Open Admissons Network.

the problem, plain and technical. the admission pipeline rests on a small number of choke points, each of which fails in a predictable way. exam results live in closed systems with no independently verifiable provenance, so when a result disappears or is flagged there is no external proof. admission decisions and cut off rules are opaque, so candidates cannot verify why they were rejected or whether quotas and overrides were applied. the application flow forces a single choice or brittle preference rules, so students are forced into risky bets. document correction and identity fixes are manual, slow and error prone, creating an endless loop of reprints and office visits. agents and fraudulent registrations exploit these manual steps. the whole setup rewards gatekeepers, not data integrity, and every failure costs a student months or years.

fix that first. the single highest value move is an independent, verifiable record of truth for every credential and every admission event. a credible solution is a simple signed credential model. when an exam board issues a result, it either produces a digitally signed record, or a trusted verifier takes the authoritative paper and issues a signed attestation. that signed record is a small JSON object containing candidate id, test id, subject scores, timestamp, issuer id, and a signature. store the signature and a hash of the record in an append-only log. expose a public verification endpoint so any institution or employer can ask: show me the signed record for candidate x and confirm the signature. that single capability lets a university stop trusting screenshots and start trusting signatures.

address the root cause of score unreliability. results are often not falsified after the fact but corrupted during testing itself. leaks, impersonation, and bribery distort actual academic ability, so even an “authentic” result can be meaningless. verification must therefore capture not only the grade but the context of its creation. each valid test sitting produces a context record: centre id, invigilator id, timestamp, and a signed session hash. when a score is uploaded, it carries that signature. schools can later filter scores by verified provenance rather than by inflated marks.

make matching logical and algorithmic, not arbitrary. stop the single-choice lock. accept ranked preferences from candidates and have institutions publish explicit, machine-readable criteria and capacity. run a transparent matching algorithm, the kind that resolves capacity and preferences in predictable rounds, and log every offer and acceptance as another signed event. when a university overrides an automatic match, say for an athlete, scholarship candidate, or special quota, the admission officer records the reason field before confirming the offer. that override becomes a signed event in the audit log, visible and searchable. discretion remains, but secrecy dies.

remove paperwork by design. replace manual document checks with a canonical upload flow, verified once. every student creates one profile, uploads scanned originals, the system computes a hash, and issues an attestation once verification is complete. verification can be done by the issuing body if they cooperate, or by trusted verifiers who check originals and sign attestations. once a record is attested, the student and every institution reference the attested id, not a pdf. corrections are handled by versioned attestations, not physical reprints. that eliminates the pilgrimage of photocopies and waiting queues.

force transparency into scoring and cutoffs. publish the exact scoring formula and departmental threshold logic in machine-readable form. when a department says "cutoff 70," the formula that maps raw scores to that 70 must be public and reproducible. if a department wants to apply nonacademic filters, they declare them and log the applied exceptions. transparency will not end bias, but it converts suspicion into data that can be audited.

secure provenance and block scams through process metadata. require centre and proctor identifiers for any cbt session, log device metadata and session hashes, and correlate anomalies across submissions. flag suspicious patterns automatically and route them to human review. require agents living off payments to have no place in the canonical flow; if the system issues a signed attestation only after verified provenance, fake registrations and ghost centres collapse.

make appeals and redress public and fast. every appeal creates a case record, logged with a timestamp and decision signature. publish processing times and give the claimant a unique case id that anyone can query. service levels for response time become system variables, not guesswork. delay is a measurable harm, not a hidden one.

operate without waiting for the state. build verification and matching primitives in a way institutions can adopt incrementally. start with a signed credential and verification api usable by a private foundation programme, a university intake, or a scholarship board. once a few institutions use signed attestations for decisions, the benefit is visible: less fraud, faster processing, fewer appeals. adoption follows utility, not permission.

handle test integrity without owning testing. oan does not design or grade exams. it defines how test data are recorded, validated, and transmitted. exam boards keep autonomy but adopt a submission protocol: each test session logs a session id, centre id, timestamp, and proctor signature. those metadata are hashed and attached to the result. any school or auditor can check that a score originated from a registered centre and a valid session. the outcome is a cryptographic chain of custody without another bureaucracy.

technical specifics that matter, without hype. sign records with standard public-key cryptography, ecdsa or rsa, store the signature and record hash in an append-only ledger in postgres, optionally publish periodic merkle roots to a public timestamping service for proof. credentials are json objects using a fixed schema. verification endpoint returns the signed record and issuer metadata. matching runs on the same dataset and produces signed offers. logs are exportable and human-readable, not proprietary blobs.

what success looks like. a student uploads an attested waec or jupeb result once, the system returns a signed credential, the student applies to five partner universities in one flow, two offers come back within days with signed offers, the student inspects both offers and accepts one. the rejected offers show the exact formula that excluded them. no office visits, no reprints, no missing scores. that single chain proves the idea.

what makes it work operationally. one or two partner institutions that agree to accept signed attestations for a single intake, a trusted attestation path for exam results when boards do not cooperate, a lightweight verification api, and a minimal public audit log. measure real metrics, time to offer, number of corrections avoided, appeals closed. those numbers become the argument that erodes monopoly legitimacy.

that is the problem and the knife-edge solution. build signed attestations, a public verification api, preference-based matching with transparent formulas, and a versioned document correction workflow. everything else is refinement.