
Sovereign Digital Persistence

The Technical Manifesto of Gvardian Vault

1. The Custody Crisis

The digital age has created a paradox: our most valuable assets—crypto keys, legal documents, and private memories—are stored in "clouds" we do not own. Traditional legacy planning relies on corporate longevity. If a company goes bankrupt, your history is deleted.

> **[ARCHITECT'S HOOK]**
>
> **"In a world where companies disappear in a decade, Gvardian Vault is built for the century. We didn't build a box you have to trust us to hold; we built a lock only you and your chosen survivors can turn."**

2. Zero-Knowledge Implementation

To ensure this 100-year durability, Gvardian Vault utilizes a **Client-Side Exclusive** encryption model.

- **Native Web Crypto API:** We bypass server-side processing entirely for data encryption.
- **Local Key Stretching:** Using Argon2id iterations performed on the user's hardware, we ensure the Master Password never leaves the device.
- **Ciphertext Transparency:** Our servers store only the AES-GCM 256-bit ciphertext. GLE is mathematically incapable of accessing user data, even under legal compulsion.

3. The Guardian Protocol: Cryptographic Continuity

The hand-off to beneficiaries is managed via a **Pre-Encrypted Heartbeat**.

1. **The Check-in:** A low-impact metadata signal.
2. **The Release:** Upon a failed check-in, a pre-calculated **Key Fragment** is transmitted to the Guardian.
3. **The Reconstruction:** The Guardian uses their own private key to unlock the fragment, completing the circuit to the user's vault.

4. Green IT & Data Sovereignty

By offloading computation to the edge (the user's browser), we adhere to our **Sustainability Mandate**, significantly reducing the carbon footprint of our data centers. Furthermore, we commit to an **Open JSON Schema**, ensuring that even if GLE ceased to exist, your data could be recovered using standard open-source cryptographic tools.