your current direction, I'm happy to contribute further or advise.

If not - I'll be grateful for the moment of consideration.

Respectfully,

Dr. Evgeny Feldman

GPT-4.5 user | Anesthesiologist | Architect by necessity