Securaa User Service - High Level Design Document

Document Information

- **Service Name**: Securaa User Service
- **Version**: 1.0
- **Date**: September 18, 2025
- **Author**: System Architecture Team
- **Related Documents**: ZONA_USER_HLD.md

Table of Contents

Executive Overview

⚠ Critical Service Classification

The Securaa User Service is a **mission-critical component** that serves as the foundation of the entire Securaa security platform ecosystem. This service is the central nervous system

for security operations, handling all aspects of user identity, access control, and tenant management across the platform.

Critical Impact Areas:

- **Security Posture**: Controls access to all security operations and sensitive data
- **Compliance Requirements**: Manages audit trails and regulatory compliance
- **Business Continuity**: Essential for all platform operations and user workflows
- **Data Protection**: Enforces data access policies and tenant isolation
- **Operational Excellence**: Enables monitoring, alerting, and incident response

Business Context & Objectives

Primary Business Functions

- **Identity & Access Management (IAM)**: Centralized authentication and authorization
- **Multi-Tenant Security**: Secure isolation and resource management across tenants
- **Compliance Management**: Audit trails, access controls, and regulatory compliance
- **Security Operations**: Real-time monitoring, threat detection, and incident response
- **Enterprise Integration**: Seamless integration with corporate identity systems

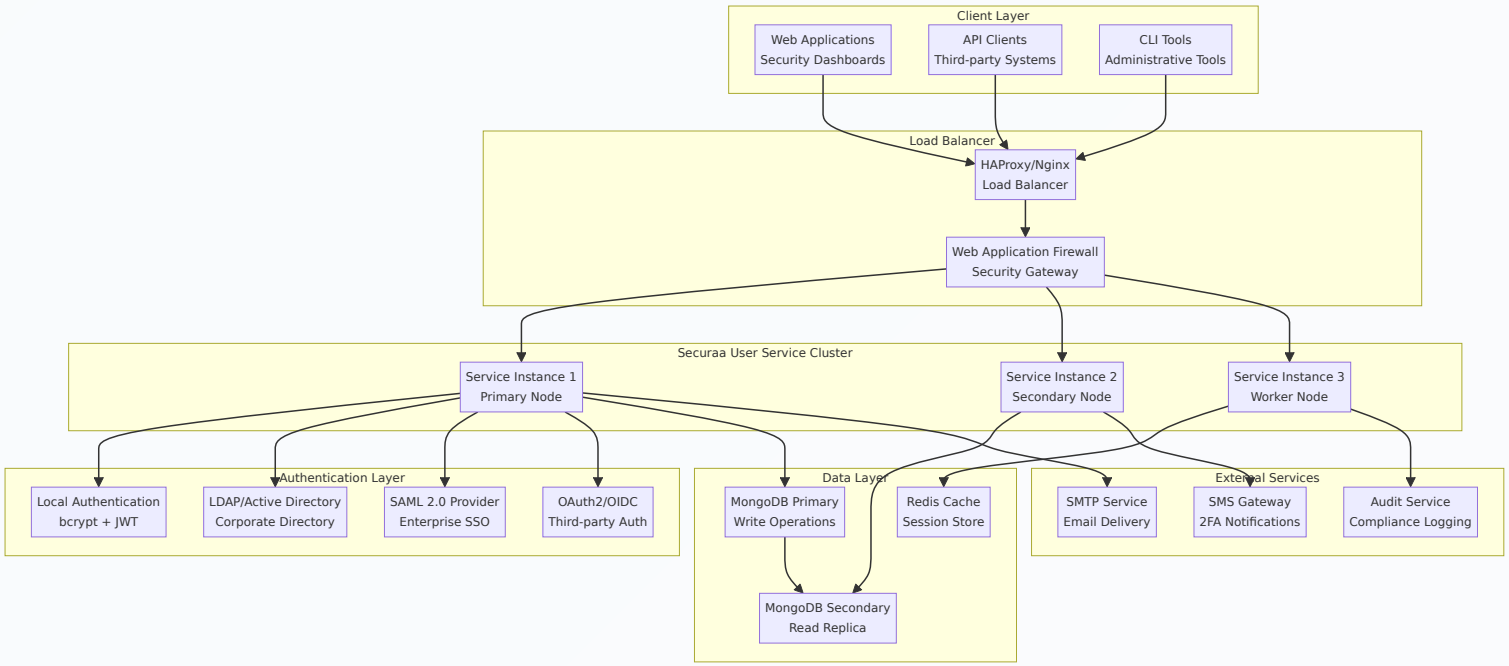
Key Business Stakeholders

- **Security Teams**: Threat analysts, SOC operators, security engineers
- **Compliance Officers**: Audit managers, risk assessors, compliance specialists
- **IT Operations**: Infrastructure teams, platform engineers, DevOps specialists
- **Business Users**: End users, administrators, tenant managers
- **Executive Leadership**: CISOs, CTOs, risk management executives

System Architecture Overview

High-Level System Architecture

The Securaa User Service follows a **microservice architecture** deployed on traditional servers or cloud infrastructure without container orchestration. The system is designed for high availability through load balancing and database replication.



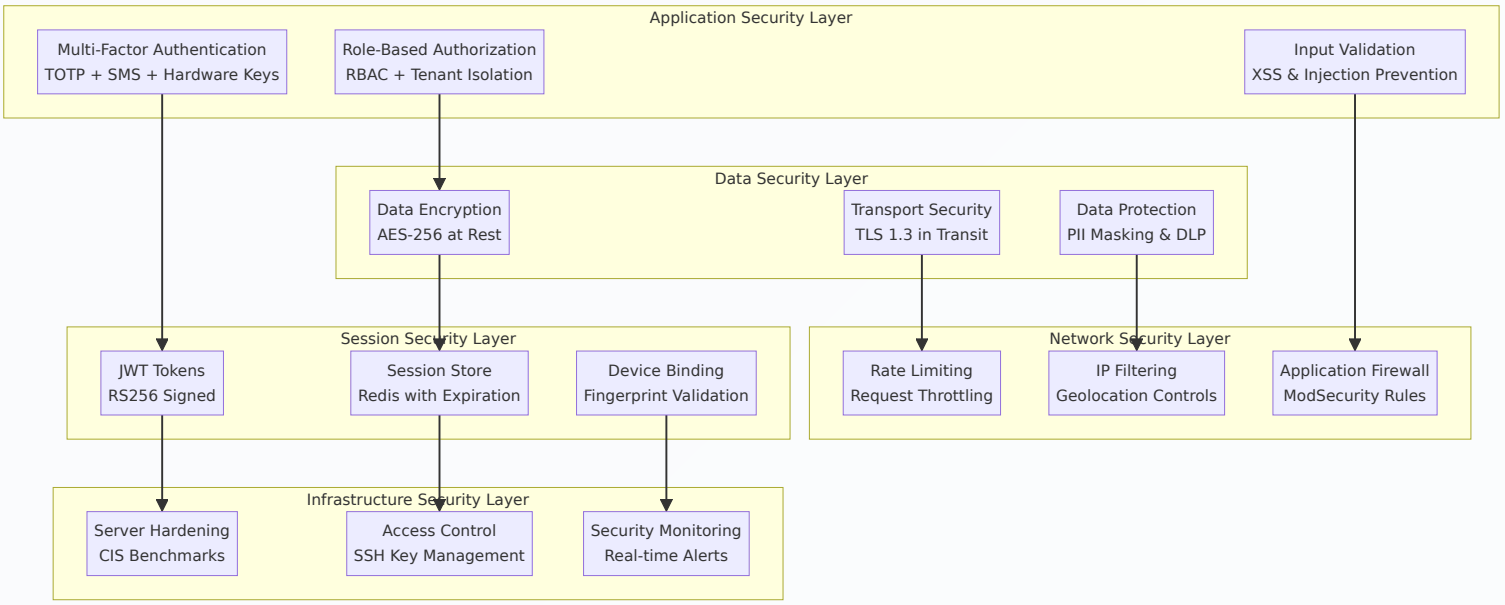
Architecture Overview:

This architecture represents a traditional three-tier application deployed across multiple servers for high availability. The system uses:

- **Load Balancing**: HAProxy or Nginx for traffic distribution
- **Service Clustering**: Multiple service instances for redundancy
- **Database Replication**: MongoDB primary-secondary setup
- **Caching Layer**: Redis for session management and performance
- **External Integrations**: SMTP, SMS, and audit services

Enterprise Security Architecture

The security architecture implements a **defense-in-depth approach** with multiple security layers protecting the Securaa User Service. Each layer provides specific security controls and works together to create a comprehensive security posture.



Security Implementation Details:

Layer 1 - Application Security:

- **Authentication**: Supports local credentials, LDAP/AD, SAML 2.0, and OAuth2 with mandatory MFA for privileged accounts
- **Authorization**: Implements RBAC with fine-grained permissions and complete tenant data isolation
- **Input Validation**: Comprehensive sanitization preventing SQL/NoSQL injection, XSS, and CSRF attacks

Layer 2 - Data Security:

- **Encryption at Rest**: All sensitive data encrypted using AES-256 with rotating keys
- **Encryption in Transit**: TLS 1.3 for all communications with perfect forward secrecy
- **Data Protection**: PII masking in logs and exports with DLP controls

Layer 3 - Session Security:

- **JWT Implementation**: Stateless tokens signed with RS256 algorithm
- **Session Management**: Redis-backed sessions with configurable timeouts
- **Device Security**: Browser fingerprinting and device binding for anomaly detection

Layer 4 - Network Security:

- **Web Application Firewall**: ModSecurity with OWASP Core Rule Set
- **Rate Limiting**: Configurable request throttling per IP and user
- **Access Controls**: IP whitelisting and geolocation-based restrictions

Layer 5 - Infrastructure Security:

- **Server Hardening**: CIS benchmark compliance with automated configuration management
- **Access Management**: SSH key-based authentication with audit logging
- **Monitoring**: Real-time security event monitoring with automated alerting

Core Business Capabilities

Enterprise Identity & Access Management

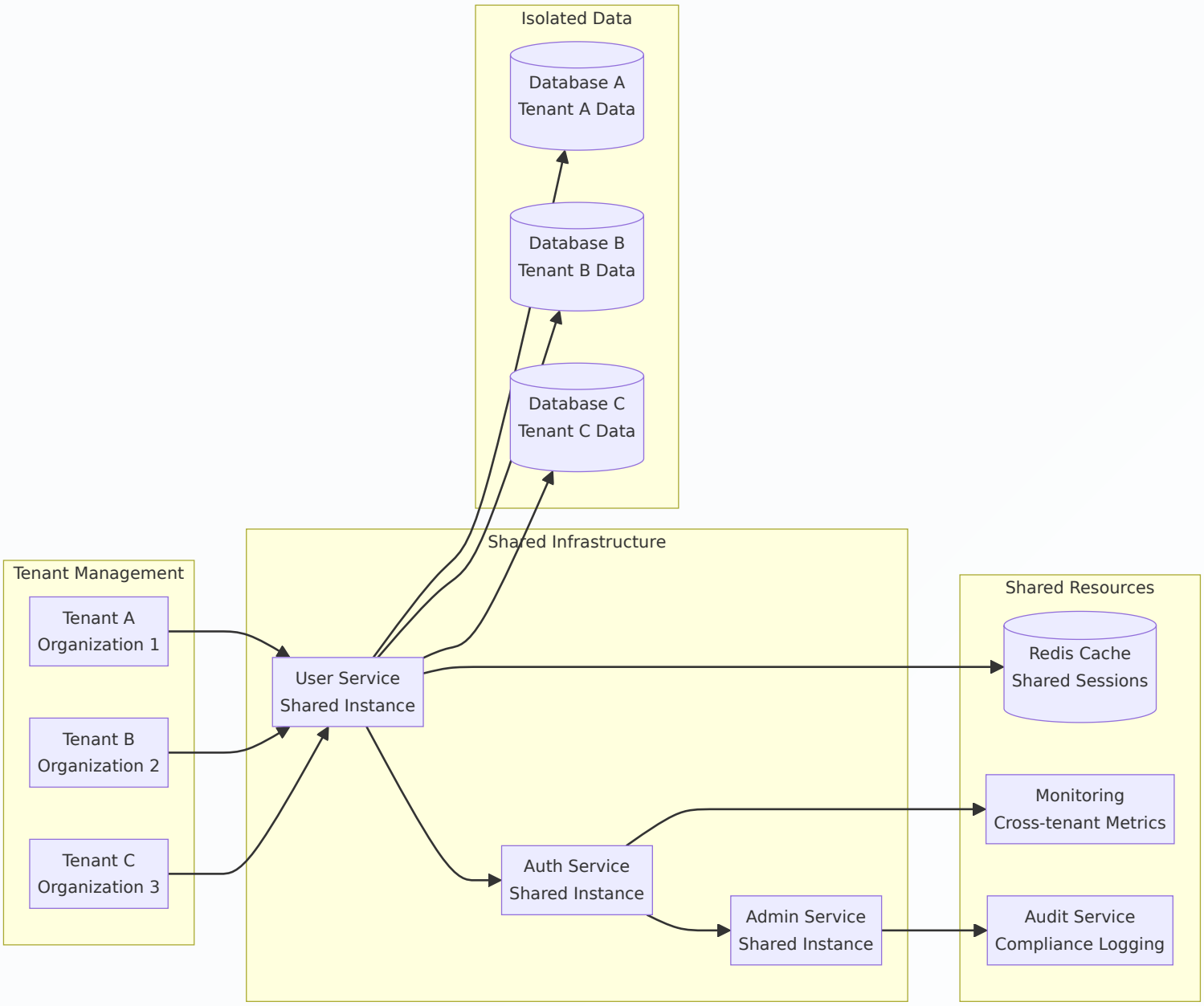
Authentication Capabilities:

- **Multi-Factor Authentication**: TOTP, SMS, hardware keys, and biometric authentication
- **External Integration**: LDAP/AD, SAML 2.0, OAuth2/OIDC, and social login providers
- **Password Security**: bcrypt hashing, complexity requirements, rotation policies
- **Session Management**: JWT tokens, session timeouts, concurrent session controls

Authorization Framework:

- **Role-Based Access Control**: Hierarchical roles with fine-grained permissions
- **Tenant Isolation**: Complete data segregation and resource boundaries
- **Resource Access**: API endpoint protection and data access controls
- **Dynamic Permissions**: Runtime permission evaluation and inheritance

Multi-Tenant Architecture Capabilities

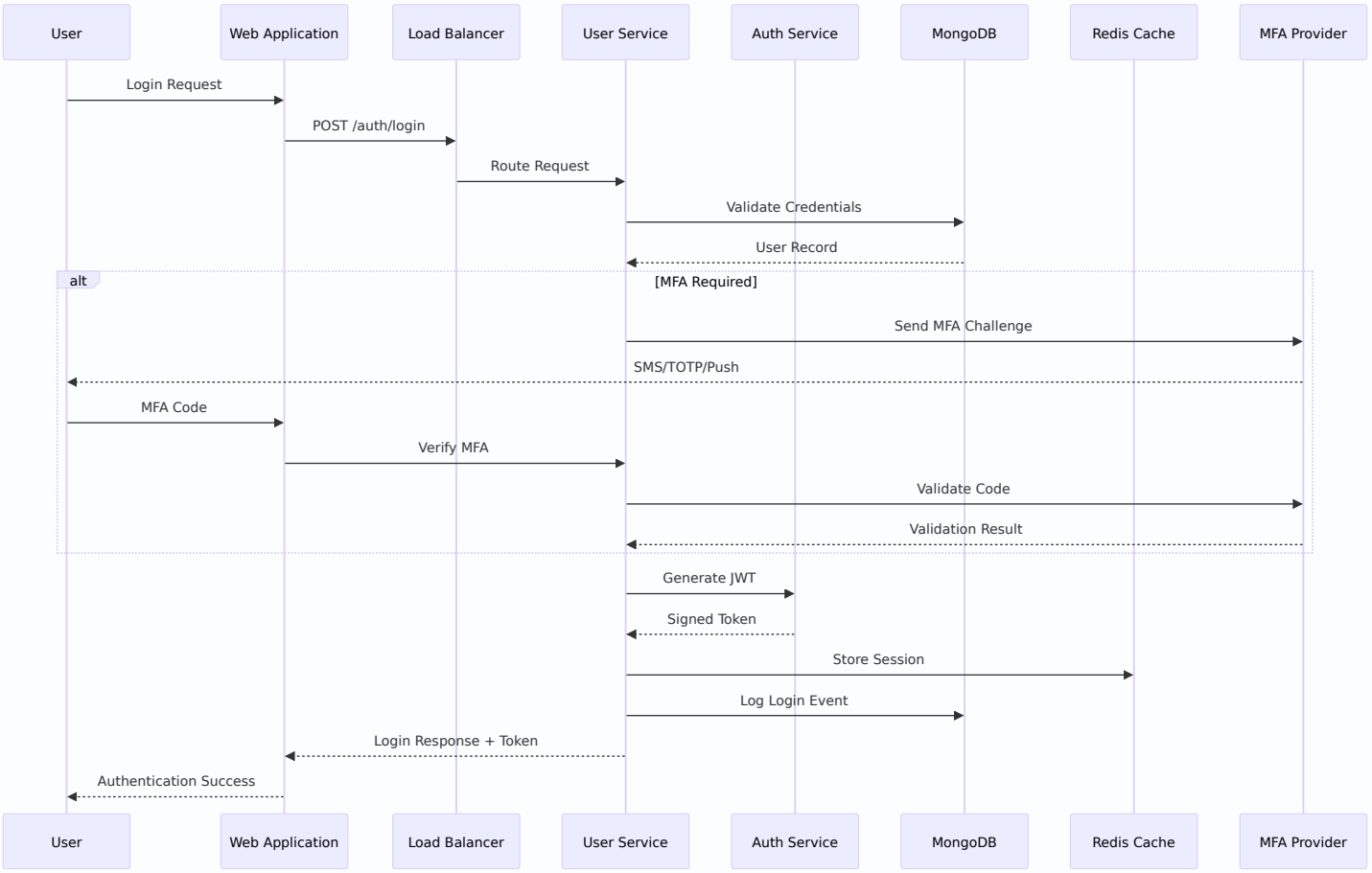


Multi-Tenancy Features:

- **Tenant Isolation**: Complete data separation with database-level isolation
- **Resource Management**: Per-tenant quotas and usage monitoring
- **Configuration Management**: Tenant-specific settings and customizations
- **Cross-Tenant Administration**: Master tenant capabilities for platform management

Critical Business Processes

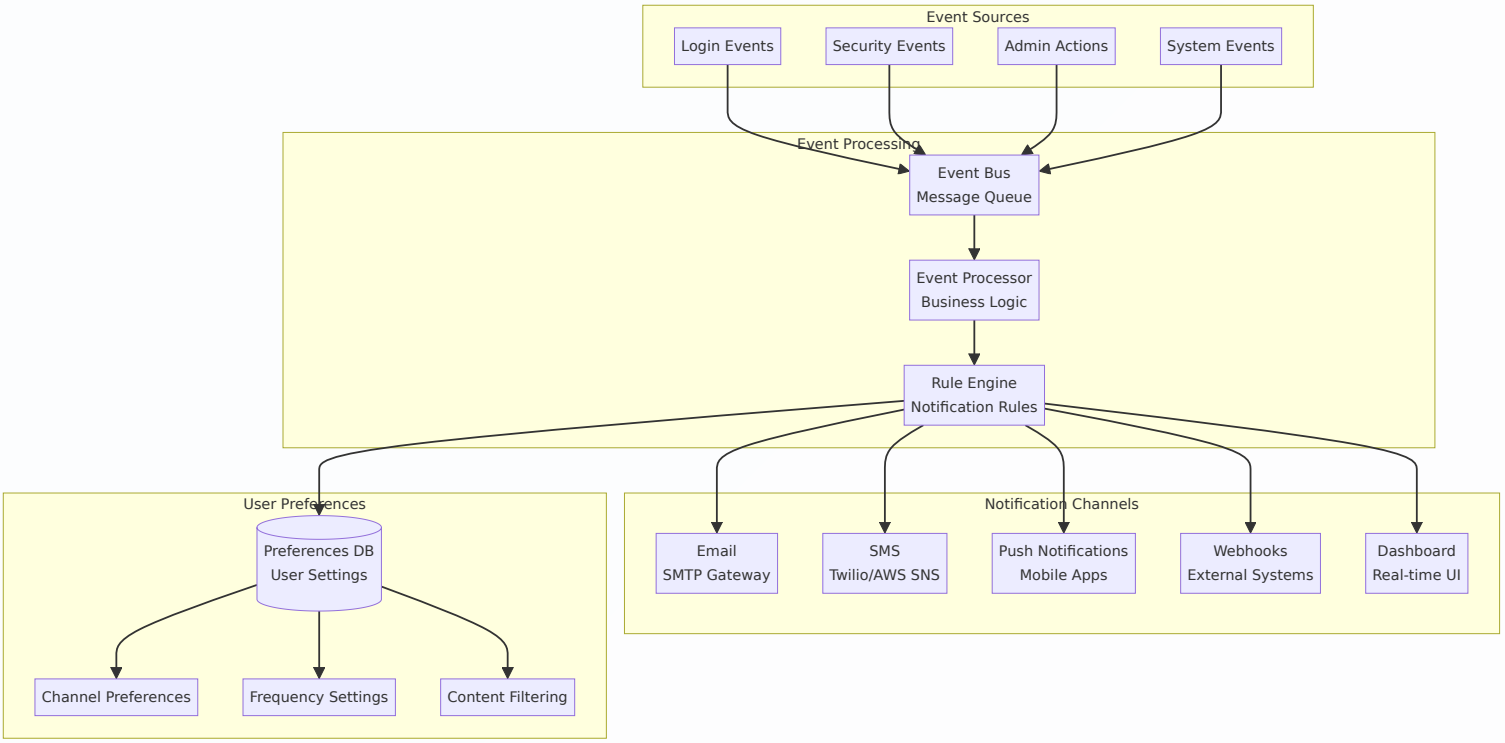
User Authentication Flow



Authentication Process Details:

1. **Credential Validation**: Username/password verification against database
2. **MFA Challenge**: Multi-factor authentication when required
3. **Token Generation**: JWT token creation with user claims and permissions
4. **Session Storage**: Redis-based session management for scalability
5. **Audit Logging**: Security event logging for compliance and monitoring

Real-Time Notification System

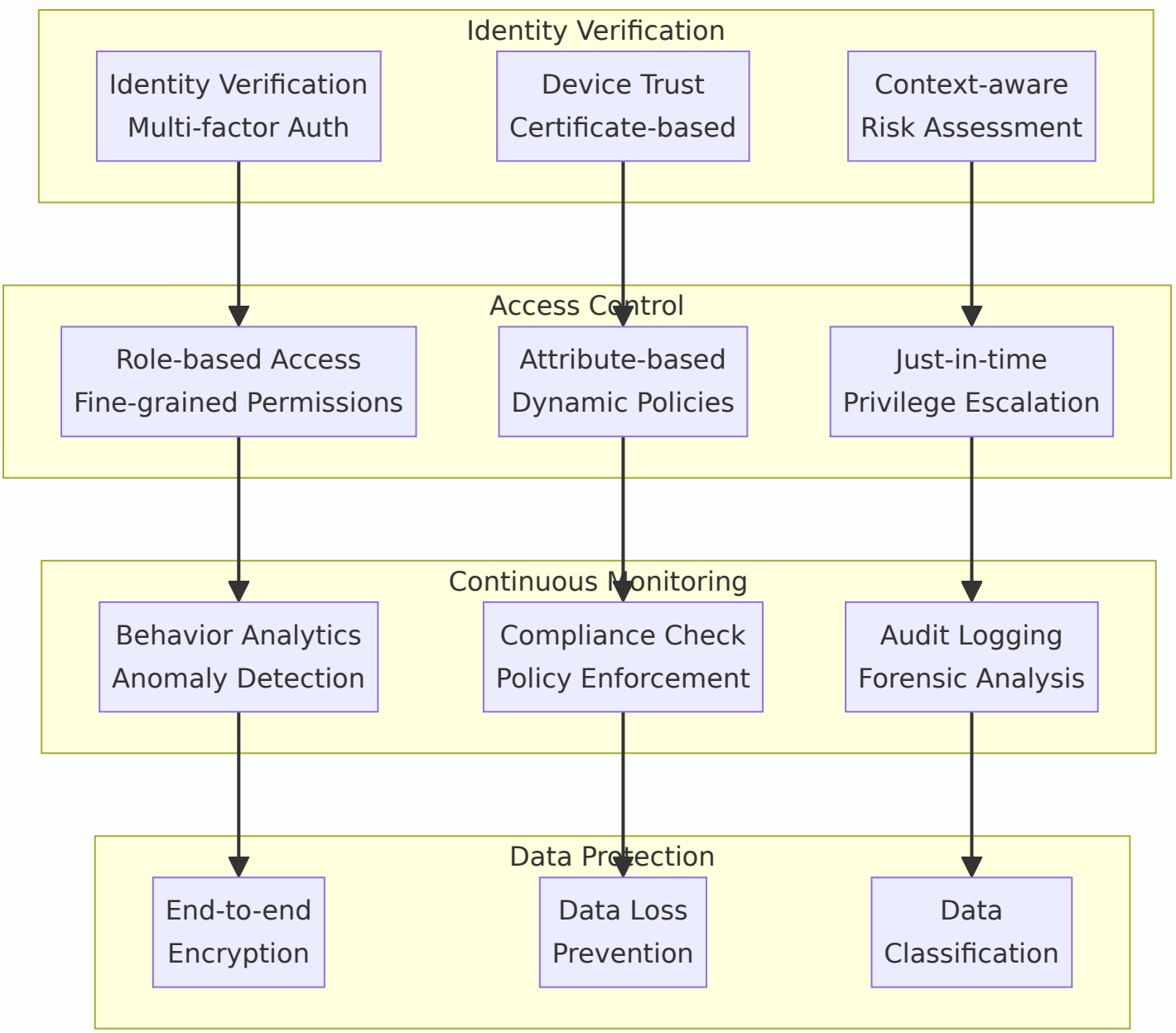


Notification Features:

- **Multi-Channel Delivery**: Email, SMS, push notifications, webhooks
- **User Preferences**: Customizable notification settings per user
- **Rule Engine**: Configurable notification rules and triggers
- **Real-Time Processing**: Immediate notification delivery for critical events

Enterprise Security Strategy

Zero-Trust Security Model

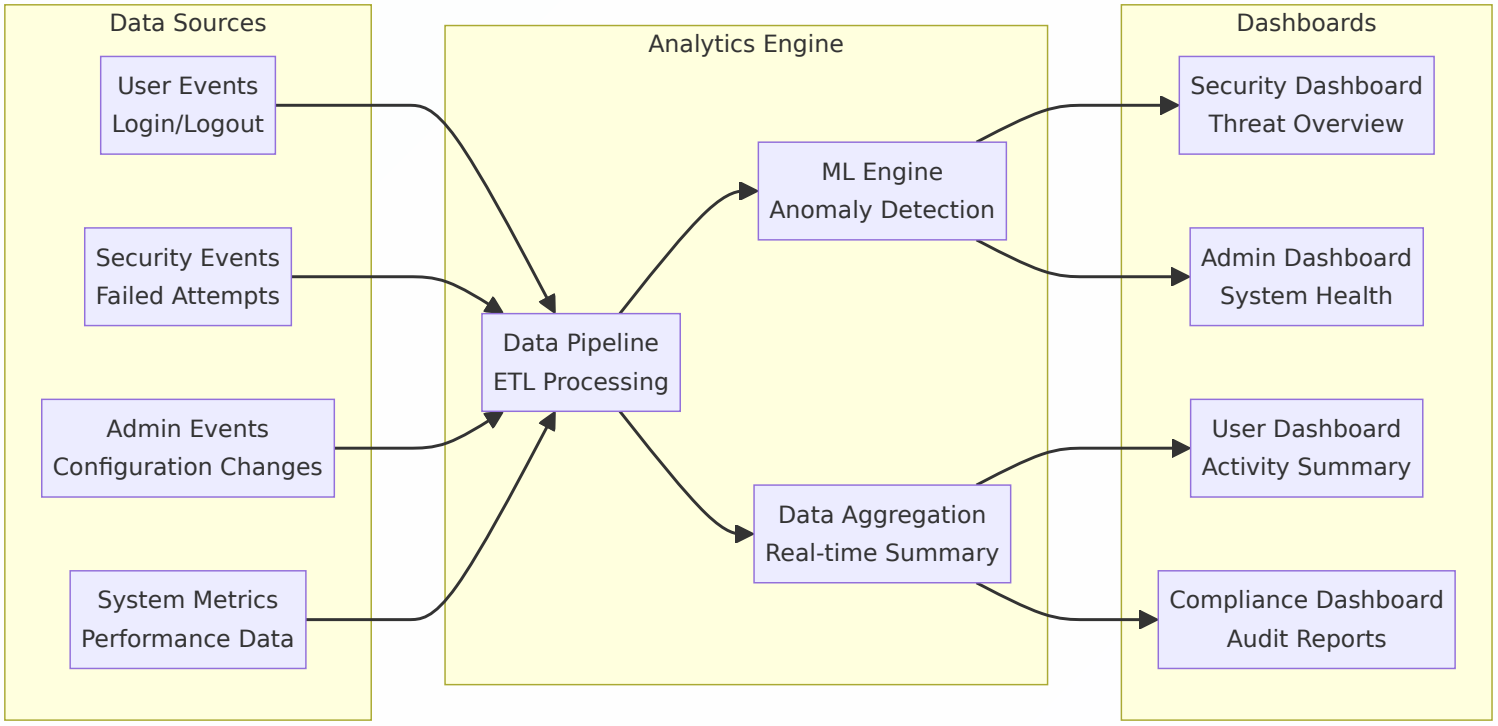


Zero-Trust Principles:

- **Never Trust, Always Verify**: Continuous authentication and authorization
- **Least Privilege Access**: Minimal required permissions with time-bound access
- **Assume Breach**: Continuous monitoring and anomaly detection
- **Verify Explicitly**: Multiple factors and context-aware decisions

Business Intelligence & Analytics

Security Operations Dashboard

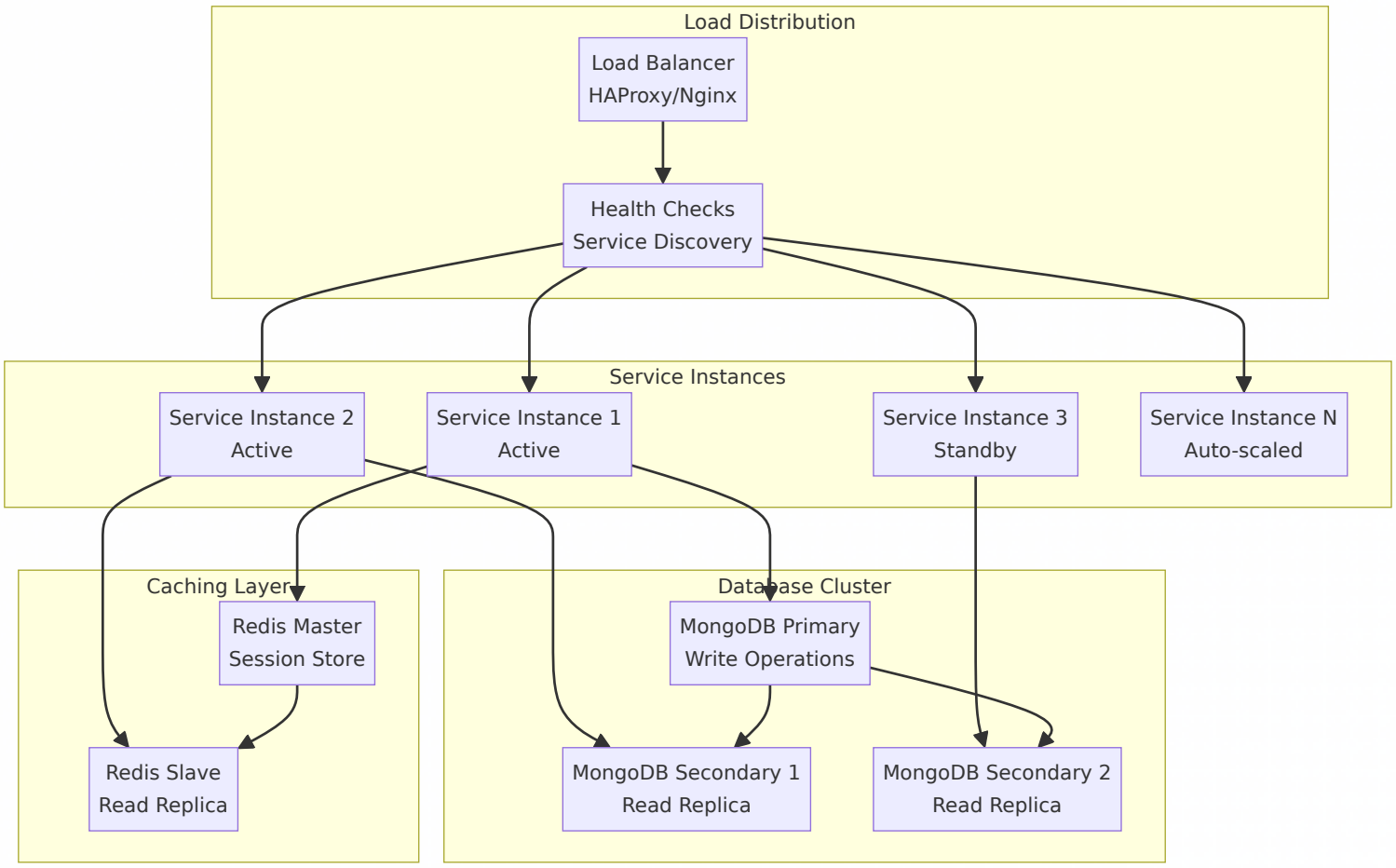


Analytics Capabilities:

- **Real-Time Monitoring**: Live dashboards with security metrics
- **Anomaly Detection**: ML-powered threat detection and alerting
- **Compliance Reporting**: Automated audit reports and compliance dashboards
- **User Behavior Analytics**: Pattern analysis and risk scoring

□ Scalability & Performance Strategy

Horizontal Scaling Architecture



Performance Optimizations:

- **Connection Pooling**: Efficient database connection management
- **Query Optimization**: Indexed queries and aggregation pipelines
- **Caching Strategy**: Multi-level caching with Redis and in-memory caches
- **Auto-Scaling**: Dynamic scaling based on CPU, memory, and request metrics

Summary

The Securaa User Service represents a comprehensive, enterprise-grade identity and access management platform. Its robust architecture, extensive security features, and scalable design make it suitable for organizations of all sizes looking to enhance their security operations and compliance posture.

The service's multi-tenant architecture, comprehensive authentication options, and real-time monitoring capabilities provide a solid foundation for building secure, scalable security platforms. The extensive API surface area and integration capabilities ensure flexibility for various use cases and integration requirements.

This high-level design serves as a blueprint for understanding the system architecture, business capabilities, and key components that make up the Securaa User Service.