# LMS -Product Requirements Document (PRD)

## 1. Purpose

The purpose of this document is to define the functional and non-functional requirements for the Learning Management System (LMS) to handle attendance tracking from an external device (e.g., biometric machine, RFID card reader, face recognition system). The system will automatically capture, store, and process attendance data from devices and integrate it with the LMS student/employee profiles.

## 2. Background

Currently, attendance is either recorded manually or through device exports that require manual uploads into the LMS. This process is error-prone and time-consuming.  
The proposed solution will automate the process by integrating the LMS with attendance devices, ensuring real-time or scheduled synchronization and accurate record-keeping.

## 3. Goals & Objectives

* Automate the capture of attendance data from devices into the LMS.
* Ensure real-time or scheduled synchronization between devices and LMS.
* Provide reporting and analytics on attendance trends.
* Allow manual adjustments with audit trails.
* Ensure compliance with institutional attendance policies.

## 4. Scope

### In-Scope

* Integration with supported attendance devices (biometric, RFID, QR scan, face recognition).
* Attendance data mapping to user profiles.
* Device configuration and management in LMS admin portal.
* Automatic and manual sync options.
* Attendance reports and analytics dashboards.
* Notifications for low attendance or anomalies.
* Data security and role-based access.

### Out-of-Scope

* Hardware procurement or device firmware development.
* Third-party analytics beyond the scope of attendance.
* Payment or payroll integration (unless in future roadmap).

## 5. Stakeholders

* **Product Owner:** [Name]
* **Project Manager:** [Name]
* **Developers:** Backend, Frontend, Integration Engineers
* **QA Team:** Testing attendance workflows
* **IT/Infrastructure:** Device network setup and maintenance
* **End Users:** Teachers, Students, HR/Admin Staff

## 6. Functional Requirements

### 6.1 Device Integration

* **FR-1:** System must support attendance data capture from at least the following sources:
  + Biometric fingerprint scanner
  + RFID card reader
  + QR code scanner
  + Face recognition device
* **FR-2:** Allow configuration of multiple devices per location.
* **FR-3:** Support both **push** (device sends data) and **pull** (system requests data) modes.
* **FR-4:** Device-to-LMS communication must be secured (HTTPS, API key/token).

### 6.2 Attendance Processing

* **FR-5:** Map raw device logs to LMS user profiles using unique identifiers (ID number, card number, biometric ID).
* **FR-6:** Support clock-in and clock-out events with timestamps.
* **FR-7:** Handle offline device scenarios with batch upload when connectivity is restored.
* **FR-8:** Detect duplicate or invalid entries and flag for review.

### 6.3 Attendance Management in LMS

* **FR-9:** Provide admin UI for:
  + Viewing attendance records
  + Filtering by date, user, device, or course
  + Editing/deleting entries with audit log
* **FR-10:** Support bulk updates for special cases (holidays, events).
* **FR-11:** Generate attendance percentage per student/course.

### 6.4 Reporting & Notifications

* **FR-12:** Generate daily, weekly, and monthly attendance reports.
* **FR-13:** Provide real-time dashboard with charts (absentees, late arrivals).
* **FR-14:** Send email/SMS alerts for:
  + Students below attendance threshold
  + Device sync failure

## 7. Non-Functional Requirements

| **ID** | **Requirement** | **Description** |
| --- | --- | --- |
| NFR-1 | Performance | Must process at least 5000 attendance records per minute |
| NFR-2 | Availability | 99.9% uptime excluding scheduled maintenance |
| NFR-3 | Scalability | Support up to 500 devices and 50,000 users |
| NFR-4 | Security | All data in transit must be encrypted (TLS 1.2+); role-based access control |
| NFR-5 | Compliance | GDPR/FERPA compliance for educational institutions |
| NFR-6 | Maintainability | Device integration layer must be modular for adding new device types |

## 8. Assumptions

* All devices can send data in a standardized format (JSON/XML/CSV) or have an accessible SDK/API.
* Network connectivity between devices and LMS server is stable.
* Unique identifiers are pre-mapped in LMS.

## 9. Dependencies

* Third-party device APIs/SDKs.
* SMS/Email gateway for notifications.
* Database (PostgreSQL/MySQL) with attendance tables.
* Cloud or on-premises hosting environment.

## 10. Risks & Mitigation

| **Risk** | **Impact** | **Mitigation** |
| --- | --- | --- |
| Device API changes | Medium | Use adapter pattern for integration |
| Network downtime | High | Implement offline data caching and batch sync |
| Data mismatch | High | Enforce unique mapping validation |

## 11. Acceptance Criteria

* Attendance data from devices appears in LMS within 1 minute (real-time mode) or within scheduled sync time.
* Reports accurately reflect device logs.
* Admin can manage and adjust attendance records.
* All device connections are authenticated and encrypted.

## 12. Future Enhancements

* AI-based anomaly detection for attendance fraud.
* GPS-based attendance for mobile learners.
* Biometric verification inside LMS mobile app.

## 13. high-level architecture diagram for the LMS

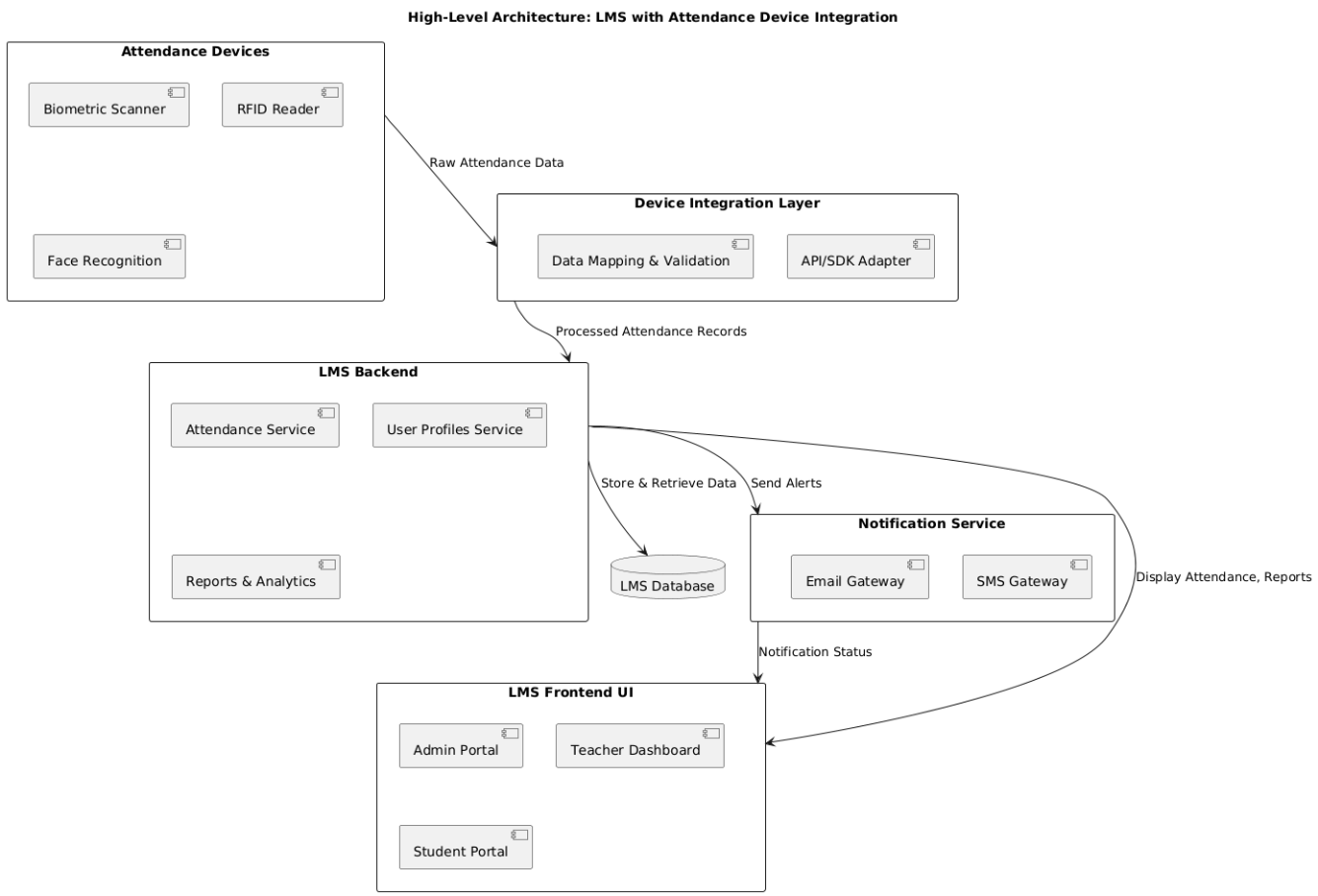


Fig 1: high-level architecture diagram for the LMS

## 14. Sequence Diagram

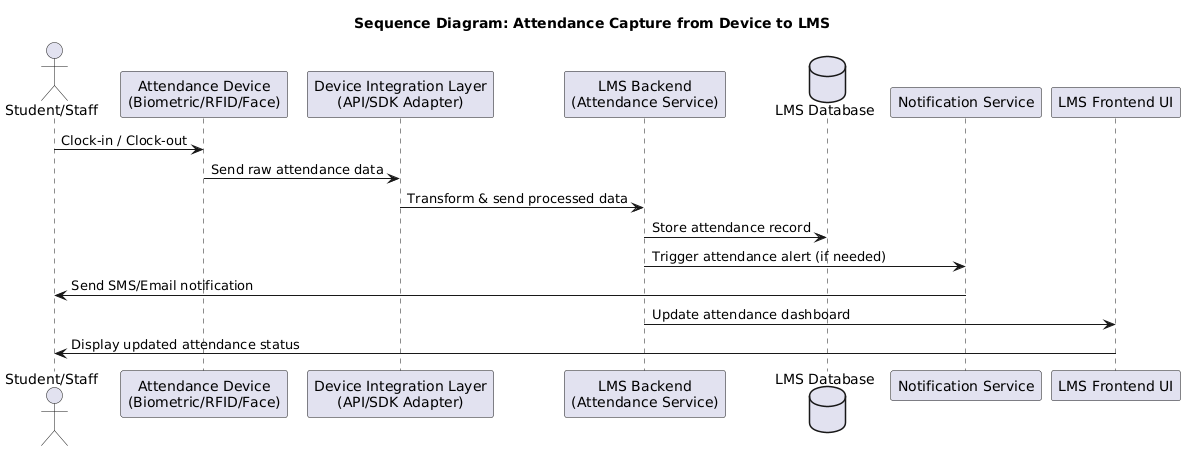


Fig 2: Sequence diagram for the LMS

## 15. Data-flow Diagram for LMS

A diagram of a service

AI-generated content may be incorrect.