ACS SECURITY SYSTEM

HIGH-LEVEL DESIGN(HLD)

1.System Overview

The Access Control System (ACS) is an enterprise-grade, vendor-neutral platform designed to centrally manage physical access devices, users, credentials, permissions, and real-time monitoring across multiple sites. The system enables organizations to operate heterogeneous access control hardware under a unified management and policy framework.

ACS is built using a microservices-based, event-driven architecture to support high-throughput device events, independent service evolution, and operational resilience. The platform is intended for large-scale enterprise deployments where availability, security, and extensibility are critical.

Key objectives include:

- Unified management of multi-vendor access control devices
- Centralized user and credential administration
- Real-time event ingestion and monitoring
- Secure and auditable access control decisions
- Horizontal scalability and fault isolation
- Long-term extensibility for new vendors and features

2.Architectural Style

ACS follows a **microservices architecture** combined with an **event-driven communication model.**

Each service has a specific business capability and operates independently. Services communicate through:

- Synchronous APIs for command and query operations
- Asynchronous events for real-time device activity and system notifications

This approach enables:

- Independent scaling of high-load components (e.g., device ingestion, event processing)
- Fault isolation between functional domains
- Parallel development and deployment
- Flexibility to integrate new device vendors

- Improved resilience through loose coupling

3.Overall System Architecture

At a high level, the system consists of the following core services:

Component / Service	Responsibility
API Gateway	Unified entry point, authentication, request routing
Identity & Credential Service	Users, credentials, and identity lifecycle
Device Management Service	Device lifecycle, configuration, and health
Device Communication Layer	Persistent device connections and command handling
Access Control Service	Policies, access levels, and time rules
Event Processing Service	Event normalization and distribution
Monitoring & Dashboard Service	Real-time visibility and alerts
License & Tenant Service	Client onboarding and module entitlement
Reporting Service	Audit logs and exports

4.Core Components Description

The ACS platform is composed of the following high-level components:

- **API Gateway**
  Acts as the unified entry point for all client applications. It enforces security policies and routes requests to appropriate backend services.
- **Device Management**
  Manages the lifecycle of physical devices, including registration, configuration, and health monitoring.
- **Device Communication Layer**
  Provides a unified abstraction for interacting with heterogeneous hardware. It maintains device connectivity and enables bidirectional communication between the platform and physical endpoints.
- **Identity & Credential Service**
  Maintains user identities and associated credentials, ensuring consistent identity representation across the platform.
- **Access Control Service**
  Evaluates access policies and determines authorization decisions based on configured rules, schedules, and permissions.
- **Event Processing Service**
  Serves as the central ingestion and distribution point for real-time device events across the platform.

5.Real-Time Event Flow (Sequence)

At a high level, real-time interactions follow this pattern:

1. A physical device generates an operational event.
2. The platform receives the event through the device communication layer.
3. The event is transformed into a unified internal representation.
4. Relevant business policies are evaluated.

5. The event persisted and propagated to dependent components.
6. User interfaces and monitoring systems reflect the updated state.

6.Security Architecture

Security is a foundational concern across all layers of the platform:

- Security is a foundational concern across all layers of the platform:
- Centralized authentication ensures that only trusted clients and users can access the system.
- Fine-grained authorization governs access to features, data, and operational capabilities.
- Tenant and module isolation ensures that each client operates within its entitled scope.
- Sensitive information is protected throughout its lifecycle.
- License enforcement controls feature availability and system activation.

7.Scalability & Deployment

ACS is designed for enterprise-scale deployments with the following characteristics:

- Services are stateless and independently scalable.
- Load balancing enables horizontal growth under increased demand.
- Components can be deployed and upgraded independently.
- Centralized logging and monitoring provide operational visibility.
- The platform supports on-premises, containerized, and hybrid deployment models.

This design enables the system to scale with organizational growth while maintaining performance and reliability.