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

Version: Spec-WheelSlot-Reusable-**v1.4.0** — **2025-12-28**

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:** VerifiableVoting-v1.3.2-2025-12-28. 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 **voterhash**; the machine then computes a **votehash = H(voterhash, selection, device-only secret, 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).

   Sample receipt for illustrative purpose only – not real hash:

   Inputs (UTF-8, '|' separator):

   - minute_key = MK_EXAMPLE_0001
   - device_secret= DEVSEED_ABC123
   - window_nonce = WIN_2025-11-12T10:05Z
   - selection_id = CID-07

Inclusion Receipt (illustrative):

Election: IN-202X-LS-Phase3

Booth: TN-123-045

Batch Root: 5d3879de4ca2463fe8b6600b172efef735429b4d439df02afc6d33d64cb952e2

voterhash: db39cf612ba0023a342053d5394ee6e4c9812b3f805228a4debfe375d7ac9695

votehash: 13c0ee0ad55b9d98a2065a3c0018c8d5b7943ff9d5ac83246aca5b49373e231e

Use any verifier to check presence on the public ledger.

QR code would be generated with the following JSON:

{"ver":1,"batchRootShort":"5d3879de4ca2463fe8b6600b172efef735429b4d439df02afc6d33d64cb952e2","electionId":"IN-202X-LS-Phase3","boothId":"TN-123-045","voterhash":"db39cf612ba0023a342053d5394ee6e4c9812b3f805228a4debfe375d7ac9695","votehash":"13c0ee0ad55b9d98a2065a3c0018c8d5b7943ff9d5ac83246aca5b49373e231e"}

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:** No artifact combination enables a voter to prove their choice.
- **SP-2 Inclusion:** Each voter can verify that **their** ballot is included (presence of either receipt value on the ledger).
- **SP-3 Uniqueness:** The ledger accepts **≤1** counted cast per valid authorization; duplicates/voids are visible and auditable.
- **SP-4 Eligibility separation:** The entity that verifies eligibility cannot link a person to a posted vote entry.
- **SP-5 Append-only public record:** Any attempt to prune/alter posted entries is detectable by independent replicas.
- **SP-6 Constant-time casting & anti-side-channels:** Choice does not affect timing, power, EM signature, audio/LED cues, or operator workflows.
- **SP-7 Accessibility parity:** Assisted voting preserves SP-1..6; assisted voters are not deanonymized by SKU or workflow.
- **SP-8 VRF verifiability:** Batch timing is chosen by a public **VRF**; anyone can recompute and detect operator discretion.
- **SP-9 Booth-binding auditability:** Every module re-bind is publicly posted; bound modules cannot cast outside the booth cert.

5) Polling-Place Hardware

5.1 Reusable Voter Module (Core, No Haptics)

- **Mechanical:** Palmable sealed unit; 2-position turnkey: **LOCK → VOTE** (clockwise). IP54 shell; tamper mesh; epoxy potting.
- **Power:** Supercap + 200–300 mAh cell; **rack charging via pogo/USB-C**; tri-dot LED for battery. *(No PV or hand-crank on default module.)*
- **Compute:** Low-power MCU; secure element (SE/HSM) with monotonic counter; RTC.
- **I/O:** Piezo beeper; 3 LEDs (status). **No NFC; no APP/user diagnostics mode.**
- **Booth binding:** Module is **cryptographically bound** to a specific booth ID and its registered machines; it **only operates** with those machines.
- **Recalibration (re-binding):** Requires an **official provisioning device**; upon re-bind, the module enters a **1-week lock/quarantine** and emits a **Rebind Event** to the public audit log.
- **Modes:**

    - **LOCK (default):** all LEDs off; cannot cast.
    - **VOTE:** 10-second pre-insert window (LED chase); on insert → **CAST 60 s** constant-time; success → 1-second ACK then LOCK; error → purge + error tone + LOCK.
- **Service/attestation:** Diagnostics/attestation only via the provisioning jig under dual-control at depot; not in-booth and not via wireless.

5.2 Accessibility SKUs (identical externals)

- **Audio SKU:** Headphone jack; voice prompts; tactile confirm ring.
- **Visual-Plus SKU:** High-contrast LED bar near bracket; big-font mirrored text.
- **Haptic SKU (deafblind):** Sealed LRA; short buzz per detent; two buzzes on align; long on confirm. Duty-cycle limited.
- **Off-Grid Power SKU (regional):** Adds PV trickle panel and foldable hand-crank/dynamo; otherwise, identical firmware/exterior.

5.3 Wheel + One-Slot Voting Interface (Retrofit)

- **Wheel:** 60–80 mm knurled; uniform detents (0.25–0.35 N·m); encoder; neutral blank home index on reset.
- **Slot & Hood:** Single aperture with deep hood and side baffles; identical behavior for all candidates; anti-jam chamfer; sealed faceplate.
- **Confirm:** Sealed button; **2-second hold** to commit; identical cues for all candidates.
- **Parity:** No per-candidate LEDs, tones, or timing variation; dummy loads equalize EM/power signatures.
- **Booth binding:** Machine carries a **booth certificate**; accepts casts **only** from modules bound to that booth.

5.4 Charging & Disinfection Rack

- **Slots:** One per module (**$N = 3 \times M_v$**). Slots mechanically mimic the machine's slot but **only** provide charging + UV-C disinfection; **no casting state** is possible in the rack.
- **Electrical: Pogo/USB-C** charging; per-slot current limit and health telemetry (voltage, temperature, cycle count).
- **Power & health:** Charge-state LEDs; cooling as required; rack reports fleet health to the station console.
- **Security:** Data-diode style ports (power/health only); no firmware writes; lockable door; inventory reconciliation at open/close.

5.5 Voter-Facing Test Mode (Spot-Check)

- **Purpose:** Allow any voter to spot-check that a module and machine are functioning correctly **without** affecting election data or revealing candidate mappings.

- **Activation:** Poll worker toggles **TEST** on the machine (keyswitch or sealed menu). Panel shows **"TEST"**; machine will not accept **CAST**.
- **Sample wheel overlay:** Removable **Test Wheel** disc printed with **random letters/symbols** (not candidate names/numbers). Mapping is randomized daily and posted on a placard for test only.
- **Flow:**
    1. Voter takes a bound module in **LOCK**; worker sets machine to **TEST**.
    2. Voter turns module to **VOTE**, inserts, rotates wheel to the prompted letter/symbol, and presses **Confirm**.
    3. Machine displays **"You selected: <symbol>"**.
- **Timing & privacy: No voterhash/votehash is ever generated; nothing posts to the ledger.** Test duration is **constant-time equal to CAST (60 s)** and uses identical cues.
- **Auditing:** TEST increments a **public Test counter** on the station dashboard; no per-module/per-voter IDs.
- **Abort & safety:** Exiting **TEST** requires keyswitch + dual-officer confirmation. Any mismatch quarantines the machine and prints a **TEST FAIL** incident code.

---

6) Eligibility & Authorization

- **Check-in:** Officer validates voter; issues a **one-time authorization** bound to that station's event.
- **Consumption:** Machine accepts at most one CAST per valid authorization; duplicates visibly rejected and logged.
- **Accounting:** Station dashboard shows **authorizations issued**, **casts accepted**, **voids with reason**; totals reconcile at close.

---

7) Cryptographic Commitments (Abstract)

- **Rotating minute-key:** Derived inside SE from secret seed + time; non-exportable.
- **Voterhash:** Computed inside the module from the minute-key, a device-only secret and a window nonce; not linkable to identity or choice.
- **Votehash:** H(voterhash, selection, device-only secret, window); does not reveal choice without the secret.
- **Receipt:** Voter receives **{voterhash, votehash}**; sufficient to prove **inclusion**, insufficient to prove **choice**.
- **Batch publication:** Ledger publishes per-candidate **counts**, sets **voters:{voterhash…}** and **votes:{votehash…}** (order randomized; no per-ballot timestamps), **VRF proof** of timing (§8.3), and **Merkle chaining** to the prior batch.

8) Consortium Ledger (Public Bulletin Board)

- **Validators:** Election Commission, recognized opposition parties, apex court IT cell, national universities. Appends require threshold signatures.
- **Snapshots:** Hourly state snapshots mirrored to public archives; divergence alarms within 5 minutes.
- **Openness:** APIs and snapshots are public; verifier source is open.
- **Batch record (conceptual):**

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

9) Operational Telemetry & Tripwires

- **Live station metrics:** uptime, queue length bands, modules in service, attestation pass-rate, **modules bound vs present**, authorizations vs casts vs voids.
- **Tripwires:** Z-score outliers auto-open incident tickets; breaches of wait-time SLO trigger surge redeployment or paper fallback.
- **Privacy:** Telemetry carries no candidate or voter identity; reported at 5–10-minute granularity.

10) Capacity Planning (Normative)

- Let **T** = voters assigned to booth; **H** = hours open; **$\lambda = T/(60H)$** votes/min required.
- Each module yields ~**1 vote/min** (fixed **60 s**).
- **Booth provisioning rule:** If a booth has **M_v** voter machines, stock **N = 3 × M_v** reusable modules. Rationale: one **casting**, one **being returned/checked**, one **on rack** per machine.
- Typical India booth (T≈1,000, H≈11, M_v≈2): **N = 6** modules suffices; urban peaks scale with **M_v**.
- Surge cache at sector depot: **+1 × M_v** sealed spares.

11) Privacy & Side-Channel Controls

- **Constant-time CAST (60 s); batch posting** per §8.3; no per-candidate signals.
- **Shrouded wheel + bracket**; no overhead line-of-sight of selection.
- **No personal wireless interfaces** on modules or machines.
- **Accessibility parity: identical enclosures with no outward label** across SKUs.

12) Attestation, Supply Chain & Tamper

- **Measured boot:** Firmware hashes on allow-list; SE holds attestation key; service-mode challenge/response only via sealed provisioning jig under dual-control.
- **Mixed vendors, lot randomization:** Prevent monoculture capture; distribution logs public.
- **Tamper mesh:** Opening zeroizes SE and raises a permanent visible flag; devices quarantined and logged.
- **Booth binding certificates:** Modules possess a **Booth-Bind Cert** signed by provisioning authority; machines verify this matches their **Booth ID** before CAST. Re-binding emits a signed **Rebind Event** to the ledger and enforces a **7-day lockout**.

13) Availability & Chaos Engineering

- **Brownout drills:** PV + crank SKU + supercap sustain CAST in off-grid precincts; local cache persists until link resumes, then batch-commit.
- **Surge redeployment:** Pre-signed logistics to move spares within 30 minutes when SLO breached.
- **Fallback:** Paper contingency sealed and reconciled to ledger by RLA rules.

14) Governance & Law (Binding Requirements)

- **In statute:** machine-readable rolls; public diffs per revision; observer access; **consortium ledger membership**; open verifier; RLAs; publication SLAs for telemetry and snapshots; whistleblower protections; procurement transparency; **VRF beacon source fixed in statute**.
- **Change control:** Supermajority + cooling-off for any rule change affecting audits, telemetry, or proofs; civil injunction path within 48 hours.

15) Audits & Acceptance

- **Pre-election:** Red-team exercises (Appendix A) with public after-action reports.
- **Election-day metrics:** Attestation pass-rate ≥ 99.95%; 95th-percentile wait ≤ 20 min (urban) / 30 min (remote); zero unauthorized ledger rewrites; inclusion verification success ≥ 99.9% on first try.
- **Post-election:** RLAs and cryptographic verification; constituency-wise transparency packs (snapshots, verifier, how-to inclusion guide in major languages).

---

16) Cost & Deployment (Indicative)

- **Module BOM (core): ~$10–$13** at national scale (PV/hand-crank removed from default).
- **Off-Grid Power SKU:** add **~$3** per unit (PV + crank) where required.
- **Wheel retrofit:** ~$15–$20 per machine.
- **Station kit (normative): N = 3 × M_v** modules + charging/UV rack + retrofit + spares, reusable for 5–7 years.
- **National roll-out:** For ~1.05M booths, hardware capex under pooled-reuse model scales with **M_v**; see Appendix E for scenarios.

---

17) Rollout Plan (Phased)

1. **Pilot (≤1%)**: mixed urban/rural; public observers; publish full data.
2. **Scale-up (10–25%)**: incorporate after-action fixes; independent audit sign-off.
3. **Nationwide**: statutory tripwires live; transparency dashboards public; bug bounty on verifiers.

---

18) VRF-Governed Sliding-Window Cadence (SWC)

Definition. For each batch, a verifiable randomness function (**VRF**) seeded with the prior batch root and a public randomness beacon selects a step Δ ∈ {−2, −1, 0, +1, +2} to shift a center index over 5-minute bins, forming a ±2 sliding window. Using the same seed, the system deterministically selects the batch interval **R** from that window. Batches close on **time**, **size**, **idle**, or **end-of-poll**—whichever occurs first. Operators have zero discretion. Observers recompute Δ, the window, and **R** from the published **VRF proof** in the batch header.

Rationale. SWC is unpredictable to adversaries, reproducible to auditors, and resistant to operator timing games. It reduces timing-correlation fingerprints while preserving bounded latency.

Requirements.

- Publish the **VRF proof** and **beacon epoch** in the batch header.
- All machines in a booth share the same **R** for a given batch.
- No per-ballot timestamps; randomize order of votes and voters sets.
- Optional publication jitter ±(30–60 s) after batch close.

---

19) Designated Paper-Trail Booths (Eco-Minimal)

Scope. Only booths pre-earmarked for paper trail produce physical artifacts; all others remain paper-quiet.

When to print. At each **batch close** (per §8.3 SWC) in an earmarked booth.

What to print (Batch Anchor Slip).

- **Batch Merkle Root (full)** and **short ID** (QR optional).
- **Prev Root (short)** to show chaining.
- **Counts per candidate** for this batch.
- Header: *Election ID, Constituency ID, Booth ID, Voter Machine ID, Batch ID, Window Label (SWC).*
- Signatures: two officers + one observer.

What never appears on paper. No votehash list, no voterhash list, no per-ballot timestamps, no mapping from votehash → candidate.

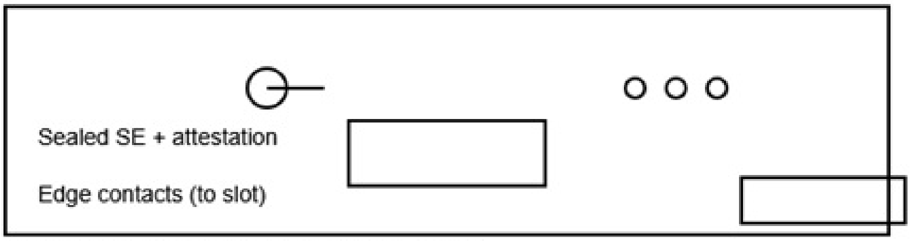
Chain of custody. Affix slips to a **Daily Audit Sheet** or store sequentially in a sealed envelope; record slip count in the booth log.

Public verification. Anyone can scan or enter the printed root to confirm it matches the public ledger; candidate counts match posted proofs. Slips are ancillary anchors, not primary records.

---

20) Representative Diagrams (stroke-only, black & white)

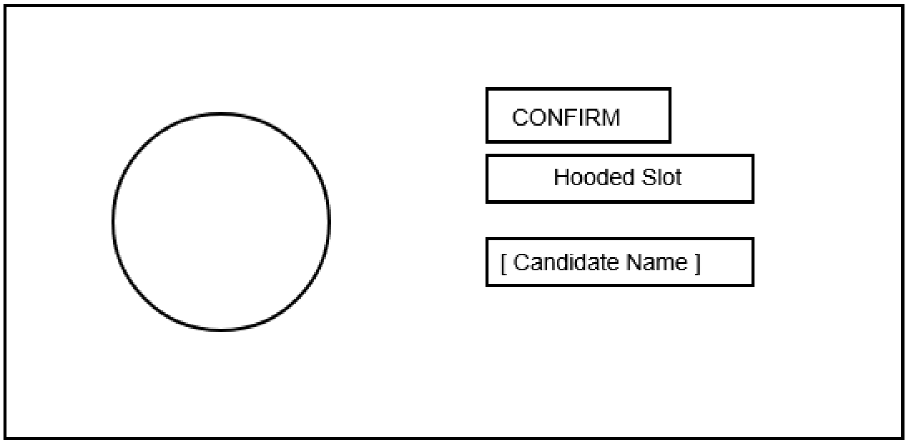
Fig. 1 - Two-position key (LOCK→VOTE); sealed secure element; edge contacts; no NFC/BLE; booth-binding.



Two-position Key: LOCK → VOTE

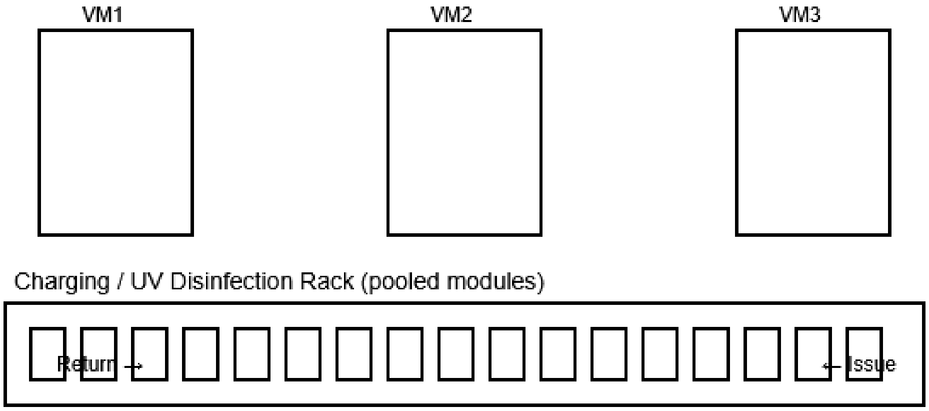
No NFC/BLE • Depot-only diagnostics • Booth-binding

Fig. 2 – Wheel can rotate either direction; wheel selects into bracket; single hooded slot; constant-time cast; confirm button.



Constant-time CAST • Shrouded bracket • No per-ballot timestamps

Fig 3 – Pooled module rack with charge/UV; flow: issue → cast → return; modules are booth-bound.



Appendices

Appendix A — Red-Team Playbook (Public)

Goal: Attempt to violate secrecy, inclusion, append-only behavior, attestation, booth-binding, or VRF cadence **without** insider privileges, and with plausible operator constraints.

A.1 Threat Matrix (examples)

1. **Timing games:** Correlate per-voter cast time with posting time to infer choice.
2. **Batch tamper:** Prune or reorder posted entries without breaking chain validation.
3. **Booth-binding bypass:** Use a bound module at the wrong booth/machine.
4. **Attestation forgery:** Boot unauthorized firmware or spoof SE attest.
5. **Side-channels:** EM/audio/power differences that correlate with candidate selection.
6. **Receipt proving:** Use receipt artifacts to prove choice to a third party.
7. **VRF manipulation:** Predict/steer the sliding-window cadence (SWC) or suppress proofs.

A.2 Test Cases (sample)

1. **Timing:** Capture ingress camera timestamps vs batch publication times; show inference failure (AUC≤0.55).
2. **Batch integrity:** Try removing one `votehash` locally; verifier must detect chain break via `prevRoot/root`.
3. **Binding:** Module from Booth X fails CAST at Booth Y; ledger logs no CAST; local audit shows “binding mismatch”.
4. **Attestation:** Swap MCU image; provisioning jig must reject SE quote; device quarantines.
5. **Side-channel:** Measure current draw for 1000 casts across candidates; distributions indistinguishable (KS-test p>0.1).
6. **Receipt proving:** Attempt to construct a provable link from receipt to candidate; must be impossible without internal secrets.
7. **VRF:** Pre-compute R from public beacon only; must be infeasible without prior batch root.

A.3 Success Criteria

- Zero successful secrecy or append-only breaks.
- Inclusion checks reproducible by any third party (≥99.9% success).
- Binding/attestation/VRF incidents auto-quarantine with logged evidence.

A.4 Reporting

- Public after-action within 30 days: scenario, exploit path, mitigations, patches, verification artifacts.

Appendix B — Glossary & Normative Language

- **CAST:** Fixed, constant-time vote casting window (nominally 60 s).
- **Receipt-freeness:** A voter cannot prove their choice to a third party.
- **Booth-binding:** Module/machine cryptographic binding to a specific booth.
- **VRF:** Verifiable Random Function; governs batch timing window and interval.
- **SWC:** Sliding-Window Cadence derived from VRF (±2 bins over 5-minute centers).
- **RLA:** Risk-Limiting Audit; statistical audit of reported outcomes.
- **MUST/SHOULD/MAY:** RFC-2119 normative keywords used throughout this spec.

Appendix C — Verifier Test Vectors

C.1 Example Receipt Payload (QR)

```
{"ver":1,"batchRoot":"5d3879de4ca2463fe8b6600b172efef735429b4d439df02afc6d33d64cb952e2","electionId":"IN-202X-LS-Phase3","boothId":"TN-123-045","voterhash":"db39cf612ba0023a342053d5394ee6e4c9812b3f805228a4debfe375d7ac9695","votehash":"13c0ee0ad55b9d98a2065a3c0018c8d5b7943ff9d5ac83246aca5b49373e231e"}
```

C.2 Example Batch Record (conceptual JSON)

```
{
 "electionId": "IN-202X-LS-Phase3",
 "constituencyId": "TN-123",
 "boothId": "TN-123-045",
 "batchId": "TN-123-045-0007",
 "machineId": "VM-A",
 "counts": { "CID-01": 103, "CID-02": 97, "CID-07": 111 },
 "voters": [
  "db39cf612ba0023a342053d5394ee6e4c9812b3f805228a4debfe375d7ac9695",
  "9a3b8e7c0b9f4d83e8e29b7f0d1bf3cd8083a7d9a2f2b3c4d5e6f7a8b9c0d1e2"
 ],
 "votes": [
  "13c0ee0ad55b9d98a2065a3c0018c8d5b7943ff9d5ac83246aca5b49373e231e",
  "9f52b7f5b2f8d4a1f0c9e8d7c6b5a4f3e2d1c0b9a8f7e6d5c4b3a29181726354"
 ],
 "vrfProof": "VRF-PROOF-BASE64",
 "beaconEpoch": "2025-11-12T10:05:00Z",
 "prevRoot": "79f0e8b3d8e6d1c0b9a8f7e6d5c4b3a29181726354c6d7e8f9a0b1c2d3e4f5a6",
 "root": "5d3879de4ca2463fe8b6600b172efef735429b4d439df02afc6d33d64cb952e2"
}
```

C.3 Verifier Cross-Checks

- sum(counts.values()) == len(votes)
- len(votes) == len(voters)
- root == Merkle(batch_body) where batch_body excludes root
- prevRoot links to previous batch’s root
- vrfProof validates (Δ,R) against prevRoot + beaconEpoch

Appendix D — Receipt & QR Specification

D.1 Canonical Receipt Payload (QR)

- Encoding: **UTF-8 JSON** (option: CBOR in future)
- Fields:
  - ver (uint) — schema version
  - batchRoot (64-hex) — full Merkle root of the batch
  - electionId (string)
  - boothId (string)
  - voterhash (64-hex)
  - votehash (64-hex)

D.2 Printing Requirements

- ECC: **Q** (25%) or **H** (30%)
- Size: ≥ **25 mm** square; high contrast; matte stock
- Quiet zone: ≥ **4 modules**

D.3 Human-Readable Lines (on paper)

- Truncate only in print preview (e.g., first/last 8 hex chars).
- **Do not** truncate in QR.

D.4 Privacy Constraints

- No per-ballot timestamps
- No operator/station PII beyond boothId already public
- No candidate identifier in receipt

Appendix E — Cost Scenarios (Indicative)

Scenario	M_v (machines /booth)	Modules per booth (N=3×M_v)	Core Module BOM	Off-Grid SKU delta	Wheel Retrofit / machine	Rack (per booth)	Notes
Base rural	1	3	$10–13	+$3	$15–20	$40–60	Low power; off-grid in 20% booths
Standard	2	6	$10–13	+$3	$15–20	$60–90	Typical India booth (T≈1k, H≈11)
Urban peak	3	9	$10–13	+$3	$15–20	$80–120	Add surge cache +3 modules/sector

Reuse horizon: 5–7 years hardware; firmware OTA under measured-boot.
National roll-out: ~1.05M booths × scenario mix; procurement diversified across vendors.

Appendix F — Accessibility Parity Checklist

- **Timing parity:** Assisted SKUs use identical **CAST 60 s** window.
- **Cue parity:** Audio/visual/haptic cues standardized (no candidate-specific signals).
- **Enclosure parity:** External appearance indistinguishable; masking caps for special ports.
- **Path parity:** No distinctive operator handling that could deanonymize.
- **Attestation parity:** Same SE/attestation; SKU flag not externally exposed.
- **Documentation:** Public guidance in major languages; tactile and audio instructions.

Appendix G — Governance Text Pack (Model Clauses)

G1. Public Rolls & Diffs (statute):

“The Commission SHALL publish machine-readable electoral rolls and SHALL publish a public diff for every revision.”

G2. Consortium Ledger:

“A public, append-only bulletin board SHALL be maintained by a consortium of validators (Commission, recognized opposition parties, apex court IT cell, national universities) with threshold signatures.”

G3. VRF Beacon Source:

“The batch cadence SHALL be governed by a VRF seeded from the prior batch root and a public randomness beacon designated by statute.”

G4. Open Verifier & Snapshots:

“The reference verifier SHALL be open-source. Hourly snapshots SHALL be published with divergence alarms ≤ 5 minutes.”

G5. RLAs & Telemetry:

“Risk-limiting audits SHALL be conducted. Station telemetry SHALL be published at 5–10 minute granularity without PII.”

G6. Change Control:

“Changes to audit/telemetry/proof rules REQUIRE supermajority approval and a 30-day cooling-off period with injunctive relief available within 48 hours.”

Appendix H — Operational Telemetry Schema (Public)

H.1 Station Metrics (5–10 min)

```
{
 "electionId": "IN-202X-LS-Phase3",
 "boothId": "TN-123-045",
 "uptimeSec": 39240,
 "queueBand": "0-5|5-15|15-30|>30",
 "modulesPresent": 6,
 "modulesBound": 6,
 "castsAccepted": 742,
 "authIssued": 760,
 "voids": 8,
 "attestationPassRate": 0.9996,
 "testModeCount": 14,
 "lastBatchRoot":
"5d3879de4ca2463fe8b6600b172efef735429b4d439df02afc6d33d64cb952e2"
}
```

H.2 Divergence/Tripwire Events

```
{
 "type": "TRIPWIRE",
 "boothId": "TN-123-045",
 "metric": "queueBand",
 "zscore": 3.2,
 "threshold": 2.5,
 "action": "SURGE_DEPLOYMENT"
}
```

Appendix I — Provisioning, Attestation & Rebind

I.1 Measured Boot & Attestation

- SE holds device keypair; MCU boots allow-listed hashes; attests (fwHash, seState, boothId) to provisioning jig.
- Station accepts CAST only after verifying attestation stamp within validity window.

I.2 Booth Binding

- Module stores **Booth-Bind Cert** signed by authority; machine presents **Booth ID**; CAST proceeds only if match.

I.3 Rebind Event & Quarantine

- Rebinding requires dual-control jig; emits on ledger:

```
{
 "event": "REBINDBIND",
 "moduleId": "MOD-XYZ-123",
 "fromBooth": "TN-120-002",
 "toBooth": "TN-123-045",
 "when": "2025-11-01T09:00:00Z",
 "sig": "BASE64-THRESHOLD-SIG"
}
```

- Module enters **7-day lockout** before activation at new booth.

Appendix J — Formal Threat Model (Summary)

J.1 Adversary Capabilities

- Partial control of logistics/procurement/media; limited insider influence; access to vendors; policy levers for quiet rule changes.

J.2 Constraints

- Must preserve plausible deniability; elections cannot be abolished; subject to public proofs and multi-party oversight.

J.3 Assumptions & Trust Roots

- Mixed vendors; SE supply diversity; threshold-sig validator set; public randomness beacon integrity.

J.4 Mitigation Mapping

- **Secrecy:** constant-time casting; receipt excludes choice; no per-ballot timestamps.
- **Inclusion:** dual-hash receipt; public sets {voters}, {votes}.
- **Append-only:** Merkle chaining prevRoot→root; hourly snapshots; third-party mirrors.
- **Binding/Attest:** Booth-Bind Certs; measured boot; public Rebind Events.
- **VRF/SWC:** Window and R from VRF(prevRoot, beacon); operator has zero discretion.

Appendix K — Change Log & Citation

- **v1.0 — 2025-11-09:** Initial consolidated master spec; booth-binding; N=3×M_v provisioning; rack charging/UV; voter-facing Test Mode; English placards; cost tables; authorship section.
- **v1.1.0 — 2025-11-09:** Removed NFC & APP user mode; two-position key (LOCK→VOTE); updated privacy and attestation; updated module BOM; clarified Test Mode (LOCK only); editorial fixes.
- **v1.2.0 — 2025-11-09:** Added **§8.3 SWC** (VRF-governed cadence; ±2 window; zero operator discretion).
- **v1.3.0 — 2025-11-09:** Dual-hash **receipt {voterhash, votehash}**; explicit **ledger sets** (voters, votes) with randomized order; **SP-8** (VRF verifiability) and **SP-9** (booth-binding auditability); clarified Test Mode (**no hashes, 60 s**); batch record box in §8; governance adds **statutory VRF beacon**.
- **v1.3.1 — 2025-11-12:** Editorial sync; version & citation alignment; text-only PDF build.
- **v1.4.0 – 2025-12-28:** Additional details; improved diagrams; JSON and QR code for improved verification.

How to cite:

Gopanna, M. (primary), & GPT-5 Thinking (co-author). *Master Specification — India-Scale End-to-End Verifiable Voting (Wheel + One-Slot + Reusable Module)*, **v1.4.0**, 2025-12-28. CC BY 4.0.