PATENT FAMILY — DETAILED SUMMARY

eMbox

Physical Tamper Response & Resilience System

Physical security for delivery vaults including accelerometer-triggered key zeroization, sender tamper broadcast, multi-unit apartment mesh …

P2 | US Provisional Filed 2026 | United States

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

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

Abstract

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.

Field of Invention

Tamper-responsive embedded security and multi-dwelling delivery infrastructure.

Background of the Invention

Outdoor-mounted devices face theft, prying, and vibration attacks. Encryption is worthless if keys extractable after slow tamper. Apartment buildings need per-unit security without per-unit outdoor internet.

Summary of the Invention

Accelerometer and enclosure break circuits trigger immediate key zeroization and signed TAMPER event to platform and senders. Building hub stores encrypted forwards per unit key. Optional drawer unlocks after glance notice for physical items (keys, cards) without outdoor content display.

Brief Description of Drawings

1. Tamper detection pipeline
2. Multi-unit mesh topology

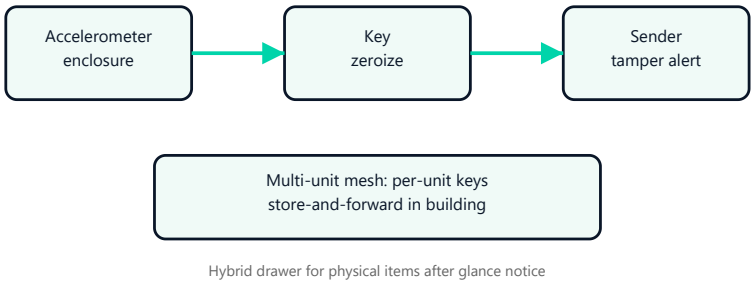

Fig. 1 — Physical tamper response and multi-unit resilience

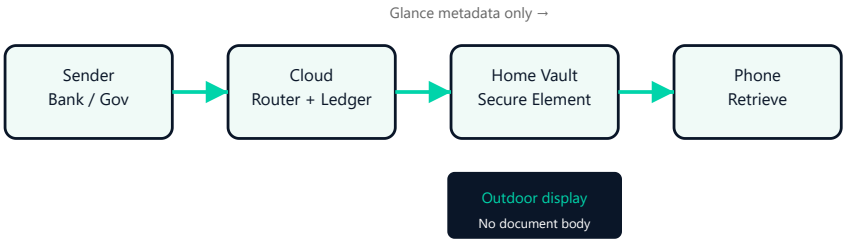

Fig. 2 — eMbox system architecture — sender to household retrieve

Detailed Description of Embodiments

Tamper zeroization

Threshold on g-force and lid switch. Zeroization completes in <200ms. Display shows "SEALED" — no metadata after tamper.

Sender tamper broadcast

Webhook TAMPER with device ID and last SECURED payload IDs so senders can re-issue to replacement device or hold delivery.

Multi-unit mesh

Lobby hub receives unit-addressed ciphertext; indoor unit polls hub over BLE; per-unit keys never shared with hub storage — hub holds only wrapped blobs.

Advantages

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

Independent Claims (Representative)

1. 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.

2. 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.

Dependent Claims (Representative)

3. The method of claim 1, further comprising disabling outdoor metadata display after tamper until re-provisioning.

4. The system of claim 2, wherein the hub cannot decrypt unit payloads.

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.