**Security & Audit Architecture Overview**

The proposed traceability platform for Saint Lucia is designed with **government-grade security**, ensuring data integrity, confidentiality, and system availability across all regulated domains. The security and audit architecture forms a foundational layer of the system, enforcing strict access controls, enabling full lifecycle traceability, and guaranteeing non-repudiation through immutable logging and blockchain-based anchoring.

This architecture follows a **multi-layered security approach**, aligning with modern zero-trust principles, and incorporates **role-based access control (RBAC)**, **multi-factor authentication (MFA)**, **end-to-end encryption**, and**penetration-tested code pipelines**. Every user interaction, data mutation, or system event is captured and traceable-making it ideally suited for compliance with international standards such as **GDPR**, **HIPAA**, and **GxP** regulations.

**1. Identity and Access Management (IAM)**

At the core of the IAM layer is **Keycloak**, a self-hosted enterprise identity provider that enforces:

* **OAuth2 Authorization Flows** - Ensures token-based secure access to services.
* **RBAC (Role-Based Access Control)** - Every action (e.g., create batch, view test result, destroy inventory) is permission-gated by user role and module scope.
* **Multi-Factor Authentication (MFA)** - Mandatory for all administrative and regulatory accounts to prevent unauthorized access.

**Users are categorized into three main roles:**

* **Operators** - Can read/write only data associated with their license or facility.
* **Regulators** - Have elevated rights to view all records, approve activities, and generate compliance reports.
* **Auditors** - Possess read-only access to all modules and logs for review and oversight.

This ensures principle-of-least-privilege access at all levels of the system.

**2. Authorization Filters & Modular Enforcement**

Each microservice (e.g., Cannabis Cultivation, Inventory, Lab Integration) includes **authorization middleware** to validate access rights at the route level. This enforces data partitioning across licensees and supports future domain-specific permission matrices (e.g., restricting lab users to upload test results only).

Modules are isolated yet share a common **authentication token and claims context**, reducing the risk of privilege escalation and ensuring consistent access rules throughout the system.

**3. Immutable Audit Logging**

All critical events-such as creation of plant batches, lab result uploads, sales, waste destruction, and user login attempts-are logged using the **ELK Stack (Elasticsearch, Logstash, Kibana)**, with additional hash-based immutability mechanisms:

* **Audit logs are timestamped, signed, and hashed using SHA-256.**
* A **blockchain anchor (e.g., QLDB or Hyperledger Fabric)** commits these hashes periodically, creating a **tamper-evident audit trail**.

Regulators and auditors can trace any change to its origin, verify its legitimacy, and detect anomalies such as backdated entries or unauthorized deletions.

**4. Encryption and Network Security**

The platform ensures **end-to-end encryption** at every level:

* **In Transit** - TLS 1.3 with Perfect Forward Secrecy (PFS).
* **At Rest** - AES-256 encryption on all data stores, with managed key rotation via **KMS**.
* **Mobile Storage** - Encrypted SQLite databases using platform-native encryption libraries.
* **Credential Storage** - All secrets are stored using secure vaults or encrypted device storage (e.g.,flutter\_secure\_storage).

Additionally, the system is deployed in **cloud environments (e.g., AWS GovCloud)** with **VPC-level firewalls**, **IAM isolation**, and **network segmentation**, preventing lateral movement in case of intrusion.

**5. Continuous Monitoring, Testing & Hardening**

Security is not a one-time event but a continuous process. The system incorporates:

* **Dependency Scanning** - Snyk, npm audit, and Trivy guard against vulnerable packages.
* **Penetration Testing** - Tools like OWASP ZAP and Nikto simulate real-world attacks.
* **Infrastructure Hardening** - Automated security checks in CI/CD pipelines validate containers, firewall rules, and IAM policies before deployment.

**Prometheus and Grafana** continuously monitor system health and detect anomalies, while structured logs via **Loki or ELK** provide observability and incident response readiness.

**6. Transparency and Regulatory Oversight**

The platform supports real-time regulatory insight via:

* **Visual dashboards** showing access logs, actions taken per user, and suspicious patterns (e.g., unusual nighttime entries).
* **Role-specific views** for regulators and auditors to analyze event flows and initiate investigations.
* **Exportable audit reports** for cross-agency cooperation (e.g., Customs, Tax Authority).

Every decision or action-whether by an operator or an internal system-is observable, verifiable, and archived.

**Conclusion**

This security and audit architecture ensures that Saint Lucia's national traceability system is **trustworthy, verifiable, and defensible**-from planting to sale, and from access to oversight. By combining robust identity management, immutable blockchain-backed audit logs, continuous monitoring, and end-to-end encryption, the platform not only protects sensitive data but also reinforces public trust in regulatory compliance.