Functional Requirements Documentation for the development of a Digital Entry Pass Management System for various Generating stations operated by Kerala State Electricity Board Limited (KSEBL).

Kerala State Electricity Board Limited

Office of the Chief Engineer (IT, CR & CAPs)
Vydyuthi Bhavanam, Pattom, Thiruvananthapuram

Version: 1.0
Date: 30-05-2025

Overview

Kerala State Electricity Board Limited (KSEBL) is the primary entity responsible for generating, transmitting, and distributing electricity in the State of Kerala, India. Established in 1957 under the Electricity (Supply) Act, 1948, KSEBL has played a vital role in electrification and the economic growth of Kerala. In 2013, it was restructured into a public sector company under the Companies Act, 1956.

Key Divisions

1. **Generation**
   KSEBL operates a wide range of power generation facilities, including hydroelectric stations, thermal power plants, and renewable energy installations such as solar and wind.
2. **Transmission**
   The transmission network spans the entire state, ensuring reliable delivery of electricity from generation plants to distribution substations. It operates at multiple voltage levels and is crucial for maintaining grid stability and efficiency.
3. **Distribution**
   The distribution wing serves millions of domestic, commercial, industrial, and agricultural consumers through an extensive network of substations, transformers, and distribution lines.

E-Governance and Technology Initiatives

KSEBL has undertaken several e-governance initiatives to enhance operational efficiency and customer service delivery.

1. Introduction

The purpose of this document is to define the functional requirements for a secure, robust, and user-friendly **Digital Entry Pass Management System** for various ***Generating stations*** of KSEBL

The proposed system will replace the existing paper-based pass issuance process and comply with the Intelligence Bureau (IB) security audit recommendations. It shall track issuance frequency, visit histories, and support multiple visitor categories while ensuring strict security and audit compliance.

2. Objectives and Scope

Support multiple types of gate passes, including visitor, employee, contractor, material (returnable/non-returnable), inward/outward, temporary/permanent. Include features for request initiation, digital generation with unique IDs (e.g., QR codes/barcodes), expiry dates, and photo/document uploads for verification.

The Digital Entry Pass Management System shall:

- Automate end-to-end processes including pass application, approval, issuance, tracking, revocation, and expiry.
- Generate unique, QR-coded digital passes and printable layouts.
- Maintain detailed audit logs in compliance with, CERT-In, and NCIIPC guidelines.
- Integrate with KSEBL's internal applications, Single Sign-On (SSO), SMS gateway, email services, Bar code /QR code readers, Mobile device and biometric modules.

In Scope: Pass categories, user roles, approval and revocation workflows, reporting, alerts, encryption, backup, archival, and user training.

3. User Roles and Permissions

Include admin, end-user, security, and visitor modules for registration, dashboard navigation, request handling, and system management

Role	**Description**	**Key Permissions**
Administrator	Manages master data, users, audit logs	CRUD(Create, Read, Update, Delete) on all entities; override approvals; revoke passes
Security Officer	Reviews and approves standard and special passes	Approve/deny/revoke passes; view entry/exit logs
Authorizing Officer	Approves VIP and high-level government passes	Elevated approvals for VIP workflows
Data Entry Operator	Creates and submits pass requests	Create/modify requests only
Auditor (Read-only)	Reviews logs and compliance reports	View-only access
Gate Operator	Validates passes at entry/exit points	Scan QR; record entry/exit timestamps; report anomalies

4. Visitor Categories and Pass Types

1. Outsourced Workers (Temporary Work Pass)
2. KSEBL Employees (Employee Visit Pass)
3. Government Agencies (Inspection/Audit Pass)
4. Visitors
5. VIP Visitors (Special Visit Pass)
6. Vehicle Pass

Each category shall support customizable validity periods, approval/revocation, and required documentation.

---

5. Functional Requirements

5.1 Pass Request and Data Entry

- Web-based(Mobile responsive) form capturing:

- Visitor details (name, address, contact)
- Proof of identity (type, number, scanned copy)
- Visitor category and sub-type
- Purpose of visit with work order/purchase order reference
- Requested duration (start/end date and time)
- Host department/section and recommending officer
- Details of accompanying persons (if any)
- Vehicle details (for vehicle passes)

5.2 Approval Workflow

Implement multi-level, automated approval processes with role-based notifications to ensure stringent reviews by authorized personnel, reducing delays and unauthorized access

- Configurable, multi-stage workflows:
    - Outsourced workers → Security Officer
    - Employees → Section Manager → Security Officer
    - Government Agencies → Authorizing Officer → Security Officer
    - Visitors → Authorizing Officer → Administrator
    - VIPs → Authorizing Officer → Administrator
- Automatic routing based on category and time.
- Real-time notifications (email/SMS) for pending approvals.
- Escalation alerts if requests exceed SLA timelines.

5.3 Pass Issuance

- Upon approval, the system shall generate:
    - Unique pass ID and QR code
    - Printable PDF layout (with photo, validity, and host details)
    - Automated email/SMS/Whatsapp dispatch to visitor and host
- Options for reprint or reissue with full audit trail.
- Emergency offline pass generation with later synchronization.

5.4 Entry, Exit, and Revocation Tracking

Enable real-time verification at gates via integration with scanners, biometrics, or mobile apps; log all entries/exits with timestamps, photos, and audit trails for compliance and security audits.

- Gate interface for QR scanning:
  - Validate status (active/expired/revoked)
  - Record timestamp, gate location, and operator ID
- Automatic expiry and overstay alerts.
- Revocation on demand by authorized officers.
- SMS/email notifications to the host on entry/exit.

5.5 Reporting and Analytics

Provide centralized dashboards for generating reports on movements, discrepancies, and trends; support data export for audits and integration with business intelligence tools

- Standard and ad-hoc reports:
  - Pass volume by type, department, or date
  - Average visit frequency and duration
  - Vehicle movement logs
  - Compliance reports against IB guidelines
- Export formats: Excel, PDF, CSV.
- Dashboard with real-time metrics and alerts.

5.6 Audit Trail and Compliance

- Immutable logs of all system actions.
- Tamper-evident storage with digital signatures.
- Role-based access to log views and exports.
- Historical data archived and retrievable for at least 7 years.

---

6. Non-Functional Requirements

6.1 Performance

- Support at least 200 concurrent users.

- Handle 1,000 pass transactions per hour with <2s average response time.

6.2 Scalability

- Modular design with horizontal scaling options for future power stations.

6.3 Security

- AES-256 encryption at rest, TLS 1.2+ in transit.
- Two-factor authentication for all roles except Data Entry Operators.
- Compliance with CERT-In and NCIIPC guidelines.
- Vulnerability assessments and penetration testing by CERT-In empaneled agencies.
- Automatic session lock and inactivity timeouts.

6.4 Availability and Reliability

- 99.5% uptime SLA.
- Automated backups every 4 hours, retained for 180 days.
- Failover clustering for critical modules.
- Offline fallback at gates with later synchronization.

6.5 Usability

- Responsive UI across desktop, tablet, and mobile.
- Multilingual support (English, Malayalam).
- Simple navigation and contextual help.
- Step-by-step user manuals and embedded tutorial videos.

6.6 Maintainability

- Version control via KSEBL's Git repository.
- Modular code with documented APIs.
- Minor enhancements/customization (≤2 person-days) included without additional cost.

6.7 Technology

- Platform-independent design (OS/browser).
- Application developed using PHP/Java and open-source database.
- Fully mobile-responsive and web-accessible.

6.8 Training

- Vendor shall conduct “train-the-trainer” sessions for KSEBL trainers/End users.

- Trainers shall conduct end-user sessions for individuals and groups.
- Training shall cover interface navigation, task execution, and system utilization.

6.9 Application Knowledge Transfer

- Vendor shall provide sessions for KSEBL's Core IT Team (≥10 staff) at Thiruvananthapuram.
- Coverage: Architecture, documentation, deployment, configuration, database schema, APIs, security, debugging, and error handling.

6.10 Project Inception

- Vendor shall prepare a project plan detailing:
  - Tasks and activities
  - Responsible personnel
  - Allocated resources
  - Timelines, milestones, and deliverables

6.11 Requirement Study

- Vendor shall review and finalize the SRS in consultation with KSEBL.
- Final SRS shall be submitted for approval, before initating the development
- The functional requirements specified in this document are indicative and may be subject to change. Any additional or revised requirements identified during the **Requirement Study Phase** shall be incorporated before the finalization of the **Software Requirements Specification (SRS)**.

6.12 User Acceptance Testing (UAT)

- Vendor shall conduct and manage UAT with KSEBL's cooperation.
- UAT shall validate compliance with all functional requirements.

6.13 Source Code, Documentation, and IPR

- Complete source code and documentation to be handed over to KSEBL.
- Documentation shall cover architecture, design, deployment, and configuration.
- All Intellectual Property Rights (IPR) shall rest exclusively with KSEBL.

6.14 Project Timeline

- Development, testing, and commissioning shall be completed within **six (6) months** from the Letter of Award (LoA).

7. Integration Points

- KSEBL Single Sign-On (SSO)
- SMS Gateway
- SMTP Email Server
- RESTful APIs for HRIS, attendance, and maintenance systems
- Biometric modules (fingerprint/face)
- Readers/Mobile devices

---

8. Assumptions and Constraints

- Hardware, network, and OS environments provisioned by KSEBL.
- External services (e.g., biometric) shall conform to agreed APIs.
- Regulatory approvals managed by KSEBL.
- All data shall reside within KSEBL servers, per CERT-In guidelines.

---

9. Future Enhancements

- Native mobile applications for pass requests and gate scanning.
- Predictive analytics for high-risk visitor identification.
- Integration with CCTV and intrusion detection systems.
- AI-driven anomaly detection on visitor behavior.

10.Application Security Audit

1. **Responsibility**
    - The selected firm shall be fully responsible for conducting a comprehensive **Application Security Audit** of the developed application prior to go-live.
2. **Cost**
    - The entire cost of conducting the security audit shall be borne by the development firm.
3. **Audit Agency**

- The audit shall be carried out only by a **CERT-In empaneled agency** approved for application security assessments.

4. **Certification Requirement**

   - The development firm shall ensure that a **“Safe to Host” certificate** is obtained from the audit agency and submitted to KSEBL before the application is commissioned for production use.

5. **Compliance**

   - The application shall not be accepted for go-live unless the above certification has been submitted.
