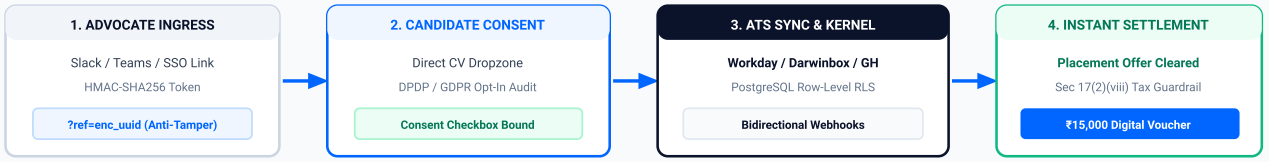
SYSTEM TOPOLOGY, INGRESS & TOKEN ATTRIBUTION

Zero-Trust Referral Pipeline • TLS 1.3 / AWS WAF Perimeter • Ephemeral HMAC Token Rails

HOSTING: **AWS ap-south-1 (Mumbai)**
Sovereignty Isolated VPC

LAYER 1 TO LAYER 4 ARCHITECTURAL PIPELINE

TLS 1.3 • HMAC-SHA256 SIGNED • AWS VPC



TOKENIZED INGRESS & URL SIGNING

Referral generation converts advocate NetIDs into ephemeral, encrypted payloads via AES-128-CBC ciphering with an appended HMAC-SHA256 signature. This prevents brute-force enumeration, URL tampering, and fraudulent advocate self-attribution.

`HMAC-SHA256 • Anti-Spoofing Nonce`

PERIMETER ISOLATION & WAF RULES

All external traffic terminates at an AWS Application Load Balancer with TLS 1.3 enforced. Requests pass through AWS WAF rules evaluating rate limiting, IP reputation, bot mitigation, and SQL injection inspection before reaching internal services.

`TLS 1.3 • AWS Shield • WAF Rate-Limiting`

TRANSIENT CV INGESTION DROPZONE

Candidate uploads are accepted via dedicated presigned S3 URLs directly into an ephemeral quarantine bucket with server-side KMS encryption. Files undergo automated ClamAV scanning before passing to metadata extraction workers.

`Presigned S3 Ingest • Ephemeral KMS`

EVENT-DRIVEN ASYNCHRONOUS PIPELINE

Ingress events decouple immediately via Amazon SQS and Redis BullMQ queues. Ingestion workers process payloads without blocking candidate-facing interfaces, ensuring low p99 latencies during heavy employee campaigns.

`BullMQ Worker Pool • <45ms Ingress SLA`

Zero-Trust Ingress Standard: No raw employee identities, candidate contact details, or job req IDs are ever passed in plain text across public routing paths. Links are bound to tenant IDs and validate cryptographic nonces before rendering candidate dropzone UI.

ATS SYNCHRONIZATION, WEBHOOK RETRIES & RLS ISOLATION

Bidirectional Enterprise Ingest • Exponential Backoff Dead-Letter Queues • Kernel Row-Level Multi-Tenancy

DATABASE: **PostgreSQL 16**
Kernel Tenant Boundary

ENTERPRISE ATS INTEGRATION SPECIFICATIONS & AUTH HANDSHAKES

PLATFORM	AUTH & CONNECTION	WEBHOOK TRIGGER HANDLER	FIELD LEVEL MAPPING
Workday Recruiting	REST / RaaS + OAuth 2.0 mTLS	`Candidate_Hired`, `Offer_Accepted`	Candidate ID, Job Req, Advocate NetID
Greenhouse Software	Harvest API v5 + Webhook Secret	`candidate.hired`, `stage_change`	Candidate UID, Email, Referral Source
Darwinbox HRMS	Event Webhooks + API Key Signature	`onboarding_completed`	Employee ID, Candidate Ref, Joining Date
SAP SuccessFactors	OData v4 API + SAML Bearer	`JobApplicationAudit`	Application ID, Advocate Staff ID

EXPONENTIAL BACKOFF

Failed ATS webhook deliveries retry automatically across 5 stages with randomized jitter: 30s, 2m, 10m, 1h, and 6h intervals to absorb downstream ATS maintenance windows.

`5-Stage Retry • Jitter Buffer`

DEAD-LETTER QUEUE (DLQ)

Payloads exceeding retry limits transition to an encrypted Dead-Letter Queue. System alerts notify enterprise integration managers with the raw unhandled payload preserved.

`AWS SQS DLQ • PagerDuty Alarm`

IDEMPOTENCY GUARD

Every incoming ATS event requires a SHA-256 idempotency key generated from event ID and timestamp. Duplicate webhooks are rejected, preventing duplicate voucher releases.

`Idempotency-Key • Redis Lock`

POSTGRESQL KERNEL ROW-LEVEL SECURITY (RLS) ARCHITECTURE

Multi-tenant database tables enforce PostgreSQL kernel-level Row-Level Security policies. Connection pooling services bind each query to an active enterprise context via `SET LOCAL app.current_tenant_id = 'tenant_uuid'`. Even if an application bug causes a developer query to omit a `WHERE organization_id = ...` clause, the PostgreSQL engine filters records at the database level. Direct cross-tenant data leaks are mathematically impossible.

`Kernel Enforced` `Zero Query Leakage` `PgBouncer Pooled`

ESCROW SETTLEMENT, AUDIT IMMUTABILITY & DATA DISPOSAL

Section 17(2)(viii) Non-Monetary Engine • Append-Only SIEM Streams • Cryptographic PII Shredding

GOVERNANCE: **DPDP Act 2023**
72-Hr Breach SLA

AUTOMATED ESCROW DISBURSEMENT

Upon receiving an authenticated hire webhook, the settlement daemon confirms available balance in the client's dedicated escrow account. It issues real-time API calls to digital gift aggregators (Amazon Pay, Flipkart, Croma) without human touch.

`Sub-3s Settlement • Zero Manual Ops`

SECTION 17(2)(VIII) TAX ENGINE

The disbursement kernel tracks annual perquisite accumulations per employee PAN/Employee ID. If aggregate payouts approach the statutory ₹15,000 threshold, the platform halts automated release and alerts HR payroll admins.

`Perquisite Capping • Rule 3(7)(iv) Safe`

APPEND-ONLY IMMUTABLE SIEM LOG

Audit events write to an append-only S3 bucket with Object Lock compliance mode enabled. Audit events stream continuously to enterprise SIEM platforms (Splunk, Datadog, Sumo Logic) for centralized security monitoring.

`S3 Object Lock • SIEM Webhook Export`

CRYPTOGRAPHIC PII ERASURE ENGINE

Candidate records older than the enterprise retention schedule (default 90 days) trigger automated cryptographic shredding: resume files in S3 are deleted, database PII columns are nulled, and only anonymized IDs remain for billing integrity.

`Right-to-be-Forgotten • Automated Purge`

PRODUCTION INFRASTRUCTURE SLA & INCIDENT GUARANTEES

Uptime Commitment:
99.9% monthly availability SLA backed by contractual service credits across all core API endpoints.

Disaster Recovery RPO/RTO:
RPO < 5 minutes (continuous WAL archiving); RTO < 30 minutes with multi-AZ automatic failover.

Incident Response:
24/7/365 On-Call SRE coverage with a guaranteed 72-hour formal breach notification SLA for Data Protection Officers.

Enterprise Procurement Note: Complete software-bill-of-materials (SBOM), annual third-party penetration testing summaries, and architecture review meetings with our Head of Engineering are available during enterprise proof-of-value evaluations.