5. Security Architecture

Security is the foundation of our e-invoicing solutions. With sensitive financial and tax data flowing through client systems, <BluelightSmartAPI>, and FIRS MBS, we implement **end-to-end protection** that is aligned with international standards, regulator requirements, and enterprise audit expectations.

<diagram: Security layers from client ERP → SmartAPI → FIRS → Archive, with encryption, signing, monitoring>

5.1 Transport Security

- **TLS 1.3** for all traffic between client systems, SmartAPI, and FIRS MBS.
- **Mutual TLS (mTLS)** with client certificates for sensitive ERP integrations, ensuring both parties authenticate each other.
- **IP allowlisting and VPN options** for clients requiring stricter connectivity controls.
- **HSTS (HTTP Strict Transport Security)** enabled on all endpoints to prevent downgrade or man-in-the-middle attacks.

5.2 Authentication and Authorization

- **OAuth 2.0 with JWT tokens** signed by our PKI for API access.
- **mTLS-based client authentication** as an alternative for clients who prefer certificate-based identity.
- **Role-Based Access Control (RBAC)** ensures least privilege access across Finance, Compliance, and IT.
- **Multi-factor authentication (MFA)** for BlueInvoice SaaS and SmartAPI dashboards.
- **Audit logging of all authentication events**, shipped to SIEM for monitoring and anomaly detection.

5.3 Data Protection and Privacy

- **Encryption in transit** with TLS 1.3 and strong cipher suites.
- **Encryption at rest** with AES-256 for all databases and archives.
- **Key Management** via HSM-backed PKI (Hardware Security Module) or client-provided PKI.
- **Tamper-evident logs** with hash chaining and immutable WORM (Write Once, Read Many) storage for invoice evidence.

- **Data minimization** – only required invoice data is processed, no unnecessary fields are persisted.

5.4 Non-Repudiation and Integrity

- Every invoice payload is digitally signed (PKCS#7) before submission.
- Signatures ensure **origin authenticity** (the invoice came from the right client), **integrity** (no changes after signing), and **non-repudiation** (the sender cannot deny submission).
- QR codes generated embed a secure reference back to the signed record, enabling external verification.

<diagram: Signature and QR integrity chain from invoice payload → signature → QR verification → audit log>

5.5 Logging, Monitoring, and Threat Detection

- **Comprehensive audit logging** for all API calls, submissions, responses, and user actions.
- Logs include correlation IDs, timestamps in UTC, user IDs, and event outcomes.
- **SIEM integration** (Splunk, ELK, Azure Sentinel) for real-time analysis.
- **Threat detection rules** for:
  - Repeated failed authentications
  - Abnormal IPs or geographies
  - Large volume spikes outside of configured limits
  - Suspicious payload patterns (e.g., injection attempts)
- **Alerts routed in real time** to Bluelight Ops and client SOC (Security Operations Center).

5.6 Compliance and Certifications

- Designed to align with **ISO 27001** (Information Security Management).
- Logging aligned to **NIST 800-92** and **OWASP API Security Top 10**.
- GDPR-equivalent data protection principles applied where personal data exists.
- **Regular penetration testing** conducted in UAT and pre-production environments.
- Regulatory **conformance tests with FIRS** to validate schema, signature, and transmission security.

5.7 Business Continuity and Disaster Recovery

- **RPO 15 minutes** (Recovery Point Objective) with database replication.
- **RTO 2 hours** (Recovery Time Objective) with active-passive failover across data centers.
- **Semi-annual DR drills** with full evidence reports provided to client compliance teams.
- **Geo-redundant backups** encrypted and stored in multiple secure locations within Nigerian regulatory jurisdiction.

5.8 Security Governance

- Security reviewed as part of every design decision by a **dedicated Security Architect**.
- **Quarterly security audits** with results reported to client leadership.
- **Certificate expiry management** – automatic monitoring with alerts at T-30, T-7, T-1 days.
- **Emergency response playbooks** for breach scenarios, aligned to international incident response standards.

5.9 Why Our Security is Different

While many providers claim to secure traffic with HTTPS, Softrust and Bluelight go far beyond:

- **Defense in depth** – layered protection from endpoint to archive.
- **Audit-grade evidence** – tamper-evident logs and immutable archives.
- **Proactive monitoring** – integrated SIEM, anomaly detection, and SOC escalation.
- **Regulator alignment** – proven against FIRS security protocols and continuously updated.

Our security is not an afterthought; it is the bedrock of our compliance solutions.