



eMbox Patent Portfolio — Complete Reference

Six US provisional applications · 18+ protected claim areas · PCT planned

Patent Pending

2026

US First

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



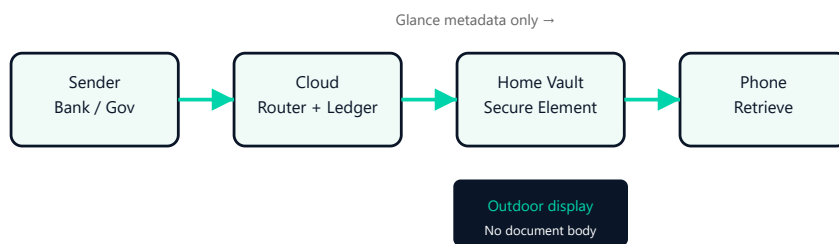


Fig. 1 — eMbox system architecture — sender to household retrieve

Portfolio Abstract

Six United States provisional patent applications filed in 2026 protect the eMbox architecture for certified digital delivery to a physical street address. The portfolio spans sender trust, address-bound cryptography, legal retrieve protocols, glance-only outdoor privacy, household multi-tenancy, and physical tamper response. Together these families create defense-in-depth around a platform that is infrastructure for regulated senders — not a consumer gadget category.

Patent Families

1. address-bound-vault
2. legal-delivery-protocol
3. sender-trust
4. glance-only-ui
5. household-vault
6. physical-security

Address-Bound Secure Delivery Vault

P0 US Provisional Filed 2026

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.

Key claims

- 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.
- 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.

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

Retrieve-or-Acknowledge Legal Delivery Protocol

P1 US Provisional Filed 2026

Methods and systems for achieving legal equivalence to physical mail delivery through retrieve-or-acknowledge actions at a secured home address. The protocol supports jurisdiction-aware statutory notice classification, deferred indoor reading without invalidating delivery timestamps, and one-tap export of affidavit bundles for courts and agencies.

Key claims

- A method comprising: securing a document at a home vault bound to a physical address; displaying urgency on an outdoor interface without document content; detecting a retrieve-or-acknowledge action at the vault via a paired user device; recording a delivery timestamp in a ledger; and permitting deferred reading of the document on the user device after said timestamp.
- A system comprising a statutory notice classifier applying jurisdiction-specific rules to sender-tagged payloads and configuring outdoor display duration and notification requirements accordingly.

Advantages

- Delivery timestamp decoupled from read time — matches physical mail law
- Jurisdiction-aware compliance without sender manual research
- Reduced process-server and certified-mail spend

Hardware-Rooted Sender Trust & Anti-Phishing

P0 US Provisional Filed 2026

Sender verification for home vaults using hardware-rooted allowlists, institution-signed payloads only, sender glance glyphs derived from certificate hashes, and a postcard enrollment ritual bridging paper trust to digital roots of trust.

Key claims

- A method comprising: maintaining in a secure element an allowlist of institution certificate identifiers; accepting only payloads signed by keys on the allowlist; rendering on an outdoor display a sender glyph derived from a certificate hash without displaying payload-supplied sender strings; and enrolling a new sender through a physical-mail verification ritual to the street address.

Advantages

- Phishing-resistant delivery channel for regulated mail
- Outdoor sender identity without content leakage
- Paper-to-digital trust bootstrap for new institutions

Glance-Only Outdoor Privacy Interface

P0 US Provisional Filed 2026

Outdoor display architecture for home vaults that communicates delivery status, urgency, and sender category while firmware-enforcing prohibition against document bodies, titles, amounts, or account numbers on exterior surfaces.

Key claims

- An outdoor display controller for a secure delivery vault configured to render only sender category, item count, urgency encoding, and a certificate-derived glyph, and firmware-prohibited from rendering document bodies, financial amounts, account identifiers, or document titles.
- A method comprising: decrypting document content only on a user device after retrieve; and supplying to an outdoor display a metadata structure of fewer than a fixed byte size excluding human-readable document fields.

Advantages

- Neighborhood privacy for sensitive recipients
- HIPAA-aligned outdoor layer for healthcare mail
- Differentiation from camera-based smart mailboxes

Multi-Tenant Household Vault Architecture

P1 US Provisional Filed 2026

Partitioned secure namespaces on a single home vault for multiple residents, expiring capability tokens for attorneys and caregivers, duress PIN coercion mode, and household policy engine governing cross-partition access.

Key claims

- A home vault comprising multiple encrypted partitions each associated with a resident slot; a router directing incoming payloads to a partition based on sender metadata; and an outdoor display aggregating delivery counts across partitions without revealing partition-specific document content.
- A method comprising: issuing an expiring capability token authorizing delegated retrieve for a specified partition and scope; and rejecting delegate actions exceeding scope or expiry.

Advantages

- One device serves multi-adult households
- Safe delegation without password sharing
- Coercion-resistant operation

Physical Tamper Response & Resilience System

P2 US Provisional Filed 2026

Physical security for delivery vaults including accelerometer-triggered key zeroization, sender tamper broadcast, multi-unit apartment mesh store-and-forward, and hybrid secure compartments for physical items notified via glance display.

Key claims

- A method comprising: detecting physical tamper of a home vault via at least one of accelerometer anomaly or enclosure breach; zeroizing cryptographic keys within the vault; and broadcasting a tamper event to a sender platform.
- A store-and-forward system for apartment buildings comprising a lobby hub storing per-unit encrypted payloads and indoor units retrieving only payloads wrapped to respective unit keys.

Advantages

- Stolen device does not expose resident documents
- Senders gain incident awareness automatically
- Apartment-scale deployment without N outdoor internet connections

eMbox · Patent Pending · May 2026

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

Full detail in individual patent family documents