NEXUSNODE

Verifiable Advisory Poll — System Specification

Public Draft v1.0.2

One-District MVP using Voter Roll + one-time codes (OTP) + Public Bulletin Board (PBB) + 2-of-3 Trustees

Authors

Vince Mbanze • Thabo Pilusa • Ofentse Pholosi

Organisation

Nexusnode

Date / Location: 8 October 2025 — Johannesburg

Provenance: Submitted as a public comment to the IEC (South Africa) consultation on e-voting/online participation (30 Sep 2025). *No endorsement implied.*

DOI: 10.5281/zenodo.17292553 • **License:** CC BY 4.0 • **Contact:** vince.mbanze@nexusnode.co.za

Contents

1 Executive Summary

Purpose

- Prove that a lean, low-cost system can deliver publicly auditable advisory poll results in one district without national-election complexity.
- Build trust and capacity: demonstrate receipts, transparency, and basic governance with independent trustees.
- Establish a clean upgrade path to the NP3 "north star" (blind tokens, kiosks, stronger privacy, more trustees) without re-architecting.
- Bound risk and cost for stakeholders while gathering real operational data to decide whether to scale.

Phase 1 Deliverables)

- **Jurisdiction:** One pilot district (urban or peri-urban) with existing voter roll snapshot.
- **Eligibility:** Existing voter roll + one-time codes via SMS/IVR. Codes are rate-limited and recorded on a public, append-only ledger (hashes only). No biometrics.
- **Channels:** Web + USSD/SMS (mobile-responsive web; concise USSD flows). Top 3 local languages; large-text and basic TTS on web. No kiosks in MVP.
- **Ballot types:** Yes/No and simple 1-of-N multiple choice.
- **Verifiability:** Per-ballot receipt hash shown to voters and posted to a Public Bulletin Board (PBB); full list of cast records is published to enable public inclusion checks. Trustee-signed tally for results (end-to-end cryptographic re-tally deferred to Phase 2).
- **Revoting:** Last-vote-wins via per-poll HMAC pseudonym (client-held secret).
- **Trustees & governance:** 2-of-3 threshold (e.g., local university, civil society NGO, audit/accountancy firm). Trustees co-sign poll manifest, roll digest, hourly PBB roots, and final results.
- **Operations:** 48–72-hour poll window; SLA 99.5%; DDoS front door; rate limits; staffed help desk. Public incident log and post-mortem within 7 days.
- **Deliverables:** Pilot plan, poll manifest, open-source verifier script, PBB artefacts (receipts, code-spend entries, hourly Merkle roots), trustee statements, results explainer.

Phase-1 trust model (explicit)

In this MVP, the server holds choices; integrity is enforced by: (a) a Public Bulletin Board (PBB) with ISSUANCE_HASH, SPEND_HASH, and RECEIPT_HASH records and hourly Merkle roots, (b) 2-of-3 trustee co-signatures on manifest, roots and results, (c) voter receipt inclusion checks, (d) a public incident log with 24-hour disclosure, and (e) a published TALLY NOTE describing all exclusions (duplicates/late/invalid). Full public re-tally with cryptographic proofs is scheduled for Phase 2.

Success Criteria (phase-gate to Phase 2)

Integrity & Transparency

- **Receipt inclusion:** $\geq$ 95% of a random sample of voters can find their receipt hash on the PBB; 0 unexplained omissions.
- **Code ledger soundness:** 0 double-spend codes accepted; all issued/consumed code hashes reconcile.
- **Independent assurance:** At least two external observer groups validate that (a) the PBB is complete and append-only, and (b) the trustee-signed tally matches the posted cast records.
- **Incident transparency:** 100% of Sev-1/Sev-2 incidents logged publicly within 24 hours; no unresolved Sev-1 at close.

Availability & Operations

- **Channel uptime:** $\geq$ 99.5% during the poll window for web and USSD/SMS; retry success $\geq$ 99% within 5 minutes.
- **Support responsiveness:** Median help-desk first response ¡ 10 min during peak hours.

Adoption & Inclusion

- **Participation target:** Meets or exceeds a pre-agreed district target (e.g., $\geq 2\times$ historical participation for comparable consultations).
- **Channel diversity:** $\geq$ 25% of valid ballots via USSD/SMS (evidence of reach beyond web).
- **Accessibility checks:** User testing in at least 3 languages; documented fixes before go-live.

Governance & Safety

- **Trustee performance:** All required trustee co-signatures delivered on time; no quorum failure.
- **No material security failures:** No verified ballot stuffing or silent edits; any attempted attacks publicly disclosed with remediation.

Exit/Advance Decision

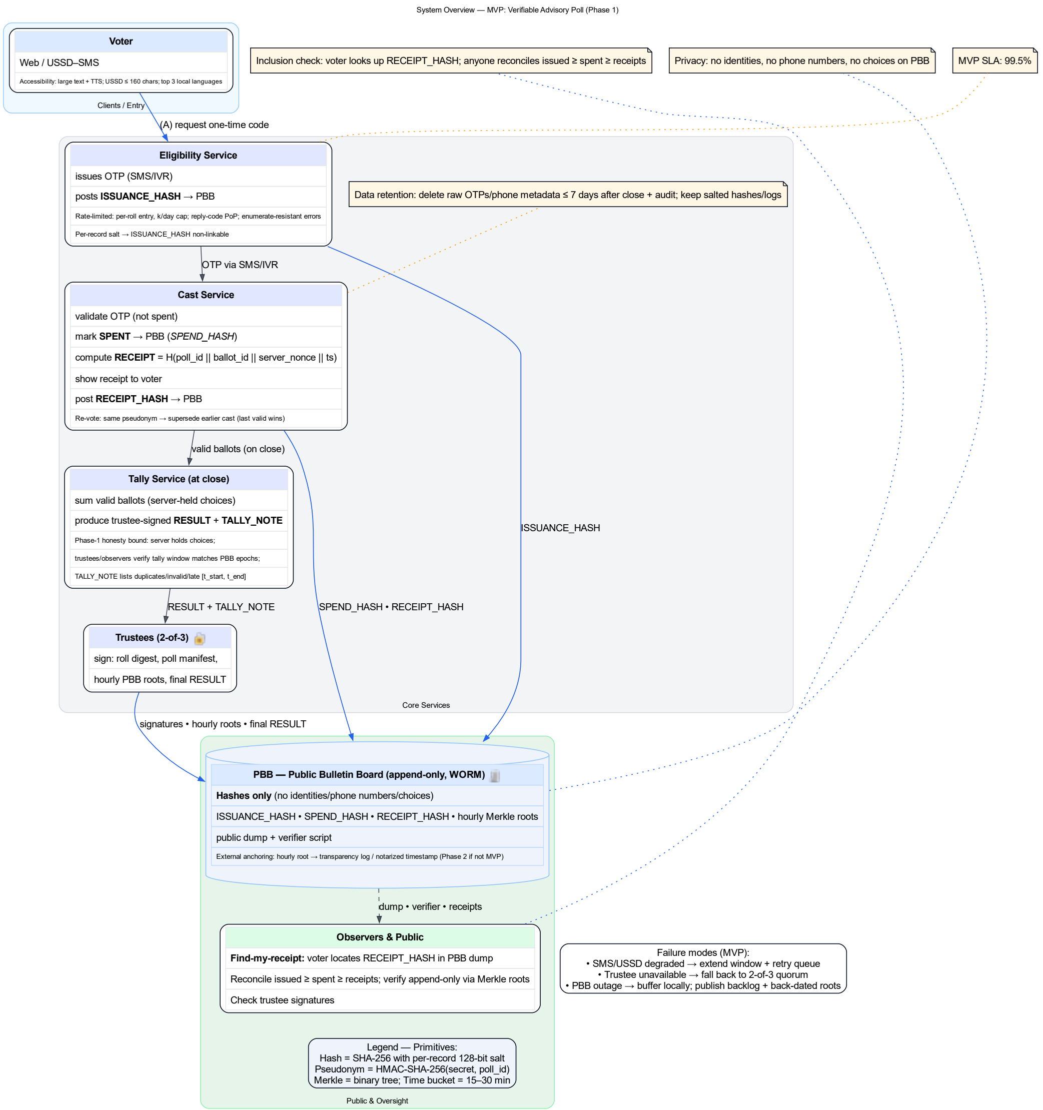
If all **bold** criteria above are met, proceed to Phase 2 (multi-channel scale-up, blind-signed tokens, 3-of-5 trustees, stronger proofs). If not, remediate and re-run within the same district before expanding scope.

Out of scope (Phase 1) biometrics, kiosks, anonymous credentials/blind tokens, homomorphic/mix-net tally, 3-of-5 ceremonies, 99.95% SLOs. See §5 Roadmap.

2 System Overview

Purpose

Deliver a lean, auditable advisory poll in one district using the existing voter roll, one-time pin (OTP), a public bulletin board (PBB) of hashed artefacts, and 2-of-3 independent trustees. Identity never enters the cast path. Stronger crypto and channels are deferred to later phases without re-architecting.



System Overview — MVP: Verifiable Advisory Poll (Phase 1)
Voter
Web / USSD–SMS
Accessibility: large text + TTS; USSD ≤ 160 chars; top 3 local languages
Clients / Entry
Inclusion check: voter looks up RECEIPT_HASH; anyone reconciles issued ≥ spent ≥ receipts
Privacy: no identities, no phone numbers, no choices on PBB
MVP SLA: 99.5%
(A) request one-time code
Eligibility Service
issues OTP (SMS/IVR)
posts ISSUANCE_HASH → PBB
Rate-limited: per-roll entry, k/day cap; reply-code PoP; enumerate-resistant errors
Per-record salt → ISSUANCE_HASH non-linkable
Data retention: delete raw OTPs/phone metadata ≤ 7 days after close + audit; keep salted hashes/logs
OTP via SMS/IVR
Cast Service
validate OTP (not spent)
mark SPENT → PBB (SPEND_HASH)
compute RECEIPT = H(poll_id || ballot_id || server_nonce || ts)
show receipt to voter
post RECEIPT_HASH → PBB
Re-vote: same pseudonym → supersede earlier cast (last valid wins)
valid ballots (on close)
Tally Service (at close)
sum valid ballots (server-held choices)
produce trustee-signed RESULT + TALLY_NOTE
Phase-1 honesty bound: server holds choices;
trustees/observers verify tally window matches PBB epochs;
TALLY_NOTE lists duplicates/invalid/late [t_start, t_end]
ISSUANCE_HASH
RESULT + TALLY_NOTE
SPEND_HASH • RECEIPT_HASH
Trustees (2-of-3)
sign: roll digest, poll manifest,
hourly PBB roots, final RESULT
Core Services
signatures • hourly roots • final RESULT
PBB — Public Bulletin Board (append-only, WORM)
Hashes only (no identities/phone numbers/choices)
ISSUANCE_HASH • SPEND_HASH • RECEIPT_HASH • hourly Merkle roots
public dump + verifier script
External anchoring: hourly root → transparency log / notarized timestamp (Phase 2 if not MVP)
dump • verifier • receipts
Observers & Public
Find-my-receipt: voter locates RECEIPT_HASH in PBB dump
Reconcile issued ≥ spent ≥ receipts; verify append-only via Merkle roots
Check trustee signatures
Failure modes (MVP):
• SMS/USSD degraded → extend window + retry queue
• Trustee unavailable → fall back to 2-of-3 quorum
• PBB outage → buffer locally; publish backlog + back-dated roots
Legend — Primitives:
Hash = SHA-256 with per-record 128-bit salt
Pseudonym = HMAC-SHA-256(secret, poll_id)
Merkle = binary tree; Time bucket = 15–30 min
Public & Oversight

Figure 1: MVP System Overview (Phase 1). **Alt text:** "Voter requests OTP → casts vote → PBB records issuance/spend/receipt hashes → trustees co-sign results; choices never appear on the PBB."

Phase-1 Trust Model (explicit)

- **Custody:** Choices are stored server-side; no identities and no choices are posted to the PBB in Phase 1.
- **Compensating controls:**
  - PBB reconciliation: ISSUANCE $\geq$ SPEND $\geq$ RECEIPT,

  - Receipt inclusion (find-my-receipt),
  - Hourly Merkle roots (append-only verification),
  - 2-of-3 trustee signatures on manifest, roots, and results,
  - TALLY NOTE (window, rules, exclusions),
  - Public incidents within 24h.
- **Roadmap:** Phase 2 introduces per-ballot validity proofs and public re-tally (homomorphic or equivalent), keeping the same PBB contract.

Components (minimal surface area)

- **Clients:** Web (mobile-responsive, large text/TTS) and USSD/SMS (concise prompts, top 3 local languages).
- **Eligibility Service:** Issues OTPs to roll-listed voters; posts `ISSUANCE_HASH` to PBB.
- **Cast Service:** Validates OTP, records choice (server-side), posts `SPEND_HASH` and `RECEIPT_HASH` to PBB; supports last-vote-wins via per-poll HMAC pseudonym.
- **Tally Service:** At close, produces counts + `TALLY NOTE` (exclusions, windows) and emits trustee-signed `RESULT`.
- **Trustees (2-of-3):** University, NGO, audit firm (example). Co-sign roll digest, poll manifest, hourly PBB roots, and final result.
- **Public Bulletin Board (PBB):** Append-only WORM feed of salted hashes + hourly Merkle roots (optionally anchored externally).
- **Cryptographic primitives (MVP):** SHA-256 with per-record 128-bit salt; HMAC-SHA-256 for revote pseudonym; Merkle tree (binary); coarse time buckets (15–30 min).
- **Privacy rule:** No identities, phone numbers, or choices on the PBB.

End-to-end flow (Phase-1)

1. **OTP request (Eligibility):** Voter (web/USSD/SMS) requests OTP → Eligibility verifies roll entry + rate limit → sends OTP and posts `ISSUANCE_HASH` to PBB.
2. **Cast (Cast Service):** Voter submits {OTP, choice, channel, timebucket}. Service verifies OTP unused, records choice internally, marks spent, derives receipt H(poll_id || ballot_id || server_nonce || timebucket), returns receipt to voter; posts `SPEND_HASH` and `RECEIPT_HASH` to PBB.
3. **Revote:** Same voter can recast; server uses HMAC(secret, poll_id) pseudonym to supersede prior casts → last valid wins.
4. **Tally & publication:** At close, Tally Service selects last-valid per pseudonym within the PBB-anchored window, computes totals, produces `TALLY NOTE` (rules + exclusions) and `RESULT`. Trustees co-sign; artefacts published.

Public artefacts (PBB schema)

- **ISSUANCE_HASH:** {`ts_bucket, kind=ISSUANCE, salted_hash, channel_tag, merkle_idx`}
- **SPEND_HASH:** {`ts_bucket, kind=SPEND, salted_hash, channel_tag, merkle_idx`}
- **RECEIPT_HASH:** {`ts_bucket, kind=RECEIPT, salted_hash, channel_tag, merkle_idx`}
- **Roots:** Hourly Merkle roots + signed daily snapshots (optional external anchoring).
- **Results bundle:** Trustee-signed `RESULT`, `TALLY NOTE`, manifest, roll-digest signature, PBB epoch references.

Verifiability (MVP bar)

- **Voter inclusion:** Each voter finds their `RECEIPT_HASH` on the PBB.
- **Observer reconciliation:** Check monotonic PBB, match counts: `ISSUANCE` ≥ `SPEND` ≥ `RECEIPT`, verify Merkle proofs and trustee signatures, and that the tally uses exactly the referenced PBB epochs.
- (Full public re-tally with ciphertexts is deferred to Phase 2.)

Operations & guardrails

- **Poll window:** 48–72 hours. SLA 99.5% for web + USSD/SMS; retries auto-queued.
- **Incident transparency:** Public incident log within 24h; post-mortem ≤7 days.
- **Failure modes (one-liners):**
  - SMS/USSD degraded → extend window + backoff + queued resend.
  - Trustee unavailable → proceed with 2-of-3 quorum.
  - PBB outage → buffer locally; publish backlog with back-dated roots.
- **Data retention:** Raw OTPs/telemetry purged ≤7 days after close + audit; hashed artefacts/logs retained; no choice data on PBB.
- **Abuse controls:** OTP rate-limits per roll entry; enumeration-resistant errors; fraud monitoring on issuance→spend deltas.

Interfaces (public)

- `POST /otp/request` → "sent" + issuance_id; emits `ISSUANCE_HASH` to PBB.
- `POST /ballot/cast` → returns receipt; emits `SPEND_HASH` & `RECEIPT_HASH`.
- `GET /pbb/feed` → NDJSON feed + hourly Merkle roots; signed daily snapshot.
- `GET /results` → trustee-signed `RESULT` + `TALLY NOTE` + PBB references.
- `GET /incidents` → live incident log.

Out of scope (Phase 1)

- biometrics, kiosks, anonymous credentials/blind tokens, homomorphic/mix-net tally, 3-of-5 ceremonies, 99.95% SLOs. See §5 Roadmap.

Upgrade path (no rewrites)

OTP → blind-signed tokens (accumulator); server attestations → ZK validity proofs; 2-of-3 → 3-of-5 trustees; add kiosks & full accessibility; optional homomorphic tally and universal re-tally in Phase 2–3.

3 Eligibility, Channels, Trustees & Verifiability

3.1 Eligibility (no biometrics)

Data basis

- **Source:** District voter-roll snapshot (CSV or DB export) taken ≤30 days before poll.
- **Fields required:** national_id, full_name, dob, district_code, msisdn (if available), address_hash (optional).
- **Pre-processing:** dedupe on national_id; export digest = SHA-256(snapshot_bytes); trustees co-sign digest.

OTP issuance (SMS/IVR)

- **Code format:** 8 digits (10^8 space), TTL 15 min, max 3 active codes per voter, 1 issuance/hour cap.
- **Request inputs:** national_id + DOB (or roll PIN if present).
- **Anti-enumeration:** identical error string for "not on roll / wrong DOB / rate limit".
- **Delivery:** SMS primary; IVR fallback (TTS reads OTP twice). Optional USSD "pull" message.
- **PBB artefact (issuance):** { `ts_bucket, kind:"ISSUANCE", salted_hash: SHA256(national_id` || `poll_id` || `salt_128), channel_tag: "SMS"|"IVR", merkle_idx` }
  (salt unique per record; salt never published.)
- **Abuse controls:** per-roll-entry quotas; device fingerprint (web) soft limit; telco throttles; graylist after 5 failures/24h.
- **Support flow (lost phone):** help desk verifies 3 roll facts + out-of-band callback; issues one manual override code logged to PBB (kind:"OVERRIDE").

SIM-swap & OTP interception mitigations (MVP)

- **Short-lived OTPs:** 8 digits, 15-minute TTL, 1 issuance/hour, max 3 active.
- **Challenge-response (optional):** IVR call-back that reads a short phrase; user types the last 2 words as confirmation.
- **Anomaly detection:** flag and rate-limit issuance patterns (per-MSISDN and per-ID); graylist after 5 failed verifications/24h.
- **Victim recourse:** help-desk override OTP (one-time) after 3 roll facts + call-back; override posted to PBB as kind:"OVERRIDE".
- **Comms hardening:** publish official short codes/USSD strings; "phrase of the day" shown in USSD/Web.
- **Budget note (MVP):** call-back + monitoring adds R87,000–R175,000 (telephony + engineering).

Spend & replay protection

- **On cast:** mark OTP "spent"; post SPEND_HASH with same salted keyspace as issuance.
- **No PII on PBB:** only salted hashes + time bucket + channel tag.

Retention & privacy

Retention & privacy

Data class	Contains	Retention	Purge verifier	Anchor
OTPs & delivery telemetry	OTP value, MSISDN, delivery status	$\leq$ 7 days after close + audit	DPO + trustee co-sign deletion attest	Daily PBB note
Cast server logs	ballot_id, pseudonym, channel, timestamps (no choice on PBB)	$\leq$ 7 days after post-mortem	Ops + trustee spot-check	Daily PBB note
PBB artefacts	salted hashes, ts_bucket, Merkle roots	Indefinite (public record)	N/A	N/A
Incident records & results	incident entries, RESULT, TALLY NOTE	Indefinite	N/A	N/A

Processing basis: public-interest consultation. Minimisation: no identities/phones/choices on PBB. Deletion attestations are referenced in the PBB daily snapshot.

Success metrics (eligibility)

- $\geq$99% OTP delivery within 60s (SMS) / 30s (IVR callback).
- 0 accepted double-spend; issuance$\geq$spend with explained deltas.

3.2 Casting Channels

A. Web

- **UX:** mobile-first; 12–16 pt fonts; high-contrast; optional TTS; 3 local languages.
- **Form:** otp, choice, language, accessibility flag.
- **Session:** CSRF token; 5-min idle timeout; no tracking cookies; no analytics scripts.
- **Rate limits:** /otp/request 5/min/IP (sliding window); /ballot/cast 2/min/IP.

B. USSD/SMS

- **USSD flow (example):**
    1. Welcome + language (isiZulu / isiXhosa / English)
    2. Enter OTP
    3. Choose option: 1) YES 2) NO (or 1-of-N MCQ)
    4. Confirm → show short receipt (Base32, 20 chars snippet)

    USSD validation gate (readiness)

    - Pre-flight test with $n \geq 200$ users in-district; require $\geq$90% completion without assistance.
    - If below threshold, auto-fallback affected cohort to SMS/Web; publish rationale on /incidents and note in TALLY NOTE.
- **Session timeout:** 20–30 s between steps (telco default).

- **SMS flow:** “Reply with OTP YES/NO or OTP ¡option¿”; server returns receipt snippet + link to “find my receipt”.
- **Store-and-forward:** if aggregator degraded, queue and retry with idempotency key; preserve first-seen ts_bucket.

C. Common cast behaviour

- **Receipt:** `receipt = Base32( SHA-256( poll_id || ballot_id || server_nonce || ts_bucket ) )[0..32]`
- **PBB artefacts (cast):**

```
SPEND_HASH:   { ts_bucket, kind:"SPEND",   salted_hash, channel_tag, merkle_idx }
RECEIPT_HASH: { ts_bucket, kind:"RECEIPT", salted_hash: SHA256(receipt || salt_128),
                channel_tag, merkle_idx }
```

- **Revote:** client stores k (32 bytes random). Pseudonym P = HMAC-SHA-256(k, poll_id). Server supersedes older casts with same P. P not on PBB.

Operational SLOs (channels)

- Uptime ≥99.5% during window; p95 cast latency ≤3 s (web) / ≤8 s (USSD).
- Retry success ≥99% within 5 minutes on transient failures.

3.3 Trustees & Governance (2-of-3)

Composition & criteria

- **Candidates:** one local university (CS/Stats dept), one civil-society NGO, one audit/accountancy firm.
- **Independence:** sign conflict-of-interest statement; publish bios and roles.

Ed25519 key custody & ceremony schedule (Phase 1)

- **Keys:** Per-poll Ed25519 signing keys for each trustee. Storage: cloud KMS/HSM or split-secret (two admins).
- **Quorum:** 2-of-3 signatures required for (a) roll digest & manifest, (b) hourly/daily PBB roots, (c) results bundle.
- **Ceremonies:**
  - T0 (-72h): co-sign roll_digest and manifest.json (hashes published).
  - Hourly (or daily): co-sign pbb_root_YYYYMMDDHH.
  - Close (+8h SLA): co-sign results_bundle (RESULT, TALLY NOTE, PBB epoch refs).
- **Availability:** at least 2 trustees reachable 10:00–22:00 during the window; sign-off SLA ≤4h.
- **Audit trail:** all signatures, key-use events, and ceremony minutes posted with the artefact bundle.

Transparency & oversight

- **Incident co-sign:** Convening authority + one trustee sign the public incident log entries (Sev-1/2).
- **Post-mortem:** combined report ≤7 days; raw PBB and verifier script attached.

3.4 Verifiability Model (MVP bar)

What the public can check

- **Inclusion:** “Find-my-receipt” — search PBB dump for RECEIPT_HASH (site + downloadable file).
- **Append-only:** Verify Merkle proofs from records to hourly roots; check roots are monotonic; (optional) external anchoring.
- **Reconciliation:** Count artefacts by kind and confirm ISSUANCE $\geq$ SPEND $\geq$ RECEIPT; differences must match TALLY NOTE (invalid/duplicate/late).
- **Result authenticity:** Validate trustees’ signatures on results_bundle and that the bundle references a specific PBB epoch range.

What observers can reproduce

- Run the open-source verifier to: (a) parse NDJSON PBB feed, (b) verify Merkle proofs & signatures, (c) recompute counts and receipt inclusion rate, (d) check tally window alignment and exclusions.

Trust & limitations (explicit in MVP)

- Server holds choices (no ciphertexts on PBB yet). Protection is via tamper-evidence, reconciliation, and multi-party signatures.
- No unlinkability guarantees beyond removing identifiers from PBB; metadata privacy hardening deferred to Phase 2–3.

Advance-to-Phase-2 gate (verifiability)

- $\geq$95% sampled voters find receipts; 0 unexplained omissions.
- Independent groups reproduce counts and match trustee-signed results.
- All Sev-1/2 incidents logged within 24h and resolved.

PBB Feed: Field Schemas (NDJSON)

```
# Common fields: ts_bucket: "YYYY-MM-DDTHH:MMZ"; channel_tag: "WEB"|"USSD"|"SMS"
{ kind:"ISSUANCE", salted_hash:"hex32", ts_bucket, channel_tag, merkle_idx: uint32 }
{ kind:"SPEND",    salted_hash:"hex32", ts_bucket, channel_tag, merkle_idx: uint32 }
{ kind:"RECEIPT",  salted_hash:"hex32", ts_bucket, channel_tag, merkle_idx: uint32 }

# Hourly root record (separate file or header)
{ kind:"ROOT", hour:"YYYY-MM-DDTHH:00Z", merkle_root:"hex32", prev_root:"hex32",
  signer:"trustee_id", sig:"base64" }
```

Receipt format shown to voter

- 32-char Base32 (groups of 4: ABCD-EFGH-IJKL-MNOP-QRST-UVWX-YZ23-4567).
- “Find my receipt” link accepts the full string or pastes a snippet to search.

Guardrails & Failure Modes

- **SMS/USSD degraded:** queue casts; extend window; post incident with impact estimate; ensure PBB includes original ts_bucket.
- **Trustee unreachable:** proceed when any 2-of-3 have co-signed; record attempts and escalation in incident log.
- **PBB outage:** buffer locally; publish backlog with original timestamps; attach proof of local WORM buffer (append-only log hash chain).

- **Suspicious spikes (fraud ops):** trigger rate caps and manual review; publish summary in TALLY NOTE.

Endpoints (public)

- `POST /otp/request` → `{status:"sent", issuance_id}`
- `POST /ballot/cast` → `{status:"ok", receipt}`
- `GET /pbb/feed` → NDJSON + hourly roots
- `GET /results` → results_bundle.json (RESULT, TALLY NOTE, signatures, root refs)
- `GET /incidents` → live log (Sev-1/2/3)

Out of scope (Phase 1)

- biometrics, kiosks, anonymous credentials/blind tokens, homomorphic tally, 3-of-5 or 5-of-7 trustees, 99.95% Service Level Objectives (SLOs). See §5 Roadmap.

4 Operations — MVP (Phase 1)

Goal: keep the one-district advisory poll stable, transparent, and cheap to run—while making every hiccup visible and accountable.

4.1 Poll window & change control

- **Window:** 48–72 hours (published in manifest).
- **Code freeze:** T-72h (infrastructure), T-48h (app config/content). Only Sev-1 fixes allowed during poll with trustee-acknowledged change record.
- **Maintenance:** none during window. All cron/batch jobs paused or rescheduled.

4.2 Service Level Objectives

- **Availability:** web and USSD/SMS ≥ 99.5% during window.
- **Latency:** p95 `/ballot/cast` ≤ 3 s (web), ≤ 8 s (USSD end-to-end); p95 `/otp/request` ≤ 2 s.
- **OTP delivery:** ≥ 99% delivered within 60 s (SMS) / 30 s (IVR callback).
- **Retry success:** ≥ 99% within 5 min on transient failures.
- **PBB freshness:** append within ≤ 2 min of event; hourly Merkle root published ≤ 5 min after hour.
- **Trustee sign-offs:** hourly/daily roots within 4 h; final results within 8 h of poll close.
- **Error budgets:** 0.5% downtime; 1% latency budget; any overrun triggers incident + post-mortem.

4.3 Monitoring & alerting

- **Probes:** HTTP health, USSD round-trip, SMS loopback, OTP issuance rate, cast success rate, queue depths, PBB append lag, Merkle root age, signature backlog.
- **Dashboards:** “Eligibility”, “Casting”, “PBB”, “Channels”, “Trustees”.
- **Alerts (examples):**
  - Cast success < 97% over 5 min (Warn) / < 95% (Sev-2).
  - PBB lag > 5 min (Sev-2).
  - OTP delivery < 95% in 15 min bucket (Sev-2).
  - Trustee sign-off > 4 h behind (Sev-3).

  - DDoS: 95th percentile IPs hitting rate cap for 10 min (Sev-2).

4.4 T-48h pre-flight incident drill (pass/fail gate)

- **Scenarios:** (1) SMS/USSD degradation, (2) PBB outage/backfill, (3) trustee unreachable, (4) fraud spike (issuance→spend delta).
- **Success:** each scenario contained in $\leq$30 min; PBB lag ¡5 min; incident template populated.
- **Gate:** if any scenario fails, no-go until remediated. Publish a short drill summary on /incidents at T-24h.

4.5 Abuse controls & rate limits

- **Eligibility:** 1 OTP issuance/hour, max 3 active codes; graylist after 5 failed verifications/24h.
- **API:** `/otp/request` 5/min/IP; `/ballot/cast` 2/min/IP; per-MSISDN throttles at aggregator.
- **Enumeration protection:** uniform error messages; time-bucketed logs.
- **Anomaly triggers:** sudden issuance→spend deltas, channel skews, or region spikes → throttle + incident note in TALLY NOTE.

4.6 Incident management & public comms

Severity taxonomy

- **Sev-1:** loss of cast/eligibility ¿ 15 min; data integrity risk; widespread OTP failure.
- **Sev-2:** PBB lag ¿ 15 min; partial channel outage; trustee quorum at risk.
- **Sev-3:** performance degradation; localized issues; delayed sign-offs without tally risk.

Roles (RACI)

- **Incident Manager (IM)** — leads response (A/R).
- **On-call Engineer (OCE)** — mitigation (R).
- **Trustee Liaison (TL)** — coordinates signatures/comms (R).
- **Comms Lead (CL)** — public statements & `/incidents` updates (A/R).
- **Ops Lead** — escalation & approvals (A).
- **Security** — forensics (C).

Timelines

- Declare within 10 min of detection (internal).
- Public log entry for Sev-1/2 within $\leq$ 24 h at `/incidents`, co-signed by convening authority + one trustee.
- Post-mortem $\leq$ 7 days, including impact, root cause, lessons, and action items.

Standard runbooks

- **SMS/USSD degraded:** queue requests, extend window, rotate to secondary aggregator; publish impact and extension rationale.
- **PBB outage:** buffer WORM log locally; backfill with original timestamps; include proof chain in post-mortem.
- **Trustee unreachable:** proceed with 2-of-3 quorum; document attempts; schedule catch-up signature.

4.7 Support & help-desk (Phase 1)

- **Staffing:** 2–3 agents (08:00–22:00), 1 lead on call.
- **SLAs:** first response ¡10 min during peak; resolution ¡60 min for OTP issues.
- **Scripts & flows:** OTP resend, SIM-swap override (with call-back), receipt lookup guidance, incident triage.
- **KPIs:** CSAT, median response/resolution, % resolved first contact, % escalations.
- **Budget note (MVP):** staffing, training, and tooling add R262,000–R349,000.

4.8 Deployment, resilience & DR

- **Topology:** active-active web tier; stateless app nodes; managed DB with point-in-time recovery; message queue for PBB appends.
- **Traffic:** CDN + WAF; per-endpoint rate caps; USSD/SMS via two MNO paths where available.
- **Backups:** DB snapshots hourly; PBB feed exported every hour to cold storage; verifier artifacts stored immutably.
- **Recovery targets:** RPO $\leq$ 5 min (PBB queue durable), RTO $\leq$ 30 min for app layer.

4.9 Access, secrets & data handling

- **Access:** least-privilege IAM; hardware keys (FIDO2) for admins; dual-control on prod changes.
- **Secrets:** KMS-backed; rotation per poll; audit all access.
- **Logging:** structured, no PII in app logs; correlate via request IDs.
- **Retention:** raw OTP/MSISDN/IP purged $\leq$ 7 days after close + audit; salted hashes & Merkle artifacts retained; DPIA attached.

4.10 Pre-flight tests & go/no-go

- **Synthetic drills:** OTP→cast→PBB→receipt→results every 15 min for 24 h pre-go-live.
- **Trustee rehearsal:** dry-run signatures on manifest and hourly root.
- **Load test:** 5× expected peak TPS for 30 min; no data loss; PBB lag ¡ 2 min.
- **Go/no-go checklist:** all SLO probes green, rollback plan validated, on-call roster staffed, trustees reachable.

4.11 Public endpoints

- `GET /status` (health), `GET /metrics` (scrape), `GET /incidents` (live log), `GET /pbb/feed` (ND-JSON + hourly roots), `GET /results` (results bundle).
- Status page links from homepage; uptime and recent incidents visible during window.

4.12 KPIs for success review

- SLO adherence; incident count & MTTR; receipt inclusion rate; issuance→spend→receipt reconciliation deltas; OTP delivery success; trustee turnaround time; public trust survey deltas.

Out of scope (Phase 1)

- 24/7 SOC, kiosk field ops, HSM ceremonies, 99.95%+ SLOs (introduced in later phases). See §5 Roadmap.

5 Roadmap & Upgrade Path — from MVP to NP3

Goal. Grow the lean MVP into a nationally trusted, privacy-preserving system without re-architecting. Each phase adds capability only after the prior one proves value.

5.1 Migration invariants (won't change as we scale)

- **PBB contract stays stable:** ISSUANCE, SPEND, and RECEIPT records + hourly Merkle roots; new artefacts are additive.
- **Receipts are forever:** same receipt format; past voters can always find theirs.
- **APIs evolve compatibly:** `/otp/request`, `/ballot/cast`, `/pbb/feed`, `/results` remain; new endpoints are additive.
- **Separation-of-concerns:** identity never in cast path; trustees sign manifests/roots/results at every phase.
- **Cryptographic agility:** proofs/keys upgraded behind the same artefact names (e.g., "validity_proof" field appears in Phase 2+).

5.2 Phase 2 — Scale & Stronger Proofs (multi-district, 6–18 months)

What we add

- **Eligibility:** swap OTP → blind-signed tokens; add spent-set accumulator.
- **Verifiability:** add per-ballot validity proofs (0/1 and 1-of-N) and a public replayable tally (homomorphic ElGamal or deterministic commitment tally + proofs).
- **Trustees:** expand to 3-of-5; introduce light ceremony runbooks and independent key custody.
- **Channels & access:** add supervised kiosks in libraries/clinics; full 11 languages + SASL planning.
- **Anchoring:** publish PBB hourly roots to an external transparency log/notary.
- **Ops:** SLO 99.7%; secondary SMS/USSD aggregator; regional redundancy.

Phase-2 advance gates (who signs the go/no-go)

Dimension	Gate	Owner(s)
Technical	≥99.9% verifier pass; 0 unexplained PBB omissions	Tech Lead + External Reviewer
Operational	SLOs met for 2 consecutive polls; DR drills passed	Ops Lead
Inclusion	≥25% non-web ballots; USSD success ≥90% in follow-up test	Inclusion Lead
Trust	2 independent observer reports endorse auditability	Convening Authority
Institutional	Trustees meet quorum/SLAs; ceremony transcripts published	Trustee Liaison
Financial	Budget for Phase 2 secured; unit costs not rising	Finance/PMO

5.3 Phase 3 — Privacy & Provincial Scale (5–8 provinces, 12–24 months)

What we add

- Anonymous credentials / unlinkable tokens (e.g., BBS+/CL) to sever metadata links.
- **Coercion resistance:** robust re-vote semantics with public cut-off markers; cover-traffic & tighter time-bucket jitter.
- **Universal re-tally:** mandate homomorphic tally (or mix-net if ballots grow) with public decryption proofs.

- **Governance:** formalize trustee independence, conflict-of-interest, and public ceremony transcripts; 3-of-5 standardized.
- **Ops:** light 24/7 on-call, formal change control, tabletop exercises; SLO 99.9%.

Success gate (advance to Phase 4)

- External privacy audit confirms unlinkability; handle 500k+ participants/poll; verified accessibility across languages & disability modalities; no Sev-1 unresolved at close.

5.4 Phase 4 — Optional Biometrics (only if justified, 6–12 months)

What we add (if fraud/impersonation data warrants)

- Selective biometric enrolment for high-risk polls/regions; cancelable templates, PAD thresholds, and opt-out paths.
- Mobile enrolment vans for rural access; independent biometric adjudication enclave.
- **PIA & governance:** full privacy impact assessment; public consultations; independent oversight.

Success gate (advance to Phase 5)

- Evidence biometrics reduce demonstrated fraud; PAD fairness across demographics; public acceptance metrics; no critical privacy findings.

5.5 Phase 5 — National Scale & Advanced Features (24–36+ months)

What we add

- Nationwide coverage; complex ballots (ranked choice, multi-select with constraints).
- **Advanced crypto:** mix-nets for complex ballots; end-to-end verifiability by default; third-party public verifiers ecosystem.
- **Ops:** 24/7 SOC, red-team programs, supply-chain attestations; SLO 99.95%+.
- **Sustainability:** stable funding line; procurement framework; training & certification for kiosk operators and trustees.

5.6 Decision gates & stop criteria (applies between every phase)

Dimension	Gate to Advance	Stop / Reassess
Technical	≥99.9% proof/verifier pass; zero unexplained PBB omissions	Any verifier mismatch; unpatched Sev-1
Operational	SLO met for 2 consecutive polls; DR drills passed	Recurring outages; PBB lag ¿ target
Inclusion	Measurable lift in underserved channels (targets per phase)	Regressing participation or accessibility
Trust	Independent observer reports endorse auditability	Public trust surveys decline
Institutional	Trustees meet quorum/SLAs; ceremonies reproducible	Quorum failures; unresolved conflicts
Financial	Budget secured for next phase; unit costs trending down	Unsustainable per-vote costs

5.7 Cost & staffing trajectory (order of magnitude, to set expectations)

Planning rate: R17.45/US$; figures rounded; see Appendix B for detail. If there is any discrepancy, Appendix B prevails.

- **Phase 1 (MVP): R8.1M – R14.3M**
Team 4–6, cloud + SMS/USSD, light external audit, 15% contingency. (Matches Appendix B total.)
- **Phase 2–3: R34.9M – R52.4M**
Multi-district ops, kiosks, proofs, 3-of-5 trustees, regional redundancy. (≈ US$2–3M at R17.45.)
- **Phase 4–5: R174.5M+**
National ops, 24/7 SOC, advanced crypto, sustainability line. (≈ US$10M+ at R17.45.)

Currency & rounding note. All amounts in ZAR using a fixed planning FX rate R17.45/US$ for this version; add ±10% buffer for FX movement. Totals are rounded to the nearest R0.1M for readability.

5.8 Backward-compatible upgrade mechanics

- **Eligibility:** OTP service remains as fallback even after tokens; switch via feature flag.
- **Proofs:** add `validity_proof` field; legacy records stay valid with "attested" type.
- **Trustees:** rotate to 3-of-5 by adding keys and updating quorum policy; old signatures remain valid.
- **Tally:** introduce homomorphic tally alongside server tally for a transition period; retire server tally after two clean runs.
- **Anchoring:** begin with daily anchors → move to hourly without changing record format.

5.9 Out of scope (Phase 1) — slated for later phases

- Biometrics, anonymous credentials, full homomorphic/mix-net tally by default, kiosks at scale, 3-of-5+ trustee ceremonies, 24/7 SOC, 99.95% SLOs.

One-line message for reviewers: We start small (receipts + PBB + 2-of-3 trustees), and every added feature is a bolt-on under the same public artefacts and APIs — no rewrites, just more assurance as value and capacity grow.

A Threat Model & Mitigations (MVP / Phase 1)

Scope reminder. MVP defends tamper-evidence and public auditability for a one-district advisory poll. We do not yet provide unlinkable ballots or homomorphic public re-tally (comes in Phase 2–3). Identity never enters the cast path.

A.1 Assets & trust boundaries

- **Assets:** voter-roll snapshot + digest; OTP issuance/spend state; cast log (choices server-side); PBB artefacts (ISSUANCE_HASH, SPEND_HASH, RECEIPT_HASH records + roots); trustee keys; results bundle.
- **Boundaries:** Clients ↔ Eligibility ↔ Cast ↔ PBB ↔ Observers; Trustees sign manifests/roots/results but don't see identities or choices.

A.2 Adversaries (personas)

- **A. External attacker:** tries SMS/USSD abuse, mass OTP guessing, DDoS, phishing.
- **B. Insider (operator):** attempts silent edits, ballot stuffing, selective suppression.
- **C. Trustee failure/collusion:** unresponsive key holder, refusal to sign, or biased sign-off.
- **D. Telco/aggregator issues:** delivery delays, misrouting, SIM-swap exposure.
- **E. Coercer/influencer:** pressures a voter; attempts to verify compliance.
- **F. Privacy snooper:** correlates timing/metadata to deanonymize voters.

Threats → Controls (MVP)

Threat	What could go wrong	MVP controls (now)	Upgrade path
OTP guessing / brute force	Cast without eligibility	8-digit codes, 15-min TTL, 1 issuance/hr, 3 active cap; uniform errors; per-MSISDN/IP throttles; anomaly alarms	Tokens + accumulator (P2)
Enumeration of voter roll	Probe who is on roll	Same error for "not on roll / wrong DOB"; rate caps; delayed responses	Anonymous creds (P3)
Ballot stuffing / silent edits	Server injects or alters choices	PBB reconciliation (ISSUANCE $\geq$ SPEND $\geq$ RECEIPT), hourly Merkle roots, public incident log; 2-of-3 trustee signatures on results + roots; TALLY NOTE explains exclusions	Homomorphic public re-tally + ZK validity (P2)
Dropping receipts / selective inclusion	Hide inconvenient votes	Voter "find-my-receipt" on PBB; receipt inclusion gate $\geq$95%; external dumps; WORM storage; backfill proofs	External anchoring by default (P2), independent verifiers
DDoS / rate exhaustion	Casting/OTP unavailable	CDN+WAF, per-endpoint caps, queue/ retry, multi-MNO where possible, extend poll window; Sev-1 runbooks	Regional redundancy SLO 99.7–99.9% (P2–3)
Trustee unavailability	No quorum to sign	2-of-3 policy; named backups; 4h sign-off SLA; incident disclosure	3-of-5 with rehearsed ceremonies (P2)
Trustee bias/collusion	Rubber-stamp bad result	Public artefacts (PBB), third-party verification; co-signed incident logs	Independent ceremony transcripts; split custody (P2–3)
SIM-swap / OTP interception	Attacker casts in victim's name	Short TTL; help-desk override (logged); last-vote-wins lets voter overwrite	Tokens + revocation; optional callback (P2)
Timing correlation	Infer who voted when	15–30 min time buckets; fixed posting cadence	Cover traffic + jitter; unlinkable tokens (P3)
Phishing / fake channels	Users tricked to send OTP	Official short codes; "phrase of the day" banner; comms kit; block look-alike domains	Signed USSD menus; app attestation (P2)
PBB desync or loss	Can't audit events	Durable local WORM buffer; hourly Merkle roots; backfill with proof chain	External transparency log anchoring (P2)

Out of scope (Phase 1): unlinkable credentials, homomorphic/mix-net tally by default, biometric fraud controls, 24/7 SOC. Each appears in the roadmap (Phases 2–4).

B Cost Estimates & Staffing (MVP / Phase 1) — ZAR

B.1 Staffing plan (3–4 months)

Role	**Headcount**	**Notes**
Tech lead / architect	1 (3 mo)	Owns design, security, go/no-go
Backend engineers	2 (3 mo)	Eligibility, cast, PBB, results APIs
Frontend/USSD engineer	1 (2.5 mo)	Web UI, USSD flows, i18n
DevOps/SRE	1 (3 mo)	Infra, monitoring, CI/CD, DR
Security engineer	0.5 (2 mo)	Threat model, hardening, drills
PM / Delivery	0.5 (3 mo)	Schedule, stakeholders, ceremonies
Help-desk / Comms	1 (1.5 mo)	Scripts, incident comms, support
Total	**∼7 FTE-months**	

B.2 Budget envelope (12-month view; scale down if pilot is shorter)

Category	**Estimate (ZAR)**
Engineering & PM	R5,235,000 – R8,725,000
Cloud & ops	R698,000 – R1,396,000
SMS/USSD	R523,500 – R1,047,000
External audit/review	R436,250 – R872,500
Accessibility & i18n	R174,500 – R349,000
Contingency (15%)	R1,047,000 – R1,919,500
Total (MVP)	**R8,114,250 – R14,309,000**

B.3 Variable unit costs (planning)

- **Per OTP (all-in):** R0.87 – R2.09 (calc of \$0.05–\$0.12 × 17.45).
- **Per cast request (compute):** R0.0087 – R0.0349 (≈ R0.01 – R0.04).
- **Per kiosk:** excluded in MVP (would add ± R35,000 – R90,000 per unit + staffing if introduced later).

B.4 Timeline (indicative)

- **Weeks 1–2:** design finalisation, trustee MoUs, telco onboarding
- **Weeks 3–6:** build eligibility/cast/PBB, USSD flows, monitoring
- **Weeks 7–8:** load tests, trustee rehearsal, comms kit, DPIA
- **Week 9:** soft-launch drill; go/no-go
- **Week 10:** poll window (48–72h) + live incident page
- **Week 11:** results + post-mortem + public artefact bundle

B.5 Deliverables checklist

- manifest.json + roll digest (signed); API services; USSD menus
- PBB feed + hourly Merkle roots; open-source verifier script
- Incident site + comms templates; help-desk scripts
- Results bundle (RESULT, TALLY NOTE, signatures, PBB epoch refs)
- DPIA memo; lightweight security review report

Out of scope in MVP: kiosks procurement/ops, HSM ceremonies, 24/7 SOC, biometrics, provincial-scale SMS volumes (budgeted in later phases).