TECHNICAL WHITE PAPER · DRAFT v0.1 · NOVEMBER 2024

Sovereign Memory, Recoverable Legacy.

A target architecture combining client-side encryption, zero-knowledge storage and Shamir's Secret Sharing for programmed, verifiable transmission across generations.

BOTTLE ON THE SEA

Preserving Humanity's Memory

Bottle on the Sea

Status: design document. Describes a target architecture, not a live or audited system.

00

Abstract

Digital lives now outlast the people who create them, yet the tools that hold them were never built for inheritance. Photos, letters, voice notes and private keys sit in accounts governed by terms of service, tied to a single provider and frequently lost when their owner dies or the provider changes course.

This paper describes the target architecture of the Bottle on the Sea Digital Memory Vault: a system designed so that (1) memories are encrypted on the owner's device before they leave it, (2) the operator never holds the keys needed to read them, (3) access is transmitted only under conditions chosen by the owner, and (4) a designated beneficiary could recover a vault through an open-source protocol, even if the legal entity Bottle on the Sea ceased to exist.

The core mechanism is a key hierarchy protected by Shamir's Secret Sharing with a 3-of-5 threshold, distributed across independent custodians, combined with a multi-signal transmission trigger and verifiable integrity proofs.

> Status disclosure. The vault is in closed development. Everything described here is a design objective under engineering and validation. No component should be read as an operating, certified or independently audited protection. Parameters (threshold, custodians, algorithms) may change following review.

01

The problem: legacy without continuity

Three failures recur when a person dies or becomes incapacitated:

— Inaccessibility. Heirs cannot open accounts, devices or encrypted files. Strong security without a succession path becomes permanent loss.

— Dependency. Existing legacy features belong to platforms. If the provider closes, changes policy or suspends the account, the legacy disappears with it.

— Loss of meaning. Even when files survive, context does not: who is in the photo, why a letter mattered, what a person actually believed.

Conventional cloud storage solves availability for the living owner. It does not solve sovereignty (who can read), succession (who receives, and when) or continuity (what happens if the service itself ends). Bottle on the Sea is designed around these three properties.

02

Design principles

Principle	Design commitment
Sovereignty	Encryption keys are generated and used on the owner's devices. The operator stores ciphertext only.
No single point of trust	No single party — including Bottle on the Sea — can decrypt a vault or trigger its transmission alone.

Principle	Design commitment
Owner-defined succession	The owner chooses recipients, timing and trigger conditions while alive and able to decide.
Continuity beyond the company	Recovery must remain possible with published, open-source tooling and independent custodians.
Verifiability	Recipients can check that what they receive is exactly what was sealed, and when it was sealed.
Honesty of AI	Any AI layer separates what was said, what is inferred and what is unknown, and never impersonates the person.

03

Threat model

The architecture is designed against the following adversaries and failure modes:

Threat	Intended mitigation
Compromise of Bottle on the Sea servers	Attacker obtains ciphertext and metadata only; no decryption keys are stored server-side.
Malicious or coerced insider	Operator holds at most one key share, below the threshold; transmission requires independent signals.
Loss of the owner's device	Vault key is recoverable by the owner with a threshold of shares; no single device is critical.
Compromise of one custodian	One or two shares reveal nothing about the key (information-theoretic property of Shamir's scheme).
Premature or fraudulent transmission	Multi-signal trigger: date or proof-of-life lapse, plus guardian quorum and, where required, legal verification.
Disappearance of the company	Open-source recovery protocol and custodian-held shares let beneficiaries reconstruct access independently.
Tampering with archived content	Content hashes, Merkle commitments and independent timestamping make alteration detectable.

Out of scope for this draft: a fully compromised owner device at sealing time, coercion of a threshold of custodians simultaneously, and long-term cryptanalytic breaks (addressed by crypto-agility in section 09).

04

Architecture overview

The vault is organised in four layers, mirroring the product journey: Capture, Organise, Program, Transmit.

4.1 Client-side encryption

Each memory object (photo, letter, audio, video, document) is encrypted on the device with a unique random content key using an authenticated cipher (target: AES-256-GCM or XChaCha20-Poly1305). Content keys are wrapped by a vault master key (VMK). Only ciphertext, wrapped keys and minimal routing metadata reach the storage layer.

4.2 Key hierarchy

Key	Role	Where it lives
Content key	Encrypts a single memory object	Wrapped under the VMK; never stored in clear
Vault master key (VMK)	Wraps all content keys of a vault	Owner devices (secure enclave where available); split into Shamir shares
Recipient keys	Public keys of designated beneficiaries	Beneficiary devices; used to re-encrypt released material
Integrity keys	Sign seals and audit records	Owner device and independent timestamp service

4.3 Zero-knowledge storage

The storage layer is designed so that the operator can prove it holds a vault, serve it and replicate it across European data centres, without being able to read it. Search, classification and AI structuring run on the owner's device or in an environment the owner unlocks explicitly; results are re-encrypted before upload. Metadata exposure (object sizes, counts, timestamps) is minimised through padding and batching.

05

Shamir's Secret Sharing: 3-of-5 custody

Shamir's Secret Sharing splits a secret into n shares such that any k of them reconstruct it, while fewer than k reveal no information at all. The target configuration splits the VMK into five shares with a threshold of three.

#	Proposed custodian	Purpose
1	Owner (primary device / hardware token)	Day-to-day control and self-recovery
2	Owner (offline backup, e.g. printed or metal recovery card)	Resilience against device loss
3	Designated beneficiary or guardian	Enables succession with the owner's prior consent
4	Independent professional (notary, lawyer or family office)	Legal anchor for verified transmission
5	Bottle on the Sea service share (or independent escrow)	Operational convenience; never sufficient alone

Consequences of this design:

— The owner alone (shares 1 + 2 + any third) retains full control while alive.

— Bottle on the Sea alone holds one share — two below the threshold — and cannot decrypt a vault.

— After a verified trigger, beneficiary + professional + one other share reconstruct access without requiring the company.

— Loss or compromise of any two shares does not compromise or lock the vault. Shares can be refreshed (proactive re-sharing) without changing the underlying key.

> Complement, not replacement. The professional custodian role is designed to support, not replace, the legal role of a notary. Succession law governs who is entitled; the vault governs how that entitlement is executed cryptographically.

06

Programmed transmission and trigger verification

The owner defines one or more transmission rules per memory or collection: recipient(s), date, and trigger. No single signal is designed to release a vault.

Mode	Conditions (target design)
Fixed date	A future date chosen by the owner (e.g. a child's 18th birthday). Release is time-locked and cancellable by the owner until then.
Proof-of-life lapse	Periodic check-ins; after missed checks and a grace period, guardians are asked to confirm. A quorum of guardians must confirm.
Legal event	Death or incapacity confirmed by documentary evidence verified by the professional custodian where required by law.
Combined	Any combination, e.g. legal event AND date not before 2035.

Every step — check-ins missed, confirmations, objections, releases — is written to a signed, append-only audit log the owner can review while alive and recipients can verify afterwards.

07

Continuity: the open-source recovery protocol

The commitment at the heart of this paper is that a beneficiary could recover a vault through an open-source protocol, even if the legal entity Bottle on the Sea ceased to exist. The intended design rests on four elements:

— Open specification and reference client. The data format, key-wrapping scheme and share format will be published under an open-source licence, with a reference recovery tool that runs offline.

— Portable ciphertext. Owners and beneficiaries can export the encrypted vault at any time. Storage is replicated, and an export bundle can be held by the beneficiary or the professional custodian.

— Independent share custody. At least three of the five shares sit outside the company by design.

— Continuity arrangements. A legal escrow and wind-down plan intended to hand stored ciphertext and the service share to an independent trustee if operations cease.

Recovery without the company therefore requires: the exported (or escrowed) ciphertext, three shares, and the open-source tool. No proprietary server is in the critical path.

08

Verifiable integrity and provenance

— Each object is hashed (target: SHA-256 / BLAKE3) before encryption; hashes are committed in a Merkle tree per seal.

— The Merkle root is signed by the owner and timestamped by an independent service (RFC 3161 and/or anchoring on a public blockchain). Only hashes are anchored — never content or personal data.

— Recipients verify that each memory is exactly what was sealed, by whom, and no later than when.

— Provenance metadata (author, date, context added by the owner) travels encrypted with the object.

09

Legacy AI governance

Legacy AI is a proposed layer allowing future generations to ask questions grounded in preserved memories. Its safeguards are architectural, not cosmetic:

— Said / Inferred / Unknown. Every answer distinguishes direct quotes with source, inferences clearly labelled, and what the archive cannot answer.

— No impersonation. The system speaks about the person, never as the person; no synthetic voice cloning without explicit prior consent.

— Owner consent and scope. The owner decides which memories may be used, by whom, and from when.

— Privacy-preserving execution. Processing on unlocked material only, with no use of vault content to train shared models.

10

Compliance and cryptographic agility

— GDPR. Data minimisation, EU hosting, encryption by default, and data-subject rights for the living owner; legal analysis of post-mortem data under member-state law.

— eIDAS. Qualified electronic signatures and timestamps where seals require legal weight.

— Succession law. Transmission rules designed to be compatible with, and subordinate to, applicable inheritance law.

— Crypto-agility. Versioned algorithms and periodic re-encryption, with a planned migration path to post-quantum key encapsulation (e.g. ML-KEM) for long-horizon archives.

11

Validation roadmap

Horizon	Milestone
Months 1-6	Publication of this white paper; threat-model review; reference implementation of key hierarchy and 3-of-5 recovery.
Months 6-12	Independent cryptographic audit by a recognised firm, with public report; pilot partnerships with notaries and family offices.

Horizon	Milestone
Months 12-18	Open-source release of the recovery specification and reference tool; public bug bounty.
Beyond	Long-term research tracks (DNA-on-silicon archival, ETERNITY infrastructure) — not required for the vault MVP.

12

Limitations and open questions

— Custodian selection, onboarding and share refresh must stay usable for non-technical families.

— Legal recognition of cryptographic transmission varies across jurisdictions and will be assessed country by country.

— Metadata minimisation is partial; a full privacy analysis is pending.

— Long-term readability of file formats requires an active format-migration policy.

— This document will be revised following independent review. Feedback is welcome.

Contact. Technical reviewers, notaries, family offices and investors: bottleonthesea.com — request access via the Investors or Pilot pages.

Disclaimer. This draft describes intended design. It is not an offer, a security certification or legal advice.