



Multi-Tenant Household Vault Architecture

Partitioned secure namespaces on a single home vault for multiple residents, expiring capability tokens for attorneys and caregivers, duress...

P1

US Provisional Filed 2026

United States

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



Abstract

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.

Field of Invention

Multi-user secure storage on embedded devices and delegated access control.

Background of the Invention

Households receive mail for multiple adults and dependents. Shared mailboxes provide no partition. Delegating access to attorneys or caregivers today means sharing PINs or physical keys.

Coercion scenarios require plausible deniability without alerting attackers.

Summary of the Invention

Sender metadata includes RECIPIENT_SLOT routing to encrypted partitions with separate wrapped keys. Capability tokens are time-bound, scope-bound (read-only, retrieve-only), and revocable. Duress PIN unlocks decoy partition with empty status while silently notifying a trusted contact via covert channel.

Brief Description of Drawings

1. Partitioned vault layout and delegate token flow

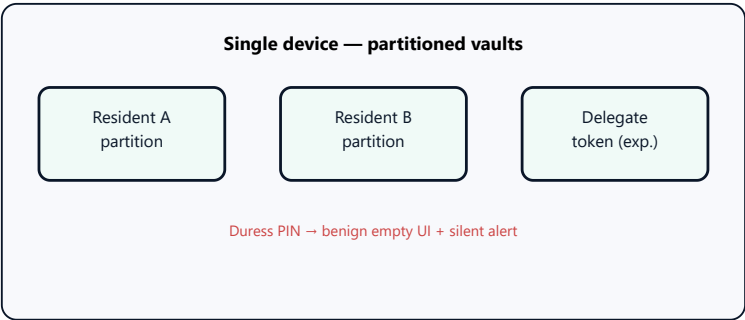


Fig. 1 — Multi-tenant household vault with capability tokens

Detailed Description of Embodiments

Per-resident partitions

Each partition has unique storage namespace and key hierarchy derived from master secret + slot ID. Outdoor display aggregates counts only ("3 new") unless single-resident mode.

Capability tokens

QR or link generates token: {slot, expiry, scopes, delegate_pub_key}. Vault accepts retrieve signed by delegate key within scope.

Duress PIN

Alternate PIN loads decoy UI and wipes session keys for real partition from RAM. Background LTE/BLE beacon sends alert to preconfigured contact.

Advantages

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

Independent Claims (Representative)

1. 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.
2. 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.

Dependent Claims (Representative)

3. The vault of claim 1, further comprising a duress PIN presenting a benign empty status while transmitting a covert alert.
4. The method of claim 2, wherein scopes include retrieve-only without read permission.

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.