Audit Logging & Configuration Security

1. Overview

The Audit Logging system provides a tamper-evident record of all security-relevant events within the library. It is designed to be high-performance, asynchronous, and "Privacy by Design" compliant.

2. Event Types

2.1 Configuration Audit (High Priority)

Every change detected by a ConfigProvider (e.g., K8s ConfigMap reload) must trigger an audit log.

- **Fields Captured:** Source (file path/URI), Timestamp, Change Delta, User/Process ID (if available).
- **Masking:** Any property containing keywords like password, secret, token, or key MUST be masked with ********.

2.2 Enforcement Audit

Triggered when a request is denied or when the system fails over to L2.

- **Fields Captured:** Limiter Name, Resolved Key (Masked), Threshold, Current Usage, Result (REJECTED/FALLBACK).

3. Data Masking & Privacy

3.1 Key Masking

To comply with GDPR/CCPA, the KeyResolver output should not be logged in plain text if it contains PII.

- **Strategy:** Logs will store a salted hash of the key: SHA-256(key + salt).
- **Salt:** A globally unique salt generated at startup or provided via configuration.

3.2 Secret Masking Implementation

The library will use a regex-based SensitiveDataFilter before any configuration object is serialized to the logs.

- **Default Patterns:** (?i).*(password|secret|key|token|credential).*

4. Audit Log SPI (AuditLogger)

A framework-agnostic interface in rl-core:

```
public interface AuditLogger {
   void logConfigChange(ConfigChangeEvent event);
```

```
    void logEnforcementAction(EnforcementEvent event);
    void logSystemFailure(SystemFailureEvent event);
}
```

5. Implementation Best Practices

- **Asynchronous Execution:** Audit logging must never block the request path. Use a non-blocking queue (e.g., LMAX Disruptor or a simple LinkedBlockingQueue).
- **Structured Logging:** All logs must be output in **JSON format** to facilitate easy ingestion by SIEM tools (Splunk, ELK, Datadog).
- **Integrity:** In high-security modes, log entries should include a sequence number to detect log deletion or tampering.