

Master Specification — India-Scale End-to-End Verifiable Voting (Wheel + One-Slot +

Spec-WheelSlot-Reusable-v1.3.1 — 2025-11-12 • License: CC BY 4.0

Authorship (page-1 header only): Madhusudan Gopanna (primary); GPT-5 Thinking (co-author)

0) Goal

Design and deploy a national-scale, low-cost, end-to-end verifiable voting system that:

- Preserves ballot secrecy and receipt-freeness (no voter can prove how they voted, not even themselves).
- Enables voter-level inclusion verification (each voter can confirm their ballot is in the final tally).
- Guarantees one person, one counted vote with public, append-only evidence.
- Operates offline-tolerant, power-frugal, and is manufacturable at low cost for low- and middle-income countries.
- Resists manipulation by powerful incumbents via protocol, law, and real-time transparency tripwires.

1) Scope

Covers: Polling-place hardware (reusable voter module, one-slot wheel interface), eligibility and authorization flow, cryptographic commitments, public bulletin board (permissioned consortium ledger), transparency telemetry, audits, governance, accessibility, operations, red-team testing, and acceptance metrics.

Excludes: Remote/Internet voting; permanent personal devices; party-specific canvassing tools; postal ballot logistics (handled under same verifier rules but outside this spec).

1A) Provenance & Authorship

Primary author & systems architect: Madhusudan Gopanna (global applicability), 2024–2025.

Technical co-author (collaborative AI): GPT-5 Thinking — drafting, pressure-testing, cost modeling, editorial clarity.

Editorial stance: Non-partisan, pro-democracy. Designed for adoption by any lawful election authority worldwide (not India-only).

Versioning: Spec-WheelSlot-Reusable-v1.3.1-2025-11-12. Change log in Appendix AB.

License: Creative Commons CC BY 4.0 — reuse with attribution (“Gopanna — primary; GPT-5 Thinking — co-author”).

Attribution presentation (PDF builds): Page-1 header only (cover is neutral). No authorship on placards.

2) Adversary Model

Capabilities: Control of parts of bureaucracy/procurement, influence over media narratives, ability to starve capacity or delay logistics, access to vendors, and policy levers for quiet rule changes.

Constraints: Must maintain plausible deniability; cannot openly eliminate elections; faces statutory tripwires and multi-party oversight.

3) System Overview (Narrative)

1. Voter is verified at check-in and issued a one-time authorization (short-lived cryptographic token or printed slip with QR/serial) bound to that station’s event.
2. Voter picks any reusable module from a pooled tray.
3. At the machine, voter turns module to VOTE, inserts into the single slot. The voter rotates a knurled wheel until the desired candidate is framed in a shrouded bracket, then confirms (2-second hold).
4. Inside the module, a rotating minute-key (SE) and a window nonce are used to compute

Master Specification — India-Scale End-to-End Verifiable Voting (Wheel + One-Slot + ...)

Spec-WheelSlot-Reusable-v1.3.1 — 2025-11-12 • License: CC BY 4.0

Authorship (page-1 header only): Madhusudan Gopanna (primary); GPT-5 Thinking (co-author)

voterhash; the machine then computes a votehash = $H(\text{voterhash}, \text{selection}, \text{device-only secret}, \text{window})$. The cast runs in fixed 60 s.

5. The voter receives a receipt that contains the pair {voterhash, votehash} (no choice revealed, no proof of choice possible).

6. The module resets to LOCK, forgets everything, and returns to the tray. The authorization is consumed (at most one accepted cast per authorization).

7. The public ledger publishes batches (per §8/§8.3) containing: per-candidate counts, a set of voters:{voterhash...}, a set of votes:{votehash...}, a VRF proof of timing, and a Merkle root chaining to the previous batch. Voters later check inclusion via either hash in their receipt.

4) Security Properties (Must-Hold Invariants)

SP-1 Secrecy / receipt-freeness. SP-2 Inclusion. SP-3 Uniqueness. SP-4 Eligibility separation.

SP-5 Append-only public record.

SP-6 Constant-time casting & anti-side-channels. SP-7 Accessibility parity. SP-8 VRF verifiability. SP-9 Booth-binding auditability.

5) Polling-Place Hardware

5.1 Reusable Voter Module (Core): LOCK→VOTE two-position key; rack charging via pogo/USB-C; secure element; no NFC/app mode; cryptographic booth binding; rebind requires official jig and triggers 7-day lockout & public Rebind Event; CAST fixed 60 s.

5.2 Accessibility SKUs (identical externals): Audio, Visual-Plus, Haptic, Off-Grid Power.

5.3 Wheel + One-Slot Voting Interface (Retrofit): shrouded slot; 2-second confirm hold; parity cues; booth certificate check.

5.4 Charging & Disinfection Rack: one slot per module ($N = 3 \times M_v$); UV-C; health telemetry; no data path.

5.5 Voter-Facing Test Mode: never generates hashes; never posts; constant-time equals CAST (60 s); public Test counter; dual-control exit.

6) Eligibility & Authorization

One-time authorization at check-in; at most one CAST per authorization; visible rejection/logging of duplicates; dashboard reconciliation.

7) Cryptographic Commitments (Abstract)

Rotating minute-key (inside SE). Voterhash: derived from minute-key, device-secret and window nonce; not linkable to identity/choice.

Votehash: $H(\text{voterhash}, \text{selection}, \text{device-secret}, \text{window})$. Receipt: {voterhash, votehash} for inclusion (not choice).

Batch publication: counts; voters:{voterhash...}; votes:{votehash...}; order randomized; no per-ballot timestamps; VRF proof (§8.3); Merkle chaining.

8) Consortium Ledger (Public Bulletin Board)

Validators: Election Commission, opposition parties, apex court IT cell, national universities; threshold signatures.

Snapshots: hourly; divergence alarms ≤ 5 min. Open APIs/verifier.

Batch record (conceptual):

```
{ electionId, constituencyId, boothId, batchId, machineId,  
  counts:{ candidateId->N }, voters:{ voterhash,... }, votes:{ votehash,... },
```

Master Specification — India-Scale End-to-End Verifiable Voting (Wheel + One-Slot +

Spec-WheelSlot-Reusable-v1.3.1 — 2025-11-12 • License: CC BY 4.0

Authorship (page-1 header only): Madhusudan Gopanna (primary); GPT-5 Thinking (co-author)

prevRoot, root, vrfProof, beaconEpoch }

9) Operational Telemetry & Tripwires

Live metrics (uptime, queues, modules in service, attestation pass-rate, bound vs present, auth vs cast vs void).

Tripwires: Z-score outliers; wait-time SLOs trigger redeployment or paper fallback. Privacy-preserving 5–10 min reporting.

10) Capacity Planning (Normative)

Each module ≈ 1 vote/min (CAST 60 s). Provision $N = 3 \times M_v$ modules per booth. Typical $T \approx 1000$, $H \approx 11$, $M_v \approx 2 \rightarrow N \approx 6$.

11) Privacy & Side-Channel Controls

Constant-time CAST; batch posting; shrouded wheel; no personal wireless; identical enclosures across SKUs.

12) Attestation, Supply Chain & Tamper

Measured boot; SE attestation; dual-control provisioning jig; mixed vendors & lot randomization; tamper mesh zeroizes SE; booth-bind certs; public Rebind Events; 7-day lockout.

13) Availability & Chaos Engineering

Brownout drills; off-grid SKU; local cache then batch-commit; surge redeployment; paper fallback reconciled by RLA.

14) Governance & Law (Binding Requirements)

Statute: machine-readable rolls; public diffs; observer access; consortium ledger membership; open verifier; RLAs; telemetry/snapshot SLAs; whistleblower & procurement transparency; VRF beacon source fixed in statute. Change control: supermajority + cooling-off; 48h injunction path.

15) Audits & Acceptance

Pre: public red-team. Day: attestation $\geq 99.95\%$; 95th wait ≤ 20 m urban/ ≤ 30 m remote; zero unauthorized rewrites; inclusion success $\geq 99.9\%$ first try. Post: RLAs + crypto checks; transparency packs.

16) Cost & Deployment (Indicative)

Module BOM (core) $\sim \$10$ – $\$13$; Off-Grid add $\sim \$3$; retrofit $\$15$ – $\$20$ /machine; station kit $N=3 \times M_v$; reusable 5–7 years; ~ 1.05 M booths scale with M_v .

17) Rollout Plan (Phased)

Pilot ($\leq 1\%$); Scale-up (10–25%); Nationwide (statutory tripwires, public dashboards, verifier bug bounty).

8.3 VRF-Governed Sliding-Window Cadence (SWC)

VRF(seed=prevRoot, beacon) picks $\Delta \in \{-2..+2\}$ over 5-min bins \rightarrow window; selects interval R. Close on time/size/idle/end-of-poll. Zero operator discretion. Publish vrfProof+beaconEpoch in header. No per-ballot timestamps; randomize voters/votes sets; optional $\pm (30\text{--}60\text{ s})$ publication jitter.

9.4 Designated Paper-Trail Booths (Eco-Minimal)

Batch-close slip prints: Merkle root (full) + short ID; prev root (short); per-candidate counts; header (Election/Const/Booth/Machine/Batch/Window); signatures (2 officers + 1 observer). Never

Master Specification — India-Scale End-to-End Verifiable Voting (Wheel + One-Slot + Reusable Module)

Spec-WheelSlot-Reusable-v1.3.1 — 2025-11-12 • License: CC BY 4.0

Authorship (page-1 header only): Madhusudan Gopanna (primary); GPT-5 Thinking (co-author)

prints voters/votes sets or mappings. Sealed custody. Public can confirm printed root against ledger.

Appendix AB — Change Log & Citation

v1.0 (2025-11-09): Initial master spec.

v1.1.0 (2025-11-09): Remove NFC/app mode; two-position key; BOM/privacy/attestation updates.

v1.2.0 (2025-11-09): Add §8.3 SWC.

v1.3.0 (2025-11-09): Dual-hash receipt; explicit ledger sets; SP-8/SP-9; Test Mode clarifications; batch record; statutory VRF beacon.

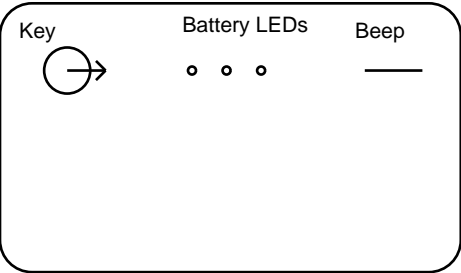
v1.3.1 (2025-11-12): Editorial sync; version & citation alignment; text-only PDF build.

Citation: Gopanna, M. (primary), & GPT-5 Thinking (co-author). Master Specification — India-Scale End-to-End Verifiable Voting (Wheel + One-Slot + Reusable Module), v1.3.1, 2025-11-12. CC BY 4.0.

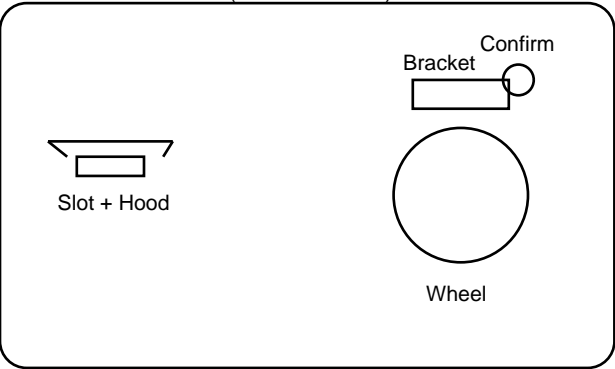
Master Specification — India-Scale End-to-End Verifiable Voting (Wheel + One-Slot + ...)

Spec-WheelSlot-Reusable-v1.3.1 — 2025-11-12 • License: CC BY 4.0
Authorship (page-1 header only): Madhusudan Gopanna (primary); GPT-5 Thinking (co-author)

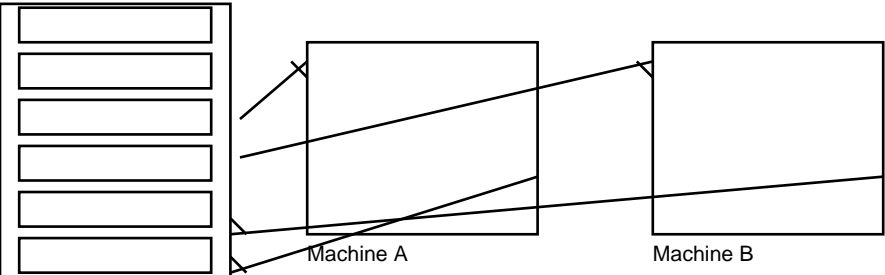
Representative Diagrams (stroke-only, black & white)



Reusable Voter Module (LOCK → VOTE)



Voter Machine (Wheel + One Slot)



Booth Layout: pooled bound modules; cast→return; rack shows health only (no data).

Charging/UV Rack ($N = 3 \times M_v$)

Conceptual figures only; no fills to ensure compatibility on mobile PDF viewers.