EXECUTIVE SUMMARY · PREPARED FOR ELECTED AND APPOINTED OFFICIALS

StrongRoom: Provable Custody for Elections

StrongRoom is an evidence system for elections. It records who handled a mail-ballot package, when, where, and under whose authority — and then seals that record so it can be proven later to an auditor, a court, or the public. It does not mark ballots, count votes, report results, or decide who is eligible to vote. Paper remains authoritative throughout. The product being offered is the ability to prove a process, not a replacement for the process.

The problem it addresses

Election offices already run disciplined chain-of-custody procedures. What they generally cannot do is **prove** those procedures after the fact in a form an outsider can check independently. Custody today is captured in binders, spreadsheets, transfer forms, email threads, and institutional memory. Each of those can be lost, reconstructed, or contested, and none of them can demonstrate that the record was not edited after the fact.

The consequence is predictable. When results are challenged, officials are asked to defend a process that was never recorded in a verifiable form, and confidence becomes a matter of whom the public trusts rather than what can be demonstrated. StrongRoom closes that gap without touching the machinery of voting itself.

What the system actually does

Records custody events. Issuance, transfer, receipt, acceptance, and envelope separation for physical mail-ballot packages, along with incidents, equipment movement, and access to secured areas.

Seals the record. Every event is written into an append-only history that is cryptographically sealed. Past entries cannot be quietly changed, deleted, or reordered without the alteration becoming visible.

Produces portable proof. Any individual record can be shown to belong to the sealed history, and any two views of that history can be checked for consistency, using only the disclosed information.

Serves the people doing the work. Poll workers, jurisdiction command, security, legal, audit, and review each get a controlled view of the same record, scoped to their role and authority.

> **Consequential actions always require a human.**
> The system includes an assistive software layer, but it is not an election authority. It does not approve, reject, certify, or decide anything on its own. Every consequential action requires a named human approval, and that approval is part of the record.

How the proof works

The mechanism is deliberately conventional cryptography applied with strict operational discipline. Four properties do the work, and each one closes off a specific way a record could be falsified.

1 · Append-only history

Events are added, never rewritten. The sealed state of the log depends on everything that came before it, so silently altering, removing, or reordering an earlier entry changes the seal and becomes detectable rather than invisible.

2 · Independent witnesses

The sealed state is counter-signed by registered outside custodians who maintain current independence attestations. This is what prevents the operator from showing one version of history to an auditor and a different version to the public. Stale, suspended, undersized, or conflicting witness conditions are treated as explicit refusals, not warnings to ignore.

3 · Split sealing authority

The keys that seal the record are generated and held across multiple guardians through a recorded ceremony, so no single person, server, or vendor holds complete sealing power. Invalid participation stops the ceremony rather than being silently accepted or repaired.

4 · Two-person control on sensitive steps

Sensitive operations — batch sealing at envelope separation, for example — require two distinct officers, a minimum batch size, and a recorded attestation. The dual-control requirement is bound into the evidence itself rather than being a policy that lives only on paper.

Voter privacy is structural, not procedural

The identifier used to track a ballot package belongs to **envelope custody**. It does not encode voter selections, and there is no public lookup that lets a stranger track a named voter's envelope. Once the envelope is separated from the ballot, no key, foreign reference, reused token, or query path is permitted to reconnect a voter's identity to their selections. That boundary is enforced in the data model, not by staff discipline.

Privacy is also tested as a whole rather than field by field. The internal attack suite probes direct linkage between published artifacts, ordering effects, timing effects, small-group disclosure, and

joins across outputs that each look safe on their own. Where a group is too small to publish safely, it is suppressed and rolled upward until the remaining disclosure still meets a minimum anonymity floor. Published records suppress precise separation timing and replace membership lists with commitments, while still carrying a digest and signature that anyone can recompute from the disclosed fields alone.

Operating posture

Deployment is local-first: sensitive evidence stays inside the authorized boundary rather than being pooled in a vendor cloud. Work is separated into three isolation tiers — public services in hardened containers, election-data processing in stronger microVM or confidential-compute isolation, and sealing keys in tightly controlled key infrastructure with no routine human login. Software is built from committed toolchains with signed changes, required adversarial review gates, staged environments, post-deployment verification, rollback, and a final release record. If key management is not properly configured, the system refuses to start and reports the refusal rather than falling back to a weaker mode.

Adoption path

The intended first step is a shadow pilot in a single jurisdiction, running alongside existing systems with no system-of-record role and no binding function. The first phase covers incident reporting, equipment tracking, ballot custody, evidence logs, procedures, and access controls. Ballot marking, tabulation, and other certification-track capabilities stay out of scope. Independent cryptographic and legal review is a gate before any expansion, and multi-jurisdiction deployment is considered only after one environment has been proven end to end.

Current status and stated limits

These limits are published rather than managed, because a system whose entire value is honest evidence cannot afford to overstate itself.

> **Not federally certified**
>
> The system is not EAC-certified under VVSG 2.0 and is not offered as a system of record for a binding election.

> **Demonstrations use synthetic data**
>
> Public proof runs use synthetic data. Real scan-event ingestion depends on authorized access to postal tracking data, which remains a near-term gate.

Independent review is still outstanding

Outside cryptographic and legal review has not yet been completed. Until it is, production use is not appropriate.

Guardian independence is not yet physical

The current threshold-key configuration can simulate multiple guardians on shared infrastructure. Until guardians run on genuinely independent infrastructure, that control does not fully protect against the operator.

Residual risks are documented

Colluding officers, guardian collusion, print-vendor access to tokens, limited coercion resistance, and dependence on verifier implementations are recorded in the threat model. Cryptography narrows institutional trust; it does not eliminate it.

What we are asking for

One jurisdiction, in shadow mode, for one cycle. No change to how ballots are counted, no change to certification, no new authority granted to software. At the end of it, the jurisdiction can prove its own chain of custody to anyone who asks — including to the people who did not like the outcome.

Related workstreams: Operation Encrypt (mail-ballot lifecycle and custody evidence), BB2G Election Command (role-based election operations), and the StrongRoom cryptographic core.