RFP- mSparsh

Contents`

Request for Proposal (RFP)

1. Introduction

BARC India invites proposals from qualified vendors for a scalable, platform-agnostic mobile solution (starting with Android) to support real-time panel management, field operations, and digital audience measurement via AI/ML-driven features.

1.1 Purpose of the RFP

1.1.1. Interactive Panel Management

Enable field agents and panel households to manage responsibilities interactively. For eg.

- Real-time panel status monitoring (e.g., active/inactive households, device health).
- Panel member onboarding, verification, and consent workflows.
- Notifications and alerts for anomalies, compliance checks, or maintenance.

1.1.2. Field Operations Support

Digitized field workflow management for agents.

- Dashboard: KPI & Alerts
- RM Leave Management: Leave Management System
- Feedback Management for RM's Visit

1.1.3. IPMS Integration (Ticketing System)

Seamless integration with the existing Internal Panel Management System (IPMS).

- Real-time ticket creation, escalation, assignment, and resolution workflows.
- Field agent visibility into pending/resolved issues.
- Audit trail and feedback capture for each ticket.

1.1.4. In-App Surveys

Customizable and dynamic surveys for panel households or field agents.

- Triggered surveys based on events (e.g., installation, anomaly).
- Support for multimedia-based responses (voice, image, text).
- Survey analytics and compliance tracking.

1.1.5. AI/ML-Powered Plugin for Forecasting, Engagement, Diagnostics & Insights

Forecasting: Task generation for Field team and help reduce maintenance visit, Meter Health, sync issues, tampering and similar use cases.

Engagement: Personalized nudges, gamification features, earn points, points conversion to incentive, content-based feedback collection to boost long-term panel participation.

Diagnostics: Predictive maintenance for panel devices (e.g., IOT devices), anomaly detection in panel behavior or data patterns.

Insights: Field agent performance dashboards, household engagement scoring, automated recommendation systems for escalations or actions.

2. Scope of Work

2.1 Communication to the Panellist

Objective: Ensure panellists are kept informed in a timely manner based on system events or routine checks.

Key Components:

- Dashboard: Panel Health & Alerts
  A central visual interface that shows the status of each panel household (HH). This can include:
  - Green/Red indicators for healthy/problematic households.
  - Summary counts of total households with issues.
  - Quick filters for field teams to identify problem households.
- HH Connectivity Compliance Status
  - Shows whether the household equipment is online or facing connectivity issues.
  - Compliance could be measured in terms of uptime percentage (e.g. 98% connected in the last week).
- Viewership Compliance Status
  - Verifies if the viewership data from households is being collected properly.

    - Compliance metric: % of expected data successfully received.

- Button Pushing Compliance Status
    - Checks if panellists are pressing the assigned buttons (e.g., to log who is watching TV) regularly.
    - Compliance metric: % of time button pushing logs received as per expectations.

- Family Member's Birthday Alert
    - System generated reminders for family member birthdays.
    - Purpose: Enable Field Team or system to send greetings, vouchers, enhancing panellist engagement and satisfaction.

2.2 Field Worker Engagement

Objective: Monitor and improve the performance and compliance of Relationship Managers.

Key Components:

- Dashboard: KPI & Alerts
    - Central interface for Field team to track key performance indicators (KPIs).
    - Visual alerts for Field team falling behind targets.

- HH Connectivity Compliance Status
    - Similar to panellist dashboard but aggregated per Field executive — showing how well the Field executive/team assigned households are performing in connectivity.

- Viewership Compliance Status
    - Field Executive/Team households' viewership data compliance — highlighting gaps for follow-up action.

- Button Pushing Compliance Status
    - Field Executive/Team assigned households' adherence to button-pushing protocols.

- SA Closure Compliance Status
    - SA (Service Activity) tickets logged and closed by the Field Executive/Team.
    - Compliance metric: % of tickets closed within SLA.

- Time Stamping Daily & Weekly
    - Field Executive log start/end time of daily visits.
    - Weekly submission of activity summary.
    - Purpose: Ensure Field Executive field activity is traceable and verifiable.

- Attendance of Field Executive
    - Daily presence/absence record.
    - Integrated with leave and visit logs.

- Field Executive Leave Management: Leave Management System
    - Track Daily Attendance
        - Simple daily check-in/check-out system via mobile app or web portal.
    - Monitor Leave Records
        - Database maintaining:
            - Leave applied
            - Leave approved/rejected
            - Leave balance remaining
    - Generate Alerts for Excessive Leave
        - Automatic alerts when:
            - Leave threshold exceeded (e.g. >10% days absent per month).

        - Unusual leave patterns detected (e.g. frequent Fridays/Mondays absent).
    - Escalation to supervisors for review and action.

2.3 Feedback Management for Field Executive Visit

Objective: Collect and analyze structured feedback after Field Executive visits to assess field quality and improve service.

Features Breakdown**:**

- Post-Visit Feedback Collection
    - Feedback should be gathered immediately after the visit:
        - Via mobile app (prompt household to submit).
        - Via SMS link.
        - Manual call center follow-up.
- Stakeholder Input Channels
    - Multiple options for feedback submission:
        - Household members (panellists)
        - Supervisors / Managers reviewing RM performance
- Standardized Feedback Forms
    - Unified structure to collect data consistently:
        - **Rating scales** (1-5 for each area)
        - **Comments section** (open text)
        - **Predefined Questions**:
            - Was the Field Executive punctual?
            - Was the Field Executive professional and courteous?
            - Were household issues resolved?

        - Did the Field Executive communicate clearly?
        - Overall satisfaction with the visit.

- Sentiment Analysis (Optional Advanced Feature)
    - Use NLP tools to analyze written comments for:
        - Positive, Neutral, Negative sentiment.
        - Extract recurring issues or praise topics.

- Feedback Scoring and Trends
    - Convert feedback to numerical scores.
    - Display trends over:
        - Weekly
        - Monthly
        - Quarterly
    - Identify top performers and struggling Field Executive.

- Alerts and Escalation Triggers
    - Auto-trigger alerts if:
        - Field Executive receives multiple low scores in a period.
        - Same issue repeatedly mentioned.
    - Supervisor notified for intervention.

- Reporting and Export Options
    - Generate periodic reports:
        - Weekly summary reports.
        - Monthly performance reviews.
    - Export formats: Excel, PDF.
    - Secure sharing with management.
    - Access via Web Dashboard for HO(Head Office)

3. AI/ML Use Cases

3.1. Forecasting for Field Operations and Meter Intelligence

- Predict when a household is likely to require a Field Executive visit based on engagement trends, usage anomalies, or historical issue patterns. Automate task creation for timely check-ins and issue resolution.
- Continuously monitor usage data to forecast potential degradation or failure of metering devices, enabling preventive maintenance.
- Identify likely occurrences of sync failures, abnormal signal drops, or communication breakdowns, and preemptively trigger support tasks.
- Use anomaly detection on meter signals and behavioral data to forecast potential tampering incidents, supporting early intervention.
- Extend forecasting to other operational areas such as vacation detection, ticket prioritization, and task routing to improve field efficiency and data integrity.

3.2. Real-time Meter Health Monitoring

- Use machine learning models to continuously monitor telemetry and usage data from metering devices.
- Detect early signs of malfunction, tampering, or data loss (e.g., drop in heartbeat signals, unusual latency).
- Classify issues as software/hardware/network and auto-prioritize them for field resolution.
- Predict future failures using historical device behaviour (predictive maintenance).

3.3. Viewership Pattern Analytics

- Analyse household-level and region-level viewing behaviour trends.
- Identify anomalies or shifts in TV consumption (e.g., sudden drop in genre-wise viewership).
- Flag unusual patterns that may indicate disengagement, manipulation, or technical issues.
- Feed insights to improve sample quality, content alignment, or program evaluation.

3.4. Incentive Optimizer with Impact Tracking

- Apply AI models to determine optimal incentive schemes based on panel participation, demographics, and engagement levels.

- A/B test different reward types (monetary, non-monetary) and track impact on behaviour.
- Adjust incentives dynamically to retain or activate disengaged households.
- Provide transparent attribution of incentive impact on viewership quality and continuity.

3.5. Smart Alert Forecasting (Meter Anomalies, Missed Sync)

- AI-driven anomaly detection to trigger real-time alerts for issues like:
    - Missed data syncs
    - Power-offs or resets
    - Abnormal usage signatures
- Predict and Prioritize alerts by severity and urgency, reducing false positives and agent overload.

3.6. Vacation Auto-detection

- Identify prolonged non-usage patterns that may indicate panel household vacations.
- Cross-check with historical vacation behaviour, calendar trends, or mobile location data (where permitted).
- Auto-flag and update panel availability status to improve measurement accuracy.
- Notify agents only if manual confirmation is needed.

3.7. Smart Ticket Pre-fill & Predictive Fixes

- Use natural language processing and classification models to:
    - Auto-fill issue types and categories based on system logs, user input, or behaviour.
    - Recommend fixes or SOP steps based on historical resolutions.
- Reduce field agent effort and resolution turnaround time.
- Improve consistency and accuracy in ticketing workflows.

3.8. SOS with Evidence Capture

- When agents or panel homes trigger an SOS, AI prioritizes alerts based on location, time, and historical context.
- Automatically attach contextual evidence like photos, logs, audio messages, or chat history.

- Help supervisors or control centres respond quickly and appropriately to field escalations or emergencies.

3.9. Household Behaviour Segmentation for Ops

- Use clustering and behavioural modelling to segment panel households by:
    - Engagement level
    - Compliance risk
    - Demographic + behavioural traits
- Tailor outreach, visits, and communication based on segment (e.g., proactive visits for high-risk HHs).
- Improve operational efficiency by focusing resources where needed most.

3.10. AI-based Visit Optimization

- Optimize field agent visit plans using AI-powered route planning:
    - Cluster tickets or tasks by location and priority.
    - Availability of the panelist
    - Factor in live traffic, geo-fencing, and historical visit effectiveness.
    - Suggest visit times when HHs are most likely to be available.
- Reduce travel time, fuel costs, and no-show visits.

3.11. Chatbot with Event History

- Intelligent chatbot for agents and panel HHs with memory of past interactions and system events.
- Handle FAQs, SOPs, ticket status queries, and data sync issues autonomously.
- Escalate to human support only when required.
- Improve support availability, especially in remote or low-connectivity areas.

3.12. KPI Dashboard (Engagement, Tickets, Anomalies)

- AI-curated dashboards for central teams and supervisors.
- Track operational health: panel engagement scores, ticket resolution rates, anomaly trends, agent productivity.
- Provide early warning indicators (e.g., rising disengagement in a region).
- Recommend corrective actions or optimizations based on historical patterns.

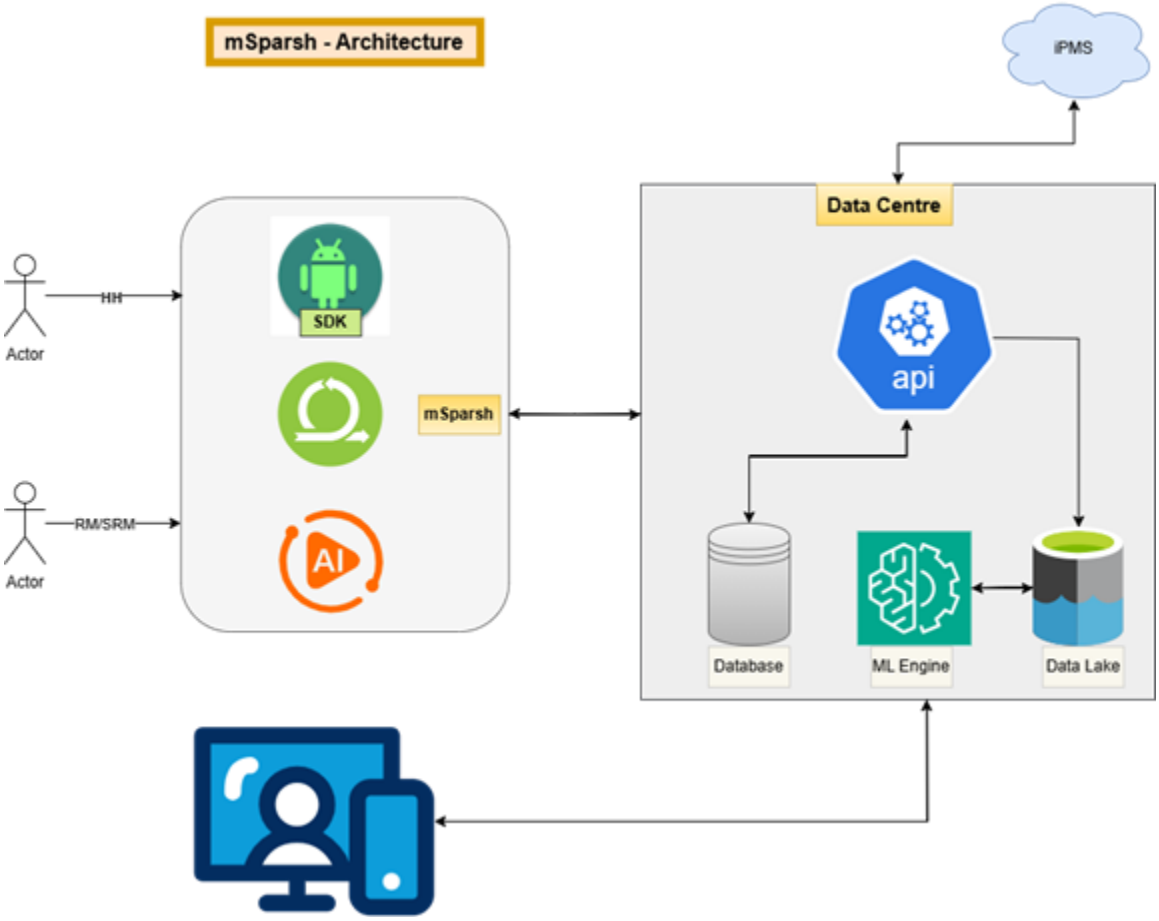
3.13 LMS

- Need to have a LMS for all profile based on some video watching.

- Need to have details what was watched and should be able to re-initiate the same.
- Should have incentive based as well which can be mapped at the backend with AI to provide the same at random instances.

4. mSparsh - Workflow

The mSparsh architecture outlines the interaction between various components of the system. It is designed to facilitate efficient data flow between the user interfaces, the processing API, and backend services like iPMS and the database.
Below is the architectural diagram and its explanation.



Architecture Explanation

1. Mobile Application (Field Interface)

Android SDK:

- Android-based mobile app.
- Used by field users like HH (Household handlers).

mSparsh Connector:

- Core application logic.
- Connects with backend APIs to communicate.
- Interfaces with backend via APIs.

AI Component:

- Integrates Artificial Intelligence.
- Provides insights like predictions, pattern detection, etc.

2. API Gateway (Integration Layer)

- Acts as a middleware between the mobile application and backend systems.
- Handles data flow in both directions.
- Ensures secure and scalable communication.

3. Data Centre (Backend Infrastructure)

Database:

- Stores structured operational data.
- Includes user data, logs, task status, etc.

ML Engine:

- Performs machine learning analysis.
- Enhances raw data with insights.
- Feed results to the Data Lake.

Data Lake:

- Central repository for all data.
- Stores raw and processed data.
- Supports large-scale analytics and model training.

4. External Integration (iPMS)

- Integrated Panel Management System.
- Communicate with the backend via APIs.
- Enables synchronization of panel data and reporting.

5. User Devices

Multi-platform Access:

- Users (RM/SRM/AM) can access the system via desktop and mobile phones.
- Enables real-time monitoring and interaction.

Data Flow Summary:

1. Data is collected via the Android app (mSparsh).

2. Data flows through the API to the backend systems.

3. The backend stores and processes the data using ML Engine.

4. Raw and processed data is archived in the Data Lake.

5. iPMS interacts with the API for external data operations.

6. Users access insights via mobile or desktop dashboards.

7. The system may need to integration with other backend systems as well.

5 Vendor Instructions

5.1 Background

This RFP has been issued to identify a vendor with experience in large-scale, AI-powered, media analytics applications.

5.2 General Instructions

- Proposal validity: 180 days

- Include/exclude features must be specified

- Responses are binding

5.3 RFP Changes, Binding Bid Process

- BARC may revise/cancel RFP without notice

- Only invited vendors considered

5.4 Disqualification

Misleading, inaccurate, or incomplete proposals may result in disqualification.

5.5 Structure of the Response

Executive Summary

Company Profile

Legal Name, Address, Year of Incorporation

Industry experience, key clients

Relevant Experience and Client References

Understanding of Requirements / Scope of Work

Eligibility Criteria Response

Compliance Matrix

Proposed Solution (with screenshots if applicable)

Architecture, components covered, scalability

Data flow, AI/ML usage, support model

Deployment Options

Cloud-based / On-premises / Hybrid

Support for both hardware and software-based deployment

Implementation Plan and Training

Compliance & Security

GDPR compliance, security certifications, data policies

Post-Implementation Support / SLA

Project Timeline

Project Management Methodology

Pricing Proposal

Pricing structure, cost breakdown

Implementation and training costs

5.7 Contacts

All questions and submissions should be directed to pmo@barcindia.co.in

5.8 Evaluation Criteria

- Completeness of Proposal
- Technical Merit and Future-readiness
- Relevant Experience and References
- Cost Effectiveness
- Post-deployment Support and SLAs
- Compliance to Technical, Security, and Performance Requirements
- Quality of Proposed Project Team and Approach

5.9 Non-Functional Requirements (NFRs)

The mobile solution proposed under this RFP must adhere to the following non-functional requirements, ensuring high performance, scalability, maintainability, security, and availability:

5.9.1 Performance

The application must load within 3 seconds under normal network conditions (5G or better).

API responses must be returned in under 300ms for 95% of requests under standard load.

Support for up to 50,000++ concurrent users without degradation in performance.

5.9.2 Scalability

Solution must be horizontally and vertically scalable to support future increases in user base and data volume.

Should support scaling up to 5x the initial load with minimal configuration changes.

5.9.3 Availability and Uptime

The mobile application and backend APIs must ensure 99.9% uptime, excluding scheduled maintenance (to be notified 48 hours in advance).

Failover mechanisms and disaster recovery (DR) plans must be defined and tested.

5.9.4 Security

All components must follow secure development and deployment practices.

Must implement role-based access control (RBAC) with session timeout and encryption of sensitive data.

Regular penetration testing and security audits are mandatory, with results shared upon request.

5.9.5 Maintainability

Codebase must be modular and documented with inline comments and architectural documentation.

Vendor must provide a knowledge transfer plan, including onboarding sessions and technical documentation.

5.9.6 Interoperability

The solution must be able to integrate with BARC's iPMS system and future internal tools via REST APIs or standardized connectors.

Mobile app must support offline mode with auto-sync upon connectivity restoration.

5.9.7 Device Compatibility

Initial version must support Android (API level 24+), with a roadmap for iOS.

Must be compatible with at least 95% of Android devices based on BARC-provided usage data.

5.9.8 Logging & Monitoring

All transactions, errors, and key events must be logged.

Integration with BARC's centralized logging system or provide custom dashboards with metrics like CPU usage, memory, errors, and API performance.

5.10 Acceptance Criteria

The following acceptance criteria will be used by BARC India to evaluate successful delivery, testing, and deployment of the solution:

5.10.1 Functional Acceptance

All functional modules as per Scope of Work (e.g., meter health, ticketing, AI routing, chatbot, incentive display) are fully implemented and demonstrable.

All critical workflows (SOS trigger, HH updates, smart alerts) must pass UAT with zero critical defects.

5.10.2 Performance Acceptance

Performance benchmarks under simulated real-world conditions meet or exceed the defined metrics.

The application should be lightweight, minimizing battery, memory, and CPU usage on user devices.

Load tests conducted with ≥ 10,000 concurrent users must reflect system stability and acceptable response times.

5.10.3 Security & Compliance Acceptance

VAPT report must be shared and all high/critical vulnerabilities fixed before go-live.

The application must pass GDPR/Indian Data Protection compliance audit with documented evidence.

5.10.4 Integration Acceptance

Seamless data exchange with iPMS system through secure APIs must be demonstrated.

Dashboard and KPI modules must reflect real-time updates based on backend triggers.

The app must be available for download via Google Play, Apple App Store, and as an APK.

It must comply with Google and Apple data and solution security guidelines.

App updates should be delivered over-the-air (OTA) from the cloud.

Minimal end-user intervention should be required.

No repeated manual settings changes during installation or usage.

Once configured by the RM on the user's device, no further changes should be needed.

5.10.5 Training and Handover

Training sessions for BARC ops and tech teams must be completed.

All source code, environment setup, deployment scripts, documentation, and admin credentials must be handed over as per SLA.

5.10.6 Support Readiness

SLAs for L1, L2, L3 support clearly defined and a support team assigned pre-launch.

24x7 helpdesk availability post-deployment with agreed escalation matrix.

5.11 Awarding of Contract

BARC reserves the right not to award the contract based solely on pricing or presentation. Final selection will be based on an overall assessment of value, capability, and strategic alignment.

6. Security and Compliance Requirements

Vendors are expected to implement robust security measures and ensure full compliance with applicable laws, industry standards, and best practices. The solution must align with modern cybersecurity frameworks and demonstrate the ability to operate in regulated environments such as those governed by Indian data localization norms, GDPR (for global applicability), and ISO standards.

6.1 Data Security

Encryption: All data must be encrypted at rest and in transit using industry-standard protocols (e.g., AES-256, TLS 1.2/1.3).

Tokenization or anonymization should be applied to any PII (personally identifiable information) if collected.

Secure APIs: All system APIs must be secured using authentication tokens, rate-limiting, and authorization rules.

6.2 Privacy Compliance

The solution must comply with **India's Data Protection Bill**, and any global privacy laws where applicable (e.g., GDPR, CCPA).

Data collected must be processed only for legitimate measurement and analytics purposes.

Privacy by design: screen grabs, audio samples, or traffic logs must **not capture user credentials, personal images, or conversations**.

Optional consent and opt-out mechanisms should be supported if using household/mobile metering.

6.3 Secure Development Lifecycle (SDLC)

The vendor must follow secure coding practices (e.g., OWASP Top 10).

Periodic **vulnerability assessments and penetration tests (VAPT)** must be conducted, with results available to BARC India upon request.

Supply chain risks must be documented and mitigated.

All Code should be available at BARC Code Report

6. Certification Requirements

Solutions should be compliant with at least one of the following (or equivalent):

ISO/IEC 27001: Information Security Management

SOC 2 Type II: Security and operational controls

CERT-IN audit (for Indian deployments)

SSAE-18/SSAE-16 for cloud-hosted platforms

7. Data Retention and Deletion

Define retention policies clearly for logs, metadata, and audio/video samples.

Data must be deletable upon request by BARC India and securely purged from all storage systems.

Backup data must also comply with the retention and deletion policy.

8. Incident Response

Defined incident response plan with 24x7 monitoring and reporting timelines.

Root cause analysis (RCA) must be provided within **48 hours** of a reported breach or service impact.

BARC must be informed of any potential or actual data breaches within **24 hours**.

9. Evaluation Criteria

- Technical capability & architecture: 30%

- Industry experience & references: 20%

- Cost effectiveness: 20%

- Innovation & future readiness: 15%

- Post-deployment support: 15%

10. Submission Timeline

- RFP Issue Date: [DD/MM/YYYY]

- Last Date for Queries: [DD/MM/YYYY]

- Proposal Submission Deadline: [DD/MM/YYYY]

- Vendor Presentations: [DD/MM/YYYY]

- Final Selection & Award: [DD/MM/YYYY]