PATENT FAMILY — DETAILED SUMMARY

eMbox

Hardware-Rooted Sender Trust & Anti-Phishing

Sender verification for home vaults using hardware-rooted allowlists, institution-signed payloads only, sender glance glyphs derived from ce…

P0 | 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

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.

Field of Invention

Anti-phishing systems, institutional document delivery, and hardware-enforced sender allowlists.

Background of the Invention

Email phishing mimics banks and government agencies with high success rates. Physical mail accepts drops from any party. Consumers cannot distinguish official correspondence from fraud at the point of delivery.

Portal login links in email are themselves attack vectors. A vault that displays sender identity without exposing document content must derive identity from cryptographic certificates, not user-supplied labels.

Summary of the Invention

Only payloads signed by enrolled institution keys enter the vault. Unknown senders are quarantined until a postcard enrollment ritual completes: sender mails a code, resident enters code, platform elevates sender cert to allowlist. Outdoor display shows a glance glyph (icon derived from cert hash) — not a spoofable string.

Brief Description of Drawings

1. Sender trust pipeline
2. Glance glyph vs blocked metadata

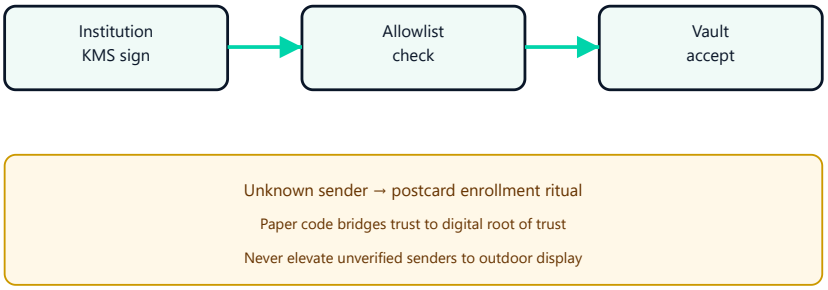

Fig. 1 — Hardware-rooted sender trust and anti-phishing

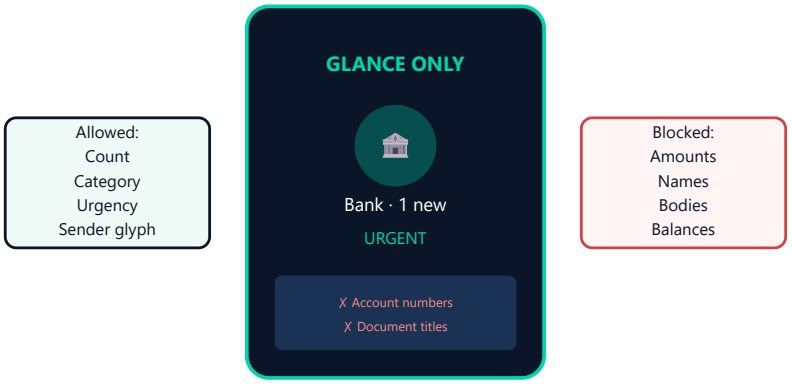

Fig. 2 — Glance-only outdoor UI — metadata without document content

Detailed Description of Embodiments

Hardware-rooted allowlist

Allowlist stored in secure element; updates require platform signature + optional user approval for new sender classes. Firmware drops unsigned payloads before cloud callback.

Sender glance glyph

Hash institution cert public key → deterministic icon/color. Outdoor UI never shows free-text sender names from payload metadata.

Postcard enrollment ritual

First-time sender requests enrollment; system mails postcard with OTP to street address; resident confirms within app; sender cert pinned to household allowlist.

Advantages

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

Independent Claims (Representative)

> **1.** 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.

Dependent Claims (Representative)

> **2.** The method of claim 1, wherein unverified senders are denied outdoor display priority.

> **3.** The method of claim 1, wherein the postcard ritual comprises mailing a one-time code to the address and requiring entry before allowlist update.

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.
