
📘 INFANT SECURITY & MOTHER–INFANT PAIRING ECOSYSTEM

SYSTEM SPECIFICATION DOCUMENT (SSD)

Version: 1.0
Prepared for: *Eagle IOT*
Prepared by: Omar
Location: Riyadh, Saudi Arabia

---

1. Introduction

1.1 Purpose of the Document

This System Specification Document (SSD) defines the complete functional, technical, architectural, and compliance requirements for the Infant Security & Mother–Infant Pairing Ecosystem.
It serves as the **single source of truth** for:

- Backend development
- Firmware development
- UI/UX design
- Simulation environments
- API generation
- Database creation
- Integration workflows

This SSD enables AI agents and engineering teams to begin development **without physical hardware**.

---

2. System Overview

The system prevents:

- Infant abduction
- Infant swapping
- Unauthorized movement
- Identity errors

- Manual logging failures

It integrates:

- Infant ankle tags
- Mother wrist tags
- RTLS/RFID readers
- Gate movement terminals
- Alarm controller nodes
- Footprint biometric scanner
- Backend platform
- Dashboards
- Compliance & audit systems

---

3. Functional Requirements

3.1 Infant Tag Functions

- Broadcast unique ID
- Detect tamper events
- Send periodic beacons
- Report battery status
- Communicate via BLE or UHF RFID

3.2 Mother Tag Functions

- Broadcast unique ID
- Passive or active mode
- Link to infant

3.3 RTLS Reader Functions

- Detect tag presence
- Map tag to zone
- Send sightings to backend

3.4 Gate Terminal Functions

- Scan infant tag
- Scan mother tag
- Scan staff ID
- Request movement authorization
- Display result
- Log movement

3.5 Alarm Controller Functions

- Receive alarm commands
- Activate siren/strobe
- Silence/reset alarms

3.6 Footprint Scanner Functions

- Capture footprint image
- Extract biometric template
- Send template to backend
- Detect duplicates

3.7 Backend Functions

- Real-time location tracking
- Pairing management
- Gate authorization
- Event & alarm engine
- Biometric engine
- Device management
- Audit logging
- User & role management

---

4. Hardware Specifications (Conceptual)

4.1 Infant Tag

- BLE SoC (Nordic nRF52832/840)

- Tamper loop sensor
- CR2032 battery
- Silicone strap
- IP67 enclosure

4.2 Mother Tag

- Passive RFID or BLE
- Silicone wristband

4.3 RTLS Reader

- UHF RFID module
- PoE power
- Multi-antenna

4.4 Gate Terminal

- 5–7" touchscreen
- HF RFID reader
- 2D barcode scanner
- Ethernet/Wi-Fi

4.5 Alarm Node

- MCU
- Relay outputs
- Siren/strobe control

4.6 Footprint Scanner

- 5–8 MP camera
- LED illumination
- Compute module

---

5. Firmware Architecture

5.1 Infant Tag Firmware

Modules:

- Bootloader
- HAL
- Power management
- Tamper detection
- Beaconing
- Secure communication
- Battery monitoring

5.2 Mother Tag Firmware

- ID broadcast
- Low-power mode
- Optional LED feedback

5.3 RTLS Reader Firmware

- RFID driver
- Tag filtering
- Zone mapping
- MQTT/HTTPS communication
- Watchdog

5.4 Gate Terminal Software

- RFID service
- Scanner service
- Gate logic
- UI service
- Offline buffer
- TLS communication

5.5 Alarm Node Firmware

- State machine
- Relay control
- Communication module

- Watchdog

5.6 Footprint Scanner Software

- Image capture
- Preprocessing
- Template extraction
- Enrollment/verification
- UI

---

6. Backend System Architecture

6.1 Core Services

- Device Gateway
- RTLS Service
- Pairing Service
- Gate Authorization Service
- Event & Alarm Service
- Biometric Service
- User & Role Management
- Audit Logging
- Configuration Service

6.2 API Gateway

- Authentication
- Rate limiting
- Routing
- Versioning

6.3 Real-Time Communication

- WebSockets
- MQTT

6.4 Deployment Model

- On-prem or cloud
- Docker/Kubernetes
- PostgreSQL + Redis

---

7. Database Schema

7.1 Key Tables

- mothers
- infants
- infant_tags
- mother_tags
- devices
- readers
- gates
- zones
- infant_mother_pairings
- movement_logs
- security_events
- alarms
- biometric_templates
- users
- roles
- audit_logs

---

8. API Specifications

8.1 Authentication

- POST /auth/login

8.2 Infant & Mother Management

- POST /infants

- POST /mothers
- GET /infants/{id}

8.3 Tag Assignment

- POST /tags/infant/assign
- POST /tags/mother/assign

8.4 Pairing

- POST /pairings
- GET /pairings/{infantId}

8.5 RTLS

- GET /location/tag/{tagUid}
- POST /rtls/readerEvent

8.6 Gate Authorization

- POST /gate/authorizeMovement
- GET /gate/movements

8.7 Events & Alarms

- POST /events/tamper
- POST /alarms/raise
- POST /alarms/silence

8.8 Biometrics

- POST /biometric/enrollInfant
- POST /biometric/verifyInfant

8.9 Device Management

- POST /devices/register
- POST /devices/heartbeat

---

9. Compliance Requirements

9.1 SFDA

- MDMA/MDEL

- Technical file
- Risk management

9.2 International Standards

- ISO 13485
- IEC 60601-1
- IEC 60601-1-2
- IEC 62304
- ISO 14971
- ISO 10993

9.3 Saudi PDPL

- Data protection
- Consent
- Access control
- Retention policies

---

10. Project Plan

10.1 Timeline

- Requirements: 1 month
- Hardware: 3–4 months
- Firmware: 2–3 months
- Backend: 3–4 months
- Dashboards: 2–3 months
- Testing: 2–3 months
- Deployment: 1–2 months

Total: **9–12 months**

---

11. Simulation Requirements (For AI Development)

Since hardware is not yet available, the AI agent must simulate:

11.1 Infant Tag Simulator

- Randomized beacon intervals
- Tamper events
- Battery drain

11.2 RTLS Reader Simulator

- Zone mapping
- RSSI variation
- Tag movement patterns

11.3 Gate Terminal Simulator

- Scan sequences
- Authorization requests

11.4 Alarm Node Simulator

- State transitions

11.5 Biometric Simulator

- Template generation
- Duplicate detection

---

12. Acceptance Criteria

The system is accepted when:

- All APIs function as specified
- All dashboards operate correctly
- All simulated devices communicate properly
- All workflows pass UAT
- Compliance documentation is complete

---

13. Appendices

- Appendix A: Hardware Schematics
- Appendix B: Firmware Architecture

- Appendix C: Backend Architecture
- Appendix D: Database Schema
- Appendix E: API Documentation
- Appendix F: Compliance Checklist
- Appendix G: Project Plan
- Appendix H: BOM & Sourcing Plan
- Appendix I: Tender Documentation