POLICYMAKER BRIEFING · 2026

Elections are trusted on assertion.
We make them provable.

StrongRoom — chain-of-custody evidence for mail ballots and election operations. Paper stays authoritative.

THE GAP

Every election already produces evidence.
Almost none of it is verifiable.

Custody today lives in binders, spreadsheets, email threads and memory. When a result is challenged, officials are asked to prove a process that was never recorded in a form anyone outside the building can check.

WHAT IT IS

A custody evidence layer that sits beside your existing systems.

Record

Every custody event for a mail-ballot package, from issuance to acceptance to envelope separation.

Seal

Each event is written into an append-only log and cryptographically sealed. Nothing can be quietly edited.

Prove

Any single record can be proven to belong to the sealed history — to an auditor, a court, or the public.

BOUNDARIES

What it deliberately does not do.

- ✕ Does not mark ballots
- ✕ Does not tabulate votes
- ✕ Does not report results
- ✕ Does not decide voter eligibility
- ✕ Does not replace certified voting systems
- ✕ Does not decide whether a ballot is valid

The narrow boundary is the point. It is what makes adoption low-risk.

THE PROOF

Four things make the record hard to fake.

01

Append-only history

Records are added, never rewritten. Any alteration to past entries changes the seal and is visible.

02

Independent witnesses

Outside custodians counter-sign the sealed history, so no single operator can show two different versions of it.

03

Split keys, no single owner

Sealing authority is split across multiple guardians. No one person or server holds the whole key.

04

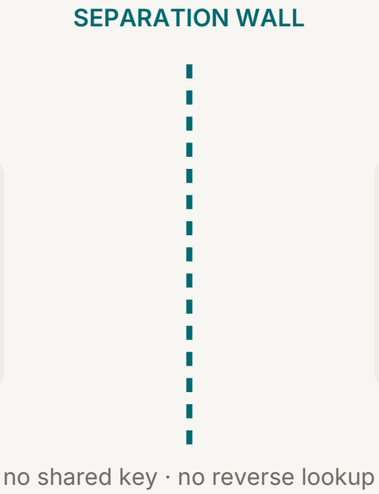
Two-person sealing

Sensitive steps such as batch separation require two distinct officers, recorded in the evidence itself.

PRIVACY

The vote is never in the custody record.

Custody identity and ballot content are separated by design. After the envelope is opened, no key, token, or query can reconnect a voter to their selections.



IN THE BUILDING

One record. Six controlled views.

Poll workers

Report incidents, log equipment, confirm handoffs.

Jurisdiction command

See status across sites in real time.

Security

Track access, anomalies, and device state.

Legal

Pull a defensible timeline on demand.

Audit

Verify inclusion and consistency independently.

Review

Approve consequential actions — always a human.

DEPLOYMENT POSTURE

Local-first. Three isolation tiers.

TIER 1

Public services

Hardened containers. No election data.

TIER 2

Election data

Stronger microVM / confidential compute isolation.

TIER 3

Sealing keys

Tightly controlled key infrastructure. No routine human login.

Sensitive evidence never leaves the authorized deployment boundary.

THE PATH IN

One county. Shadow mode. Nothing binding.

01

Shadow pilot

Run alongside existing systems in a single jurisdiction. No system-of-record role.

02

Custody first

Incidents, equipment, ballot custody, evidence logs, access controls.

03

Independent review

Outside cryptographers and counsel examine the core before any expansion.

04

Then scale

Multi-jurisdiction only after the first environment is proven end to end.

WHERE IT STANDS TODAY

We lead with the limits.

Not EAC-certified

Not certified under VVSG 2.0, and not offered as a system of record for a binding election.

Proof runs use synthetic data

Public demonstrations run on synthetic data, not real voter or ballot data.

Independent review pending

Outside cryptographic and legal review is a gate on production use, not an afterthought.

Residual risk is published

Colluding officers, guardian collusion, vendor access and coercion limits are documented, not hidden.

THE ASK

Give us one county, in shadow mode, for one cycle.

No change to how ballots are counted. No change to certification. At the end of it, a jurisdiction can prove its own custody chain to anyone who asks.

StrongRoom · Operation Encrypt — Mail Ballot Lifecycle · BB2G Election Command