PKI Implementation in IEBC Critical Infrastructure

End-to-end trust for KIEMS, RTS, onboarding, disinformation defence & the IEBC public site

PKI across the voting-to-declaration process

- **Voter authentication (KIEMS):** biometric match on device; kit identity attested by device certificate.
- **Physical voting & manual count:** offline, in the open, agents present — no digital dependency.
- **Form 34A capture & signing:** Presiding Officer's **personal eMudhra signing certificate** binds the transcribed figures and image hash to a named human at a timestamp.
- **Transmission to RTS:** mutual TLS over dual-SIM / satellite; KIEMS & RTS mutually authenticate with X.509 certificates.
- **RTS ingestion:** every payload signature verified against the officer's cert & the device cert before acceptance.
- **Tally & publication:** constituency & national tallies signed by IEBC certs; public portal serves signed artefacts.
- **Declaration & audit:** signed logs + hash chain give a court-admissible evidence trail (Kenya Evidence Act §106B).

Why PKI = 100% compliance

- **Authenticity:** every digital Form 34A traceable to a named officer & kit.
- **Integrity:** any post-signing tampering invalidates the signature immediately.
- **Non-repudiation:** officers cannot deny submissions bearing their private key.
- **Confidentiality in transit:** mTLS prevents interception or injection on the wire.
- **Chain of custody:** cryptographic timestamps + signed audit logs meet evidentiary standards.
- **Court-admissibility:** aligns with Kenya Evidence Act §§78A, 106B on electronic records.

AI-assisted voter & official onboarding (PKI-anchored)

- **Liveness & face match:** AI verifies the applicant against ID/passport photo — blocks spoofs, deepfakes and duplicate enrolments.
- **Document intelligence:** OCR + tamper detection on Kenyan ID / passport MRZ & security features before biometrics are captured.
- **Risk scoring:** ML flags anomalies (mass enrolments, geo-inconsistencies, synthetic identities) for human review.
- **Certificate issuance:** on approval, eMudhra CA issues a **personal signing certificate** to Presiding Officers, Returning Officers & IEBC staff — bound to the vetted identity.
- **Key protection:** keys generated in a hardware token / secure element; never exportable; PIN + biometric unlock at the kit.
- **Lifecycle:** automated renewal, revocation (CRL/OCSP), and role-based re-issuance controlled from the IEBC PKI console.

AI-assisted disinformation management

- **Real-time monitoring:** AI scans social platforms, messaging channels & news for narratives targeting the election, tallies or officials.
- **Deepfake & synthetic media detection:** models flag manipulated audio/video/images purporting to be IEBC communications.
- **Claim triage:** NLP clusters emerging false claims (e.g. 'server hacked', 'Form 34A altered') and routes them to the IEBC rapid-response desk.
- **Authoritative counter-signal:** verified rebuttals published on the IEBC site are **digitally signed** — so the rebuttal itself cannot be forged.
- **Provenance for official media:** IEBC statements, press releases & result artefacts carry C2PA-style signed provenance so citizens & media can verify origin.
- **Feedback loop:** confirmed disinformation cases retrain models & inform takedown requests to platforms.

PKI-secured IEBC website — authenticating the source of information

- **Extended Validation TLS:** IEBC domain served under an EV certificate so browsers show verified organisation identity.
- **Signed content artefacts:** Form 34A images, constituency tallies & national results published with detached digital signatures + hash manifests.
- **Public verification tool:** citizens, media & observers can upload any downloaded artefact and verify the signature against IEBC's published CA chain.
- **Signed press releases & advisories:** every official communication carries a verifiable signature — anything unsigned is, by definition, not from IEBC.
- **Tamper-evident audit portal:** hash-chained log of every result submission, revision & publication event, exportable for court proceedings.
- **Anti-impersonation:** DNSSEC, DMARC/DKIM/SPF on IEBC mail, and CAA records restricting who may issue certs for iebc.or.ke.

Lipafo Payment Solutions · eMudhra — Trust infrastructure for Kenyan elections. Aligned to Kenya Evidence Act (§§78A, 106B), Data Protection Act 2019, and IEBC ICT policy.