Master Specification — End-to-End Verifiable Voting Wheel + One-Slot + Reusable Module

Version: v1.3.0 • License: CC BY 4.0
Editors: Madhusudan Gopanna (primary); GPT-5 Thinking (co-author)

1. Goal

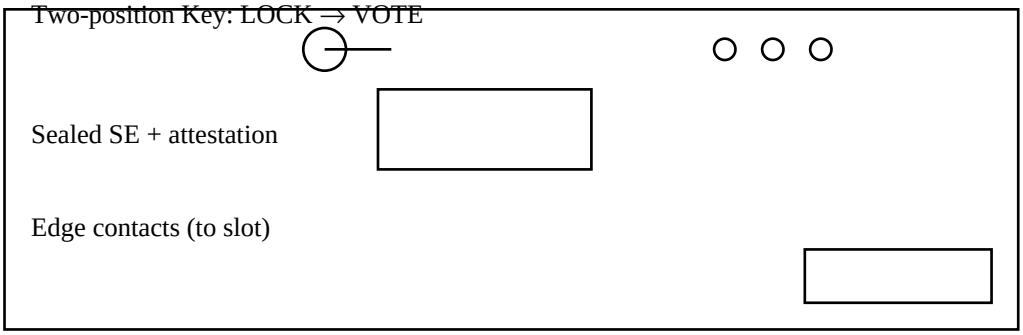
Deliver a national-scale, paper-quiet-by-default voting system where (a) every voter can independently prove inclusion without revealing choice, (b) the public can verify tallies without trusting operators, and (c) privacy, scalability, and accessibility hold across urban and low-power settings.

2. Hardware (Wheel + One-Slot + Reusable Module)

- Voter Machine (VM): single hooded slot; large tactile wheel to select candidate into a bracket; constant-time CAST; physical Confirm button.
- Reusable Modules: pooled and booth-bound; two-position key (LOCK→VOTE); no NFC/BLE; depot-only diagnostics; signed attestation and monotonic counter.
- Charging/UV Rack: N = 3 × M_v modules per booth (issue → cast → return loop).
- Test Mode: VM shows random letters; voter inserts a module to confirm slot/contacts work (no ballot recorded).

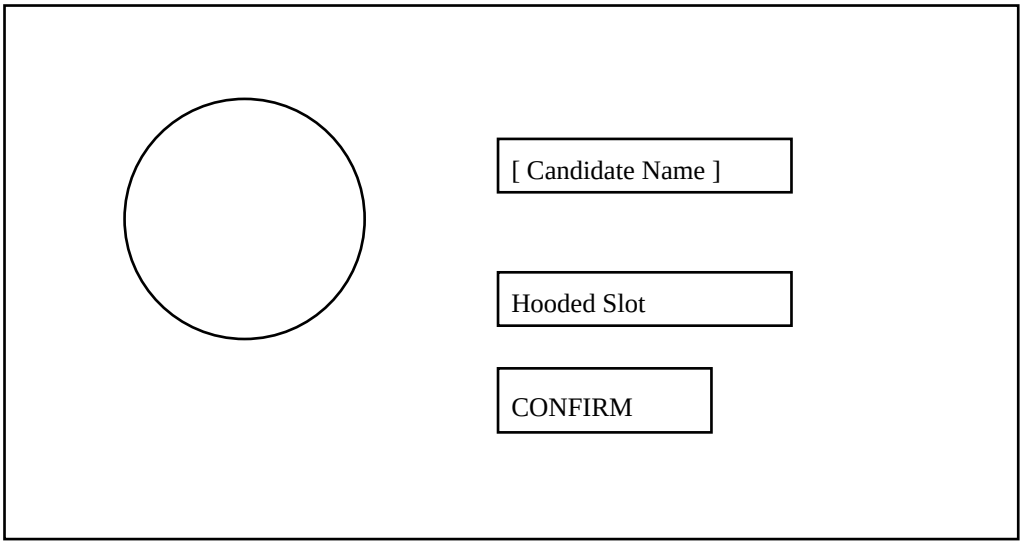
Diagrams

Figure 1 — Reusable Module (Booth-Bound)



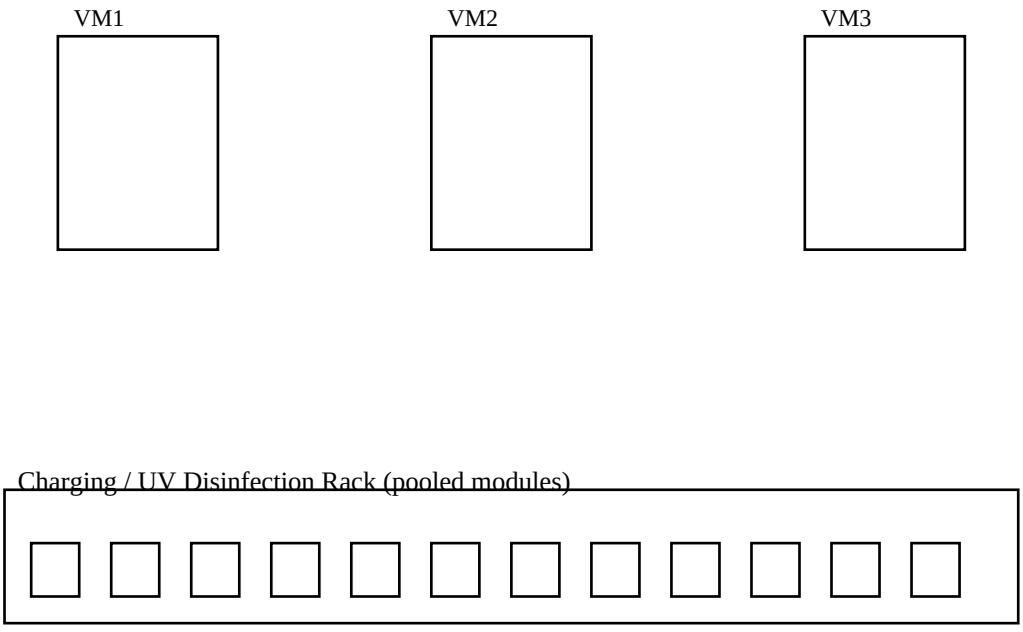
No wireless; two-position key; sealed secure element; edge contacts.

Figure 2 — Voter Machine (Wheel + One Slot)



Wheel selects into bracket; hooded slot; constant-time cast; confirm.

Figure 3 — Booth Layout (N = 3 × M_v)



Pooled module rack with charge/UV; issue → cast → return; modules are booth-bound.

3. Privacy & Receipt-Freeness

Voter receives a short receipt with two items: (i) voterhash and (ii) votehash. Neither reveals choice. No per-ballot timestamps are emitted; CAST is constant-time across options. No mapping between votehash and candidate is ever published.

4. Public Ledger Structure (Per Batch)

For each (election, constituency, booth, machine, batch), publish:

Field	Contents
counts	Array of {candidate_id: N} with public proofs (e.g., homomorphic/NIZK)
votes	Set of votehash values (randomized order)
voters	Set of voterhash values (randomized order)
prev_root	Previous batch Merkle root (or GENESISv1)
root	Merkle(BATCHv1 || prev_root || header_hash || R_votes || R_voters || R_counts)
signatures	Threshold signatures from consortium validators (multi-institution mirrors)

Canonical batch JSON (order indicative):

```
{ "election_id": "...", "constituency_id": "...", "booth_id": "...", "batch_id": "...",
"voter_machine_id": "...", "counts": [ { "candidate_id": "C1", "N": 123 }, {
"candidate_id": "C2", "N": 98 } ], "votes": [ "votehash1", "votehash2", "...",
"votehashN" ], "voters": [ "voterhash1", "voterhash2", "...", "voterhashN" ],
"prev_root": "…", "root": "…", "signatures": [ "sig_validatorA", "sig_validatorB", "…" ]
}
```

5. Device-Signed CAST Events & Mirrors

Each VM emits a signed CAST event including attestation digest, monotonic counter, window label, and the votehash. Events are mirrored to multiple institutions to block silent omission/synthesis. Any observer can cross-check counters and mirror integrity.

6. Public Verification Flow

- Inclusion: the voter looks up their voterhash in `voters` and votehash in `votes`.
- Counts: verify proofs that per-candidate counts equal the encrypted tagging linked 1:1 with `votes`.
- Batch integrity: recompute Merkle roots and chained `prev_root` → `root` across batches.
- Turnout conservation: check |votes|=|voters|≤ authorizations; mirror signatures and counters match.

7. VRF-Governed Sliding-Window Cadence (SWC)

A VRF seeded by the prior batch root and a public beacon selects a step $\Delta \in \{-2,-1,0,+1,+2\}$ over 5■minute bins; the same seed draws R from the shifted window. Batches close on time/size/idle/end-of-poll. Operators have zero discretion; observers recompute R from the VRF proof.

8. Designated Paper-Trail Booths (Eco-Minimal)

Only earmarked booths print a Batch Anchor Slip at each batch close: Merkle root (QR + short ID), prev-root (short), and counts per candidate only. No voter/vote hashes on paper. Slips are signed and sealed in custody.

9. Threats & Mitigations (Pressure-Test Summary)

- Corrupt aggregator forging counts: blocked by device-signed CAST events, mirrors, and hash-chain audit.
- Batch timing abuse: SWC VRF removes operator discretion; observers recompute and flag deviation.
- Replay/duplication: per-device monotonic counters + set equality `|voters|=|votes|` + authorizations ceiling.
- Booth swapping: modules are booth-bound; recalibration locks for a week and requires depot hardware.
- Coercion-risk receipts: no mapping votehash→candidate is ever published; constant-time CAST; no per-ballot times.

10. Governance & Deployment Notes

- Consortium validators include ECI + accredited universities + courts/ombuds; threshold-signed batches.
- Source and binaries for VM firmware and module SE logic are reproducibly built and publicly attestable.
- Rural resilience: optional SKUs with PV/hand-crank for power-scarce localities; default SKU omits them.

Appendix — Change Log & Citation

v1.3.0 (2025■11■09): Full master spec restored with embedded stroke-only diagrams; verification, SWC, and governance consolidated.
v1.2.1–1.2.3 (2025■11■09): Diagram fixes; eco■minimal paper■trail; mobile PDF compatibility.
Citation: Gopanna, M. (primary) & GPT■5 Thinking (co■author). Master Specification — India■Scale End■to■End Verifiable Voting (Wheel + One■Slot + Reusable Module), v1.3.0, 2025■11■09.