



Address-Bound Secure Delivery Vault

A home delivery vault system and method that accepts digital payloads only when cryptographically bound to a fixed street address, geographi...

P0

US Provisional Filed 2026

United States (PCT expansion planned)

May 2026 · <https://embox-site.pages.dev>



Abstract

A home delivery vault system and method that accepts digital payloads only when cryptographically bound to a fixed street address, geographic coordinates, and device identity. The invention creates legally attributable delivery to a physical residence without rendering document content on an exterior display. A digital address token links payload hashes to geolocation and serial number; a dual-anchor receipt combines secure-element attestation with geofenced retrieve; and an append-only chain-of-custody ledger records each hop from sender key management through vault secure to user device read.

Field of Invention

The present invention relates to secure document delivery systems, and more particularly to cryptographic methods for binding digital correspondence to a physical delivery address using a home-mounted vault, cloud routing platform, and mobile retrieve device.

Background of the Invention

Regulated senders — including banks, tax agencies, courts, and healthcare providers — must prove that sensitive documents reached a recipient's registered physical address. Email lacks standardized proof of delivery to a street address and is vulnerable to phishing. Traditional paper mail provides drop-off proof through certified mail services costing ten dollars or more per piece, yet documents still arrive in unlocked or easily defeated containers where content is visible and theft is common.

Smart mailbox products focus on package detection or outdoor imaging of mail pieces, which exposes privacy and does not establish institution-verified sender chains. Virtual post office boxes redirect mail away from the home and do not serve as address-bound receivers at the residence.

There remains an unmet need for a digital receiver at the household that (1) cryptographically binds each payload to the delivery address, (2) maintains tamper-evident custody from sender to recipient, and (3) separates outdoor status from indoor reading.

Summary of the Invention

According to one embodiment, a sender system signs a document payload and attaches a digital address token comprising a street-address hash, geographic bound, device serial, payload hash, and sender certificate reference. A cloud platform validates the chain and routes encrypted content to a registered home vault. The vault rejects payloads failing verification. An outdoor interface receives metadata only. A user device performs retrieve at the anchor point, updating the ledger to RETRIEVED before private read.

Brief Description of Drawings

1. System architecture showing sender, cloud, vault, and phone
2. Digital address token field layout and verification chain
3. Append-only custody ledger state machine

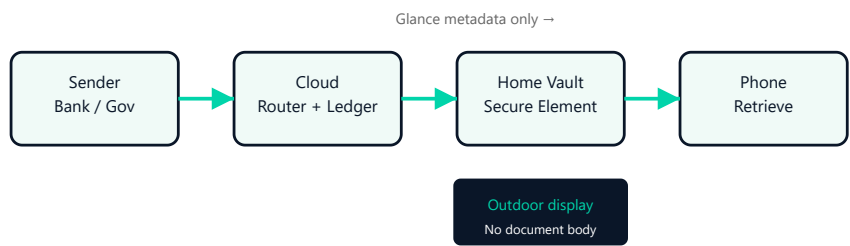


Fig. 1 — eMbox system architecture — sender to household retrieve

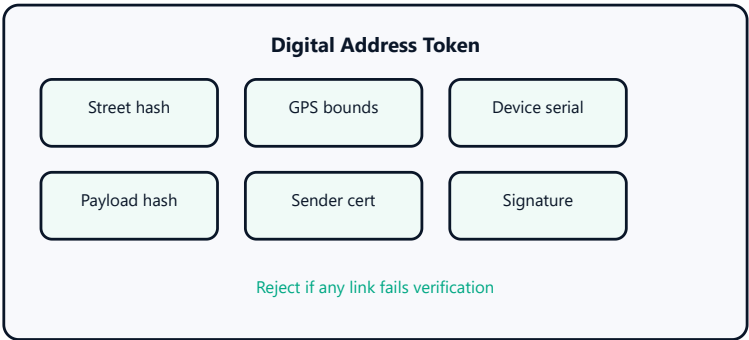


Fig. 2 — Address token binding payload to physical delivery anchor

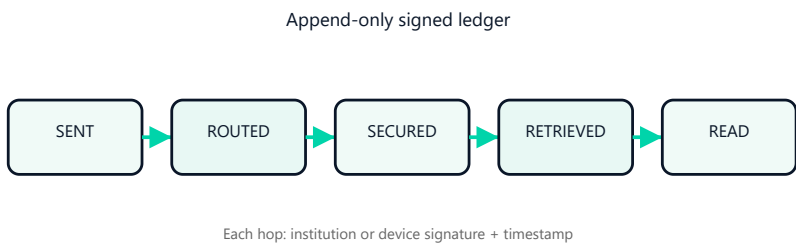


Fig. 3 — Chain-of-custody from sender KMS to user device

Detailed Description of Embodiments

Digital address token structure

The token is a signed data structure. Fields include: ADDR_HASH (normalized street + unit), GEO_BOUNDS (lat/long envelope), DEVICE_ID (manufacturing serial + secure element ID), PAYLOAD_HASH (SHA-256 of ciphertext), SENDER_CERT_ID, and TIMESTAMP. Verification requires Ed25519 or equivalent signature from the sender KMS and a secondary signature from the platform router after registry lookup.

Dual-anchor receipt

Upon SECURED state, the vault secure element emits attestation quote binding firmware version, compartment state, and payload ID. Upon RETRIEVED, the phone presents a signed challenge verified within a geofence (e.g., 15m radius of registered coordinates). Court-exportable bundles combine both anchors with ledger entries.

Chain-of-custody ledger

States progress SENT → ROUTED → SECURED → RETRIEVED → READ. Each transition appends a signed record. Senders receive webhooks on SECURED and RETRIEVED for operational proof without call-center follow-up.

Advantages

- Legally attributable delivery without outdoor content exposure
- Automatic rejection of misaddressed or spoofed payloads
- Court-exportable custody chain by default
- Sender webhook proof replacing certified paper

Independent Claims (Representative)

1. A method for secure document delivery comprising: receiving at a home vault a digital payload accompanied by a digital address token binding the payload to a street address hash, geographic coordinates, and a device identifier; verifying a sender cryptographic signature and the address token chain; rejecting the payload when verification fails; storing the payload encrypted in the vault; transmitting metadata only to an outdoor display; and recording a secured event in an append-only ledger.
2. A home vault apparatus comprising: a secure element storing device keys; a network interface; an outdoor display controller configured to render only sender category, document count, and urgency indicators; and a processor enforcing rejection of payloads lacking valid address-token binding.
3. A non-transitory computer-readable medium storing instructions that, when executed, cause a cloud platform to validate address tokens, route encrypted payloads to registered vaults, and maintain a chain-of-custody ledger from sender through retrieve.

Dependent Claims (Representative)

4. The method of claim 1, wherein the digital address token further comprises a payload hash and wherein the vault compares the hash to received ciphertext before acceptance.
5. The method of claim 1, further comprising emitting a dual-anchor receipt including secure-element attestation at secure and geofenced phone challenge at retrieve.
6. The method of claim 1, wherein the outdoor display is firmware-prohibited from rendering document titles, account numbers, or balances.
7. The apparatus of claim 2, further comprising accelerometer-based tamper detection triggering key zeroization.

Related Innovations

This family relates to eMbox platform components documented in the Solution Architecture and Engineering briefs. Cross-reference patent families in the Portfolio Overview document.

eMbox · Patent Pending · May 2026

Confidential summary for partnership and planning discussions. Patent pending — not legal advice. Not a filed USPTO application.

Patent family: address-bound-vault