Digital Infrastructure and API Governance - Section 1: CORE ARCHITECTURE OVERVIEW

BlueLoans4all's digital infrastructure is designed for scalability, security, and reliability. It powers real-time loan application processing, transaction tracking, and service delivery across customer, agent, and partner interfaces.

The infrastructure is microservice-based and deployed using container orchestration over Azure Kubernetes Service (AKS). Key modules include:

- Authentication & IAM Service
- Loan Origination System (LOS)
- Loan Management System (LMS)
- Notification Engine (Email, SMS, WhatsApp)
- API Gateway and Rate Limiter
- Data Analytics & Reporting Stack (Snowflake + Power BI)

Services communicate using encrypted RESTful APIs and asynchronous messaging via Azure Service Bus queues. A centralized configuration management service ensures consistent deployment of features across environments (dev, UAT, prod).

Digital Infrastructure and API Governance - Section 2: API CATALOG & ACCESS MECHANISMS

The API ecosystem at BlueLoans4all is modular, secure, and conforms to OpenAPI 3.0 standards.

Key APIs:

- `/loan/summary` - Fetch active loan status
- `/emi/schedule` - Generate EMI amortization table
- `/repayment/record` - Log manual or UPI-based payments
- `/customer/kyc` - Submit or verify eKYC
- `/policy/query` - NLP-based retrieval of policy clauses

Access Methods:

- Client applications authenticate via OAuth2.0 client credential flow
- Tokens issued with role-based access scopes (`read:loan`, `write:repayment`)
- Developer sandbox uses scoped test tokens, isolated from production

Client onboarding requires registration via the Developer Portal and is governed by terms-of-use and key-rotation policies.

Digital Infrastructure and API Governance - Section 3: SECURITY, ENCRYPTION & COMPLIANCE

All infrastructure components and APIs adhere to a zero-trust model with multiple layers of security:

1. Transport Security:

- TLS 1.3 enforced on all API endpoints
- HSTS headers and secure cookies for web interfaces

2. Data Protection:

- Customer PII and financial data encrypted using AES-256 at rest
- Field-level masking for Aadhaar, PAN, and bank account numbers

3. Access Control:

- All admin functions protected by Azure AD + MFA
- Role-based access (RBAC) enforced via JWT scope inspection
- Tokens expire in 15 minutes; refresh via silent SSO only

4. Compliance:

- Adheres to RBI's IT Framework for NBFCs, PCI-DSS (for payment APIs), and SOC 2 controls
- Quarterly VAPT audits and code review for critical modules
- Data residency ensured within Indian regions (Azure Central India and South India)

Logs of all API invocations, error traces, and access attempts are stored in tamper-proof Cloud Logging pipelines.

Digital Infrastructure and API Governance - Section 4: MONITORING, OBSERVABILITY & SLA MANAGEMENT

All services and APIs are continuously monitored using Prometheus, Grafana, and Azure Application Insights.

Monitored Metrics:

- Uptime (per service)
- Response latency (p50, p95, p99)
- API success/error codes
- Token issuance and expiry
- Queue processing times

Alerts are configured via Azure Monitor to trigger on-call Slack notifications or PagerDuty alerts for:

- Error rate > 5% in 5-minute window
- Response time > 2s on critical endpoints
- Queue backlog > 100 messages

SLA Commitments:

- 99.9% uptime for all public APIs
- Mean Time to Recovery (MTTR) < 15 minutes
- Client-impacting changes communicated with minimum 48-hour notice

Observability dashboards are available to Product, Engineering, and Compliance teams in real time.

Digital Infrastructure and API Governance - Section 5: DEVELOPER PORTAL, GOVERNANCE & AUDIT TRAIL

The Developer Portal (https://developer.blueloans4all.in) is the single source of truth for partner and internal teams to explore, register, and test APIs.

Features:

- API Explorer with schema visualization
- Test token generation for sandbox calls
- Changelog subscription and release history
- Auto-generated documentation via Swagger UI

Governance Policies:

- Every API must have a designated Product Owner and SLA matrix
- All new API deployments require pre-production security review
- Breaking changes must follow semantic versioning (v1 -> v2)

Audit Trail & Logs:

- Every token issuance, refresh, and revoke is logged with timestamp and IP
- Endpoint access logs retained for 365 days
- Audit reports are reviewed quarterly by Compliance Ops

Policy Review Cycle:

- This governance policy is reviewed bi-annually by the CTO Office
- Critical changes mandated by regulators may trigger an interim revision

Partner developers are bound by the API License Agreement and must acknowledge the Acceptable Use Policy at every major version update.