Request for Proposal

for

Selection of Master System Integrator for Implementation of Smart Solutions in Rajkot City

TENDER No. : RSCDL/SMART CITY/05/2017-18

RSCDL

Smart,Livable,Sustainable

Issued by

Chairman & The Municipal Commissioner

For

Rajkot Smart City Development Limited (RSCDL)

Volume 2 – Scope of Work and specification

Part-1

Disclaimer

The information contained in this Request for Proposal document ("**RFP**") whether subsequently provided to the bidders, ("**Bidder/s**") verbally or in documentary form by Rajkot Smart City Development Limited (henceforth referred to as "**RSCDL**" in this document) or any of its employees or advisors, is provided to Bidders on the terms and conditions set out in this Tender document and any other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is not an offer or invitation to any party. The purpose of this RFP is to provide the Bidders or any other person with information to assist the formulation of their financial offers ("**Bid**"). This RFP includes statements, which reflect various assumptions and assessments arrived at by RSCDL in relation to this scope. This Tender document does not purport to contain all the information each Bidder may require. This Tender document may not be appropriate for all persons, and it is not possible for the Managing Director, RSCDL and their employees or advisors to consider the objectives, technical expertise and particular needs of each Bidder. The assumptions, assessments, statements and information contained in the Bid documents, may not be complete, accurate, adequate or correct. Each Bidder must therefore conduct its own analysis of the information contained in this RFP and to seek its own professional advice from appropriate sources.

Information provided in this Tender document to the Bidder is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. RSCDL accepts no responsibility for the accuracy or otherwise for any interpretation of opinion on law expressed herein.

RSCDL and their employees and advisors make no representation or warranty and shall incur no liability to any person, including the Bidder under law, statute, rules or regulations or tort, the principles of restitution or unjust enrichment or otherwise for any loss, cost, expense or damage which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, reliability or completeness of the RFP, and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process.

RSCDL also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. RSCDL may in its absolute discretion, but without being under any obligation to do so, can amend or supplement the information in this RFP.

The issue of this Tender document does not imply that RSCDL is bound to select a Bidder or to appoint the Selected Bidder (as defined hereinafter), for implementation and RSCDL reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by RSCDL or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and RSCDL shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation for submission of the Bid, regardless of the conduct or outcome of the Selection process.

Table of Contents

Terms	Meaning
Authority	Rajkot Smart City Development Limited (RSCDL)/ Rajkot Municipal Corporation (RMC)
AMC	Annual Maintenance Contract
ANPR	Automatic Number Plate Recognition
ATCS	Adaptive Traffic Control System
AP	Access Points
BOM	Bill of Material
BEC	Bidders Evaluation Committee
CC	Capital Cost
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
DC	Data Centre
DD	Demand Draft
ECB	Emergency Call Box
EMD	Earnest Money Deposit
ERP	Enterprise Resource Planning
FMS	Facility Management Services
GCP	Ground Control Point
GIS	Geographical Information Systems
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HOD	Head of Department
ICT	Information and Communication Technology
ICCC	Integrated Command and Control Centre
IT	Information Technology
ITMS	Intelligent Traffic Management System
IP	Internet Protocol
INR	Indian Rupee
LoI	Letter of Intent
MMTS	Multi-Modal Transport Systems

Terms	Meaning
MRCOS	More Rajkot City Operations System
MSI	Master System Integrator
NPV	Net Present Value
OEM	Original Equipment Manufacture
OFC	Optical Fiber Cable
O&M	Operations & Maintenance
PA	Public Address
PBG	Performance Bank Guarantee
PDD	Proposal Due Date
PoC	Proof of Concept
PoP	Point of Presence
PQ	Pre-Qualification
PTZ	Pan Tilt Zoom
PV	Present Value
RFP	Request for Proposal
RLVD	Red Light Violation Detection
SLA	Service Level Agreement
SOP	Standard Operating Procedures
SVD	Speed Violation Detection
TPA	Third Party Auditor
TQ	Technical Qualification
TRV	Total Revenue
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
VM	Virtual Machine
VMS	Variable Message Sign
WSP	Wi-Fi Service Provider

Acronyms & Abbreviations

1. Introduction

The City of Rajkot has emerged as one of Gujarat's hi-tech city in technological development and innovation. The city has established its position as a pioneer in implementing numerous Smart initiatives in areas ranging from transit, e-Governance, solid waste management to water supply and many more. Additionally, Rajkot has been selected among the top 100 smart cities in India for which it receives funding from Ministry of Urban Development (MoUD) for projects under its smart city proposal.

RMC has completed the citizen's consultation round where views and suggestions were called, to arrive at the City's Vision and define goals to be achieved in next 5, 10 or 20 years. Rajkot smart city proposal includes several Pan City and Area Based Development initiatives with a focus on both infrastructure and ICT advancements in the city and at strategic locations. Most of the ICT initiatives have been identified with a predominant objective to improve public safety and surveillance, traffic management, quality of public services, and real time tracking of services.

1.1 About Rajkot Municipal Corporation

Rajkot Municipal Corporation (RMC) is a local government body committed to provide basic infrastructure facilities including entertainment facilities to the people of the city. RMC is very well known for the managing the city by using private sector participation as well as introduction of innovative mechanism in management to serve people efficiently. City has prepared different plans for improving services and to nullify gap between services and demands.

1.2 About Rajkot Smart City Development Limited

The Government of India launched the Smart Cities Mission on 25th June, 2015 with an objective to promote sustainable and inclusive cities that provide core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment and application of 'Smart'
Solutions.

Rajkot secured 3rd rank among 30 new cities announced on 23rd June, 2017 by Ministry of Urban Development (MoUD) for development as smart cities under the Smart City Mission.

The implementation of the Mission at the City level will be done by a Special Purpose Vehicle (SPV) created for the purpose. The SPV will plan, appraise, approve, release funds, implement, manage, operate, monitor and evaluate the Smart City development projects. Each smart city will have a SPV which will be headed by a full time CEO and have nominees of Central Government, State Government and ULB on its Board.

A Special Purpose Vehicle (SVP), Rajkot Smart City Development Limited (RSCDL), is formed for Rajkot city to incorporate Smart Solutions. Rajkot Smart City proposal consists of two components – (i) Area Based Development & (ii) Pan City Solution.

As a part of Area based development projects, Raiya area in the western part of the city will be developed with world class facilities. Major ABD projects include exhibition and convention centers, amusement parks, business and incubation centers, skill development center, affordable housing etc.

The pan city solution includes intelligent traffic and integrated transport management, smart water and waste management, real-time environment monitoring, CCTV surveillance Wi-Fi services across city and online service delivery to improve public service delivery and digital inclusion.

2. About Project

2.1 Project Background

One of the primary objective of Rajkot under its smart city mission is to enhance the safety and security, improve efficiency of municipal services and promote a better quality of life for residents. In order to achieve these objectives, Rajkot desires to foster the development of a robust ICT infrastructure that supports digital applications and ensures seamless steady state operations, traffic management, surveillance, emergency response mechanisms and real time tracking of services and vital city metrics throughout the city and in government departments.

RSCDL is considering the appointment of an agency to set up these priority initiatives identified under the Smart City mission which will include Integrated Command and Control Center (ICCC)

and Smart Elements; including Intelligent Traffic and Integrated Transport Management System (ITITMS), smart parking, smart poles etc.

In addition to above, Rajkot Smart City Development Limited intends to carry out the work of Preparation of Base map , Property and Utility mapping (Water/Sewerage/Wastewater/storm water drain/sanitation facilities (Household / public / private) / solid waste management) for various zones/wards of Rajkot Smart City Development Limited using latest high resolution satellite imagery and superimposition of town survey maps and town planning sheets, Field Measurement book, existing administrative boundaries, slum boundaries, generation of building footprints / plots, infrastructure details, water bodies, landmarks, etc. and also develop a customized GIS applications for departments in RSCDL based on the inputs received from the Survey being carried out by RSCDL

2.2 Project Objectives

The key objective of this project is to establish a collaborative framework where input from different functional departments of Rajkot Municipal Corporation and other stakeholders such as transport, water, fire, police, meteorology, e-governance, etc. can be assimilated and analyzed on a single platform; consequently resulting in aggregated city level information. Further this aggregated city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens.

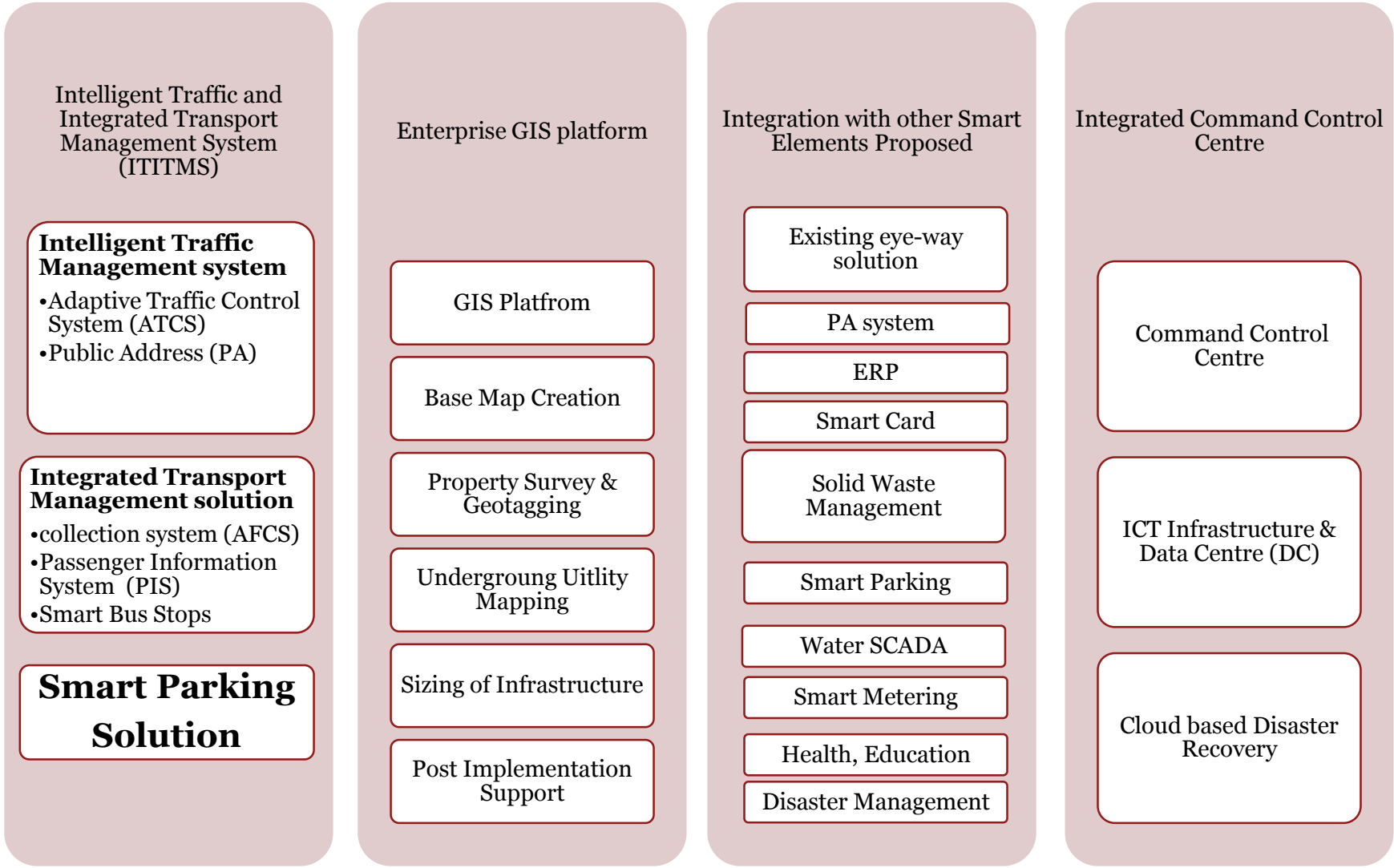
Following are the intangibles that should be addressed by the proposed interventions:

a. Efficient traffic management
b. Efficient Transport management
c. Enhanced safety and security
d. Better management of utilities and quantification of services
e. Asset Management
f. Disaster Management and Emergency Response
g. Integration with all existing and future services as identified by Rajkot Smart City Development Limited (RSCDL) in the city including but not limited to(with provision for future scalability):
    - City Surveillance System
    - Intelligent Traffic Management System
    - Solid waste management
    - Smart Parking
    - Public Address System
    - Environmental sensors
    - Smart Poles
    - Smart Lighting
    - Smart Governance
    - City Network
    - City Wi-Fi
    - Water SCADA & Smart Meters
    - Sewerage

- Storm water Drainage
- Electrical SCADA and Smart Meters
- E-Medicine/Health
- E-Education
- Disaster Management
- Grievance Management
- Geographical Information System/Citizen Portal
- Public Bike Sharing System
- Rajkot Mitra Travel Card/Wallet/Smart Payment
- Fire
- GIS based Property Management
- Rajkot City MobileApp and Portal
- Any other sensors/systems

2.3 Project Components

The Master System Integrator (MSI) shall be responsible for the implementing the Smart Solutions Project consisting as described in this section. The Key components of the Smart Solutions Project that the MSI shall implement that builds from the Pan City proposal are shown in below. Description of these components follows the illustration. The Rajkot Command and Control Centre shall be a central platform for integration.


Intelligent Traffic and Integrated Transport Management System (ITITMS)
Intelligent Traffic Management system
•Adaptive Traffic Control System (ATCS)
•Public Address (PA)
Integrated Transport Management solution
•collection system (AFCS)
•Passenger Information System (PIS)
•Smart Bus Stops
Smart Parking Solution
Enterprise GIS platform
GIS Platfrom
Base Map Creation
Property Survey & Geotagging
Undergroung Uitlity Mapping
Sizing of Infrastructure
Post Implementation Support
Integration with other Smart Elements Proposed
Existing eye-way solution
PA system
ERP
Smart Card
Solid Waste Management
Smart Parking
Water SCADA
Smart Metering
Health, Education
Disaster Management
Integrated Command Control Centre
Command Control Centre
ICT Infrastructure & Data Centre (DC)
Cloud based Disaster Recovery

3. Scope of Services for the Project

The section below details out the scope of various components to be provided as part of this project.

3.1 Components & Services Overview

The Master System Integrator (MSI) should ensure the successful implementation of the proposed "Smart Solutions in Rajkot City" and provide capacity building support to city authorities as per the scope of services described below. Any functionality not expressly stated in this document but required to meet the needs of the RSCDL to ensure successful operations of the system shall essentially be under the scope of the MSI and for that no extra charges shall be admissible. MSI shall implement and deliver the following systems and components: Establishment of ITITMS system, smart parking solution, Enterprise GIS,Enterprise resource planning and Integrated Command and Control Center with provisioning of ICT infrastructure for Data Centre and Disaster Recovery.

The MSI's scope of work shall include but will not be limited to the following broad areas. Details of each of these broad areas have also been outlined in **Annexure II**.

1. Assessment, Scoping and Survey Study: Conduct a detailed assessment, scoping study and develop a comprehensive project plan, including:

a. Assessment of existing systems, datasets, infrastructure and connectivity within the city for the scope items mentioned in section 3.1

b. Conduct site survey for finalization of detailed technical architecture, gap analysis and project plan

c. Conduct site surveys to identify need for site preparation activities

d. Obtain site Clearance obligations & other relevant permissions

2. Design, Supply, Installation, Commissioning and Testing which includes the following components:

a. Part I: Implementation of following Systems:

- Intelligent Traffic and Integrated Transport Management System (ITITMS)
- Integrated Command and Control Center
- ICT Infrastructure for Data Centre (DC) and Disaster Recovery
- Enterprise GIS
- Enterprise resource planning
- Smart Parking

b. Part II: Phase wise Integration of the ICT systems with Integrated Command and Control Centre

- Existing Eye-way solution
- Intelligent Traffic Management System
- Integrated transport management system
- Smart Parking
- Public Address System
- Smart Governance
- City Network
- Smart Card
- Sewerage
- Health
- Education
- Disaster Management
- GIS based citizen portal and datasets such as Property Management, Utility Survey data, etc.
- Smart Metering & SCADA
- Water leak identification system

3. Operation and Maintenance Phase

The selected vendor will also be responsible for O&M of deployed IT solution including management of hardware and application software, networking, installation, Training, for 5 year from the Go Live date.

4. Integrate with provisions available for Network Connectivity within the city which includes

a. Lease line/MPLS connectivity procured through a separate tender

b. Fiber optic network planned in future

c. Internet connectivity procured through a separate tender

5. Provisioning Hardware and Software Infrastructure which includes design, supply, installation, and commissioning of IT Infrastructure at Integrated command control center and DC. This consist of:

a. Basic Site preparation services

b. IT Infrastructure including server, storage, other required hardware, application portfolio, licenses

c. Command Center infrastructure including operator workstations, IP phones, joystick controller etc.

d. Establishment of LAN and WAN connectivity at command center and DC limited to scope of infrastructure procured for the project

e. Application integration services with other RSCDL applications

6. Capacity Building for RSCDL and any other department which includes preparation of operational manuals, training documents and capacity building support, including:

a. Training of the city authorities, police personnel and operators on operationalization of the system

b. Support during execution of acceptance testing

c. Preparation and implementation of the information security policy, including policies on backup and redundancy plan

d. Preparation of revised KPIs for performance monitoring of various urban utilities monitored through the system envisaged to be implemented

e. Developing standard operating procedures for operations management and other services to be rendered by ICCC

f. Preparation of system documents, user manuals, performance manuals, Operation manual,user help, etc.

7. Operations and Maintenance services for 5 years for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live.

3.2 Scope of services - Phases

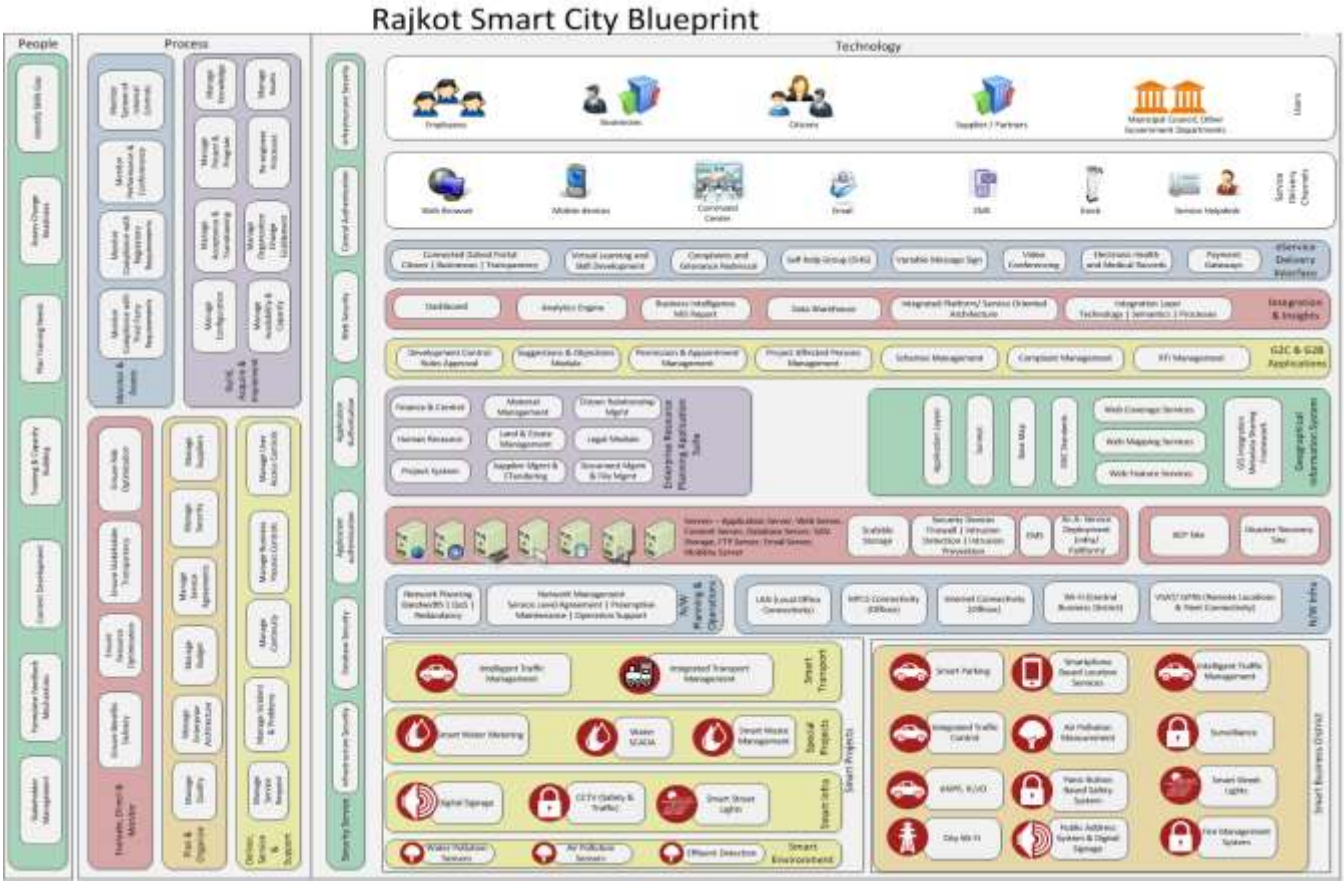
The following is a summary of the geographical extent of the project.

No.	System Description	Implementation	Integration	Phases
1.	Integrated Command and Control Centre	✓	×	Phase I
2.	Existing eye-way solution	×	✓	Phase I
3.	PA system	✓	✓	Phase I
4.	Intelligent Traffic and Integrated Transport Management System	✓	✓	Phase II
5.	Smart Governance (City Level Application Platform + ERP)	✓	✓	Phase II
6.	City wide - GIS Platform	✓	✓	Phase I
7.	Smart Card for Transport	×	✓	Phase II
8.	Solid Waste Management	×	✓	Phase II
9.	Smart Parking	×	✓	Phase II
10.	Sewerage (SCADA at treatment plant)	×	✓	Phase II
11.	Health	×	✓	Phase II
12.	Education	×	✓	Phase III
13.	Disaster /Emergency Management	×	✓	Phase III
14.	Smart Metering & SCADA for distribution network (water)	×	✓	Phase III
15.	Water leak identification system	×	✓	Phase III

Phase I – 0-6 months, Phase II – 6-12 months, Phase III- 12-18 months

3.3 Solution Architecture of ICCC

Indicative architecture of the components envisaged under the ""Integrated Command and Control Center" is as given below.



a. Sensor and actuator layer

The sensor layer will help the city administration gather information about the ambient city conditions or capture information from the edge level devices like intelligent traffic signals, cameras, enforcement sensors, emergency call boxes, etc. Rajkot city is expected to have multiple environmental sensors across the city, to measure ambient conditions such as light intensity, temperature, water level (for chronic flood spots), air pollution, noise pollution and humidity.

b. Data Collection Layer (Controllers)

Controller processes data, that is input from the sensor applies the logic of control and causes an output action to be generated. This signal may be sent directly to the controlled device or to other logical control functions and ultimately to the controlled device.

The controllers function is to compare its input (from the sensor) with a set of instructions such as set point, throttling range and action, then produce an appropriate output signal. It usually consists of a control response along with other logical decisions that are unique to the specific control application. After taking the logical decision of the information it will hand over the information to the next layer (Network Layer) which will subsequently available at the ICCC.

c. Network Layer

The secured network layer will serve as the backbone for the project and provide connectivity to gather data from sensors and communicate messages to display devices and actuators. It will support the Wi-Fi services and other smart elements (sensors and displays) at given locations. The network layer will be scalable such that additional sensors, actuators, display devices can be seamlessly added and more Wi-Fi spots created in future. Provisioning of bandwidth will not be included in the scope of the Implementation Vendor; however, entire network backbone shall be provided by RSCDL.

d. Data Center Layer

The data center layer will house centralized computing power required to store, process and analyze the data to decipher actionable information. This layer includes servers, storage, ancillary network equipment elements, security devices and corresponding management tools. Similar to the network layer, it will be scalable to cater to the increasing computing and storage needs in future.

e. Smart Application and Integration Layer

The smart applications layer will contain data aggregation and management systems (rules engines, alerting systems, diagnostics systems, control systems, messaging system, events handling system), and reporting / dashboard system to provide actionable information to city administrators and citizens. It will be an evolving layer with applications added and integrated as and when new applications are developed at RSCDL. While aspects of ambient conditions within the city will be gathered through various sensors deployed, some city specific data will come from other government and non-government agencies. It is through the integration layer – that data will be exchanged to and from the under lying architecture components and other data from system developed by government (such as police department, meteorological department, street lights department, water department, irrigation department, transport organizations within Rajkot , etc.) and non-government agencies.

f. Service delivery and consumption Layer

The output field devices layer will contain display devices or bi-directional (input & output) devices connected to the network which will be used by citizens to consume - and for administrators to provide - actionable information. Such field devices include digital messaging boards, environmental data displays, etc.

g. Control Units & Command Centre Layer

The command center and control units will enable citizens and administrators alike to get a holistic view of city conditions. Such control units will take shape of either an exhaustive command center or control applications which can be viewed over a web browser or available in form of a mobile application. The implementation vendor will have to develop a command center at a site location determined by RSCDL and web/ mobile based viewing tools for understanding the ambient city conditions.

h. Security Layer

As ambient conditions, actuators and display devices are now connected through a network, security of the entire system becomes of paramount significance and the MSI will have to provide:

- Infrastructure security- including policies for identity and information security policies
- Network security- including policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources, etc.
- Identity and Access Management – including user authentication, authorization, SSL & Digital Signatures
- Application security- including Hosting of Government Websites and other Cloud based services, Adoption of Technical Standards for Interoperability Framework and other standards published by GoI for various eGovernance applications
- End device security, including physical security of all end devices such as display boards, emergency boxes, kiosks etc.

Following security parameters should be included for all smart elements, but not limited to:

- Identity and access management
- User/administrator audit log activity (logon, user creation, date-time of PA announcements, voice recording etc.)
- Secured data storage (storage of video/image/voice/location/data captured by various smart elements)
- SSL/TLS encryption for web and mobile application based interfaces for sensitive data transfer
- Protection against Denial of Service (DoS) and Interference attacks to public Wi-Fi Devices

3.4 Intelligent Traffic and Integrated Transport Management System (ITITMS) Architecture and Scope

The Intelligent Traffic and Integrated Transport Management solution caters to two different areas namely (i) Intelligent traffic management & (ii) Integrated Transport management solution. The MSI shall ensure the successful implementation of the proposed Intelligent Traffic Management System and provide capacity building support to city authorities as per the scope of services described below. Any functionality not expressly stated in this document but required to meet the needs of the RSCDL to ensure successful operations of the system shall essentially be under the scope of the MSI and for that no extra charges shall be admissible.

Intelligent Traffic Management system

1. Adaptive Traffic Control System (ATCS)
2. Public Address (PA)

The MSI's scope of work shall include but will not be limited to the following broad areas. Details of each of these broad areas have also been outlined in subsequent sections of this document:

1. Assessment and Site Survey: Conduct a detailed assessment, site survey and develop a comprehensive project plan, including:
   a. Assess the existing infrastructure of traffic junctions, traffic management systems, applications. etc. including traffic signalling systems and junction management
   b. Conduct the site surveys to finalize the location of traffic signal controller, number of traffic signal aspects, Camera distribution systems, locations and height of poles, cantilever, junction box, and cable routing etc.
   c. Finalization of detailed technical architecture, gap analysis and project plan
   d. Develop traffic management plans for individual signal controls and groups of signal controllers along with pre-planned intervention strategies for special scenarios
   e. Obtain site Clearance obligations & other relevant permissions

2. Design, Supply, Installation and Commissioning of Field Equipment which includes the following components:
   a. Adaptive Traffic Control System (ATCS)
   b. Public Address (PA)

3. Requirement analysis and design of Network Connectivity for Intelligent Traffic Management.
    a. MSI is required to carry out detailed network requirement analysis and design for supporting ITMS solution and live data streaming to Data Centre, ICC or any other envisaged command centres.
    b. Based on the network requirements shared by bidder, RMC EDP Team will arrange necessary connectivity. All the connectivity requirements including customer premise equipment (CPE) will be responsibility of RMC EDP team/ RSCDL.
    c. Integration and migration onto the city fibre network backbone envisaged as future Smart Solution Projects under Rajkot Smart City initiatives.

4. Hosting of Hardware and Software Infrastructure which includes design, supply, and installation and commissioning of IT Infrastructure for the solution at Data Centre, Interim ICCC and ICCC. This consist of:
    a. IT Infrastructure including server, storage, other required hardware, application portfolio, licenses
    b. Interim ICCC/ICCC infrastructure including video walls, operator workstations, IP phones, joystick controller etc.
    c. Establishment of LAN and WAN connectivity at Interim ICCC/ICCC and DC limited to scope of infrastructure procured for the project
5. Capacity Building for Rajkot Police, RSCDL and RMC which includes preparation of operational manuals, training documents and capacity building support, including:
    a. Training of the city authorities, Rajkot Police personnel and Interim ICCC/ICCC operators on operationalization of the system
    b. Support during execution of acceptance testing
    c. Preparation and implementation of the information security policy, including policies on backup and redundancy plan
    d. Preparation of revised traffic signal control plans, alternate signal control plans, KPIs for performance monitoring of transport network, dashboards for MIS
    e. Developing standard operating procedures for operations management and other technical services to be rendered by Interim ICCC/ICCC
    f. Preparation of system documents, user manuals, performance manuals, etc.

6. Operations and Maintenance services for the software, hardware and other IT and Non-IT infrastructure installed will start after the final Go-Live of the solution. The O&M will be for a tenure of 5 years post Go-Live.

3.4.1 Geographical Scope of services

The following is a summary of the geographical extent of the project.

No.	System Description	Locations
1.	Adaptive Traffic Control System (ATCS)	30 Locations
2.	Public Address (PA) System	82 Locations
3.	ICCC	1 Location (proposed location is approximately 1800 Square Feet. at Multi activity center on 150 Feet Ring Road)

The Indicative list of locations to be covered under this project are provided as **Annexure VIII.**

3.4.2 Assessment and Site Survey for finalization of detailed technical architecture and project plan

After signing of contract, the Systems Integrator needs to deploy local team (based out of Rajkot) proposed for the project and ensure that a Project Inception Report is submitted to RSCDL which should cover following aspects:

1. Names of the Project Team members, their roles and responsibilities
2. Approach and methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project).
3. Responsibility matrix for all stakeholders
4. Risks the MSI anticipates and the plans they have towards their mitigation
5. Detailed project plan specifying dependencies between various project activities / sub-activities and their timelines
6. Installation locations geo mapped preferably on google earth to visually identify the geographical area

The MSI shall conduct a comprehensive As-Is study of the existing infrastructure of traffic junctions/intersections (identified for Intelligent Traffic Management) during various time periods of day including peak and non-peak hours to establish the key performance indicators(KPI) for the project. The KPIs of the study shall be included in the survey. The following minimum parameters should be captured during the comprehensive study

1. Volumes of vehicles moving in the road network within the area identified for implementation
2. Vehicle type distribution
3. Directional distribution
4. Physical and visual characteristics of the area
5. Travel times, delays between different points of the network
6. Additional dependencies with respect to the available infrastructure and geometry at the junctions
7. Any other relevant data which the MSI anticipates will assist in establishing the benchmarks for the project

The report shall also include the expected measurable improvements against each KPI as detailed out in the above 'As-Is' study after implementation of Intelligent Traffic Management project. The benchmarking data should also be developed to track current situation and desired state.

The MSI shall study the existing business processes, functionalities, existing traffic management systems and applications including MIS reporting requirements.

The MSI will be responsible to propose transition strategy for dismantling of existing signal , and setting up of new signals and field components. The proposed strategy should clearly provide approach and plan for implementing the new signals and field components while ensuring minimum disturbance to the road traffic and shall use appropriate static signage designating the work in progress status.

Additionally, the MSI should provide a detailed To-Be designs (Junction layout plans) specifying the following:

1. High Level Design (including but not limited to) Application architecture, Logical and physical database design, Data dictionary and data definitions, ER diagrams and other data modelling documents and Physical infrastructure design for devices on the field
2. Application component design including component deployment views, control flows, etc.
3. Low Level Design (including but not limited to) Application flows and logic including pseudo code, GUI design (screen design, navigation, etc.), Database architecture, including defining data structure, data dictionary as per standards laid-down by Government of India/ Government of Gujarat.
4. Location of all field systems and components proposed at the junctions, (KML /KMZ file plotted on GIS platform like google earth etc.)
5. Height and foundation of Cameras, Traffic Signals and Standard Poles for Pedestrian signals, Height and foundation of Poles, cantilevers, gantry and other mounting structures for other field devices
6. Location of Junction Box
7. Location of Network Provider's Point of Presence (PoP)
8. Electrical power provisioning

The MSI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the project. The report should take into consideration following guiding principles:

1. Scalability - Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the Rajkot city. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system imposed restrictions on the upward scalability in number of field devices. Main technological components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure), software / application performance. In quantitative terms, there may not be major change in number of Command Centres. However, command centre should have to be shifted from Interim ICCC to ICCC, once ICCC gets operational.

2. Availability - Components of the architecture must provide redundancy and ensure that are no single point of failures in the key project components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system.

3. Security - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion detection systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worms attacks should be well defended with gateway level Anti-virus system, along with workstation level anti-virus mechanism. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. RSCDL may carry out the Security Audit of the entire system post acceptance / operationalization through a Third Party Auditor (TPA) if required. The following guidelines need to be observed for security:
    a. Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
    b. Access controls must be provided to ensure that the system is not tampered or modified by the system operators.
    c. Implement data security to allow for changes in technology and business needs.

d. The security of the field devices must be ensured with system architecture designed in a way to secure the field devices in terms of physical damage & unauthorized access.

4. Manageability - Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the scalability of the system

5. Interoperability - The system should have capability to take inputs from other third party systems as per situational requirements

6. Open Standards - System should use open standards and protocols to the extent possible without compromising on the security

7. Convergence - RSCDL has already initiated many projects which have state of the art infrastructure at field locations deployed under them. The Intelligent Traffic Management Infrastructure should be made scalable for future convergence needs. Under the smart city program, RSCDL has envisaged to create a state of the art infrastructure and services for the citizens of Rajkot, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence the MSI is required to ensure that such infrastructure will allow for accommodation of equipment's being procured under other smart city projects. Equipment like Junction Boxes and poles deployed under the Intelligent Traffic Management project at the field locations will be utilized to accommodate field equipment's created under the other projects of RSCDL and vice versa. The procedure for utilization of the infrastructure will be mutually agreed between the RSCDL and MSI.

Sub-contracting / Outsourcing shall be allowed only for the work which is allowed as mentioned in the clause with prior written approval of RSCDL. However, even if the work is sub-contracted / outsourced, the sole responsibility of the work shall lie with the MSI. The MSI shall be held responsible for any delay/error/non-compliance etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to RSCDL. Sub-contracting / outsourcing would be allowed only for work such as:

1. Passive Networking & Civil Work during implementation,
2. FMS staff for non- IT support during post-implementation
3. Services of professional architect for design of Interim ICCC/ICCC

3.4.3 Site Clearance obligations & other relevant permissions

3.4.3.1 Survey and Commencement of Works

Prior to starting the site clearance, the MSI shall carry out survey of field locations as specified in Annexure VIII, for buildings, structures, fences, trees, existing installations, etc. The RSCDL shall be fully informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the RSCDL.

3.4.3.2 Existing Traffic Signal system

The infrastructure of existing traffic signal systems including the aspects, controllers etc. will be dismantled and replaced with the new systems which are proposed and required under the scope of the ITMS project. The dismantled infrastructure shall be delivered at the RSCDL designated location without damage at no extra cost.

3.4.3.3 Road signs

All existing road signs which are likely to be effected by the works are to be carefully taken down and stored. Signs to be re-commissioned shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with RSCDL guidelines. Road signs, street name plate, etc. damaged by the MSI during their operation shall be repaired or replaced by MSI at no additional cost.

3.4.3.4 Electrical works and power supply

The MSI shall directly interact with RSCDL for provision of mains power supply at all desired locations for Intelligent Traffic Management system. MSI is expected to clearly define the power availability and requirements as part of AS-IS report and same will be taken care by RSCDL.

3.4.3.5 Lightning-proof measures

The MSI shall comply with lightning-protection and anti –interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying. The MSI shall describe the planned lightning-protection and anti –interference measures in the As-Is report. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof function & should capable to bear certain mechanical external force. Signal separation of low and high frequency; equipment's protective field shall be connected with its own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the earthling. The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security system, server data path and other communication equipment. Data line protection shall be installed as per zone defined in IEC 62305.Type 1 device shall be installed between zone 0B and zone 1. Type 2 devices shall be installed before the equipment in zone 2 and 3.

3.4.3.6 Earthing System

All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. The entire applicable IT infrastructure i.e. signal junction or command center shall have adequate earthing. Further, earthling should be done as per Local state national standard in relevance with IS standard.

1. Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units, etc. so as to avoid a ground differential. RSCDL shall provide the necessary space required to prepare the earthing pits.
2. All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
3. There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
4. The earth connections shall be properly made.

5. A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit needs to be in place for this copper mesh.
6. Provide separate Earthing pits for Servers, & UPS as per the standards.

3.4.3.7 Junction Box, Poles and Cantilever

1. The MSI shall provide the Junction Boxes, poles and cantilever to mount the field sensors like the traffic sensors, traffic light aspects, active network components, controller and UPS at all field locations, as per the specifications given in the RFP.
2. The Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions, and the MSI should design the Junction box for 1.5 times the actual size the MSI requires for utilization under the Intelligent Traffic Management project.
3. The Additional 50% space in the Junction Box shall be utilized by RSCDL to accommodate any future requirements under other projects
4. The Junction Box for UPS with Battery bank needs to be considered separately
5. It should be noted that the MSI would have designed the Junction box keeping in mind the scalability requirements of Intelligent Traffic Management project, and the additional 50%volume needs to considered over and above such requirement
6. The junction box should be designed in a way that, separate compartment will be available for separate system (i.e. Controller, Mini server, Active component, etc.). Each compartment shall have lock & key facility. There should be provision made to integrate the systems if required.

3.4.3.8 Cabling Infrastructure

1. The MSI shall provide standardized cabling for all devices and subsystems in the field, Viewing Centers and Interim ICCC/ICCC.
2. MSI shall ensure the installation of all necessary cables and connectors between the field sensors /devices assembly, outstation junction box, for pole mounted field sensors /devices the cables shall be routed down the inside of the pole and through underground duct to the outstation cabinet.
3. All cables shall be clearly labelled with indelible indications that can clearly be identified by maintenance personnel. The proposed cables shall meet the valid directives and standards.
4. Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by the MSI.

3.4.4 Design, Supply, Installation & Commissioning of the Field Equipment for Intelligent Traffic Management

The Scope includes Supply, Installation, commissioning and Customization (as required) of various field systems which include Adaptive Traffic Control System (ATCS) at Traffic Junctions, PA System, Intelligent Pedestrian Crossing system, and other IT infrastructure required for successful operation of the Intelligent management system modules.

Based on the approved Survey report, the MSI will undertake the system configuration and customization in line with the changed, improved or specific requirements of Rajkot Police and RSCDL including:

1. The implementation methodology and approach must be based on the global best practices in-order to meet the defined Service Levels during the operation.
2. Best efforts have been made to define major functionalities for each sub- system of Intelligent Traffic management solution. However, MSI should not limit its offerings to the functionalities proposed in this RFP and is suggested to propose any functionality over and above what has already been given in this tender.
3. The MSI shall design the field level equipment architecture to ensure maximum optimization of network equipment, poles, cantilever, mounting infrastructures, power supply equipment including, electric meters and junction box.
4. Finally approved/accepted solution for each component of Intelligent Traffic Management solution shall be accompanied with “System Configuration” document and the same should be referenced for installation of the solution at Junctions that are identified within the scope of this project.
5. The MSI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.
6. The MSI shall be responsible for obtaining all permits and approvals necessary to install the Intelligent Traffic Management components as per the approved design.

The sub-components included as part of the project for which field equipment needs to be deployed and integrated are given in the subsequent sections.

3.4.4.1 Adaptive Traffic Control System (ATCS)

The broad scope of work to be covered under ATCS sub module will include the following, but is not limited to:

1. Preparation of Solution Architecture as per project blueprint to develop a final BOQ for installation traffic signalling systems.
2. Installation of controllers, Traffic light aspects, poles, cantilevers, Junction Box and other required accessories at 45 traffic junctions for successful operation of the ATCS for RSCDL and Rajkot Traffic Police
3. Integration of ATCS field infrastructures with the proposed ATCS software application
4. Configuration of traffic signal at each of the junction along with development of signal control plan for individual operations, coordinated signal plan for the junction in sync with the area wide signal plan for different operating conditions. The operating conditions may include different peak and off-peak conditions, special events, contingency plans etc.
5. The MSI may design and propose energy saving signalling system by using solar powered signals or other advanced technologies.
6. For more details on technical and functional specifications of ATCS, MSI should refer to Annexure I for Functional and Technical specifications.

3.4.4.2 Public Address (PA) System

The broad scope of work to be covered under this sub module will include the following, but is not limited to:

1. The MSI shall install IP based Public Address System as part of the information dissemination system at 82 locations in the city. These systems shall be deployed at identified junction to make public interest announcements. The system deployed shall be IP based and have the capability to be managed and controlled from the Interim ICCC/ICCC
2. The MSI, in consultation with Traffic Police can propose alternate locations apart from the locations mentioned in this RFP for installing the PA system where their effectiveness in communicating information about traffic conditions in Rajkot will be maximized.
3. Rajkot Traffic Police shall review and approve the proposed locations. The MSI shall install the PA system on the approved locations.
4. For more details on technical and functional specifications of IP based PA system, the MSI should refer to Annexure I for functional requirements and technical specifications.

3.5 Integrated Transport Management System Architecture and Scope

As part of the Integrated Transport Management System project RMC intends to install LED based PIS at all BRTS bus stands to inform users about the location of the buses. Additionally at each BRTS bus stop RMC intends to implement turnstile and validator to restrict passage to people who pay through "Rajkot Mitra Card" or QR code based ticket. Furthermore to boost the image of public transportation system RMC intends to roll out smart bus stops.

The essential components of the Integrated Transport management system are:

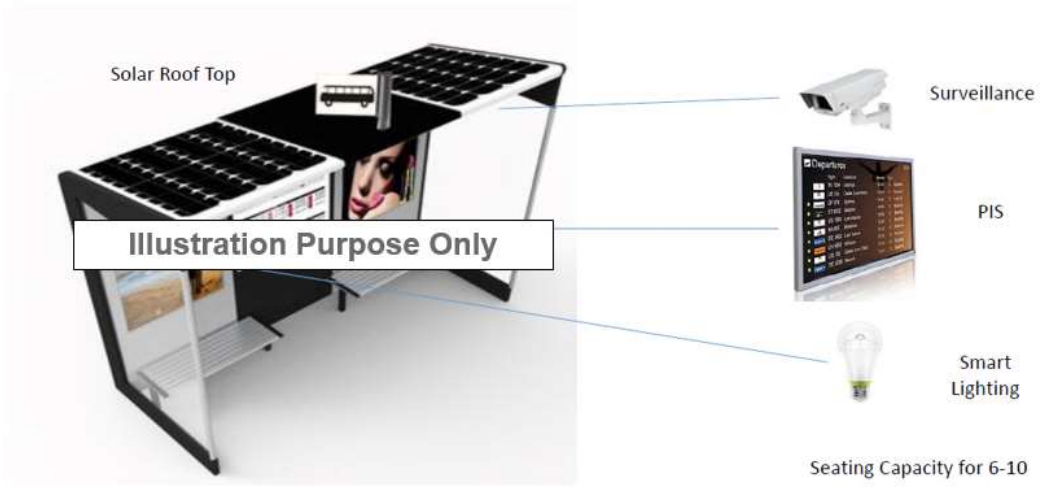
1. LED based Passenger Information System at BRTS

The passenger information system is an important component of integrated ITS system and renders an important consumer facing services. Accurate and timely PIS delivery facilitates consumer trust on public transport service and also aids modal shift in long term, as the reliability and availability becomes evident to the users.

As part of the project bidder is required to install PIS system at BRTS bus stop. The other hardware and software to display ETA etc., will be procured by RMC from existing vendor.

2. Smart Bus stops

Smart bus stop will essentially comprise of four major components (i) Surveillance (iii) PIS and (iii) smart lighting (iv) Solar Roof Top (depending on feasibility). The idea behind smart bus stop is to make bus stops more passenger friendly and safe.



Bus Prototype

3. Automatic Fare collection system

a) The functional specifications section provides specification for major components for AFCS:
   - Automatic Fare Collection System
   - Handheld Fare Collection Devices

The core objective of implementing AFCS is to create an integrated fare collection mechanism using interoperable standards, hence the devices and media thereby has to be complementary in nature. The end state requirement of this implementation shall be that of integrated fare management and collection regime which will render its services to all types of transit system operated within the city in a unified manner.

In-order to meet diverse need of commuter and application, following media types shall be offered to users for payment of fare purposes:

- Contactless Smartcards
- QR code based Paper Tickets Mobile application based ticketing using QR code

These AFCS fare media shall be made available to user at several locations such as BRTSs setup within the city, designated branches, Web application, Mobile application, etc.).

AFC Devices: The station ticketing facility shall facilitate the commuter travel by providing an ecosystem for issuance and acceptance of fare media. The station ticketing facilities shall consist of the following:

Turnstile Type Automatic Gates with ticket validators: The Automatic Gates shall be equipped with acceptance infrastructure capable of reading and authenticating all types of fare media. The acceptance infrastructure shall interface with the gates for communicating the access controls.

Point of Sale: Bidder needs to integrate the turnstile/validator and AFCS with existing POS system of RMC. RMC existing POS system supports QR code based ticketing, same needs to be integrated to AFC devices.

Handheld Ticket Terminal (HTT): Hand held electronic ticketing terminals shall be deployed for checking/ validating the fare media with the commuters and shall be used by station AFC staff for issuing Barcode/QR code based paper tickets. This equipment is a portable hand-held device to facilitate the ticket checking capability as well.

Enhancement to existing Mobile App& Web portal for ticketing: RRL Mobile application and web portal shall be enhanced to enable users to generate secure Barcode/QR based tickets for use on ticket validation devices.

Central system of AFCS: The Central system shall consist of the AFC transaction & Configuration Application integrated with a smart card host system provided by Bank. The system shall be used to set configuration parameters (such as tariff tables etc.) that would be required to operate the system.

Central Back office system/AFC Software is the heart of entire AFC ecosystem consisting of the core components for daily operations of AFC system. The system shall be used to set configuration

parameters (such as tariff, device configuration, product configuration, user configuration etc.) that would be required to operate the system. The system would host all the information required for processing the fare media within the transit ecosystem. It shall function as a Management Information System (MIS).

Solution should include Paper based ticketing, Smartcard based ticketing, Passenger Pass management. AFCS system shall dynamically control Concession/Discount Management vs. Passenger category, Special services, Pre-planned change/configuration at fare update etc, Ticket Stock Management, Dynamic configuration of Shift times etc, HHT allocation, Pass issuing management, etc.

Solution Components

- Hardware Components
  - Turnstile
  - Gate mounted ticket validators with inbuilt barcode/QR code scanner, Contactless reader
  - Handheld Ticketing Terminal
- Fare Media
  - Paper based Barcode/QR Code Ticket
  - Contactless Smartcard
  - Mobile based ticketing

The MSI's scope of work shall include but will not be limited to the following broad areas. Details of each of these broad areas have also been outlined in subsequent sections of this document:

1. Assessment and Site Survey: Conduct a detailed assessment of existing IT systems and Infrastructure of RRL and develop a comprehensive project plan, including:
   a. Assess the existing IT systems used by RRL for BRTS, RMTS buses, site survey of BRTS & RMTS bus shelters/stops
   b. Site Survey for smart bus stops including finalization of location, feasibility of solar roof top, Civil and ICT design of smart bus stop
   c. Finalization of detailed technical architecture, gap analysis and project plan
   d. Obtain site Clearance obligations & other relevant permissions

2. Design, Supply, Installation and Commissioning of Field Equipment which includes the following components:
   a. LED Passenger information system and at BRTS bus stops
   b. Smart Bus stop – Modern bus stops/shelter with LED PIS, Surveillance , Charging points, smart lighting, Solar/Glass roof-tops at bus shelter/stops
   c. Automatic fare collection system (AFCS)

3. Requirement analysis and design of Network Connectivity for Integrated Transport Management.
   a. Design , supply, installation and commissioning of PIS to ICCC connectivity (to be worked out in conjunction with existing vendor)
   a. MSI is required to carry out detailed network requirement analysis and design for supporting Smart Bus stop solution, AFCS solution at BRT bus stops and live data streaming to Data Centre, and ICC. All the connectivity requirements including customer premise equipment (CPE) will be responsibility of RMC EDP team/ RSCDL.
   b. Integration and migration onto the city fiber network backbone envisaged as future Smart Solution Projects under Rajkot Smart City initiatives.
4. Hosting of Hardware and Software Infrastructure which includes design, supply, and installation and commissioning of IT Infrastructure for the solution at Data Centre, Interim ICCC and ICCC. This consist of:
   a. IT Infrastructure including server, storage, other required hardware, application portfolio, licenses
   b. Interim ICCC/ICCC infrastructure including video walls, operator workstations, IP phones, joystick controller etc.
   c. Viewing Centre infrastructure including LED displays, operator workstations, IP phones etc.
   d. Establishment of LAN and WAN connectivity Interim ICCC/ICCC and DC limited to scope of infrastructure procured for the project

5. Capacity Building for RSCDL, RRL and RMC which includes preparation of operational manuals, training documents and capacity building support, including:
   a. Training of the city authorities, Rajkot Rajpath Limited personnel and Interim ICCC/ICCC operators on operationalization of the system
   b. Support during execution of acceptance testing
   c. Preparation and implementation of the information security policy, including policies on backup and redundancy plan
   d. Developing standard operating procedures for operations management and other technical services to be rendered by Interim ICCC/ICCC
   e. Preparation of system documents, user manuals, performance manuals, etc.

6. Operations and Maintenance services for the software, hardware and other IT and Non-IT infrastructure installed will start after the final Go-Live of the solution. The O&M will be for a tenure of 5 years post Go-Live.

3.5.1 Geographical Scope of services

The following is a summary of the geographical extent of the project.

No.	Items	Location
1	Handheld Electronic Ticketing System	120
2	Turnstile + Validator	100
3	Smart bus stops • Surveillance • LED PIS • Smart Lighting • Solar Roof Top	40
4	LED PIS at BRTS	36

Software Requirements	
1	AFCS
2	Web Portal & Mobile application enhancements

3.5.2 Assessment and Site Survey for finalization of detailed technical architecture and project plan

After signing of contract, the Systems Integrator needs to deploy local team (based out of Rajkot) proposed for the project and ensure that a Project Inception Report is submitted to RSCDL which should cover following aspects:

1. Names of the Project Team members, their roles and responsibilities
2. Approach and methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project).
3. Responsibility matrix for all stakeholders
4. Risks the MSI anticipates and the plans they have towards their mitigation
5. Detailed project plan specifying dependencies between various project activities / sub-activities and their timelines
6. Installation locations geo mapped preferably on google earth to visually identify the geographical area

The MSI shall conduct a comprehensive As-Is study of the existing Transport network of Rajkot which includes understanding current operating model, existing infrastructure of both RMTS and BRTS buses and bus stops. The output of the As-Is study should be identification of the key performance indicators (KPI) for the project. The KPIs of the study shall be included in the survey. The following minimum parameters should be captured during the comprehensive study

1. Current ridership of BRTS & RMTS
2. Peak hour identification
3. Coverage of current transportation network
4. Physical and visual characteristics of the bus stops and buses
5. Travel times, delays between different points of the transportation network
6. Additional dependencies with respect to the available infrastructure and geometry at the junctions
7. Feasibility study of solar roof top at bus stops
8. Any other relevant data which the MSI anticipates will assist in establishing the benchmarks for the project

The report shall also include the expected measurable improvements against each KPI as detailed out in the above 'As-Is' study after implementation of Integrated Transport Management project. The benchmarking data should also be developed to track current situation and desired state.

The MSI shall study the existing business processes, functionalities, existing transport management systems and applications including MIS reporting requirements.

The MSI will be responsible to propose transition strategy for dismantling of existing bus stops, and setting up of new smart bus stops with field components. The proposed strategy should clearly provide approach and plan for implementing the new bus stop while ensuring minimum disturbance to the road traffic and shall use appropriate static signage designating the work in progress status.

Additionally, the MSI should provide a detailed To-Be designs for integrated transport management specifying the following:

1. High Level Design (including but not limited to) Application architecture, Logical and physical database design, Data dictionary and data definitions, ER diagrams and other data modelling documents and Physical infrastructure design for devices on the field
2. Application component design including component deployment views, control flows, etc.
3. Low Level Design (including but not limited to) Application flows and logic including pseudo code, GUI design (screen design, navigation, etc.), Database architecture, including defining data structure, data dictionary as per standards laid-down by Government of India/ Government of Gujarat.
4. Location of all field systems and components proposed at the bus stops and in Bus, (KML /KMZ file plotted on GIS platform like google earth etc.)
5. Height and foundation of Cameras, PIS, turnstile etc. at bus stops or any other field equipment.
6. Location of Smart Bus stops
7. Location of Network Provider's Point of Presence (PoP)
8. Electrical power provisioning

The MSI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the project. The report should take into consideration following guiding principles:

1. Scalability - Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the Rajkot city. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system imposed restrictions on the upward scalability in number of field devices. Main technological components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure), and software / application performance. In quantitative

terms, there may not be major change in number of Command Centers. However, command center should have to be shifted from Interim ICCC to ICCC, once ICCC gets operational.

2. Availability - Components of the architecture must provide redundancy and ensure that are no single point of failures in the key project components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system.

3. Security - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion detection systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worms attacks should be well defended with gateway level Anti-virus system, along with workstation level anti-virus mechanism. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. RSCDL may carry out the Security Audit of the entire system post acceptance / operationalization through a Third Party Auditor (TPA) if required. The following guidelines need to be observed for security:

    a. Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
    b. Access controls must be provided to ensure that the system is not tampered or modified by the system operators.
    c. Implement data security to allow for changes in technology and business needs.
    d. The security of the field devices must be ensured with system architecture designed in a way to secure the field devices in terms of physical damage & unauthorized access.

4. Manageability - Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the scalability of the system

5. Interoperability - The system should have capability to take inputs from other third party systems as per situational requirements

6. Open Standards - System should use open standards and protocols to the extent possible without compromising on the security

7. Convergence - RSCDL has already initiated many projects which have state of the art infrastructure at field locations deployed under them. The Integrated Transport Management Infrastructure should be made scalable for future convergence needs. Under the smart city program, RSCDL has envisaged to create a state of the art infrastructure and services for the citizens of Rajkot, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence the MSI is required to ensure that such infrastructure will allow for accommodation of equipment's being procured under other smart city projects. The procedure for utilization of the infrastructure will be mutually agreed between the RSCDL and MSI.

Sub-contracting / Outsourcing shall be allowed only for the work which is allowed as mentioned in the clause with prior written approval of RSCDL. However, even if the work is sub-contracted / outsourced, the sole responsibility of the work shall lie with the MSI. The MSI shall be held responsible for any delay/error/non-compliance etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to RSCDL. Sub-contracting / outsourcing would be allowed only for work such as:

1. Passive Networking & Civil Work during implementation,
2. FMS staff for non- IT support during post-implementation
3. Services of professional architect for design of Interim ICCC/ICCC

3.5.3 Site Clearance obligations & other relevant permissions

3.5.3.1 Survey and Commencement of Works

Prior to starting the site clearance, the MSI shall carry out survey of field locations as specified in Annexure VIII, for buildings, structures, fences, trees, existing installations, etc. The RSCDL shall be fully informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the RSCDL.

3.5.3.2 Existing Bus stops

The infrastructure of existing bus stops will be dismantled and replaced with the new systems which are proposed and required under the scope of the ITMS project. The dismantling of existing bus stop will be taken care by RSCDL. No extra cost should be considered for dismantling and transportation of dismantled bus stops.

3.5.3.3 Electrical works and power supply

The MSI shall directly interact with RSCDL for provision of mains power supply at all desired locations for Integrated Transport Management system. MSI is expected to clearly define the power availability and requirements as part of AS-IS report and same will be taken care by RSCDL.

3.5.3.4 Lightning-proof measures

The MSI shall comply with lightning-protection and anti –interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying. The MSI shall describe the planned lightning-protection and anti –interference measures in the As-Is report. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof function & should capable to bear certain mechanical external force. Signal separation of low and high frequency; equipment's protective field shall be connected with its own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the earthling. The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security system, server data path and other communication equipment. Data line protection shall be installed as per zone defined in IEC 62305.Type 1 device shall be installed between zone 0B and zone 1. Type 2 devices shall be installed before the equipment in zone 2 and 3.

3.5.3.5 Earthing System

All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. The entire applicable IT infrastructure i.e signal junction or command

centre shall have adequate earthing. Further, earthling should be done as per Local state national standard in relevance with IS standard.

1. Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units, etc. so as to avoid a ground differential. RSCDL shall provide the necessary space required to prepare the earthing pits.
2. All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
3. There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
4. The earth connections shall be properly made.
5. A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit needs to be in place for this copper mesh.
6. Provide separate Earthing pits for Servers, & UPS as per the standards.

3.5.3.6 Cabling Infrastructure

1. The MSI shall provide standardized cabling for all devices and subsystems in the field, Viewing Centers and Interim ICCC/ICCC.
2. MSI shall ensure the installation of all necessary cables and connectors between the field devices.
3. All cables shall be clearly labelled with indelible indications that can clearly be identified by maintenance personnel. The proposed cables shall meet the valid directives and standards.
4. Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by the MSI.

3.5.4 Design, Supply, Installation & Commissioning of the Integrated Transport Management solution

The Scope includes Supply, Installation, commissioning of PIS, AFCS, and smart bus stops and other IT infrastructure required for successful operation of the Integrated Transport modules.

Based on the approved Survey report, the MSI will undertake the system configuration and customization in line with the changed, improved or specific requirements of RRL and RSCDL including:

1. The implementation methodology and approach must be based on the global best practices in-order to give public transportation in Rajkot the required facelift.
2. Best efforts have been made to define major functionalities for each sub- system of PIS, AFCS and Smart Bus stops. However, MSI should not limit its offerings to the functionalities proposed in this RFP and is suggested to propose any functionality over and above what has already been given in this tender.
3. The MSI shall design the field level equipment architecture to ensure maximum improvement in operational efficiency of RRL/Transportation system in city of Rajkot.
4. Finally approved/accepted solution for each component of Integrated Transport Management System shall be accompanied with "System Configuration" document and the same should be referenced for installation of the solution at bus stops that are identified within the scope of this project.
5. The MSI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

The MSI shall be responsible for obtaining all permits and approvals necessary to install the Integrated Transport Management System components as per the approved design.

3.6 Integrated Command and Control Centre

The Bidder has to integrate all the smart components at centralized command and control center with an integrated operations and dashboard application that will integrate various Smart City components implemented in this project and in future.

The Integrated command and control center can monitor and control, via the centralized application, the smart components like Intelligent Traffic and Transport solutions, Smart LED, Smart Surveillance, and Access Points for the public Wi-Fi, Smart Billboards and Environmental Sensors etc.

3.6.1 Design of Last Mile Connectivity for ITITMS

1. Last Mile Connectivity is an important components of the project and needs very careful attention in assessment, planning and implementation. It is important not only to ensure that the required connectivity is provisioned within the required timelines but also ensure that it is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance.

2. MSI is not required to procure bandwidth, procurement of Bandwidth is responsibility of RSCDL, however MSI is expected to design and provide last mile connectivity requirement to RSCDL.

3. It is also envisaged that the ITITMS project shall leverage the City Network Backbone infrastructure that will be implemented as one of the smart solution projects under smart city initiatives in future.

4. It will be the responsibility of the MSI to migrate the ITITMS systems onto the City Network backbone once implemented.

5. The provisioning of the connectivity at the Junction and other field locations will be mutually agreed upon by the RSCDL and the MSI for the ITITMS project.

6. The MSI should provide a detailed network architecture of the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real time data streams to the Data Centre. All the components of the technical network architecture should be of industry best standard and assist MSI in ensuring that all the connectivity SLAs are adhered to during the operational phase.

7. The MSI is also responsible for the design and implementation of integration between DC and ICCC

8. The MSI shall review and validate the network architecture provided by RSCDL/service provider.

9. MSIs are also required to do the estimation of bandwidth requirements considering following benchmark parameters:

No.	ITITMS Components	Consideration
1	ATCS	Minimum 1 MB per controller
2	PA System	Minimum 1 MB for each location
3	Smart Bus stops	Minimum 5 MB for each location

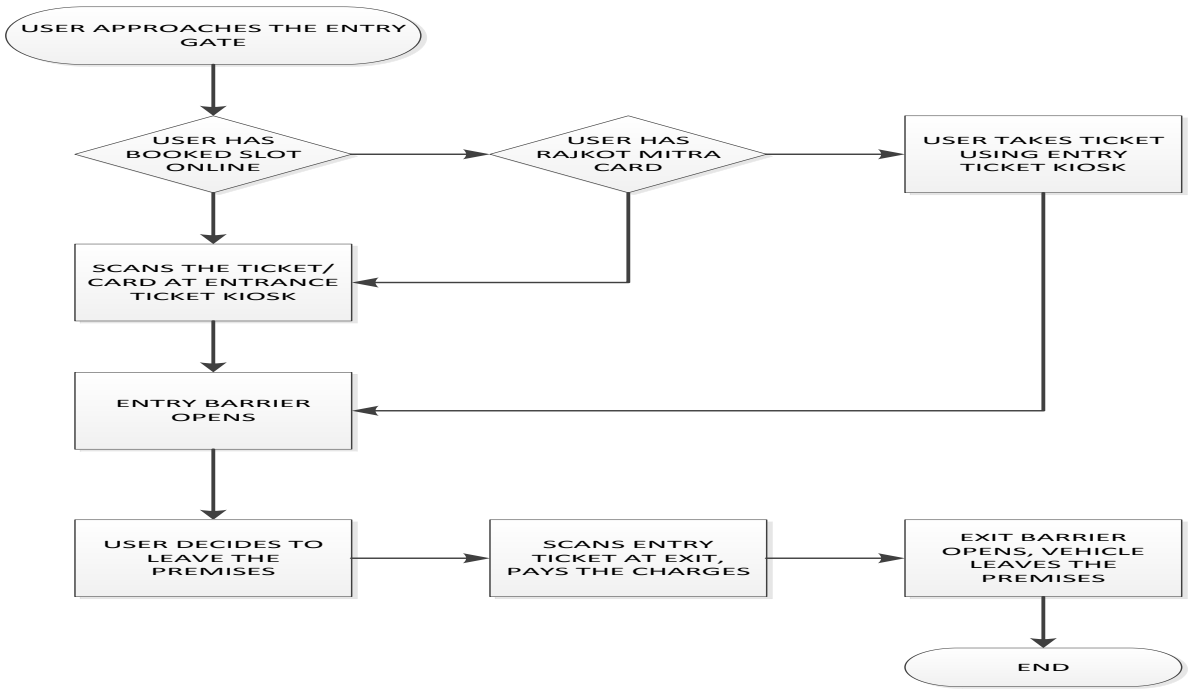
10. The actual bandwidth requirement to cater the above mentioned bandwidth parameters and to meet SLAs would be calculated by the MSI and the same shall be clearly proposed in the technical proposal with detail calculations. RSCDL also requires the MSI to meet the parameters of video feed quality, security & performance and thus MSIs should factor the same while designing the solution. RSCDL reserves its right to ask the Systems Integrator to increase the bandwidth if the provided bandwidth is not sufficient to give the functionality of the system mentioned in the RFP and adhere to the SLAs.

11. The MSI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

12. The MSI shall be required to submit a detailed migration report post switching of all the field equipment to fibre network envisaged under another smart city project.

3.7 Smart Parking

Rajkot Municipal Corporation intends to implement smart parking solution in closed parking areas within the city. Below is the flow chart depicting end to end process during normal operation of SmartParking:



The major components of smart parking solution will include

1. A video analytics based solution to identify no of vehicle entering and exiting the parking area
2. Visibility of vacant parking spaces and Fare Revision on digital signboard
   a. The total number of slots and free slots for parking must be displayed on a digital signboard near the entrance of the parking lots
   b. The smart parking solution should report occupancy of parking lots to a central software application deployed at the Integrated Command and Control Center.
   c. The smart parking solution should enable RMC to obtain real time situational awareness about the occupancy of parking lot through smart dashboard.
   d. The smart parking solution should enable citizens to obtain real time space availability and slot reservation capability via mobile app or web client.
   e. The smart parking solution should facilitate real time revision of parking fees and should enable real time communication of rules to parking kiosks and smart card readers.

3. Smart Parking Ticketing
   a. The smart parking solution needs to have parking ticket vending machine at the entrance where the ticket can be issued by the machine on pressing the button by the user/ operator.

b. The ticket, QR Code or any other technology used by the SI should be capable of capturing data that is easily retrievable at the exit.
c. Provision to support below use cases
    i. Walk-In Parking: This category of parking will include the citizens who drive in to the parking without any prior booking. The citizens can be provided with a QR coded ticket or any other advanced technology as deemed fit by the System Integrator.
    ii. Online Reservation of Parking spots: The citizens should be able to reserve parking spots through online web application or the Citizen Mobile app. The pre-booking would be retained for a specific period of time and reassigned in case of no show. The motorists booking parking slots under this category can be identified with a QR code based or any other advanced technology as deemed fit by the System Integrator
    iii. Smart Card based Parking: There should also be an option for users to be able to enter by flashing the smart card without any need to generate ticket.

4. Payment methods
    a. The payment collection can be done via card as well as cash (manually) at the kiosk where parking ticket can be scanned at the exit. On completion of payment the printed receipt should be provided to customer.
    b. The system must be tamperproof.
    c. End user should be able to pay using Rajkot Mitra Smart Card

5. Information of real time Parking space availability over Web client and Mobile App
    a. The smart parking solution should provide real time location based view to citizens about proximity of parking lots and availability of parking lots.
    b. The smart parking solution should have a mobile and a web delivery channel for citizens to get real time parking availability and pre book parking lots using online payment of parking charges facilitated through a payment gateway.
    c. A mobile application and web based user interface should be provided with the following features:
        i. The application should have citizen module and officer module.
        ii. The citizen should be able to see all the parking lots with exact available space in a real time mode.
        iii. While locating nearest parking lot, the most updated parking slot availability should be given to the user.
        iv. Through the citizen module, the user should be able to locate nearest parking lot and also pre -book based on his geographical coordinates. The same information must be made available on map with routing information.
        v. Citizens should be given an option to extend the pre-booked parking space

vi. There should be provision for some penalty levied in case of cancellation after the specified time period.
vii. The application should have a compliance officer module where Rajkot Municipal Corporation designated inspector / operator will be able to check compliance of slot occupancy against the fees paid by the citizen.
viii. The citizens should be able to generate MIS report to view their occupancy of parking lots over a defined time period.
ix. The administrators should be able to generate MIS report to view occupancy, collection and other usage statistics over a defined time period.

3.7.1 Geographical Scope of services

The smart parking solution will be implemented at 5 different locations

Below is the detail of the locations

S.No	Location
1	Open plot, HUDCO Quarter
2	Open plot , Dhebar Road
3	Madhav Parking , Open plot near Khotharia
4	Z blue , Open plot
5	Jubeli Market

3.8 Enterprise GIS

The GIS Project at RSCDL is proposed to provide a robust, reliable and futuristic Enterprise GIS platform, aimed to provide decision support system to RSCDL officials by integrating the GIS data and the other IT applications at RSCDL.

Various scope sub-activities that are imperative to achieve the proposed Enterprise GIS Solution, to be delivered by Successful Bidder/SI shall include:

- Design of Enterprise GIS Architecture, to meet the requirements specified in this RFP

- Supply and installation of the GIS Solution (Platform) for creation, storage & maintenance of GIS data
- Sizing and Supply & Installation of servers required for hosting the GIS Solution
- Creation/updating of the base map using the high resolution satellite imagery (made available by RSCDL)
- Conducting Underground utility Survey for Rajkot City
- Development of Mobile application for Property Survey for RSCDL
- Geo-tagging of already assessed as well unassessed properties for Rajkot Municipal Corporation
- Development of GIS application Suite and citizen portal.
- Testing, Training and Go-Live of the System
- Annual Technical Support for 5 years for the Enterprise GIS Solution implemented as part of this RFP
- Post Implementation Software Enhancements / Customizations and maintenance of GIS software platform and applications for 5 years

The indicative requirements to be delivered by the successful bidder/SI against various scope activities are given below:

3.8.1 Design of Enterprise GIS Architecture, to meet the requirements specified in this RFP

RSCDL needs a GIS platform to support enterprise wide GIS, development of web based GIS applications and desktop based GIS for smooth editing of GIS data. Following are the details of the approximate usage of the proposed GIS application:

Following are the estimates of the approximate usage of the proposed GIS application:

- Minimum No. of users on Intranet simultaneously viewing GIS data – 300
- Minimum No. of users on Intranet simultaneously editing GIS data – 25
- Minimum No. of users on Internet simultaneously viewing GIS data through RSCDL web portal – 500

Above indicative numbers of users is given to get a fair idea to the prospective bidders on overall usage of the Enterprise GIS System. Bidders are required to propose the system which can be scaled up to higher usage in future.

As a part of implementation services the selected bidder will have to setup an enterprise GIS environment for Rajkot Smart City Development Limited using the proposed GIS platform. This setup will have a centralized GIS database having all departmental GIS datasets within one Enterprise GIS database of RSCDL. All the departments will be accessing this centralized GIS database for editing and managing their own departmental layers using web based, desktop based and mobile based interface. The SI / Selected Bidder will have to provide support to all the department officials in using the enterprise setup. The SI/ selected bidder will also have to manage and support the centralized GIS setup. The GIS System and Database Administrators from the SI / selected bidder's side will have to manage and support the system.
Various features required in the GIS platform and Application Software are given in **Annexure-I(Compliance Matrix)**

3.8.2 Supply & Installation of the GIS Solution (Platform) for creation, storage & maintenance of GIS data

SI shall deliver the requisite Enterprise GIS Software licenses to RSCDL and carry out its installation for RSCDL.

3.8.3 Sizing and supply & Installation of servers required for hosting the GIS Solution

The bidders will have to do proper Sizing and undertake Supply, Installation & Maintenance of the Server for Database & Application Software for GIS.

The servers will be centrally located at data center being commissioned at RSCDL office. The bidder should include a list of the proposed hardware elements as part of their response to the Tender.

3.8.4 Creation / Updating of base map using High Resolution satellite Imagery:

To achieve effective output and benefits from the E-Governance implementation for all the services of the ULBs, large scale and detailed GIS base maps are required. The bidder is hence required to prepare Base map using latest high resolution satellite imagery.

The primary objective of GIS Solution is to prepare a detailed base map encompassing RSCDL boundaries with various layers like property, utility, assets, etc. and setup an enterprise wide GIS for RSCDL to support in better decision making and revenue generation.

Interpretation, Updating and digitization of all physical features such as Building(foot prints), Roads (Tar/cemented portion), and other visible features from satellite imagery. The satellite imagery would be procured in the name of RSCDL and delivered to the Bidder/SI. The digitization process shall include vector creation, Symbol creation, layering, edge matching, topological integrity, and data base linking and QA/QC.

Bidder/SI is expected to suggest inclusion of any important information other than that mentioned above, during the pre-bid meeting and subsequently during the project execution, for improving the overall Urban Management. All the data available with RSCDL, with respect to above proposed GIS layers, would be shared with the selected bidder/SI.
Following activities needs to be carried out for successful implementation of the GIS project at RSCDL:

Collection of Data

The Bidder/SI shall collect all the available data from RSCDL (soft copy and or hard copy) namely; municipal boundary, Zone boundary, wards boundary maps, slum related data. The Bidder/SI shall also incorporate data sets for locality, ward, zone and municipal boundaries. RSCDL at present has base map layers already developed in GIS based platforms. The details of the same are as below:

- Department – Housing department
- No. Of layers – >30 Layers
- Coverage - ~120 Sq. Km
- Base Layer Developed in – 2010-2011

Data validation

The Bidder/SI shall check the source and reliability of the collected data from RSCDL and document the details which can be taken into account and usage. Type of validation to be carried out on the available datasets from RSCDL with **t**he satellite imagery shall be:

- **Positional Accuracy:** The Bidder/SI shall check whether the positional accuracy of the existing data available with RSCDL is in sync with the Satellite Imagery provided by RSCDL. Selected Bidder/SI needs to digitize the satellite imagery fetched by RSCDL.

Further Bidder/SI would have to carry out Geo-referencing of the available data by using GCP and DGPS survey instruments as required for the process and also spatially adjust in case of vectors Data.
The Bidder/SI also needs to prepare Base Map using the available and fetched data and validation of the same will be carried out by the authorized officials of RSCDL.

- **Accuracy Requirement:** The 10% of GCPs will be randomly selected as sample for the accuracy. If any incorrectness in accuracy is found in any sample, the entire work of GCPs shall be rejected and bidder/SI shall be required to rework.

- **Reliability:** The Bidder/SI shall also check from the available data with RSCDL, whether the data (spatial or non-spatial) is recent or accurate enough to be used and not obsolete.

- **Data Validity:** The Bidder/SI shall make sure by taking a signoff from authorized officials of RSCDL on the authenticity of the data taken from any department of RSCDL.

Data Dictionary / Data Model:

The Data Model for storing the spatial & Non-Spatial shall be created by the SI/Bidder with the help of detailed round of discussion with each concerned RSCDL department officials. The bidder shall user proper tools to create the data model. The final data model shall be approved by the RSCDL

and before proceeding further the data model needs to be finalized. Once the data model is finalized, the Bidder/SI shall give the details of the data model diagram (ER Diagram) to RSCDL for future references or for any modifications in future. The data model shall be created in such a way that all the layers that are already available with RSCDL are considered while finalizing the data model. The data model may include the few layers that may not have any data. However provision of the same shall be kept in the enterprise GIS database.

The bidder shall take care of the changes in the Data Model as per the requirements from the RSCDL users and shall maintain the changes history for the entire period, the selected bidder is working with RSCDL under the contract. An indicative list of layers and its relevant attributes are added in the **Annexure I.**

Preparation of GIS Base Map

The selected bidder/SI is expected to provide technical and management support during the planning, design, development and implementation phases of GIS base maps preparation and other department layers mapping activities as described below but not limited to, for satisfactory performance of the services within the Project Duration.
The main objective of the project is to develop a detailed GIS Base map on a scale of 1:2000 for all the wards/zones of RSCDL. The details of features to be interpreted are given later in the document. The preliminary interpreted map should be ground verified and the final map is to be prepared by incorporating the ground truth data.

Satellite Imagery

RSCDL would supply cloud free high resolution multispectral imagery data sets (Ortho Ready) to the selected Bidder/SI.

Area coverage: At Present, spread of RSCDL with sufficient buffer is ~140 Sq. Km
Data Products: Digital copy images
Image type : High Resolution

On supply of satellite imagery by RSCDL, the Bidder/SI will verify the correctness of theimagery and data with truth data of field. The correctness of image is to be checked with respect to any issues in the coverage, and file format. The imagery that does not confirm to the correctness with respect to Coverage and file format must be reported within one week. RSCDL will discuss the same with the bidder and provide further instructions

Only the supplied imagery must be used for the preparation of Base Maps. Use of data from alternative online sources such as Google Earth / Google Maps is strictly prohibited as this is strictly against the usage policies of the respective services. The Bidder/SI will be solely liable for any legality and any such deviations will lead to disqualification of the Bidder/SI.

Post Processing of Satellite Imageries

To correct various geometric anomalies in raw satellite imagery, Ground Control Points (GCP) collected through Differential Global Positioning System (DGPS) survey will be used for Geo referencing of the imagery.

i. The Bidder/SI shall carry out Geo Referencing and Geo-coding of data on WGS-84 with projection on UTM.
ii. For the DGPS Survey, the Bidder/SI should select the Ground Control Points (GCPs) at well-defined sharp points both on the ground and on imagery. The Ground Control Points (GCPs) should be located at nearly desired locations and should be clearly visible on the imagery. Sketch, coordinate both in latitude, longitude and Easting, Northing of GCP's including GPS observation and adjustment data should be provided to RSCDL for necessary approval.
iii. The Bidder/SI shall make sure that while taking DGPS survey all positions fixes must use at least four satellites.
iv. The horizontal accuracy of the GCPs should be 0.3– 0.5 meters.
v. During static point-mode surveys, the minimum recording duration at each survey point shall be 60 seconds with at least 60 individual position fixed during that period.

vi. The Bidder/SI shall make sure that the pair of GCP's to be established is collected at minimum 2 km (depending upon the size and shape of the Municipal Corporation Boundary) and these should be evenly distributed over the RSCDL City area.

vii. The Bidder/SI shall also ortho-rectify the geo-referenced imageries by creating DEMs from contours or other sources of DEMs available.

viii. The Bidder/SI shall also do a mosaicking of the image tiles which are geo-referenced and ortho-rectified. The mosaics shall be verified once by the GIS representatives from RSCDL before proceeding for Base Map Creation/Updation.

Base Map Preparation and Digitization

Post the processing of the satellite imagery by removing the geometric anomalies (if any), the Bidder/SI shall prepare a Grid of 1Km x 1Km for positioning RSCDL with respect to its Geographic Location. These grids then further shall be divided into 250m x 250m scenes for future usage like Map Book creations, Smart Asset ID creation etc. and future analysis. All the grids and scenes shall have unique IDs.

The Bidder/SI shall then take sufficient number of Ground Control Points (GCPs) collected through Differential Global Positioning System (DGPS) survey. The Bidder/SI shall prepare an up-to-date large-scale base map (Scale 1:2000) of all the wards/zones of Rajkot City using satellite imageries. The Bidder/SI shall then prepare a new GIS Database as unified Geo-spatial Data with infrastructure details.

Using the heads on digitization technique, the satellite image is to be digitized to prepare a base map by digitizing all the features available in the satellite map like Buildings, Vacant Plots, Roads, Bridges, Railway Tracks, Parks, Gardens, Stadiums, Slums, Traffic Squares, Water Bodies (River, Lake, Pond, Drainage, Canal etc.), Over Head Tanks, etc. While doing the digitization, a special care of data correctness to be taken like no overshoots / undershoots, proper layering, proper symbology etc. The bidder has to ensure that the existing GIS layers that are already available with RSCDL are used while preparing the base map. These base layers will be provided by the concerned department of RSCDL as mentioned above.

The Bidder/SI shall also integrate information of Utilities features such as Street lighting, Water supply line, Sewerage network, Wastewater, Storm water drain, sanitation facilities (Household/public/private), Solid Waste management and unauthorized properties as and when provided by RSCDL as layers with base map.

Bidder has to undertake the Base Map Creation/Updation activity at RSCDL premises only (Room of 10 X15 Sq Feet), bidder has to bring all the required IT and Non- IT infrastructure for undertaking this activity. RSCDL will only provide raw power and empty room.

The digital map data should be GIS compatible. Each map object should be defined uniquely by its feature code and symbology (point, line, and polygon) and should be approved by RSCDL. Demonstration on digital map production line, producing digital base map using any of the digital mapping system should be made to the RSCDL.

Town Planning

The GIS application shall integrate all details of town planning schemes in terms of spatial data viz. Survey Map, Original Plot, Final Plot, etc. and non-spatial data like F-form, B-form, etc. The in depth details of each and every TP Schemes will be made available to the selected bidder by RSCDL. Apart from TP Schemes maps, DP maps and Revenue map shall be included. The ownership of the non T P Scheme map shall also be integrated. The details of the Mapped TP schemes and not to scale and non-mapped TP schemes are as below:

TP Scheme Details		
Sr. No	**Details**	**Count**
1	AutoCAD files available	24
2	Hard Copy and no digital	16

The selected bidder has to carry out a detailed total station survey for the TP schemes which has not been mapped / surveyed and available in digital format with RSCDL. The already surveyed TP schemes available with RSCDL shall be mapped on the base map prepared by selected bidder. The selected bidder shall hence overlay TP schemes and, Final plot, original plots, DP plans and other maps over the base map to have clear land information mapped. Bidder has to also undertake survey for all the non-TP area under RSCDL boundary (**130 Sq. km**).

At the stage of creation of FRS and SRS, the selected bidder shall have a detailed requirement gathering from the town planning department to detail out all the requirements to be developed in the GIS application for the town planning as well development & planning department.

Final Base Map

The bidder shall prepare a final base map incorporating the data collected, processed and digitized. Hard copy base maps are to be prepared at a scale desired by RSCDL which will be ward-wise. The base map will be prepared in various layers for ease of operation in GIS application. The details of the various layers (indicative not exhaustive) to be part of the final base map are given as below:

Sr. No	Layer Name	Vector Representation	Data Source	Availability with RSCDL
1.	Municipal Boundary	Polygon	RSCDL	Available (2010-2011)
2.	Area of Interest Boundary	Polygon	RSCDL	Not Available
3.	Ward Boundary	Polygon	RSCDL	Available (2010-2011)
4.	Zone Boundary	Polygon	RSCDL	Available (2010-2011)
5.	Election Ward	Polygon	RSCDL	Not Available
6.	Slum Boundary	Polygon	RSCDL	Available (2010-2011)
7.	Buildings foot prints	Polygon	RSCDL and Imagery	Available (2010-2011)

8.	Open Streams/Drainage/Canal	Line	Imagery	Not Available
9.	DGPS Points	Point	Field Survey	Not Available
10.	Bridges/Flyover	Line	Imagery	Not Available
11.	Parks/Gardens	Polygon	Imagery	Not Available
12.	Traffic Square	Point	Imagery	Not Available
13.	Railway Network	Line	Imagery	Not Available
14.	Road Network	Line	RSCDL and Imagery	Not Available
15.	Footpath	Line	Imagery	Not Available
16.	Landmarks	Point	Imagery	Not Available

Checking and Verification of digitized map

From the base map created by the bidder/SI 5% of each ward base layers will be randomly selected as sample for the accuracy. The deviation between ground and map should not be more than permissible limits decided by RSCDL (~1 meter) of a single line/edge. If the incorrectness in accuracy is found in more than 5% of samples, the entire ward will be rejected and bidder/SI will be required to carry out re-digitization of that ward.

3.8.5 Development of Geo-enabled Property Tax Survey Application and Door to Door Property Tagging Survey

The overall scope of the work is:

1. Development of Property Tax Survey Mobile Application.

2. Geo enabled property geotagging survey for 4 Lakh properties and yet to be assessed properties in within RMC limits.

Development of Property Tax Survey Mobile Application

RSCDL intends to carry out a household level geotagging survey. The selected bidder must design, develop, deploy and end user training of GIS database and a customized Mobile based GIS application for geotagging all the properties within RMC jurisdiction. The scope of work is as follows:

- Mobile app android based surveyor module for GPS enabled handheld device with good accuracy for effective and real time geospatial property tax survey.

- Provide documented functional requirements, as and when gathered throughout the period, for validation with the RSCDL's stakeholders, or persons appointed thereby.

- Develop wireframes for new UI or existing UI revamps, wherever required, upon written request by the RSCDL or representatives thereof. Please note that this includes creation of new UI or enhancements or adjustments to be made to existing UI, in response to external events, change in functionality or other factors.

- Provide robust design and solutions considering the integration with backend systems and the integration with existing systems.

- Provide web services and APIs for the mobile applications, on written request by the RSCDL or representatives thereof.

- Design, development, testing, deployment and end user training of the mobile application developed. End user training may be required more than once.

- Deliver and provide handover for the source code and any additional software components that are developed to fulfil the project requirements

- Provide technical documentation: requirements, design, architecture, installation, configuration, testing related documents.

- Suggest UI and UX improvements based on current trends and technology available.

- Integrate the latest developments from the mobility space into the mobile application, as and when deemed suitable by the RSCDL or representatives thereof.

- The mobile application provided by vendor should comply with CERT-IN guidelines for web security and should be audited by a CERT-IN empaneled Security Auditor. Vendor shall be required to submit security audit certificates of all the deliverables.

- Provide development and testing environments for any and all software components in the mobile applications. UAT and production environments shall be provided by the RSCDL.

- Develop components keeping in mind performance issues specific to mobility, such as call interruption behaviour, battery consumption and usability according to the form factor specified.

- The application should have capability to integrate with digital measurement devices like laser distometer for carpet area calculation.

- Develop components that are W3C, WCAG and GIGW compliant.

- At the end of the engagement, the bidder will be required to submit a learnings document that must contain the content including, but not limited to, the following:
    i. Best practices for software development employed
    ii. Learnings from the engagement
    iii. Recommendations for new features in the mobile app

Key Features

The following are the indicative features of the Property Tax Survey Mobile Application

- Provision for field related Data entry for every property as per RSCDL requirement
- The separate data should be collected for Under Construction / Incomplete Buildings including geo-tagged and geo-controlled with timestamp Photograph
- Attach photograph which should be geo-tagged and geo-controlled with timestamp. The photograph capture should not be allowed beyond particular distance (in meter) and this distance should be configurable as RSCDL will decide it later
- Application should restrict upload photograph facility from gallery so that Surveyor has to click the property photograph on the field within allowed area.
- Surveyor should be provided very user friendly dashboard which can directly take him to the location where he stands as soon as he logs in. The surrounding buildings should provide clear distinction between work done, work not done and work in progress for his benefit.
- The distinction of properties should be configurable which can be decided by RSCDL about indicators like outlines and color.
- As surveyor completes field level data entry he should be able to submit details from field
- Surveyor should be able to work on any properties within his allocated area that are also rejected by office users
- Surveyor should also be able to search properties by giving property number

- Provision for new property addition
- Provision for Alpha numeric GIS IDs for all property
- Provision for Property Ground Truthing
- Provision for other Asset layers Ground Truthing
- Provision for uploading documents from site for new assessment
- GIS Navigation facilities and Search Tool
- Geofencing "Wardwise"

Functional Requirements

Some of the major modules in the application are as follows:

No.	Module	Key Features
1.	Login Module	User Role based login
2.	New Property Geotagging Modules	Property locations tagging, Pictures, new polygons creation, etc.
3.	Old Property Geotagging Module	Identification of property assessed or non-assessed. Property locations tagging, Pictures, new polygons creation
4.	Rejected Properties Module	Details for properties submitted, reasons of rejections
5.	Duplicate properties module	Duplicate properties records details, provision to delete or merge these duplicate records
6.	Alerts & Notifications	Alerts for rejection, duplications and notifications of reassigned Properties

7.	Reports	Users can view and customize the reports as per his/her role and requirements., Reports auto generated by system
8.	User Management	User administration module

Data Requirements

- Mobile Application has to be integrated with Property Management System managed by Property Tax Department.
- Data must flow seamlessly between mobile application to application
- Data exchange between application and Property Management System must be secure and encrypted.

Key Assumptions and Dependencies

- Property Tax department will be providing access to the Property Management System
- Property Tax department will provide all required forms

Data Transfer and Size of Content

Uploaded photos, signature and details need to be light weight for quick data transfer and also provision need to be provided for surveyors facing technical problem in data transfer through cellular data network should be able to transfer the collected data to server over internet as a package.

Geo enabled door to door Property tagging survey

1. Bidder should conduct Geo-enabled tagging of all already assessed and yet to be assessed properties, Private Properties, Government Properties, Properties owned by RMC, Mobile towers, religious properties, all type of properties etc. under RMC jurisdiction, ground truth of location on map and real time updates in the database of property tax assessment system.

2. Bifurcation of property and verification of ground realities of Residential / non-residential and open Plot.

3. Bidder should use Mobile devices for property tax geotagging survey which will help in effective property tax survey completion and real time updates in centralize GIS database.

4. The Mobile device shall have a data dictionary developed by the surveyor for geo-enabled field survey. Bidder has to ensure that the survey is carried out by the same Mobile device and same data dictionary is used for data collection on the field.

5. In case of any deviation / change of use / unassessed properties identified by the selected bidder, the information of this change must be informed to the Department through Mobile Application

6. The selected bidder will be responsible for loading the reference map in the Mobile device.

7. It is selected bidder's responsibility to bring the Mobile handheld devices as per the number of surveyors bidder chooses to put on field.

8. The Mobile device should have camera with active data connection and having good minimum 3G internet connectivity during the period of survey.

9. The cost of handheld Mobile device, service provider Sim Card and data connection for every device will have to be borne by selected bidder.

10. The survey team will have to maintain decorum while carrying out the survey activity keeping citizen's convenience at prime. In case of any activity that is out of acceptable limits, RSCDL may take legal actions against the selected Bidder.

11. Any complaints related to device and device network connection will not be entertained by RSCDL and selected bidder will have to resolve it without hampering the ongoing survey work. Any such delay will not be attributable to RSCDL.

12. The bidder can perform survey work all days including public holidays from SUNRISE till SUNSET.

13. The captured property tagging details should be sent to higher levels of hierarchy for further addition of office level data. The indicative list of fields that will have to be verified from the field is attached in **Annexure I**.

14. The 5% of each ward properties will be randomly selected as sample for the accuracy.

System Documents, User documents

The Successful Bidder will provide documentation, which should follow the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the project undergoes various stages of implementation. Indicative list of documents include:

- Project Commencement Documentation: Project Plan in giving out micro level activities with milestones & deadlines.
- Resource and team plans
- Details of ward wise division of work
- Template for project tracking and review
- Any other document(s) deemed necessary for implementation, operation and maintenance of the overall system.

- The bidder shall prepare a process document in accordance with the ISO 9001 standard; containing all the process being carried out during the entire tenure of the project and share the same with RSCDL.
- Periodic reviews (at least once every month) shall be carried out for measurement of effectiveness for each of the process implemented and the same shall be shared by the System Integrator with RSCDL
- Escalation Mechanism
- Exit Management Plan

Note: The successful bidder will ensure Upkeep & Updating of all documentation and manuals.

Minimum Qualification and Experience for Key Resources

The following are minimum qualifications and experience for key resources carryout geo-enabled Mobile device based survey. The following personnel would be required for the same.

Implementation Team

Sr. No.	Role and Quantity	Min. Educational Qualification & Experience
1	Project Manager (1 Manager for 1 Zone)	B.E. / B.Tech Computer Science / IT. + M.B.A. (preferable) 8+ Years of Experience; 2+ years of Experience as Project Manager in Geo enabled survey Projects 4+ Years of experience in Geo enabled survey Implementation projects
2	Survey Team Leader (1 Team Leader for every ward)	M.E / M.Tech / M. Plan / M.Sc., in Geography / Remote Sensing / Computer Science/Geo informatics with 8+ years of experience in surveying Skills: Experience in Spatial Data bases / Remote Sensing / Urban Planning / Socio-economic data with GIS and Handling a Team of 15

		persons 5 Years of Experience in performing similar work
3	Surveyors (6 surveyors for every ward)	The Survey Team Head must have a relevant diploma in Engineering with At least 3 years' Experience in All types of Topographic survey Or Graduate (12+3) fluency in English, Hindi, and Gujarati
4	Helper (12 helpers for every ward)	Minimum 10+2

3.8.6 Underground Utility Survey

Under Ground Utility Mapping for Rajkot City is intended to capture information about following sub surface utilities:

- Water Networks – Including all Pipe Lines, Valves, Underground storage tanks, Storm network
- Sewerage Networks – Including main holes treatment plants and booster pumps
- Underground Power Cables
- Underground Communication Cables

The indicative figures for various utilities for area under scope are as follows:

S No	Type of Utility	Length (m)
1.	Sewer pipelines (Pressure Pipelines and Sewer Lines)	2600-2800
2.	Water Pipelines (Water Feeder and Water Distribution)	2500
3.	Storm water drainage	<100

The indicative figures for road length as per width from center line under the RMC boundaries are as follows:

S No		Length (km)
1.	Road Network	3600 (considering both sides)

The Survey shall be carried out as per following technical standards:

- **Scale of Mapping**: 1:2,000
- **Mapping accuracy:** Required planimetric / XY accuracy- as per mapping standards. Theminimum accepted accuracy for planimetry is 25 cm. The depth of the utility should be accurate within +/- 50 cm or 10% of the utility depth whichever is less
- **Projection System**- All co-ordinates are to be based on the following parameters:

  Projection : Universal Transverse Mercator (UTM)
  Spheroid : WGS 84
  Vertical Datum : Mean Sea Level

Refer**Annexure I** for details of features to be captured and survey deliverables and formats.

Survey of Underground Utilities

The Utility Vendor shall locate and identify all underground services within the area to be mapped. All the connections, bends, sudden change in depth /direction should be captured and shown. Underground utilities, associated surface features, change of direction and bifurcation shall be located and X, Y and depth is recorded at intervals not exceeding 50 meters. Wherever bands of utilities are identified, the upper and lower utility should be placed in such a way that it provides a cross section of the utility bands. At any significant change (more than 0.3m) change of depth below the ground, an annotation should be provided. This annotation shall be placed at the same z -value (depth level) as recorded at that very point. Each service shall be annotated with the type of utility, depth and diameter of pipe at appropriate intervals.

The bidder will be responsible for co-ordination with various city agencies and State Government Departments & utilities whenever and wherever necessary on the behalf of RSCDL for the purpose of survey. In case of major problems, RSCDL will assist. This includes taking permission, clearance after restoring back the works & handing over. Bidder will have to incur all cost/charges related to Right of Way and Reinstatement.

All required manpower, DGPS survey, Survey equipment as required, Total Station Equipment, Induction Cable Locator, etc. shall be arranged by the bidder at their own cost. Other necessary

activities as leveling of surface (if required for carrying out survey), taking necessary permission from local civic authorities to produce the desired output will be in the scope of bidder, RSCDL will assist in this regard.

Before start of utilities detection survey successful bidder will have to submit the execution plan and project schedule etc. to RMC. The survey should be conducted with adequate advanced technologies (GPR, total station, DGPS, etc.), in such a manner that all types of utilities, sewer line, cable/duct etc. are identified and requirements and SLA's mentioned in the RFP are met. In case of any other methodology / technology is proposed by the bidder, the same may be agreed by RSCDL provided that end results are same. However for any such changes approval of RSCDL shall be obtained by the bidder after giving all technical details of the methodology / technology proposed to be adopted as part of technical proposal.

Underground utilities which can be located without excavation, such as cables and connected metal pipes which can be located by surface detection equipment, and drains, manholes, chambers and draw pits shall be located and mapped to the accuracy as specified under mapping accuracy heading above.

Underground utilities shall be mapped continuously and recorded in three dimensions ensuring that sub surface features are captured at each change of direction and bifurcation. Positions and levels shall be related to the specified grid and datum and shall normally be related to the center of metallic pipes or cables, crown of ducts and inverts of sewers and drains.

Any known underground utilities or information which cannot be mapped to the accuracies stated under mapping accuracy other than by excavation, shall be entered in a unique layers defined as "uncharted", as approved by the RajkotSmart City Development Limited. The Vendor shall itemize in his Reports the types of utilities which have been classified as "uncharted" and other circumstances, such as local areas of interference, where the specified accuracies cannot be achieved.

If the utility corridor falls on both foot path and on carriage way, scanning to be done on both foot path and carriage way and if there are any obstruction in the survey corridor, the readings to be taken before and after the obstruction and also whatever readings possible in between. The survey should also pick up all surface projections of utilities such as manhole valves, chambers, junction box, fire hydrants etc falling in the corridor.

As part of input data/material to conduct survey, RSCDL will provide following to the selected bidder:

i. Utility drawings (hardcopy) of utilities to be mapped.
ii. Available GIS data / base maps generated by RSCDL

Separately the bidder shall provision for any correction/local correction required for the positional accuracy before the start of the survey so that the underground survey data can be superimposed over the base map survey proposed as part of the scope the project.

Note: All data supplied and collected as part of the survey is the property of Rajkot Smart City Development Limited and no data will be retained bythe bidder.

Wherever full details of underground utilities cannot be determined without excavation, these details shall be deduced from the drawing supplied as Input data by utility owner record drawings and entered into the drawing in a unique layer defined as 'records".

The Utility Mapping of Rajkot City to be carried out by the vendors using their own Hardware, Software and Manpower. No extra cost to this effect shall be paid by Rajkot Smart City Development Limited. The data processing etc. will be done in the RSCDL Premises or as intimated to the vendor. The bidder shall consider all cost components such as manpower, labor, logistics, post processing efforts, etc. at time of putting commercials of for the underground utility survey.

Wherever access is available from the surface, the Vendor shall cross check the depth to underground utilities.

The bidder shall make necessary provisions to ensure the safety of manpower employed in the survey work by taking steps not limiting to the following:

- Ensuring proper training of the workforce regarding hazards that may be encountered during the site work and the particular hazards attached to their own function within the operation
- Issuing photo identity card duly signed by the authorized representative of the bidder and if required from RSCDL before they are engaged for any work
- Providing protective gears such as High visibility clothing, helmets, etc.
- Ensuring First-aid boxes at the site

Proof of Concept (POC) for Underground Utility Survey

As a part of the scope, all bidders will have to carry out a POC for 1 Sq. KM or line sections having turns, cross junctions and having utility networks of interests as identified by RSCDL. The POC will be carried out by the bidder before the final Technical submission of this RFP.

Only if the POC is concluded by RSCDL as successful, the scope, timelines, payment terms, commercials and the other related conditions in the RPF document will be considered for the final

technical & commercial evaluation, else all the conditions related to underground utility survey will be considered null and void and will not be considered as a part of the final scope and technical & commercial evaluation of the this RFP.

The POC should be conducted using the combination of proposed devices and technology which is offered as part of technical proposal. The POC shall be carried out as per the technical standards mentioned in the above section and guidelines mentioned in below as per the evaluation of the POC.

The bidder is required to submit the raw data and processed survey data in geospatial format at 1:2000 scale superimposed over RSCDL existing base map for evaluation in CD/DVD/Pen drive/USB stick to RSCDL for evaluation.

The cost of carrying out the POC shall be borne by the bidder and RSCDL along with help of RMC will facilitate in providing necessary approvals from concerned authorities as well in providing Base Map and Utilities data available for the Pilot Area. The duration of POC should not exceed 15 Days.

The bidders will be awarded marks based on the relative accuracy levels and quality of surveyed data visactual ground situation alongside the specifications mentioned in the RFP. The key areas based on which the POC will be evaluated and relative marking will be awarded are as following:

- Accuracy of surveyed data as per specifications of the RFP
- Ability to detect number of utilities

The final evaluation criteria of the POC will be given to all the applicants before the POC work is commenced. RSCDL will reserve the right to ask all / few applicants from the list of interested applicants to carry out the POC.

3.8.7 Development of GIS application Suite and Citizen Portal

The selected bidder should develop a web base GIS applications suite for RSCDL. This will cater to the viewing, analyzing, & utilizing the Geographic Information needs of the different departments of RSCDL. This should also play a role of decision support system for RSCDL departments for which the field information and geographic data plays a vital role.

Once the base map is digitized and enterprise GIS setup is done by the selected bidder, the GIS applications suite and Citizen Portal is to be developed for core GIS web based platform for RSCDL departments and citizens of Rajkot city. The selected bidder is expected to follow the complete SDLC for the development of the GIS application suite. An indicative FRS for GIS application for RSCDL is attached in **Annexure I and department specific applications is also given in Annexure I.**

Proposed/Developed GIS Application Suite should follow National Spatial Data Infrastructure (NSDI) Meta standards and should be compatible with National Urban Information System (NUIS) Scheme. The application suite should also have mobile compatibility for field users from RSCDL.

The selected bidder should develop a web base GIS enabled Citizen portal for the citizens. This will facilitate the citizens to view and utilize the Geographic Information of different departments of RSCDL. The bidder is expected to provide technical and management support during the planning, design, development and implementation of GIS based Citizen Portal of RSCDL. The bidder must gather all the data and information, which needs to be kept open for citizens to view and utilize, from all the departments of RSCDL.

The indicative list of functionalities which the bidder has to incorporate in Citizen Portal is attached in **Annexure I**.

3.8.8 Testing, Training and Go-Live of the System

User Acceptance Testing (UAT)

The primary goal of Acceptance Testing is to ensure that the proposed GIS System meets requirements, standards, and specifications as set out in this RFP and as needed to achieve the desired outcomes. The Bidder/SI will prepare the UAT criteria document and sample data for UAT, and take approval from RSCDL, well in advance before start of the UAT process.

For UAT the test cases should be discussed and the test data will have to be formally requested from each of the departmental users to ensure that each of the module user get real time feel of the application. This approach would also help in availing faster acceptance from respective user departments of RSCDL and their key stakeholders.

RSCDL reserves its right to undertake this exercise of Testing, Acceptance and Certification through a third party.

The basic approach for UAT should ensure that the following are associated with clear and quantifiable metrics for accountability:

- Functional requirements
- Performance
- Security
- Manageability
- SLA Reporting System
- Project Documentation
- Data Quality Review

Training

- Prepare and organize training programs to facilitate the departmental users in the efficient usage of the whole system.

- The Bidder/SI shall provide training to departmental users to efficiently use the system. The staff thus trained would subsequently train the other staff as and when required.
- The Bidder/SI shall provide training as per the proposed training plan schedule to be shared as part of Approach and Methodology section in technical bid.
- Bidder has to conduct a proper Training Needs Analysis of all the concerned staff and draw up a systematic training plan in line with the overall project plan. For all these training programs the bidder has to provide necessary course material and reference manuals (user/ maintenance/ administration)
- Based on the roles and responsibilities of the RSCDL officials at various levels, the training plan should be proposed; it should address level wise functional and general training requirements in accordance with the existing skill set and capacity of the RSCDL officials.
- The Bidder/SI shall provide training to the selected officials of RSCDL as decided by the authorized official. The training batch size should not be more than 25 officials.
- Bidder has to train around 75- 100 key department users for hands on training regarding the GIS application usage.
- The selected bidder will have to take 5 training session for each user department
- A detailed training schedule, including the dates, areas to be covered, time and the training literature (to be supplied to RSCDL) at various stages of the training cycle and feedback for effectiveness will be agreed to by both parties (RSCDL and the Bidder/SI) during the performance of the Contract.
- Training shall also be provided for teaching the basic trouble shooting activities in case of problems.
- For imparting training; SI will have to provide training material, trainer, along with training infrastructure such as Training Rooms, Sitting arrangement, overhead projector, computing infrastructure for the trainees, etc.
- Trainings shall be provided as per the training schedule provided by SI/Bidder.
- Training shall be imparted in Gujarati and English language as per the requirement of the trainees. The printed manuals and training manuals should also be available in Gujarati and English Language.
- The trainers imparting the training should be well versed in Gujarati and English language.
- Training is an important aspect of every project, and RSCDL expects the successful bidder to undertake it in a very professional manner. All the module users will have to be trained with respect to the functionality of the corresponding modules.
- Trainings have to be imparted at a location mutually agreed by bidder and RSCDL and within the City limits.
- Bidder has to provide CBT for each of the functional module on the intranet for reference of the departmental users. CBT has to be in both Gujarati and English Language

- Training to be imparted to users:

Functional Training: This training would focus on the usage of application software so that the users are aware of all the operations of the application systems, ensuring a smooth run of Citizen Services or Departmental Operations. It would be covered for each of the functional module.
Administrative Training: This training would focus on the administration of Application Software and Server Infrastructure and would be imparted to the relevant staff of RSCDL.

System Documents, User Documents

The Successful Bidder will provide documentation, which should follow the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the project undergoes various stages of implementation. Indicative list of documents include:

- Project Commencement Documentation: Project Plan in giving out micro level activities with milestones & deadlines.
- Training Material: Training Material will include the presentations used for trainings and also the required relevant documents for the topics being covered.
- User Manuals: For all the Application Software Modules, required for operationalization of the system.
- System Manual: For all the Application Software Modules, covering detail information required for its administration.
- Installation Manual
- Test Plans and Test cases (including Unit Test Plan, System/Integration Test Plan, User Acceptance Test Plan, Security Test Plan, Load Test Plan, Regression Test Plan)
- Software Testing Documentation (including details of defects/bugs/errors and their resolution)
- Source Code versioning document
- Inspection and testing procedures manual including QA Policy as per STQC framework and Procedures for the software/hardware equipment

- Any other document(s) deemed necessary for implementation, operation and maintenance of the overall system.
- Software Design Document
    - High Level Software Design document including Software Architecture design, Logical and Physical Database Design etc.
    - Low Level Software Design document including Programming Logic, Workflows etc.
    - Complete Source Code with documentation
- The bidder shall prepare a process document in accordance with the ISO 9001 standard; containing all the process being carried out during the entire tenure of the project and share the same with RSCDL.
- Periodic reviews (at least once every quarter) shall be carried out for measurement of effectiveness for each of the process implemented and the same shall be shared by the System Integrator with RSCDL
- Escalation Mechanism
- Exit Management Plan

Note: The successful bidder will ensure Upkeep & Updating of all documentation and manuals.

Outputs and Deliverables

The desired output and deliverables to be shown and submitted to RSCDL includes:

- **Satellite Data**
    - Rectified satellite data along with GCP files.
    - Soft copies of images in .img and Geo tiff/JPEG formats.

- **DGPS Survey Data**
    - The processed data of the DGPS survey with a photograph of each GCP .
    - A neat sketch of each DGPS point showing the location on A4 size drawing.

- **Base Map**
  - Digital data of base map inclusive of all utilities in proposed GIS platform compatible format.
  - Hard copies of Ward wise Maps, depicting all entities to be delivered.
  - Geo-PDFs of the base map of each ward depicting all layers.

Application Software Certification

Upon successful UAT and prior to the Go Live, the bidder shall undertake testing and certification of the Software by the Standardization Testing and Quality Certification (**STQC**) Directorate or any other CERT-In empaneled IT Security Auditing Company from functional and security perspective.

Test & Live Implementation

Upon completion of above activities, Successful Bidder will have to submit detailed plan for live implementation of the system. Successful Bidder has to ensure that the Application Software is completely operational as per the requirements in this RFP and all the acceptance tests are successfully concluded as per the satisfaction of RSCDL or RSCDL Consultant.

RSCDL reserves the right to undertake Test Implementation of the system before making it public.

3.9 E-Governance System and ERP

The client aims to implement consistent and less paper processes throughout the organization and wishes to synergize the municipal operations to bring about transparency, efficiency and accuracy in its functions. With this aim, the client has felt a need to implement a standardized and integrated electronic system across the various stakeholders of the organization.

Automation of Municipal Operations is one of the critical aspect of the Smart City initiative of client which shall be augmented by initiatives of the State Government and Central Government (like Digital India, Smart Cities, Open Data, JAM and Cashless Society). The solution proposed should be

line with National Municipal Accounting Manual and other guidelines by competent authorities and should have capabilities to integrate with such initiatives for which necessary details and APIs will be made available for integration. The envisaged architecture for the client contains the solution which has components mentioned below.

1. **Enterprise Resource Planning (ERP)**: The SI will be required to implement an ERP which will aid in institutionalization of best practices, will facilitate business processes, ensure flexibility in communication, smoothen data exchange, will make process traceable and would be scalable to meet the requirements of client. The SI will be required to customize COTS based ERP in a manner that it supports the functionality, laws and language of the client including its needs evolving from time to time. The ERP software consists of various modules out of which there are some modules (such as Finance, Human Resource, Material Management, etc.) whose functionality closely resembles the working of departments within the client and such modules have been referred to as core modules.

    - Financial Management, Asset accounting, Grants & Investments
    - Human Resource, Payroll & Employee self-service
    - Procurement, Material Management & Vendor Management
    - Project & Portfolio Management
    - Enterprise Asset Management with Planned Maintenance
    - Quality and audit management

    For the non-core modules like Workflow and File Management System & DMS, the SI will be required to implement COTS product meeting the functional requirement of the RFP. For the other non-core modules, the SI may choose to implement COTS product/Custom Developed Solutions meeting the functional requirement of the RFP.

    The existing IT applications developed by RMC for specific purposes falling under the scope of the RFP, will cease to operate post ERP implementation and bidder is required to rebuild the same as part of the proposed implementation.

2. **Citizen Services and Internal Operations**: Citizens are the primary stakeholders in the functioning of a public body. To support the needs to citizens the client provides various services to them. For managing the city, the client also performs various operations which are internal in nature. The SI will be required to implement a solution which would automate all the citizen centric services and internal operations

3. **Electronic Office Application**: The government agencies create and maintain the files. To make the process more efficient and transparent, the SI will be required to implement an electronic solution which will maintain an electronic record of files (file noting & correspondence, its history, present status, etc.). However, the client will take a call on closing the physical filing process later; till then it is envisaged both i.e. the electronic and manual procedure of filing will be run on a parallel basis for 1 year from the date of go-live. After 1 year from the date of go-live, the physical filing process will cease to work and will be taken over by electronic record of files

4. **Document Management System**: The client creates / receives and maintains (as per government procedures) the documents during the day-to-day operations. The archival and efficient retrieval of these documents is of high importance to the client. With this aim, SI will be required to implement the Document Management System.

5. **Workflow Management System**: The citizen centric services and internal operations have a well-defined flow of approvals. The SI will be required to implement a workflow management system and configure the flow of approvals for various types of citizen services as well as internal operations.

6. **Integrated Web-Portal based on Content Management System**: The SI will be required to implement a web based solution comprising of website, service delivery modules, citizen dashboard, etc.
    - Citizen collaboration platform
    - Citizen Dashboard
    - Citizen Service Delivery

- Grievance Management Module

7. **Mobile Application**: The SI will be required to develop and maintain the platform agnostic comprising mobile application. The mobile application should cater to the requirements of external users (citizens, etc.) as well as internal users (officials, staff, etc.).

8. Aadhaar enabled biometric attendance system

The scope of the implementation of Aadhaar enabled biometric attendance system will include:

1. Supply and installation of Aadhaar enabled biometric attendance devices.
2. Enrollment of RMC employees in the solution linked with Aadhaar enabled biometric attendance devices.
3. Maintenance of Aadhaar enabled biometric attendance devices for the entire project duration.
4. In-Warranty Annual Technical Support for a period of 5 years from Go-Live

In addition to this, the proposed system should have capabilities to integrate the employee attendance details with the payroll processing module.

The scope of work of the intended engagement broadly encompasses the following high level requirements:

1. Supply
2. Installation
3. Testing
4. Commissioning
5. Operating System Software Licenses
6. Peripheral Drivers installation and integration
7. Services and support

The following are additional points for the scope of the Implementation Agency:

- The Fingerprint Biometric Attendance Machines shall be connected to Local Area Network.

- Fingerprint Biometric Attendance Machines firewall (inbuilt feature of OS etc.) should be made active that denies all unnecessary incoming network connection attempts
- The supplier shall disable unnecessary services, protocols, and ports.
- When installing software, ensure that only required software is installed, making sure to install the latest versions of all software including all recommended security patches that are available.
- Unnecessary software (including application, system utilities and network services) should be removed or disabled.

Functionality

The attendance solution will encompass the following functionalities:

- Capture fingerprints and other details (including photographs) and create a databank of bonafide employees
- Encryption of all data
- Provide conditional access to employees at specified locations
- Keep a record of employee attendance
- Integrate employee attendance particulars to Payroll module of ERP

Services of component (one time)

- Customization
- Integration with payroll module of ERP
- UAT
- Implementation
- Parallel / Independent runs
- Capture photographs, fingerprints and other details of all bonafide employees

Recurring (post implementation)

- Support (AMC) and ATS for a period of 5 years from date of go-live
- System Administration
- Database Base Administration

- Change Management Process
- Warranty Period
- Onsite Support
- Capture fingerprints and other details of employees

Hardware Installation

RMC/RSCDL will be providing power connections for the equipment. It will be bidder's responsibility to procure, supply, configure, install, commission, integrate and test the client side IT Infrastructure at RMC offices. If any other items that are required (in addition to the bill of material given in this bid document) such as cables etc, the bidder has to provide, install and configure them, without any additional cost.

The illustrative deliverables for this activity are mentioned below.

- Installation and Commissioning Report of Aadhaar enabled biometric attendance system
- Devise a Replication-and-Restore policy
- Managing the storage of back-up media in a safe and secure manner during the warranty and maintenance period
- Preparation of Business Continuity Plan (BCP)/Disaster Recovery (DR) Plan
- Drill Exercise (including roll back) and improvement in BCP.

The SI has to take approval of client for deliverables of this activity such as Installation and commissioning Report, BCP/DR plan etc.

8. The overall scope of work for the solution implementation has been divided into two phases:

Phase-I (Establishment and Go-Live)	Phase-II (Operations and Maintenance)
i. Project planning and mobilization ii. Requirement Gathering iii. Solution Design iv. Software Customization v. Testing and UAT vi. Supply of licenses vii. Capacity Building and Training viii. Third Party Audit and Go-Live of the solution ix. Preparation of standard operating procedures x. Solution Stabilization	i. User Handholding ii. Refresher Training iii. Periodic Audits iv. Business Continuity Support v. Help Desk Support vi. Ongoing scanning, indexing, digitization and uploading of documents vii. Monitoring and Maintenance viii. Miscellaneous Operations ix. Exit Management and Knowledge Transfer

The detailed scope of work in each phase is provided below:

Phase I: Establishment and Go-live of solution

The Phase-I of the solution shall include the following activities:

Project Planning and Mobilization

The SI needs to plan all the important tasks to ensure that all pre-requisite are met and the SI team is able to deliver the project as per the timelines, requirements and service levels. The first step to initiate the project is to prepare the project plan and mobilize the implementation team. The SI needs to submit the CVs of implementation team for client's approval before mobilization. During the course of project the SI would be required to prepare project plan, project initiation document, progress reports, risk register, issue register and other project management related documents. The indicative list of project management documents would include the following:

- **Project Schedule**: A detailed week-wise timeline indicating various activities to be performed along with completion dates for the same shall be provided by the SI.

- **Project Initiation Report**: The project initiation report shall be prepared by the SI after the initiation of the project. The report shall contain manpower deployment plan, project plan, risk mitigation plan, escalation matrix, etc.

- **Progress Reports**: Detailed weekly, fortnightly, monthly Progress Report along with issues/ escalations/risks. The format shall be finalized by the client prior to start of the project.

- **Risk Register**: SI shall be required to maintain a risk register which shall enlist all possible risks which shall impact the solution along with their occurrence and likelihood. The SI shall also propose the mechanism to mitigate the identified risks.

- **Issue Register**: Apart from the risk register the SI shall also maintain the issue register which shall list down the issue that have occurred in the project and the decision/remedial measures taken in reference to the issue.

- **Stakeholder Register**: To keep the information about the stakeholders, the SI will be required to prepare a stakeholder register containing details about each stakeholder or group of stakeholders. This will be an input into the requirement gathering and communications plan.

- **CVs of implementation team**: The SI will be required to provide CVs of the implementation team and various resources which it intends to deploy on the project and ensure their mobilization to the project site.

- Other reports which shall be required to be delivered as part of implementation of the solution

Requirement Gathering

An indicative functional requirements has been undertaken for the most of the modules as mentioned at **Annexure IX Functional Requirement Specifications**. The SI shall carry out a detailed systems study to refine the Functional Requirements Specifications and formulate the System Requirements Specifications (SRS) incorporating the functional specifications and get it approved by the client. The system study should also include different integration points with external agencies such as ICCC, Enterprise GIS etc. as per the requirement of project. The SRS document should necessarily contain the following details:

- User groups, roles and types of access
- Method of access such as website, handheld device, etc.

- Use cases for workflows
- Sequence diagrams for workflows identified
- Functional logic and checks expected from the system while executing the project
- Reporting requirements
- Interfaces with other external systems
- Security requirements
- Audit and application logging requirements
- Archival requirements
- Migration requirements
- SLA monitoring requirements
- Provide a mapping between SRS and FRS as provided in the RFP, detailing how SRS is addressing the requirements.
- Any other relevant details which are required to clearly articulate software requirements

SI will conduct workshops with relevant users of the systems wherever necessary, to obtain more details on the requirements of the project and have to get a sign-off on the requirements from the appropriate authorities. The SI should identify the customization requirements for the implementation. Any requirement will have to be explicitly discussed and agreed with relevant stakeholders of the client.

1. Process Study: The SI should study relevant processes of the for the application development. The client will provide the relevant support, available reports and information required for completing the study

2. Review and Updating of FRS: The SI will review and make any addition of functionalities in the FRS based on the System Requirement Specification (SRS) report for the services identified for implementation under the project.

The indicative deliverables under this item shall be:

- Functional Requirement Specification (FRS), Software Requirement Specification (SRS) and its sign-off from the client which shall cover the functional requirements, data integration requirements, data management requirements, non-functional requirements, etc.
- Requirement Traceability Matrix
- Gap Assessment Report

Solution Design

During this phase, the SI will be required to develop a detailed design document which shall meet the user requirements captured during requirements gathering stage. SI during this phase shall be required to perform at least the below mentioned activities:

- Preparation of Solution Architecture specifying the Functional, Infrastructure, Data, Deployment, Network and Security Architecture
- Preparation of System Design Document specifying the construction details of the system, each system component's interaction with other components and external systems, and the interface that allows end users to operate the system and its functions
- Development of Security Plan
- Exceptions and Business Alerts definitions

The illustrative deliverables for this activity are mentioned below.

- Solution Design and Architecture Document (including ER Diagram and Data Flow Diagram)
- High Level Design Document and Low Level Design Document (including Schema Diagram)
- User Interface and Prototypes
- Data Modelling
- User Reports
- Hosting Infrastructure requirements in accordance with functional and technical requirements and service levels
- Policy, Plan and Methodology Documents covering aspects mentioned above
- The SI has to take approval of client for deliverables of this activity such as User Interface and Prototypes, hosting infrastructure requirements etc.

List of Core Modules and Non-Core functions

Description of the all the modules with initial set of functionalities required provided in detail in section

1. List of Core Modules to be implemented (in order to achieve Functional Requirements as specified in subsequent sections)

   Core Modules

   - Financial Management, Asset accounting, Grants & Investments
   - Human Resource, Payroll & Employee self-service
   - Procurement, Material Management & Vendor Management
   - Project & Portfolio Management
   - Enterprise Asset Management with Planned Maintenance
   - Quality and Audit management

Integrated Application Requirements

Following are the requirements for the integrated applications covering above Core Modules and Other Functional Requirements as specified in subsequent sections.

- The integrated application should offer all the functionalities required as per scope.
- Noncore Modules which are not a part of standard ERP must be integrated with offered ERP as well as solution.
- The integrated application should provide wide range of security features such as Authentication, Single Sign-On (SSO), Authorization (at various authorization levels) and Integrated User Management.
- The integrated application must be cross-device compatible/OS independent/browser independent and SI/bidder will provide the OS as suggested by the respective COTS OEM ERP vendor

The integrated application should be able to configure and host various types of dashboards to provide graphical and tabular reports/data as per requirements, at various viewing levels and filters.

Existing IT Setup

RMC has a number of existing applications currently serving the citizens, the list of such application is as following:

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
1	Fire and Emergency	NA	NA	NA	Manual	
2	Central Store	Storeand InventoryMa	URL – NA Desktop	☐ Stock Management	Automated	

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
	Department	nagement System	based system in CNo. & SQL server 2012	☐ Inventory Management ☐ Purchase Order ☐ Work Order ☐ MIS		
3	RMCpolice department	NA	NA	NA	Manual	
4	Professional Tax Department	Frontend- RMC Portal Backend- Desktop based System	Front End - http://www.rmc.gov.in/rmcwebsite/professional_tax_history.aspx Back End - Desktop based professional tax module in CNo. & SQL server 2012	☐ Professional Tax payment ☐ Professional tax history ☐ MIS	Automated	Professional Tax feature in FAS module takes care of professional tax processing in back end
5	Propert	Frontend-	Front End -	☐ View property tax	Automated	Property

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
	y Tax Department	RMC Portal Backend-Desktop based System	https://www.rmcegov.gov.in/payonline/ Back End - Desktop based professional tax module in CNo. & SQL server 2012	☐ Property Tax payment ☐ MIS		Tax feature in FAS module takes care of professional tax processing in back end
6	General &administrative Department	Frontend-RMC Portal Backend-Desktop based System	Front end - http://www.rmc.gov.in/rmcwebsite/birth_death_certificate.aspx Back End - Desktop based professional tax module in CNo. & SQL server 2012	☐ Birth & Death Certificate ☐ MIS	Automated	

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
7	Commissioner's office	InwardOutward System	Back End - Desktop based module in CNo. & SQL server 2012	☐ Booking appointment with Commissioner, RMC	Automated	
8	Secretary Department	Document Management System	Back End - Desktop based module in CNo. & SQL server 2012	☐ Document Management of any communication with political wing of RMC	Partially automated	
9	Audit Department	Audit Management System	Back End - Desktop based module in CNo. & SQL server 2012	☐ Project & financial Audit functionalities are offered as part of Audit Management System	Automated	
10	Electricity Department	NA	NA	NA	Manual	
11	Baandh Kam Department	NA	NA	NA	Manual	

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
12	Water Works	System used for new water connection to payment	Front End - https://www.rmcegov.gov.in Back End - Desktop module in CNo. & SQL server 2012	☐ Water Connection request ☐ View water usage bill ☐ Pay Water usage charges ☐ MIS	Partially automated	
13	Drainage Department	New drainage connection	Front End - https://www.rmcegov.gov.in Back End - Desktop module in CNo. & SQL server 2012	☐ New drainage connection form	Partially automated	The solution is partially automated, drainage form can be downloaded online however no option to submit the form
14	Accounts Department	FAS	Back End - Desktop module in CNo. & SQL server 2012	☐ Budget planning & preparation ☐ Revenue management ☐ Procurement	Automated	

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
				☐ Department wise budget management		
15	Computer Department	Hardware Management System – Asset tracking and management	Back end system in CNo. and SQL server 2012	☐ IT Asset tracking and management	Automated	The solution is limited to EDP department IT asset tracking only
16	RTI	RTI – website and separate software	RMC website - http://www.rmc.gov.in/rmcwebsite/rti_status.aspx Back end system in CNo. and SQL server 2012	☐ RTI Status Tracking ☐ Proactive Disclosure		
17	Awas Department	Housing Management system	Back end system in CNo. and SQL server 2012	☐ Awas Grant Management ☐ Project Management		

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
18	Garden Department	NA	NA	NA	Manual	
19	Vigilance Department	NA	NA	NA	Manual	
20	Establishment Departments	PIS system – Recruitment to Payroll	RMC website – http://117.240.113.212/ for Recruitment Attendance, payroll & loans- Back end system in CNo. and SQL server 2012	☐ Payroll ☐ Staff attendance ☐ Job recruitment ☐ Staff Loan		
21	Health Department	NA	NA	NA	Manual	
22	Solid Waste Manage	NA	NA	NA	Manual	

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
	ment Department					
23	Legal Department	Legal Information system	Back end system in CNo. and SQL server 2012SQL 2012	Case Management including new case, alert for hearing dates, case documentation		
24	Cultural Development Department	NA	NA	NA	Manual	
25	ICDS (Integrated Child Development Scheme) Department	NA	NA	NA	Manual	
26	Town Planning	Town planning system	Back end system in CNo. and	☐ Plan authorization ☐ Construction permission		

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
			SQL server 2012	☐ Compliance reporting ☐ Billing & invoice ☐ MIS		
27	Estate Department	Asset & Hold booking Management	CNo. - Website Backend – VB.net SQL 2012	☐ Database of Public holdings ☐ Asset tracking ☐ Rent management		
28	Election Department	NA	NA	NA	Manual	
29	Parking Management Department	NA	NA	NA	Manual	Parking Charge collection accounted under FAS module
30	Project Department	NA	NA	NA	Manual	
31	Shop Department	Shop & establishment system	Back end system in CNo. and	☐ Shop and Establishment management		

S.No	Application Name	Descriptions	URL	Function Area covered	Present Status	Observations
			SQL server 2012	payment and invoice		
32	ANCD (Animal Nuisance Control Department)	NA	NA	NA	Manual	
33	Building Plan permission	Building permission management		License management, building permission	Automated	

The existing functional IT user base at RMC is as follows:

S No	User Group	Count
1.	Audit Bill & Misc Collection	380
2.	Bank Collection	106
3.	Birth & Death	20
4.	Financial Accounting System	40
5.	Hospital	160
6.	Single Window Collection	80
7.	Fuel & Stationary	220
	Total	1006

eGovernance system & ERP Project Locations &User base

The list of various categories of employees along with their department is as follows:

S No	Name of the Department	Class I	Class II	Class III	Class IV	Grand Total
1. 1	Animal Nuisance Control Department (A.N.C.D.)		1	20	67	88
2.	Account branch		1	25	6	32
3.	Audit branch		1	6	11	18
4.	Avas yojana	1	5	22	3	31
5.	Bandhkam	2	26	81	21	130
6.	Bhader scheme		3	13	19	35
7.	Central store			4	2	6
8.	Commissioner branch		3	7	7	17
9.	Drainage		23	51	16	90
10.	Emergency response cell (fire)			6	12	18
11.	Election branch			6	3	9
12.	Estate branch		1	16	20	37
13.	Filter plant		3	52	18	73
14.	Fire brigade		1	120	46	167
15.	Garden	1		7	46	54
16.	General administration Department	1	23	20	18	62
17.	General conservancy			16	39	55
18.	Health branch	1	10	51	27	89
19.	Integrated child development services programme cell (I.C.D.S.)			3	1	4
20.	Integrated child development services programme cell (I.C.D.S. – 2)			1	1	2
21.	IT department		1	8	4	13

S No	Name of the Department	Class I	Class II	Class III	Class IV	Grand Total
22.	Jnnurm	1	5	5	2	13
23.	Legal branch		1	7	6	14
24.	Mahi.mob.pustakalaya			1	3	4
25.	Market branch		1	28	31	60
26.	P.J.N.library		1	8	3	12
27.	Project		1	7	2	10
28.	Racecourse snanagar			31	11	42
29.	Roshni branch		8	52	11	71
30.	S. W. M. (labour)				9	9
31.	S. W. M. (vokala)				11	11
32.	Sanskrutik development department		1	8	18	27
33.	Sarojini high school			1		1
34.	Secretary branch	1	1	1	9	12
35.	Shop & establishment branch			2	1	3
36.	Solid waste		14	123	51	188
37.	Special conservancy			27	59	86
38.	Tax branch		6	93	18	117
39.	Town planning		18	40	18	76
40.	Traffic & turns Cell		7	13		20
41.	Urban malaria			29	91	120
42.	Vigilance branch			17	68	85
43.	Water works(indoor)	1	23	69	5	98
44.	Water works(outdoor)			2	89	91
45.	Workshop		1	14	9	24
46.	Zoo		3	5	16	24
	Grand Total	9	193	1118	928	2248

Additional Employee Information

S No	User Group	Count
1.	Sweepers	2310
2.	Daily wagers	122
3.	Pensioners	1747
4.	Pensioners – sweepers	850

The list of corporation office locations to be covered under the project scope is as follows:

S NO	Category	Count
1	Corporation offices	3
2	Civic Centres	6
3	Corporation Halls	21
4	Indoor Stadium	1
5	Ward Offices	18
6	Zoo	1

The SI is required design and develop the system keeping in mind the proposed user base as mentioned in below table. However the SI is expected to do a detailed assessment at the time of requirement study. Some of these user groups are only payroll users, and do not participate in other transactions. (For i.e. Grade 3 & 4 employees).

S No	User Group	Count	Remarks
1.	Employee base	2250	
2.	ESS user	1331	Assumptions: Class I, II, III user base considered; class I user considered as 20
	The estimated users for ESS (for leaves, salary slip, service book etc.) are 1331. The estimated concurrent logged in users for ESS would be 20% of the total user's i.e.267 users.		
3.	Payroll users	7249	Considering all class users, pensioners and sweepers
4.	Functional users	100	
	The core functional users for all the functional modules in the system are estimated to be 100 nos. The estimated concurrent logged in users would be 40% of the total users i.e. approximately 40 users.		

	Additional Licenses
	• RMC will purchase only a subset of Core ERP License during the implementation phase. • The selected vendor shall be responsible for supply of additional licenses for packaged solution modules or user expansion capacity for developed applications. The selected vendor is required to give a regular feedback to the RMC on the overall usage of the application software to understand the usage of the already procured licenses/user base/load. Based on this usage statistics and as per project requirement, RMC will be free to purchase additional ERP Licenses from the bidder at the same unit rate mentioned (i.e. derived) in commercial formats of this RFP document.

Software Customization

The SI shall customize the software in accordance with best practices in software development life cycle and the approved requirement specifications, design specifications, and according to the project plan. This software should be integrated with legacy systems and other Smart City Solutions (such as ICCC, ITMS, Enterprise GIS, etc.) being developed for client. The SI needs to ensure that the solution is compliant to e-Governance Standards (WCAG, GIGW etc.) and the solution is in compliance with the Security Policy and Guidelines released by GoI. The SI has to implement application software using latest available technologies after in-depth study of the prevailing ground conditions, processes and workflows. SI shall maintain a software configuration management system with appropriate version control for the software deployed. SI has to demonstrate the software that has been customized so as to meet the client's requirement and take client's approval on the same.

Other details and requirements relating to Application Development

The SI shall customize the software in accordance with best practices in software development life cycle and the approved requirement specifications, design specifications, and according to the project plan. This software should be integrated with legacy systems and other Smart City Solutions (such as ICCC, ITMS, Enterprise GIS, etc.) being developed for client. The SI needs to ensure that the solution is compliant to e-Governance Standards (WCAG, GIGW etc.) and the solution is in compliance with the Security Policy and Guidelines released by GoI. The SI has to implement application software using latest available technologies after in-depth study of the prevailing

ground conditions, processes and workflows. SI shall maintain a software configuration management system with appropriate version control for the software deployed. SI has to demonstrate the software that has been customized so as to meet the client's requirement and take client's approval on the same.

Other details and requirements relating to Application Development

1. Gateway Integration: The SI shall ensure integration with different types of gateways such as payment, mobile service delivery gateway (MSDG) etc.
2. Deploying an Integrated System for Municipal Collections and Reconciliation
3. Improving Citizen (front end) interfaces for payments
4. Opening up APIs
5. Instituting processes for disputed or double payments
6. Establishing back-end system for reconciliation of collections vis-à-vis credit in bank account
7. Creating a Standardized Interface for all Municipal Payments regardless of Payment Channel
8. Integrating revenue systems with the common collection platform
9. Undertaking Capacity Building for Revenue, Accounts and Audit Departments
10. Integration with Other existing modules
11. Confirming With Standards
12. SMS and e-mail Integration: SI shall be responsible for sending SMS and e-mails to tax payers/tax officials/ other stakeholders. The SI needs to provision for SMS charges in its commercial proposal. In its proposal SI needs to make provision for SMS API integration (http based & SMTP protocol based) gateways during the contract duration.
13. Integration with Banks: Client will provide the list of agencies/ banks with whom the system needs to be integrated. The integration may be done in phases also and the same shall be finalized during SRS stage.

There should be unified collections covering integration of existing revenue systems to a single platform, and opening up payment methods both physical and digital including but not limited to Cash/Cheque/DD collection at Counters, Collection over PoS at Counter and by Feet-On-Street, Netbanking and Online Credit/Debit Cards, eWallets and Prepaid Instruments, NEFT/RTGS/IMPS transfers, UPI Payments using BHIM or acquired on the WebSite, Mobile App initiated Payments, Payments through third party channels for example Bank Branches, Business Correspondent Networks, Bill Payment Outlets and other Offline, Online and Mobile points of presence.

It is further recommended 2 levels of Reconciliation:

1) Daily Transaction Reconciliation between the Payment Channel and the Revenue System

2) Daily Settlement Reconciliation between the Channel and the Bank Account.

It is also recommended to have a unified process for handling grievances, disputes, refund requests, double payments, chargebacks, dishonored cheques and all exception scenarios on the Platform ensuring that post collection query interfaces are provided for Citizens and grievance raising and redressal is controlled and managed on the platform.

- The service ensures that commissions for each channel are deducted as per the Agreements for each Instrument like Netbanking, Credit/Debit Cards, Rupay Cards, UPI etc.
- The service ensures that the actual credits received in the Bank match Settled Amounts from each Channel on a day-to-day basis

The illustrative deliverables for this activity are mentioned below.

- Supply, Customization, Configuration and Installation of Software
- Workflow Management
- Installation guides
- Standard Operating Procedures
- Manuals and Guidelines such as Operational manual, Technical manuals, Library Files, Setup Programs, etc.
- All licenses supplied by the SI for the purpose of this project shall be perpetual in nature and shall be in the name of client.

Testing and UAT

Test Plans for Unit Testing, Integration Testing, Data Migration Test, UAT, etc. would be prepared by the SI. The SI will plan all aspects of testing (including the preparation of test data and test environment) and obtain required assistance to ensure its success. The SI will perform rigorous testing and shall correct any defects identified during the testing. It is mandatory for SI to incorporate / consider test cases as part of test cases for those customized and/or extensions and/or configured functionalities identified from traceability matrix.

For UAT, the client will nominate representatives from different user groups based on inputs from the SI and would facilitate UAT. The SI would make the necessary changes to the solution to ensure that it successfully passes through UAT. The UAT should also include reconciliation of accounts, etc.

The client would issue certification of acceptance for which it shall verify availability of all the defined services as per the contract signed between the SI and the client. The SI shall be required to demonstrate all the services / features / functionalities as mentioned in the agreement. Prerequisite for carrying out UAT activity shall be:

- All documentation related to solution and relevant acceptance test document should be completed & submitted before the user acceptance test to client.
- Licenses / manuals / brochures / Data Sheets / CD / DVD / media for all the supplied components have been provided to the client.

The illustrative deliverables for this activity are mentioned below:

- Test Plan
- Test cases
- Test data
- Testing Reports and Bug Reports
- Necessary modification in software for defects identified during the testing and Bug Closure Report

Supply of licenses

The SI shall be responsible for supplying licenses for the ERP application. All licenses supplied by the SI for the purpose of this project shall be perpetual in nature and shall be in the name of client and will include AMC for the entire duration of the contract. SI will maintain an inventory of all software components procured, license renewals etc. This list will be made available to the client on request.

Capacity Building and Training

A critical factor for the success of this project is the need to build capability within the employees and the officials by training and enabling them to use and seek benefit of the solution. In view of the above capacity building and training hold importance and prominence for this project. The indicative set of activities to be performed by the SI are as follows:

- **Training Need Assessment**: SI has to conduct a proper Training Needs Analysis of all the concerned staff and draw up a systematic training plan in line with the overall project plan. Based on the roles and responsibilities of the client officials at various levels, the training plan

should be proposed; it should address level wise functional and general training requirements in accordance with the existing skillset and capacity of the client.

- **Training Calendar**: A detailed training calendar, including the dates, areas to be covered, time and the training literature (to be supplied to client) at various stages of the training cycle and feedback for effectiveness will be agreed to by both parties (client and the SI) during the performance of the Contract.

- **Training Venue:** The overhead projector for training and other associated items (such as training material, printouts, computers for trainees, etc.) will be arranged by the SI. The venue will be arranged by the client.. For these items, there should be no extra payment to the SI. Trainings have to be imparted at a location within the city limits.

- **Training Sessions**: Organize training programs as per training calendar to facilitate the user departments in the efficient usage of the whole system. The staff trained by the SI should be able to use the system on their own. Training shall encompass the knowledge of detailed functionalities of department specific modules for each of the concerned departmental users along with basic functionality of the entire solution.

- **Method of Training:** SI has to provide Computer Based Training (CBT) for each of the functional module on the intranet for reference of the departmental users. At the end of training, there should be a detailed survey to be filled in by the participants. The result of training should be compiled by the SI and submitted to the client within one week of training.

- **Language of Training and Training Material**: Training shall be imparted in Gujarati, Hindi and English language as per the requirement of the trainees. The printed manuals and training manuals should also be available in Gujarati and English Language. For all these training programs the bidder has to provide necessary course material and reference manuals (user/ maintenance/ administration)

- **Professional Trainers**: Training is an important aspect of this project, and client expects the successful bidder to undertake it in a very professional manner. All the module users will have to be trained with respect to the functionality of the corresponding modules. The trainers imparting the training should be well versed in Gujarati, Hindi and English language.

- **Types of Training**: The SI shall provide two types of trainings:
  - *Functional Training*: This training would focus on the usage of application software so that the users are aware of all the operations of the application systems, ensuring a smooth run of Citizen Services or Departmental Operations. It would be covered for each of the functional module.
  - *Administrative Training*: This training would focus on the administration of solution Software and would be imparted to the IT Department staff of client.

- **Frequency of Training**: The SI shall provide trainings:
  - *First Training:* SI will have to provide training to all the employees
  - *Refresher training*: SI will have to provide refresher training to all employees at the end of every year (both functional and administrative).

The illustrative deliverables for this activity are mentioned below.

- Training Calendar and Curriculum
- Training Material, Training Manuals, Troubleshooting Manuals, etc.
- Training Sessions, Questionnaire and Evaluation Results

Supply of licenses

The SI shall be responsible for supplying licenses for the ERP application. All licenses supplied by the SI for the purpose of this project shall be perpetual in nature and shall be in the name of client and will include AMC for the entire duration of the contract. SI will maintain an inventory of all software components procured, license renewals etc. This list will be made available to the client on

request. All the software licenses will be supplied to the client only after the successful completion of UAT and AMC will be invoked after the signing of End user license agreement (EULA).

Third party audit and Go-Live of the solution

The client shall appoint a CERT-In empaneled agency who shall be responsible for conducting the Performance and Security Audit of the solution. The CERT-IN empaneled agency appointed by the client shall conduct audit before Go-Live and in case of any major change or annually whichever is earlier. The cost of audit and the cost of rectification of non-compliances shall be borne by the SI. The audit shall be performed at least on the below mentioned aspects.

- WCAG
- GIGW
- Performance Testing
- Application Security Audit
- Penetration Testing
- Vulnerability Testing
- Database Server Controls

The illustrative deliverables for this activity are mentioned below.

- First Round Audit Report (by Auditor)
- Rectified solution and submission of next round of audit (by SI)
- Next Round Audit Report (by Auditor)
- If required, rectified solution and submission of next round of audit (by SI)
- Compliance Confirmation by the Auditor (by the Auditor)

All the above mentioned activities should get completed before the commencement of go-live. The key activities that need to be performed before go-live of the solution are as follows:

- Business readiness check before handing over to user
- Exit Management and Knowledge Transfer Plan
- Mobilization of manpower for hand holding support
- Data Migration to solution
- Approval from client

The client will operate the system of 2 weeks and will report any issues faced to the SI. The SI should be responsible to fix the aforementioned issues within stipulated time. The client will authorize the go-live of the solution.

Preparationof Standard Operating Procedures

SI shall prepare Standard Operating Procedures and Practices for operating and maintaining the solution, risk mitigation strategies, periodic status reports, training guidelines and modules, knowledge management protocol. SI has to submit the SOPs and risk mitigation strategies to the client for approval.

SolutionStabilization (for 3 months post go-live)

Once the solution has gone live, there will be a solution stabilization performed by the SI for a period of 3 months post go-live. During this period, the OEM team is expected to ensure transition and takeover of all the tasks by implementation team. The SI should handhold the functional users proactively and there should be end user transaction processing reports in the system. The issues faced by the users should be resolved immediately so that users are confident of using the solution. The illustrative deliverables for this activity are mentioned below.

- End user transaction reports
- Issue logs and RCA document for issues raised during solution stabilization
- O&M team sign off on knowledge transfer received along with above two documents

3.9.1 Data Migration

The SI is responsible for data migration from legacy system (i.e. Hard copies of documents and existing data in IT system) to be made available and accessible in the solution. The SI shall interact and discuss with client and its other stakeholders to finalize the migration of the data available in the databases of the existing IT systems to the new database implemented for the proposed project. The existing database in use is SQL server 2012 and side of data in electronic form is approx. 3 TB

The procedure for data digitization and migration activities suggested is as follows:

- The SI will ensure that the data migration task is completed before shifting to the new application.
- The SI has to design data migration and acceptance methodology and plan and get it approved from the client.
- Develop own data migration schema etc. as well as procure any software which may be required for data migration at no additional cost to the client.
- The client shall provide the available data to the SI for migration purposes. The SI will migrate the existing data and will get it verified from the client
- The SI shall provide checklists for migrated data to client for verification, including number of records, validations (where possible), other controls etc.
- The SI will submit a report on the quality assurance/control and the process adopted duly ensuring the accuracy in the migrated data (100 % accuracy is required).
- Any corrections as identified in the migrated data during Data Quality Assessment and Review shall be addressed by selected vendor at no additional cost to the RMC. The selected vendor is required to ensure the high accuracy during data digitization exercise and as per the data digitization plan.

3.9.1.1 Scanning and data entry of documents

The SI is responsible for data migration from legacy system of RMC including all its subsidiaries (i.e. Hard copies of documents and existing data in IT system) to be made available and accessible in the solution. RMC does not aim to close the physical filing process i.e. the electronic and manual procedure of filing will be run on a parallel basis for 1 year from the date of go-live. After 1 year from the date of go-live, the physical filing process will cease to work and will be taken over by electronic record of files.

The scope of services for data digitization and migration shall comprise the following:

- Scanning, binding/unbinding of pages
- Open DMS for citizens

- Upload scanned data to DMS

RMC will provide space to SI for scanning purposes at designated corporation offices, the SI in consultation with the client can manage the scanning operation in parallel mode from its multiple offices. The details about the above mentioned services are covered in subsequent sections.

Volume of work

The total volume of work for all departments of RMC and its subsidiaries is about approximately one (1) crore pages, which are stored at offices of RMC and its subsidiaries. The bidder shall revisit the volume again the time of requirement gathering. The bidder shall be paid for the scanning fees on per pages basis and on the actual number of pages scanned. This volume is a mix of A0 to A4 pages, which has been compiled from information received from each record room across the city. The volume mentioned in this document is a tentative volume which can increase or decrease, based on actual count during actual scanning work done at various departments.

Scanning, binding/unbinding of papers

Scanning and digitization of files and pages of RMC and its subsidiaries will be the responsibility of the Service Provider. There are about approx. One (1) crore pages which need to be scanned. These papers could be either in loose, hard bound files or soft bound files of various types.

1. The SI may visit ward offices and various departments of RMC and its subsidiaries for survey as well as for scanning and digitization work.
2. Establish type (A0/A1/A2/A3/A4, etc.) wise volume of pages to be digitized.
3. Identify various locations where scanners need to be setup and the type of scanner required.
4. Setup scanners at RMC.
5. Establish correct convenient and safe methods of collecting the pages so identified. Nodal officers of RMC appointed at respective location would present their pages/papers/files to the SI and SI would note details of documents from them such as name of the document, number of pages, category, page type, etc. in a pre-specified format. The nodal officers shall also provide the indexing and tagging information to the service provider with details such as file/document name, department, sub department, creator name, creation date, etc. in a pre-specified format when handing over the pages to the SI for scanning. After scanning is completed, the SI would return these pages/papers/files to RMC along with details such as name of the document, number of pages, category, page type, etc. in a pre-specified format. The service provider shall also fill the location of the scanned file on the DMS when returning the pages/papers/files back to RMC.

6. After collection of the pages from the nodal officers of RMC, it would be the responsibility of the SI to maintain and return the pages in their original form to this department. Any damage to the pages collected shall make the SI directly responsible for the same.
7. The SI should set up the processing Centre at designated location.
8. Activity of document pre-processing by the SI is as follows:
    a. Removal of tags, pins, threads, rubber bands etc.
    b. Sorting of pages in the document in the correct order.
    c. Special preparation of pages that may not be in good physical condition and may not be directly scanned. SI should prepare such pages like normal scanner can scan it.
9. Complete the activity of tagging/un tagging of nasti/semi stiff files
10. The document /pages shall be scanned on a minimum 200 dpi resolution, black and white with digitized file size not exceeding 75 kb for one side of the page.
11. The scanned pages shall be converted into PDF/A files. All the pages of a single file have to be stitched together to generate an exact replica of the physical file. The stitched document should be represented in a PDF/A format.
12. Page size of the physical file can vary across subject.
13. SI should ensure that quality of scanned images are enhanced up to the optimum level and required image enhancement activities like De-skew (to make the images straight), contrast ratio setting etc. has been done on the pages.
14. The SI must be able to carry out cropping and cleaning of images like removing black noises around the text, and providing the equal margins all around the text.
15. In case the pages are not legible, it will be the vendors responsibility to scan the pages on high resolution i.e. 600 dpi or higher.
16. No document shall be digitized more than once. The file numbering will be checked by the vendor and if there is any discrepancy in numbering, it should be sorted out with the concerned nodal officers at that location before proceeding.
17. No blank page should be deleted if they are part of the file except when both sides of the page are blank. The blank page in a file is a page that is entirely blank, or has only page number, or has rubber stamp.
18. The SI will use its own infrastructure. This shall include, but is not limited to computers (for scanning, storage, quality check etc.) UPS, Generator sets, etc. for document scanning. The space and furniture (Table, Chairs, etc.) for setting the infrastructure as well as the raw power connections will be provided by RMC where scanning would be done.
19. The SI would deploy its own human resource for all above aforementioned activities. The SI shall deploy adequately skilled manpower resources to complete the job within the specified time period. The scanning and data entry staff to follow RMC office calendar for working days.
20. The data on DMS should also be backed up on a separate media and handed over to RMC. The procurement and maintenance of hardware for backup/disaster recovery will be the responsibility of the service provider.
21. Each page shall be serially arranged and shall be counted while giving the pages back.
22. Scanned file naming convention and folder structure and naming convention to be used to store the scanned files shall be customizable and will be able to accommodate RMC's policies for file naming conventions.
23. Save the electronic document in a print ready non editable form in proper "Folder" as per the departments.
24. Check for quality, efficiency and fidelity.

25. Random sampling of the pages scanned and entered into the system will be done by the nodal officers. The pages would be deemed to have been verified only upon signoff by the concerned nodal officers.
26. The pages that are blank on both the sides would be non chargeable. However, pages that are not blank on minimum one side will be chargeable for both sides. e. g.
    a. A page has text on side A and is blank on side B-chargeable for both sides.
    b. A page has text on side A and side B- chargeable for both sides.
    c. A page is blank on both side A and side B-not chargeable.
    d. A3/A2 size papers will be considered as two A4 size.
    e. A1/A0 size papers will be considered as four A4 size.

Configure solution for specified features

The service provider has to perform the necessary customizations as below to suit the needs of RMC:

1. Security – Provide proper security for all the scanned data such as encryption, SSL, etc.
2. Electronic Signature – Provision to electronically sign documents when uploading it to the DMS and publishing documents to citizens. It should be possible to turn this feature ON/OFF as and when needed.
3. File Access Rights – Provision for role based access to the DMS system. Provision for editing only specific users based on their access level.
4. Optical Character Recognition (OCR) – Provision for converting documents through OCR engine. It should be possible to turn this feature ON/OFF as and when needed.
5. Indexing, tagging and Storage – Provision for indexing and storing documents, creating custom indexing fields, creating custom tags, etc. in English and/or Gujarati languages.
6. Printing, Emailing and Faxing – Provision for printing, emailing and faxing the documents from the DMS system directly.
7. Retrieval – Provision for search function for document retrieval based on database management approach using key fields
8. User Interface – Provision of uniform web based UI across multiple platforms and modules of DMS. Also have thick client application for bulk uploading of documents along with indexing and tagging data.
9. Other media archival – Provide unlimited storage on archival media for archiving data and make it available for future use whenever needed.

Upload scanned data to DMS

Approximately One(1) crore need to be indexed and tagged by the SI. The SI shall also upload the existing scanned data along with indexing, tagging and folder structure into the DMS system

implemented. This will ensure that the existing data is stored in a safe and secure way and will be accessible by users once the DMS system is live.

3.10 Disaster Recovery

1. MSI shall propose to host Applications and storage on cloud for complete Data Recovery (DR) operations.
2. MSI should select the Cloud Service Provider from the empanelled vendors of Meity.
3. Below are the key factors to be considered for cloud hosting-
    a) The MSI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security.
    b) The MSI should consider 30% of actual capacity for mission critical application for cloud DR.
    c) The MSI should consider both Infrastructure (storage, compute, backup, network and security) as well as licencing cost while calculating the overall cost of DR.
    d) MSI should be be responsible for cloud security DDOS Migration, Firewall -with WAF enabled, IDS, IPS Monitoring, Domain SSL, Log Manager and 2 security audit per year.
    e) Government Community Cloud should only be used by MSI.
    f) There should be physical and logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers.
    g) The system will be hosted in the site identified by the MSI and as agreed by the RSCDL for DR (backup only).
    h) There should be sufficient capacity (compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the RSCDL) during any unanticipated spikes in the user load.
    i) DR site will be located in India only.
    j) Ensure redundancy at each level
    k) MSI shall provide interoperability support with regards to available APIs, data portability etc. for the RSCDL to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.

l) The MSI is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the MSI.
m) RSCDL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the RSCDL's application. RSCDL retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time
n) Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels
o) Cloud services should be accessible via internet and MPLS.
p) Required Support to be provided to the RSCDL in migration of the VMs, data, content and any other assets to the new environment created by the RSCDL or any Agency (on behalf of the RSCDL) on alternate cloud service provider's offerings to enable successful deployment and running of the RSCDL's solution on the new infrastructure.
q) The MSI should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications
    i. Perform and store data and file backups consisting of an initial full back up with daily incremental backups for files;
    ii. For the files, perform weekly backups;
    iii. For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
    iv. Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.
    v. Retain database backups for thirty (30) days
r) The MSI should offer dashboard to provide visibility into service via dashboard.
s) MSI shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the RSCDL.

Preparation of Disaster Recovery Operational Plan

The bidder should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with Authority during the project kick off.

1. Business as usual: the primary site is functioning as required, procedures for ensuring consistency of data availability at secondary site.
2. Disaster: Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site.
3. Operations from DR site: Ensuring secondary site is addressing the functionality as desired
4. Configure proposed solution for usage

The service provider shall provide DR Management Solution to Authority meeting following specifications:

No.	Features
1	The proposed solution must offer a workflow based management& monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts(including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions
5	The proposed solution should facilitate out-of-the-box, workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication
7	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment

No.	Features
8	The proposed solution must support all major platforms including Linux, Windows, Solaris, HP-UX, and AIX with native high availability options. It must support both physical and virtual platforms
9	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10	The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11	The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned

Periodic Disaster Recovery Plan Update

The service provider shall be responsible for –

- Devising and documenting the DR policy discussed and approved by Authority.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit

3.11 Responsibility Matrix

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
Project Inception Phase										
1	Project Kick Off	R/A	C	C	I	I	I	I	C	I
2	Deployment of manpowe	R/A	C	C	I	I	I	I	C	I

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
	r									
Requirement Phase										
3	Assess the requirement of IT Infrastructure and Non IT Infrastructure	R/A	C	C	C	C	C	C	C	C
4	Assessment of Business processes	R/A	C	C	I	I	I	C	C	I
5	Assessment of requirement of Software requirements	R/A	C	C	I	I	I	C	C	I
6	Assess the Integration	R/A	C	C	C	C	I	C	C	C

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
	requirement									
7	Assess the connectivity requirement all locations (including Building)	R/A	C	C	C	C	C	C	C	I
8	Assessment the Network laying requirement	C	C	C	R/A	I	I	C	C	I
9	Assessment of training requirement	R/A	C	C	I	I	I	C	C	I
Design Phase										
10	Formulation of Solution	R/A	C	C	C	I	I	C	C	I

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
	Architecture									
11	Creation of Detail Drawing	R/A	C	C	C	I	I	C	C	I
12	Detailed Design of Smart City Solutions	R/A	C	C	C	I	I	C	C	I
13	Development of test cases (Unit, System Integration and User Acceptance)	R/A	C	C	C	I	I	C	C	I
14	Preparation of final bill of quantity and material	R/A	C	C	C	C	I	C	C	I
15	SoP	R/A	C	C	C	C	C	C	C	I

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
	preparation									
Development Phase										
16	Helpdesk setup	R/A	C	C	I	I	I	I	C	I
17	Physical Infrastructure setup	R/A	C	C	I	I	I	I	C	I
18	Procurement of Equipment , edge devices, COTS software (if any), Licenses	R/A	C	C	I	I	I	I	C	I
19	IT and Non IT Infrastructure Installation	R/A	C	C	I	I	I	I	C	I
20	Development, Testing	R/A	C	C	I	I	I	I	C	I

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
	and Production environment setup									
21	Software Application customization (if any)	R/A	C	C	I	I	I	I	C	I
22	Development of Bespoke Solution (if any)	R/A	C	C	I	I	I	I	C	I
23	Data Migration	R/A	C	C	I	I	I	I	C	I
24	Integration with Third party services/ applicatio	R/A	C	C	I	I	I	I	C	I

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
	n (if any)									
25	Unit and User Acceptance Testing	R/A	C	C	I	I	I	I	C	I
26	Implementation of Solutions	R/A	C	C	I	I	I	I	C	I
27	Preparation of User Manuals , training curriculum and training materials	R/A	C	C	I	I	I	I	C	I
28	Role based training(s) on the Smart City Solutions	R/A	C	C	I	I	I	I	C	I

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
Integration Phase										
29	SoP implementation	R/A	C	C	C	C	C	C	C	I
30	Integration with GIS	R/A	C	C	C	C	C	C	C	I
31	Integration of solutions with Command and Control Centre	R/A	C	C	C	C	C	C	C	I
Go –Live										
32	Go Live	R/A	C	C	I	I	I	I	C	I
Operation and Maintenance										
33	Operation and Maintenance of IT, Non IT infrastructure and Applicati	R/A	C	C	I	I	I	I	C	I

No.	Key Activities	Successful Bidder	RMC	RSCDL	Network Vendors	Electricity Providers	Other Utilities	Other Departments	PMC	Existing ICT Vendors at RSCDL
	ons									
34	SLA and Performance Monitoring	R/A	C	C	I	I	I	I	C	I
35	Logging, tracking and resolution of issues.	R/A	C	C	I	I	I	I	C	I
36	Application enhancement	R/A	C	C	I	I	I	I	C	I
37	Patch & Version Updates	R/A	C	C	I	I	I	I	C	I
38	Helpdesk services	R/A	C	C	I	I	I	I	C	I

Note: All decisions will be taken by RSCDLRSCDL which will be abided by all the stakeholders in the above matrix.

- R/A = Responsible/Accountable
- C = Consulted
- I = Informed

3.12 Project Deliverables

3.12.1 ICCC, DC, ITITMS, Smart Parking

No.	Key Activities	Deliverables
1	Project Kick Off	1. Project Plan 2. Risk Management and Mitigation Plan
2	Deployment of manpower	
3	Assess the requirement of IT Infrastructure and Non IT Infrastructure	1. Functional Requirement Specification document 2. System Requirement Specification document 3. Requirements Traceability Matrix 4. Site Survey Report
4	Assessment of Business processes	
5	Assessment of requirement of Software requirements	
6	Assess the Integration requirement	
7	Assess the connectivity requirement all locations (including Building)	
8	Assessment of network laying requirement	
9	Assessment of training requirement	
10	Formulation of Solution Architecture	1. Final Bill of Quantity 2. HLD documents 3. LLD documents 4. Application architecture documents. 5. Technical Architecture documents. 6. Network Architecture documents. 7. ER diagrams and other data modeling documents. 8. Logical and physical database design. 9. Data dictionary and data definitions. 10. GUI design (screen design, navigation, etc.). 11. Test Plans
11	Creation of Detail Drawing	
12	Detailed Design of Smart City Solutions	
13	Development of test cases (Unit, System Integration and User Acceptance)	
14	Preparation of final bill of quantity and material	
15	SoP preparation	

		12. SoPs 13. Change management Plan
16	Helpdesk setup	1. IT and Non IT Infrastructure Installation Report 2. Completion of UAT and closure of observations report 3. Training Completion report 4. Application deployment and configuration report
17	Physical Infrastructure setup	
18	Procurement of Equipment , edge devices, COTS software (if any), Licenses	
19	IT and Non IT Infrastructure Installation	
20	Development, Testing and Production environment setup	
21	Software Application customization (if any)	
22	Development of Bespoke Solution (if any)	
23	Data Migration	
24	Integration with Third party services/application (if any)	
25	Unit and User Acceptance Testing	
26	Implementation of Solutions	
27	Preparation of User Manuals , training curriculum and training materials	
28	Role based training(s) on the Smart City Solutions	
29	SoP implementation	1. Integration Testing Report
30	Integration with Smart Components	
31	Integration of solutions with Command and Control Centre	
32	Go Live	1. Go-Live Report
33	Operation and Maintenance of IT, Non IT infrastructure and Applications	1. Detailed plan for monitoring of SLAs and performance of the overall system

34	SLA and Performance Monitoring	2. Fortnightly Progress Report 3. Monthly SLA Monitoring Report and Exception Report 4. Quarterly security Report 5. Issues logging and resolution report
35	Logging, tracking and resolution of issues.	
36	Application enhancement	
37	Patch & Version Updates	
38	Helpdesk services	

3.12.2 Enterprise GIS

Sr. No.	Item	Completion Milestone (Weeks)	Deliverables
1	Delivery & Installation of Servers & GIS platform	T+4	1) Hosting Infrastructure requirements and GIS platform in accordance with functional and technical requirements and service levels 2) Installation and Commissioning Reports
2	Post Processing of Satellite Imagery	T+6	QA/QC
3	Data Model Finalization	T+6	1) ER Diagram and Data Flow Diagram 2) High Level Design Document and Low Level Design Document
4	Final Digitized Base Map	T+12	QA/QC of Base Map

Sr. No.	Item	Completion Milestone (Weeks)	Deliverables
5	System Requirement Specifications	T+13	SRS and FRS documents
6	GIS Application Suite (web based) with Citizen portal development first UAT	T+19	Test Plan, Test cases, Test logs, User sign off
7	Successful Testing of the Customized GIS Application suite with citizen portal	T+21	Test logs, User sign off
8	Complete survey, mosaicking and superimposition of 50% of the total TP schemes	T+21	Updated Mosaicked image
9	Submission of System Documentation & User Documentation	T+25	System Documents and User Documents
10	Training	T+29	Feedback from RSCDL officials
11	Complete survey, mosaicking and superimposition of remaining 50% of the total TP schemes	T+31	Updated Mosaicked image
12	Project Completion Certificate by RSCDL (After completion of Enterprise GIS, Geotagging of Properties and Underground Utilities Survey)	T+50	Completion Certificate by RSCDL

3.12.3 Enterprise Resource Planning

The table below mentions the deliverables and timelines for the project. SI needs to strictly adhere to the timelines mentioned in the table below. If the SI fails to offer the deliverables within the specified timelines as mentioned below, client shall, without prejudice to its other remedies under the contract, deduct from the performance bank guarantee or future payments to be made, as liquidated damages.However, if the cumulative delay is more than 45 days, client has the right to terminate the contract and forfeit the performance bank guarantee

PHASE	ACTIVITIES		COMPLETION MILESTONES
PHASE I	Establishment and Go-Live of the solution		To+54 weeks
	A	Project planning and mobilization	To + 6 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Project Schedule	
	ii	Project Initiation Report	
	iii	Progress Reports	
	iv	Risk Register	
	v	Issue Register	
	vi	Stakeholder Register	
	vii	CVs of implementation team	
	B	Requirement Gathering	To + 18 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Functional Requirement Specification (FRS)	
	ii	Software Requirement Specification (SRS) and get it approved from client	
	ii	Data integration requirements	

PHASE	ACTIVITIES		COMPLETION MILESTONES
	i		
	iv	Requirement Traceability Matrix	
	v	Gap Assessment Report	
	C	Solution Design	To + 24 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Solution Design and Architecture Document (including ER Diagram and Data Flow Diagram)	
	ii	High Level Design Document and Low Level Design Document (including Schema Diagram)	
	iii	User Interface and Prototypes	
	iv	Data Modelling	
	v	User Reports	
	vi	Hosting Infrastructure requirements in accordance with functional and technical requirements and service levels	
	vii	Policy, Plan and Methodology Documents covering aspects mentioned above	
	D	Provisioning of hosting Infrastructure and Client Site Infrastructure	To + 28 weeks
		ACTIVITIES AND DELIVERABLES	

PHASE	ACTIVITIES		COMPLETION MILESTONES
	i	Installation and Commissioning Report	
	ii	Deployment Architecture	
	iii	Standard Operating Procedures	
	iv	DC & DRC Infrastructure Dashboard	
	v	Devise a Replication-and-Restore policy	
	vi	Managing the storage of back-up media in a safe and secure manner during the warranty and maintenance period	
	vii	Preparation of Business Continuity Plan (BCP)/Disaster Recovery (DR) Plan	
	viii	Drill Exercise (including roll back) and improvement in BCP	
	E	Software Customization	To + 38 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Supply, Customization, Configuration and Installation of Software	
	ii	Workflow Management	
	iii	Installation guides	
	iv	Standard Operating Procedures	

PHASE	ACTIVITIES		COMPLETION MILESTONES
	v	Manuals and Guidelines such as Operational manual, Technical manuals, Library Files, Setup Programs, etc.	
	F	Testing and UAT	To + 42 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Test plan	
	ii	Test cases	
	iii	Test Data	
	iv	Testing reports and Bug reports	
	v	Necessary modification in software for defects identified during the testing and Bug Closure Report	
	G	Supply of licenses	To + 42 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Supply of licenses pertaining to solution	
	ii	Submission of undertaking mentioning supply of licenses	
	H	Capacity building and training	To + 46 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Training Calendar and Curriculum	
	ii	Training Material, Training Manuals, Troubleshooting Manuals, etc.	
	iii	Training Sessions, Questionnaire and Evaluation Results	

PHASE	ACTIVITIES		COMPLETION MILESTONES
	I	Third party audit and Go-Live of the solution	To + 50 weeks
		ACTIVITIES AND DELIVERABLES	
	i	First Round Audit Report (by Auditor)	
	ii	Rectified solution and submission of next round of audit (by SI)	
	iii	Next Round Audit Report (by Auditor)	
	iv	If required, rectified solution and submission of next round of audit (by SI)	
	v	Compliance Confirmation by the Auditor (by the Auditor)	
	vi	Business readiness check before handing over to user	
	vii	Exit Management and Knowledge Transfer Plan	
	viii	Mobilization of manpower for hand holding support	
	ix	Data Migration to solution	
	x	Approval from client	
	J	Preparation of standard operating procedures	To + 54 weeks
		ACTIVITIES AND DELIVERABLES	
	i	SOP	
	ii	Risk mitigation strategy	
	K	Solution Stabilization (for 3	T_g + 3 months

PHASE	ACTIVITIES		COMPLETION MILESTONES
		months post go-live)	
		ACTIVITIES AND DELIVERABLES	
	i	End user transaction reports	
	ii	Issue logs and RCA document for issues raised during solution stabilization	
	iii	O&M team sign off on knowledge transfer received along with above two documents.	
PHASE II	Operation and Maintenance		T_g + 5 years
	A	User Handholding (functional)	As and when required
	B	Refresher Training	At the end of every year
	C	Periodic Audits	In case of any major change or annually, whichever is earlier
	D	Helpdesk Support	
	E	Ongoing scanning, indexing, digitization and uploading of documents	
	F	Business Continuity Support	
		ACTIVITIES AND DELIVERABLES	
	i	Regular Drill Exercises at pre-decided frequencies (tentatively quarterly) and improvement in BCP	
	ii	Assist in bringing up as well as rolling back the solution in case of any systems failure in consonance with the BCP approved by client.	
	G	Monitoring and Maintenance	

PHASE	ACTIVITIES		COMPLETION MILESTONES
	H	Miscellaneous Operations	
	J	Exit Management and Knowledge Transfer	
	K	Post Go-Live Support	

Note:

a) 'To' refers to the date of issuance of LOI to the SI

b) 'Tg' refers to the date of Go-Live of the project

3.13 System Acceptance

The SI will develop acceptance test procedures and the same will need to be approved by relevant stake holders of RSCDL. The purpose of this acceptance is to ensure conformance to the required process operations response time, the integrity of the application after installation, and to eliminate any operational bugs.

This will include:

1. Fine tuning of the application, ensuring all required related component software are installed and any debugging required.
2. The acceptance tests will be carried out before Go-Live at site.

At the satisfactory conclusion of these Acceptance tests to the satisfaction of RSCDL, the implementation of the application shall be considered to be complete however if any bugs/errors is reported by RSCDL, the SI shall be responsible for taking the corrective action immediately.

3.14 Cutover and Go-Live

The scope of Cut over would be for each of the core and support processes. The Cutover Strategy needs to detail the sequence of activities required to achieve this and propose drawing up of a schedule for the tasks, dates, data conversion and the upload of the necessary balances and open items into the system before Go Live.

The key requirements for cut over are as follows:

1. The Cut over plan should detail the strategy by which the data will be uploaded for the different sites and the nature and volume of backlog transactions. Specified forms/formats/templates to put the data in.
2. It should detail the Data elements and open item strategy logic used for planning cut over before go-live.
3. It should describe the various pre requisites and assumptions used for each of the data elements before uploading in the live system.
4. It should detail the various business decisions to be taken collaboratively by RSCDL and SI for finalizing the cut over strategy.

RSCDL will consider Go-Live date of the system once "Certificate of System Acceptance" is provided to SI. RSCDL shall provide the certificate on following acceptance criteria:

1. The SI is required to undertake the following to review readiness for "Go Live":
   a) Facilitate in setting up central help desk for any queries
   b) Review the usage and performance of the system till it stabilizes
   c) Ensuring resolution / Documentation of all issues raised during implementation
   d) Final configuration/ integration, volume and stress testing
   e) Switch over to production environment.

2. Declaration of "Go Live" – the system will be declared "Go Live" when the following tasks/activities are accomplished satisfactorily
   a) Acceptance testing
   b) Installation and commissioning of Hardware
   c) Data migration
   d) Training
   e) User creation / role identification

The Final Go Live will be after go live is achieved foreach of the smart solutions proposed as part of the scope of the RFP completing the following:

3. User Adoption Support: The SI shall provide User adoption support, by deputing technical and functional consultants at the client site after implementation of system at that site. During the Implementation period prior to "Go Live", the SI shall support RSCDL users in using the system.
4. Final Go live: The system will be declared Final go live when the following tasks are accomplished
   a) Stabilization period after all smart solutions have achieved go live

3.15 Post Go-Live Stabilization Support

The SI shall provide post Go-Live support, as part of this scope; by continuing the deployment of the same technical and functional consultants at site for full three months after implementation and Go-Live. During the stabilization period the SI would help RSCDL users to correct any errors/bugs incurred while executing transactions, generating reports, handholding for one financial quarter closure. The SI will update the user manuals and configuration manuals accordingly.

3.16 Implementation Approach and Project Timelines

The overall implementation of the system is envisaged to be completed in with multiple timelines. The entire implementation would consist of various smart system software and customization to meet the requirements of RSCDL. Implementation is expected to be completed within X months from the date of signing of agreement with the SI.

Project Management Plan

The SI is expected to follow the schedule as mentioned. Each of the milestones should be accompanied with a presentation on the deliverables by the SI, related to that milestone. The submission of deliverable will be deemed complete after the submission of the hard / soft copy of the deliverable and the presentation by the SI.

The "Expected Date of Completion" as mentioned in the table above is the date by which the deliverable shall be submitted to RSCDL. The SI shall ensure that the deliverable is accepted by RSCDL as per schedule mentioned in the table above post review.

The SI shall follow prudent project management practices commensurate with the best international standards during the course of the project implementation. While the actual process of application customization will remain an internal activity of the SI, it is important that RSCDL or their nominated agencies shall have adequate visibility into such processes.

The following are some of the major guidelines to be kept in mind for Project Management.

1. **Scope Management:** The requirements in general and the customization requirement in particular, shall be collected and documented clearly. The scope and requirements shall be controlled against a baseline and any changes shall be communicated to RSCDL and documented.
2. **Time Management:** The SI shall prepare a detailed project schedule conforming to the stake-holder expectations and exercise stringent control of the schedule. A periodic report on the progress and deviations should be shared with RSCDL. Any schedule conflicts with respect to project and/or deliverable timelines will have to be resolved by SI in consultation with RSCDL and/or its nominated agencies and approved by RSCDL.

Thereafter the approved timelines will have to be adhered to by the SI, unless specified otherwise.

3. **Quality Assurance and Quality Control:** A detailed Quality Assurance Plan shall be prepared and shared with RSCDL. The same shall be monitored and SI shall share a periodic report on the quality activities. These shall include:
   a) Architecture and Design Review Reports
   b) Test Plans Review Reports
   c) Test Execution Review Reports
4. **Project Risk management:** The SI shall document the risks during implementation and share the same with RSCDL. This shall be periodically reviewed and shared with RSCDL. A report on the periodic risk analysis, risk responses planned, mitigation strategies executed shall be shared with RSCDL.

The SI shall store all the Project Management and Delivery artifacts into a secure configuration database and give access to RSCDL for view purposes. During the O&M period, any change requests and enhancements to the software shall be similarly documented so as to create a comprehensive repository of all artifacts relevant to RSCDL stakeholders. This will serve as a valuable knowledge input during Exit Management and also for any statutory audit.

3.16.1 ICCC, DC, ITITMS & Smart Parking

Services	Approximate Time for Issuance of Request Order	Tentative Scope/ Approximate Sizing	Tentative Lead Time
Request Order 1 (for RSCDL)	One week post issue of LOI/ completion of site survey activity	Command and Control Center (ICCC) IT hardware Command and Control Center (ICCC) non-IT equipment Command and Control Center (ICCC) – software Smart DC – Hardware Smart DC – Software Smart DC – non-IT equipment Smart Disaster Recovery (DR)	6 months post issuance of request order

Services	Approximate Time for Issuance of Request Order	Tentative Scope/ Approximate Sizing	Tentative Lead Time
		Implementation and Integration of Public address System Integration with existing eye-way solution	
Request Order 2	6months post issuance of LOI	Implementation and Integration of Intelligent Traffic Management Implementation and Integration of Integrated Transport Management Partial Integration of Smart Governance (City Level Application Platform + ERP) Integration with City wide - GIS Platform Integration with Smart Card for Transport Integration with Solid Waste Management Integration with Smart Parking Integration with Sewerage (SCADA at treatment plant) Integration with Health Solution	6 months post issuance of Work Order

Services	Approximate Time for Issuance of Request Order	Tentative Scope/ Approximate Sizing	Tentative Lead Time
Request Order 3	12 months post issuance of LOI	Integration of ICT solution for Education Integration with Disaster /Emergency Management Integration with Smart Metering & SCADA for distribution network (water) Integration with Water leak identification system Migration of interim ICCC to ICCC	6 months post issuance of request order

3.16.2 Enterprise GIS

SI is required to adhere to the following timelines (T is the date of Work Order / PO / Letter of intent from RSCDL)

Below mentioned is the timeline for Enterprise GIS scope of the project.

Sr. No.	Item	Completion Milestone (Weeks)
1	Delivery & Installation of Servers & GIS platform	T+4
2	Post Processing of Satellite Imagery	T+6
3	Data Model Finalization	T+6
4	Final Digitized Base Map	T+12

5	System Requirement Specifications	T+13
6	GIS Application Suite (web based) with Citizen portal development first UAT	T+19
7	Successful Testing of the Customized GIS Application suite with citizen portal	T+21
8	Complete survey, mosaicking and superimposition of 50% of the total TP schemes	T+21
9	Submission of System Documentation & User Documentation	T+25
10	Training	T+29
11	Complete survey, mosaicking and superimposition of 50% of the total TP schemes	T+31
12	Project Completion Certificate by RSCDL	T+33

The below mentioned are the timelines for the GPR survey.

Sr. No.	**Description**	**Timelines in weeks (T=T0+12,Completion of Final Digitized Base Map, T0=Date of Issuance of WO)**
1	On provisional acceptance of surveyed data for 1/3rd of kms surveyed in the given period	T+ 12
2	On provisional acceptance of surveyed data for next 1/3rd of kms surveyed in the given period	T+ 24
3	On provisional acceptance of surveyed data for next 1/3rd of kms surveyed in the given period	T+36

The below mentioned are the timelines for the Geo enabled Property Tax Tagging survey.

Sr. No	Activities/Deliverables	Milestone Description	Timelines in weeks (T=T0+12,Completion of Final Digitized Base Map, T0=Date of Issuance of WO)
.	Development of Geo-enabled survey mobile app	Tested and verified mobile app ready for on field survey	T+4
.	Earmarking of the required manpower by the survey agencies (SA)	1-2 weeks from the date of project awarding	T+6
.	Work schedule with resources deployment plan	6 months consolidated plan to be submitted before the start of the project Detailed monthly plan containing the details about deployment of field survey team to be submitted to RSCDL, 7 days before the start of the following month	T+7
4.	20% of Total Properties in assigned Zone with Monthly Report	Tagging, Validation and Notice Generation/ Acknowledgement, Validation plan	T+10
5.	40% of Total Properties in assigned Zone with Monthly Report	Tagging, Validation and Notice Generation/ Acknowledgement, Validation per plan	T+13
6.	60% of Total Properties in assigned Zone with Monthly Report	Tagging, Validation and Notice Generation/ Acknowledgement, Validation as per plan	T+16
	80% of Total Properties in assigned Zone with Monthly Report	Tagging, Validation and Notice Generation/	T+19

.		Acknowledgement, Validation as per plan	
.	100% of Total Properties in assigned Zone with Monthly Report	Tagging, Validation and Notice Generation/ Acknowledgement, Validation as per plan	T+22
.	Final Validation and Sign off		T+25

3.16.3 Enterprise Resource Planning

The table below mentions the deliverables and timelines for the project. SI needs to strictly adhere to the timelines mentioned in the table below. If the SI fails to offer the deliverables within the specified timelines as mentioned below, client shall, without prejudice to its other remedies under the contract, deduct from the performance bank guarantee or future payments to be made, as liquidated damages.However, if the cumulative delay is more than 45 days, client has the right to terminate the contract and forfeit the performance bank guarantee

PHASE	ACTIVITIES		COMPLETION MILESTONES
PHASE I	Establishment and Go-Live of the solution		To+54 weeks
	A	Project planning and mobilization	To + 6 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Project Schedule	
	ii	Project Initiation Report	
	iii	Progress Reports	
	iv	Risk Register	

PHASE		ACTIVITIES	COMPLETION MILESTONES
	v	Issue Register	
	vi	Stakeholder Register	
	vii	CVs of implementation team	
	B	Requirement Gathering	To + 18 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Functional Requirement Specification (FRS)	
	ii	Software Requirement Specification (SRS) and get it approved from client	
	iii	Data integration requirements	
	iv	Requirement Traceability Matrix	
	v	Gap Assessment Report	
	C	Solution Design	To + 24 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Solution Design and Architecture Document (including ER Diagram and Data Flow Diagram)	
	ii	High Level Design Document and Low Level Design Document (including Schema Diagram)	
	iii	User Interface and Prototypes	
	i	Data Modelling	

PHASE		ACTIVITIES	COMPLETION MILESTONES
	v		
	v	User Reports	
	vi	Hosting Infrastructure requirements in accordance with functional and technical requirements and service levels	
	vii	Policy, Plan and Methodology Documents covering aspects mentioned above	
	D	Provisioning of hosting Infrastructure and Client Site Infrastructure	To + 28 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Installation and Commissioning Report	
	ii	Deployment Architecture	
	iii	Standard Operating Procedures	
	iv	DC & DRC Infrastructure Dashboard	
	v	Devise a Replication-and-Restore policy	
	vi	Managing the storage of back-up media in a safe and secure manner during the warranty and maintenance period	
	vii	Preparation of Business Continuity Plan (BCP)/Disaster	

PHASE		ACTIVITIES	COMPLETION MILESTONES
		Recovery (DR) Plan	
	viii	Drill Exercise (including roll back) and improvement in BCP	
	E	Software Customization	To + 38 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Supply, Customization, Configuration and Installation of Software	
	ii	Workflow Management	
	iii	Installation guides	
	iv	Standard Operating Procedures	
	v	Manuals and Guidelines such as Operational manual, Technical manuals, Library Files, Setup Programs, etc.	
	F	Testing and UAT	To + 42 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Test plan	
	ii	Test cases	
	iii	Test Data	
	iv	Testing reports and Bug reports	
	v	Necessary modification in software for defects identified during the testing and Bug Closure Report	
	G	Supply of licenses	To + 42 weeks

PHASE		ACTIVITIES	COMPLETION MILESTONES
		ACTIVITIES AND DELIVERABLES	
	i	Supply of licenses pertaining to solution	
	ii	Submission of undertaking mentioning supply of licenses	
	H	Capacity building and training	To + 46 weeks
		ACTIVITIES AND DELIVERABLES	
	i	Training Calendar and Curriculum	
	ii	Training Material, Training Manuals, Troubleshooting Manuals, etc.	
	iii	Training Sessions, Questionnaire and Evaluation Results	
	I	Third party audit and Go-Live of the solution	To + 50 weeks
		ACTIVITIES AND DELIVERABLES	
	i	First Round Audit Report (by Auditor)	
	ii	Rectified solution and submission of next round of audit (by SI)	
	iii	Next Round Audit Report (by Auditor)	
	iv	If required, rectified solution and submission of next round of audit (by SI)	
	v	Compliance Confirmation by the Auditor (by the Auditor)	
	vi	Business readiness check before handing over to user	

PHASE		ACTIVITIES	COMPLETION MILESTONES
	v ii	Exit Management and Knowledge Transfer Plan	
	v iii	Mobilization of manpower for hand holding support	
	i x	Data Migration to solution	
	x	Approval from client	
	J	Preparation of standard operating procedures	To + 54 weeks
		ACTIVITIES AND DELIVERABLES	
	i	SOP	
	ii	Risk mitigation strategy	
	K	Solution Stabilization (for 3 months post go-live)	T_g + 3 months
		ACTIVITIES AND DELIVERABLES	
	i	End user transaction reports	
	ii	Issue logs and RCA document for issues raised during solution stabilization	
	ii i	O&M team sign off on knowledge transfer received along with above two documents.	
PHASE II	Operation and Maintenance		T_g + 5 years
	A	User Handholding (functional)	As and when required
	B	Refresher Training	At the end of every year
	C	Periodic Audits	In case of any major change or annually, whichever is earlier
	D	Helpdesk Support	

PHASE		ACTIVITIES	COMPLETION MILESTONES
	E	Ongoing scanning, indexing, digitization and uploading of documents	
	F	Business Continuity Support	
		ACTIVITIES AND DELIVERABLES	
	i	Regular Drill Exercises at pre-decided frequencies (tentatively quarterly) and improvement in BCP	
	ii	Assist in bringing up as well as rolling back the solution in case of any systems failure in consonance with the BCP approved by client.	
	G	Monitoring and Maintenance	
	H	Miscellaneous Operations	
	J	Exit Management and Knowledge Transfer	
	K	Post Go-Live Support	

Note:

c) 'To' refers to the date of issuance of LOI to the SI

d) 'Tg' refers to the date of Go-Live of the project

4. Annexure I- Functional Requirements & Technical Specifications

4.1 Intelligent Traffic Management

4.1.1 Adaptive Traffic Control System (ATCS)

4.1.1.1 Functional Requirement - Adaptive Traffic Control System

No.	Building Blocks	Bidder Compliance(Yes/No)
1	Traffic Signal Controller	
2	Vehicle Detectors	
3	Communication Network	
4	Software Application	

4.1.1.2 Functional Requirement -Traffic Signal Controller

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
1	**Make**	<to be provided by the bidder>	
2	**Model**	<to be provided by the bidder>	
3	The Traffic Signal Controller equipment is a 32 bit or 64 bit microcontroller with solid state traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases and junction groups. The controller will ideally have a conflict monitoring facility to ensure that conflicting, dangerous are pre-flagged at the programming stage and these are disallowed even during manual override phase.		
4	The Traffic Signal Controller will be adaptive so that it can be controlled through the central traffic control center as an individual junction or as part of group of traffic junctions along a corridor or a region. The signal controller design must be flexible for the junction could be easily configured to be part of any corridor or group definition and could be changed through central command controller easily		
5	Site specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through keypad or laptop. A minimum of 512KB flash memory and 128KB RAM shall be provided. Volatile memory shall not be used for storing the junction specific plans or signal timings.		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
6	All timings generated within a traffic signal controller shall be digitally derived from a crystal clock which shall be accurate to plus or minus 100 milliseconds.		
7	The controller shall provide a real time clock (RTC) with battery backup that set and update the time, date and day of the week from the GPS. The RTC shall have minimum of 10 years battery backup with maximum time tolerance of +/- 2 sec per day.		
8	The controller shall have the facility to update the RTC time from ATCS server, GPS and through manual entry.		
9	The traffic signal system including controller shall have provision for audio output tones and should be disabled friendly.		
10	The controller shall be capable of communicating with the ATCS server through Ethernet on a managed leased line network or any other appropriate stable communication network.		

A) Police Panel

The controller shall provide the following facilities in a separate panel with provision for lock and key arrangements for use by the Traffic Police.

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
1	Four Hurry Call switches: The Hurry Call mode will provide the means to force the controller to a defined stage, without violating safety clearances. A preemption input may be used to demand the Hurry Call mode to give right of way to emergency vehicles. It should be possible to configure the Hurry Call switches to any stage as per site requirements.		
2	One Forced Flash Switch: Activation of this switch should force the signal to Flashing Amber / Flashing Red.		
3	One Auto / Manual Switch: Activation of this switch should enable manual operation of the controller. Deactivation of the manual switch shall continue from the current stage without interruption.		
4	One Manual Advance Pushbutton Switch: In manual operation mode, the stages appear in the sequence specified in the signal plan timetable. Activating the pushbutton switch shall terminate the currently running stage and start the next, without violating safety clearances.		
5	One Junction OFF Switch: Activating this switch should put OFF all signal lamps. On deactivation of the switch the traffic signal controller shall resume its normal operation without violating any safety clearances.		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference

B) Modes of Operation

The traffic signal controller shall have the following modes of operation:

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
1	Fixed Time: In fixed time (pre-timed) mode the traffic signal controller shall execute stage timings according to the site specific timetable maintained in the traffic signal controller FLASH memory. Inputs from vehicle detectors shall be ignored in this mode and no preemption shall be made on any stage. Cycle time remains constant in every cycle execution for a given time period.		
2	Vehicle Actuation with All Stages Preemption: In the vehicle actuation with all stages preemption mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. Preemption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.		
3	Semi-Actuation: In the semi-actuation mode, the traffic signal controller shall execute stage		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
	timings in the vehicle actuated stages as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. All other stages shall execute the Maximum green time configured for the stage. Preemption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.		
4	Stage Skipping: The traffic signal controller shall not execute the stage enabled for skipping when there is no vehicle demand registered for the stage till clearance amber time of the previous stage.		
5	Transit Signal Priority (TSP) for BRT buses: The traffic signal controller shall provide transit signal priority for buses in dedicated lane to ensure minimum stop delay at the intersection, without violating safety clearances.		
6	Vehicle Actuation with Fixed Cycle length: In vehicle actuation with fixed cycle length mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time shall be maintained constant during a given timeslot. Preemption for all demand actuated stages except for Priority Stage shall be possible.		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
7	Full ATCS (FATCS): In FATCS mode, the traffic signal controller shall execute stage timings as per demand within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time specified by the Central Computer during every cycle switching. Preemption for all demand actuated stages except Priority Stage shall be possible in this mode. The traffic signal controller shall identify a communication failure with the central computer within a specified time period. In such an event the signal plan timings shall be executed from the local timetable stored in the traffic signal controller FLASH memory. Fallback mode of the traffic signal controller shall be vehicle actuated. On restoration of the communication with central computer the traffic signal controller shall automatically resort to FATCS mode. The traffic signal controller shall accept commands for remote selection / de-selection of the following from the Central Computer at Interim ICCC/ICCC. Hurry Call Flashing Amber / Flashing Red Junction Off If not reverted to the normal operation within the time period listed below, the traffic signal controllers shall timeout the commands and		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
	operate normally Hurry Call – 5 Minutes Flashing Amber / Flashing Red – 30 Minutes Junction Off – 30 Minutes The traffic signal controller shall report the following to the Central Computer through the communication network every cycle or on an event as appropriate. Green time actually exercised for each approach (stage preemption timing) against the Green running period set for the approach by the Central Computer Mode of Operation Lamp failure, if any Output short circuit, if any Detector failure, if any		

C) Traffic Signal Controller Operating Parameters

Phases - The controller shall have facility to configure 32 Phases either for vehicular movement, filter green, indicative green, pedestrian movement or a combination thereof.

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
1	It shall be possible to operate the filter green (turning right signal) along with a		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
	vehicular phase. The filter green signal shall flash for a time period equal to the clearance amber period at timeout when operated with a vehicular phase.		
2	The pedestrian phase signal shall be configured for flashing red or flashing green aspect during pedestrian clearance.		
3	It shall be possible to configure any phase to the given lamp numbers at the site.		
4	Stages – The controller shall have facility to configure 32 Stages		
5	Cycle Plans – The controller shall have facility to configure 24 Cycle Plans and the Amber Flashing / Red Flashing plan. It shall be possible to define different stage switching sequences in different cycle plans. The controller shall have the capability for a minimum of 32 cycle-switching per day in fixed mode of operation.		
6	Day Plans – The controller shall have facility to configure each day of the week with different day plans. It shall also be possible to set any of the day plans to any day of the week. The controller shall have the capability to configure 20 day plans.		
7	Special Day Plans – The controller shall have facility to configure a minimum of 20 days as special days in a calendar year.		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
8	Starting Amber – During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. Facility shall be available to configure the time period of Starting Amber within the given limits at the site.		
9	Inter-green – Normally the inter-green period formed by the clearance Amber and Red extension period will be common for all stages. However, the controller shall have a facility to program individual inter-green period from 3 Seconds to 10 Seconds.		
10	Minimum Green – The controller shall allow programming the Minimum Green period from 5 Seconds to 10 Seconds without violating the safety clearances. It should not be possible to preempt the Minimum Green once the stage start commencing execution.		
11	All Red – Immediately after the Starting Amber all the approaches should be given red signal for a few seconds before allowing any right of way, as a safety measure. The controller shall have programmability of 3 Seconds to 10 Seconds for All Red signal.		
12	Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
	status		
13	Green – Green Conflict Monitoring – The controller shall have a facility to list all conflicting phases at an intersection. The controller should not allow programming of these conflicting phases in a Stage. A hardware failure leading to a conflict condition (due to faulty devices or short circuit in the output) shall force the signal into Flashing Amber / Flashing Red.		
14	Cable less Synchronization – It shall be possible to synchronize the traffic signal controllers installed in a corridor in the following modes of operation, without physically linking them and without communication network. GPS enabled RTC shall be the reference for the cable less synchronization.		
15	Fixed Time mode with fixed offsets		
16	Vehicle Actuated mode with fixed offsets		

D) Input and Output facilities

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
1	Lamp Switching: The controller shall have maximum 64 individual output for signal lamp switching, configurable from 16 to 32 lamps. The signal lamps shall be operating on appropriate DC/AC voltage of applicable rating		
2	Detector Interface: A minimum of 16 vehicle detector inputs shall be available in the controller. All detector inputs shall be optically isolated and provided with LED indication for detection of vehicle.		
3	Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server		
4	Power Saving: The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions thereby saving energy.		
5	Real-time Clock (RTC): The GPS receiver for updating time, date and day of the week information of the traffic signal controller should be an integral part of the traffic signal controller.		
6	The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals.		
7	Manual entry for date, time and day of week		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
	shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).		
8	It shall be possible to set the RTC from the Central Server when networked		
9	Keypad (optional): The traffic signal controller shall have a custom made keypad or should have provision for plan upload and download using PC/laptop/Central Server		
10	Operator Display (optional): The traffic signal controller shall optionally have a LCD backlit Liquid Crystal Display (LCD) as the operator interface.		

4.1.1.3 Functional Requirement -Camera based Vehicle Detector

The detector equipment is a separate logic unit, which may be integrated into the controller, or alternatively mounted in its own housing. The outputs of the detectors indicate the presence of vehicles and are used to influence the operation of the traffic signal controller and shall generate counts, demands and extensions for right-of-way. Means shall be provided so that a detector may be connected to demand and / or extend a phase movement as specified.

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
1	**Make**	<to be provided by the bidder>	
2	**Model**	<to be provided by the bidder>	
3	The contractor shall clearly specify the placement of the detector (upstream,		

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
	downstream, stop-line, exit etc.) for independent straight and right turn signals.		
4	The detector shall be able to count vehicles in non-lane based mixed traffic flow conditions. The accuracy of counts shall be bigger than 90% over all light and weather conditions. The contractor shall clearly specify how this is accomplished.		
5	The contractor shall give an estimate of the total number of vehicle presence detection zones and vehicle detectors required and the type of detection system recommended.		
6	A detector that does not change its status at least once during a stage execution shall be notified to the Central Computer (in ATCS mode) at the termination of the associated stage.		

4.1.1.4 Functional Requirement -Countdown Timer

Countdown Timer shall be installed at each traffic junction under ITMS & City Surveillance System Project.

No.	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
1	**Make**	<to be provided by the bidder>	
2	**Model**	<to be provided by the bidder>	
3	Count Down Timer to be configured in Vehicular Mode.		
4	The Vehicular countdown timer should be dual color,		

	• Red for Stop or STP • Green color for Go
5	There should be alternate Red and Balance phase time for STOP or STP in Flashing
6	Alternate Green and Balance Phase Time for Go in Flashing

4.1.1.5 Functional Requirement -Communication Network

Function of the Communication network is for remote monitoring of the intersection and its management. Real time data (like RTC time, stage timing, mode, events, etc.) from the traffic signal controller is required to be sent to the Central Computer in Interim ICCC/ICCC. Central Computer running the ATCS application shall calculate and send optimum signal timings to all intersections in the corridor. The contractor shall clearly specify the bandwidth requirements and the type of network recommended for the ATCS.

The contractor shall specify the networking hardware requirements at the Interim ICCC/ICCC and remote intersections for establishing the communication network.

4.1.1.6 Functional Requirement -ATCS Software Application

Objective of the ATCS is to minimize the stops and delays in a road network to decrease the travel time with the help of state-of-the-art technology. The adaptive traffic control system shall operate in real time with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it. These calculations will be based up on assessments carried out by the ATCS application software running on a Central Computer based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system.

The ATCS application software shall do the following:

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	Identify the critical junction of a corridor or a region based on maximum traffic demand and saturation.		
4.	The critical junction cycle time shall be used as the group cycle time i.e. cycle time common to all intersection in that corridor or region.		
5.	Stage optimization to the best level of service shall be carried out based on the traffic demand.		
6.	Cycle optimization shall be carried out by increasing or decreasing the common corridor cycle time based on the traffic demand within the constraints of Minimum and Maximum designed value of cycle time.		
7.	Offset correction shall be carried out to minimize number of stops and delays along the corridor for the priority route. Offset deviation measured using distance and speed between successive intersections shall be corrected within 5 cycles at a tolerance of +/- 5 seconds maximum.		
8.	The system shall have provision to configure priority for upstream signals as default. The ATCS software shall continuously check the traffic demand for upstream and		

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	downstream traffic and automatically assign the priority route to the higher demand direction.		
9.	Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand		
10.	Propose timing plans to every intersection under the ATCS in every Cycle		
11.	Verify the effectiveness of the proposed timing plans in every cycle		
12.	Identify Priority routes		
13.	Synchronize traffic in the Priority routes		
14.	Manage and maintain communication with traffic signal controllers under ATCS		
15.	Maintain database for time plan execution and system performance		
16.	Maintain error logs and system logs		
17.	Generate Reports on request		
18.	Graphically present signal plan execution and traffic flow at the intersection on desktop		
19.	Graphically present time-space diagram for selected corridors on desktop		
20.	Graphically present network status on desktop		
21.	Make available the network status and report viewing on Web		
22.	The ATCS shall generate standard and		

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	custom reports for planning and analysis		
23.	It shall be possible to interface the ATCS with a popular microscopic traffic flow simulation software for pre and post implementation analysis and study of the proposed ATCS control strategy		
24.	Shall have the ability to predict, forecast and smartly manage the traffic pattern across the signals over the next few minutes, hours or 3-5 days and just in the current real time.		
25.	Shall provide a decision support tool for assessing strategies to minimize congestion, delays and emergency response time to events via simulation and planning tools liked with real time traffic data fusion and control of traffic signaling infrastructure on ground.		
26.	Shall collect continuously information about current observed traffic conditions from a variety of data sources and of different kind (traffic states, signal states, vehicle trajectories, incidents, road works, …)		
27.	Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from abovementioned observations, including vehicle trajectories, through a number of map matching, data validation, harmonization and fusion		

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	processes		
28.	Shall extend the measurements made on only a number of elements both on the rest of the unmonitored network, and over time, thus obtaining an estimation of the traffic state of the complete network and the evolution of this traffic state in the future		
29.	Shall forecast the traffic state with respect to current incidents and traffic management strategies (e.g. traffic signal control or variable message signs), improving the decision making capabilities of the operators even before problems occur		
30.	Shall calculate customizable Key Performance Indicators (KPI) to quickly assess the results		
31.	Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control		
32.	Shall generate alerts to the operator that trigger on customizable conditions in the network (starting with simple drops in flow, up to total queue lengths along emission sensitive roads surpassing a definable threshold)		
33.	Shall distribute both collected and		

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	calculated traffic information via a variety of communication protocols and channels, ensuring high interoperability degree and thus acting as a "traffic data and information hub"		
34.	Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.		
35.	Shall operate in real time that is continuously updating the estimates on the state of the network and the travel times on the basis of data collected continuously over time.		
36.	Shall operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network		
37.	Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller		

A) Reports

System shall generate Corridor based and Intersection based reports. The application software shall generate the following reports, but not limited to the below. All the reports shall be possible for selected dates.

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Intersection based reports		
2.	Stage Timing report – The report shall give details of time at which every stage change has taken place. The report shall show the stage sequence, stage timings and stage saturation of all stages of all cycles for a day. The saturation is defined as the ratio between the available stage timings to the actual stage timing executed by the traffic signal controller for the stage (stage preemption time).		
3.	Cycle Timing report – The report shall give details of time at which every cycle has taken place. The report shall show the cycle sequence and cycle timings for all the cycles in a day.		
4.	Stage switching report – The report shall give details of time at which a stage switching has taken place. The report shall show the stage sequence, stage timings and stage saturation for a day.		
5.	Cycle Time switching report – The report shall give details of time at which a cycle switching has taken place. The report shall show the cycle sequence and cycle timings for the cycle in a day.		
6.	Mode switching report – The report shall give details of the mode switching taken place on a day.		

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
7.	Event Report - The report shall show events generated by the controller with date and time of event.		
8.	Power on & down: The report shall show time when the master is switched on, and last working time of the master controller.		
9.	Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through keypad or automatically by LDR with time stamp.		
10.	Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server.		
11.	RTC Failure – The report shall show the time when RTC battery level goes below the threshold value.		
12.	Time Update – The report shall show the time when the Master controller updated its time either manually through keypad, automatically by GPS or through remote server.		
13.	Mode Change – The report shall show the time when Master controller's operating mode is changed either manually through keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL.		

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
14.	Lamp Status Report – The report shall show lamp failure report with date and time of failure, color of the lamp and associated phase		
15.	Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase.		
16.	Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase.		
17.	Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day		
18.	Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day		

B) Graphical User Interface

The application software shall have the following Graphical User Interface (GUI) for user friendliness.

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	User login – Operator authentication shall be verified at this screen with login name and password		
2.	Network Status Display – This online display shall indicate with appropriate color coding on site map whether an intersection under the ATCS is online or off. On double clicking the intersection a link shall be activated for the traffic flow display for the intersection.		
3.	Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed and elapsed stage time.		
4.	Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.		
5.	Reports Printing / Viewing – This link shall allow selection, viewing and printing of different reports available under ATCS		
6.	Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history.		
7.	Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis.		

No.	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
8.	Junction names shall be identified with each plot.		
9.	Facility shall be available to plot the time-space diagram from history.		
10.	Currently running stage and completed stages shall be identified with different colors.		
11.	Stages identified for synchronization shall be shown in a different color.		
12.	Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions.		
13.	It should be possible to freeze and resume online plotting of Time-Space diagram.		
14.	The system shall have other graphical interfaces for configuring the ATCS, as appropriate.		

4.1.1.7 Adaptive Traffic Control System Technical Specifications -

4.1.1.7.1 Adaptive Traffic Control- Traffic Sensor

Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined.

4.1.1.7.2 Adaptive Traffic Control- Traffic Controller

Appropriate controller technology may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined. The proposed traffic controller shall be disabled friendly and shall also provide audio tones output.

4.1.1.7.3 Adaptive Traffic Control- Traffic Light Aspects

	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	**Key Features:**		
a.	lowest power consumption for all colors, maximum 8 watts for each color		
b.	Meets or exceeds intensity, color and uniformity specifications		
c.	Temperature compensated power supplies for longer LED life		
d.	Uniform appearance light diffusing		
e.	Should be Intertek/ETL/EN compliant		
f.	All units operate at voltage of - 12 / 24 volts DC		
g.	LED shall be single source narrow beam type with clear lens & Luminance uniformity of 1:15		
h.	Pedestrian traffic lights should be provided with clearly audible signals for the benefit of pedestrians with visual impairments		
i.	Phantom Class 5 or equivalent. IP Rating: IP65		
4.	**LED aspects:**		
a.	Red, Amber, Green-Full (300 mm diameter) : Hi Flux		
b.	Green-arrow (300 mm diameter): Hi flux		
c.	Animated Pedestrian-Red and Green Animated c/w countdown (300 mm) Hi Brite with diffusions		
5.	**LED Retrofit Specifications:**		
a.	Power supply:230 Vac +/- 10% and frequency 50+/-5Hz		
b.	Standards: EN 12368 compliant		
c.	Convex Tinted Lens: Available		

	Description	Bidder Compliance(Yes/No)	Product Documentation Reference
d.	Fuse and Transients: Available		
e.	Operating Temperature Range: 0 degree Celsius to 55 degree CelciusTurn Off/Turn On Time: 75 milli seconds max		
f.	Total Harmonic Distortion: <20%		
g.	Electromagnetic interference: Meets FCC Title 47,Subpart B, Section 15 Regulation or equivalent EN/IRC standard		
h.	Blowing Rain/Dust Spec: MIL 810F or Equivalent EN/IRC standard complaint		
i.	Minimum Luminous Intensity (measured at intensity point)(cd): Red 400		
j.	Amber 400		
k.	Green 400		
l.	Dominant Wavelength (nm): Red 630 Amber 590		
m.	Green 490		
n.	Lamp conflict compatibility system: Compatible with lamp failure and conflict detection		

4.1.1.7.4 Countdown Timer

No.	Parameters	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		
2.	**Model**	<to be provided by the bidder>		
3.	**CPU**	**Micro Controller**		
4.	**Mechanical Specifications**			
A	Structural Material	Polycarbonate strengthened against UV rays		
B	Body Color	Light Grey/Black		
C	Dimensions	360mm x 370mm x 220mm		
5.	**Display Specification**			

No.	Parameters	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
A	Lamp Diameter	300mm		
B	Digit Height	150 -165mm		
C	Display Type	Dual Colored (Red & Green)		
D	No. of Digit	3		
6.	**LED Specifications**			
A	LED Diameter	5mm LED		
B	Viewing Angle	30°		
C	LED Wave Length	630-640nm (Red), 505nm - 520nm (Blue-Green)		
D	LED Dice Material	AIInGap (Red), InGaN (Blue-Green)		
E	LED Warranty period	5 years		
7.	**Technical Features**			
A	Power Consumption	20 - 30 Watt Per Lamp		
B	Input Power	85-260V AC, 50Hz		
C	Operating Temperature	-20 to + 60 °C		
D	Humidity	0% to 95% Relative Humidity		
E	Water & Dust Ingress	IP 65		
F	Standard	En12966 Compliant		

4.1.1.7.5 Poles for Traffic Signals

Sr. No	Component		Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		

Sr. No	Component		Bidder Compliance (Yes/No)	Product Documentation Reference
2.	**Model**	<to be provided by the bidder>		
3.	Material	GI Class 'B' pipe		
4.	Paint	Pole painted with two coats of zinc chromate primer and two coats of golden yellow Asian apostolate paint or otherwise as required by architect and in addition bituminous painting for the bottom 1.5 m portion of pole.		

4.1.1.7.6 Cables for Traffic Signals

Sr. No	Component		Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		
2.	**Model**	<to be provided by the bidder>		
3.	No's of core	7 and 14 core 1.5 sq. mm. 3 Core 2.5 sq. mm.		
4.	Materials	PVC insulated and PVC sheathed armored cable with copper conductor of suitable size as specified in BOQ.		
5.	Certification	ISI Marked		
6.	Standards	Indian Electricity Act and Rules		
A.	IS:1554	PVC insulated electric cables (heavy duty)		

4.1.2 Public Address (PA) System

No.	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		
2.	**Model**	<to be provided by the bidder>		
3.	PAS system	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all locations (1: many) simultaneously. The PAS should also support both, Live and Recorded inputs		
4.	Speaker	Minimum 2 speakers, To be used for Public Address System		
5.	Connectivity	IP Based		
6.	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.		
7.	Integration	With VMS and Command and Control Centre		
8.	Construction	Cast Iron Foundation		

No.	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
		and M.S. Pole, Sturdy Body for equipment		
9.	Battery	Internal Battery with different charging options (Solar/Mains)		
10.	Power	Automatic on/off operation		
11.	Casing	IP-55 rated for housing		
12.	Operating conditions	0° to 50°C		

4.2 Integrated Transport management system

4.2.1 PIS Technical Specification

No.	Particular	Specifications	Bidder Compliance (Yes/No)	Product document reference
1	LED Based Industrial PIS Size	55 Inch Display		
2	Resolution	Full HD		
3	Connectivity	HDMI/VGA		
4	Internet Connectivity	GPRS and Wi-Fi (inbuilt or through additional unit)		
5	Security	Anti-glare Enclosure with IP67 front and back cover		
6	Brightness	Minimum 350		

	NITS	
7	Operating Temperature range	**0°C to +55°C**
8	Humidity	**95%**
9	Display Format	**Multimedia content, Text in Gujarati, Hindi & English**

4.2.2 Controller

No.	Parameters	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Processor	Broadcom BCM2387 chipset. 1.2GHz Quad-Core ARM Cortex-A53 802.11 b/g/n Wireless LAN and Bluetooth 4.1 (Bluetooth Classic and LE)		
2	CPU	ES 2.0, hardware-accelerated Open VG, and 1080p30 H.264 high-profile decode. Capable of 1Gpixel/s, 1.5Gtexel/s or 24GFLOPs with texture filtering and DMA infrastructure		
3	Memory	1GB LPDDR2		

4	Operating System	Boots from Micro SD card, running a version of the Linux operating system or Windows 10 IoT
5	Dimensions	85 x 56 x 17mm
6	Power	Micro USB socket 5V1, 2.5A
7	Connectors:	
8	Ethernet	10/100 BaseT Ethernet socket
9	Video Output	HDMI (rev 1.3 & 1.4 Composite RCA (PAL and NTSC)
10	Audio Output	Audio Output 3.5mm jack, HDMI USB 4 x USB 2.0 Connector
11	GPIO Connector	40-pin 2.54 mm (100 mil) expansion header: 2x20 strip Providing 27 GPIO pins as well as +3.3 V, +5 V and GND supply lines
12	Camera Connector	15-pin MIPI Camera Serial Interface (CSI-2)
13	Display Connector	Display Serial Interface (DSI) 15-way flat flex cable connector with two data

		lanes and a clock lane
1	Memory	Push/pull Micro SDIO
4	Card Slot	

4.2.3 CCTV Surveillance

Functional Requirement of the overall Surveillance System can be categorized into following components:

1. Information to be Captured by Edge Devises
2. Information to be analysed at Interim ICCC/ICCC
3. Role Based Access to the Entire System
4. Storage / Recording Requirements
5. Other General Requirements

4.2.3.1 Information to be captured by Edge Devices

Surveillance Cameras being one of the core sub modules of ITITMS project, it is important that their selection and placement is carefully done to ensure the full coverage of the Bus shelters and nearby area. Information captured by these cameras should be accurate, and since they will be deployed on bus stops, traffic junctions etc., they are rugged, durable & compact. These cameras need to work on 24 X 7 basis and transmit quality video feeds to the Interim ICCC/ICCC and would capture the video feeds at 15 FPS during entire duration of day. However, Rajkot Police/RSCDL may take the regular review of the requirements for video resolution, FPS and may change these numbers to suit certain specific. Video feeds will be stored at 15 FPS for a minimum of 30 days at the Data Centre.

4.2.3.2 Information to be analyzed at Interim ICCC/ICCC

The proposed Video Management System should provide a complete end-to-end solution for security surveillance application. The control center shall allow an operator to view live / recorded

video from any surveillance camera on the IP network. The combination of control center and the IP network would create a virtual matrix, which would allow switching of video streams around the system.

It has been envisaged that all surveillance cameras would not be simultaneously viewed at Interim ICCC/ICCC.

4.2.3.3 Role Based Access to the Entire System

Various users should have access to the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of implementation) could be Administrator, Supervisor, Officer, Operator, etc. Apart from role based access, the system should also be able to define access based on location. Other minimum features required in the role based authentication systems are as follows:

a. The management module should be able to capture basic details (including mobile number & email id) of the Police Personnel & other personnel requiring Viewing / Administration rights to the system. There should be interface to change these details, after proper authentication.
b. Rights to different modules / sub-modules / functionalities should be role based and proper log report should be maintained by the system for such access.
c. The system should be with login name & password enabled to ensure that only the concerned personnel are able to login into the system
d. There should be provision to specify hierarchy of operators / officers for control of the cameras from various locations.
e. The number of users shall increase as per phase wise implementation. MSI is expected to estimate and provision the same based on the phase wise requirements.
f. Windows Active Directory/LDAP or any such system can be used to design role based access.

4.2.3.4 Storage/Recording Requirements

It is proposed that the storage solution shall be modular enough to ensure compliance to the changes in storage / recording policy, to be evolved upon initial deployment of the system. The following storage requirements shall be fulfilled by the MSI as scope for the project:

a. The Data Centre (DC) will be hosted at Multi activity centre on 150 ring road.

b. 30 days storage of all the surveillance camera feeds to be stored at Data Centre and Flagged data (critical incidents) will be stored for approximately 90 days, permanent storage envisaged on secondary/backup storage
c. 365 days storage of traffic junction data for ATCS at Data Centre and Flagged data will be stored for approximately 4 years.
d. Above systems except ATCS are required to be stored on Primary storage for 7 days & on Secondary Storage for remaining days respectively at Data Centre.
e. For ATCS, Primary storage will be for 90 days and Secondary Storage for 275 days. Back up storage for 4 Years approximately.
f. Data on storage would be over-written automatically by newer data after the stipulated time period. If some data is flagged by police personnel (or by designated personnel) as important data / evidence data due to some reporting of crime or accident in the area or due to court order or due to suspicious activity, it would need to be stored for longer duration, as per requirements. Rajkot Police would analyse such flagged data every 3months to take such decisions for preservation of the flagged data beyond 90 days.
g. Full audit trail of reports to be maintained for 90 days.
h. Bidder is expected to carry out the storage requirement estimation and supply as per the solution proposed.
i. Archival/Backup to be done on NAS / Scale-out NAS / SAN / Unified or equivalent storage solution
j. Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data.
k. The recording servers / system, once configured, shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.
l. The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.
m. The system shall support H.264 or better, MPEG-4 and MJPEG compression formats for all analog cameras connected to encoders and all IP cameras connected to the system.
n. The system shall record the native frame rate and resolution supplied by the camera or as configured by the operator from the system administration server.
o. The system should not limit amount of storage to be allocated for each connected device.
p. The on-line archiving capability shall be transparent and allow Rajkot Police/RRL/RSCDL to browse and archive recordings without the need to restore the archive video to a local hard drive for access.
q. The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure

groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.

r. The system shall support archiving or the automatic transfer of recordings from a camera's default database to another location on a time-programmable basis without the need for user action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording the system should have the ability to trigger actions such as the automatic sending of email alerts and sound alerts to necessary personnel.

s. Bandwidth optimisation
   - The Recording Server / System shall offer different codec (H.264, MJPEG, MPEG-4, etc.) and frame rate (CIF, 4CIF, QCIF) options for managing the bandwidth utilisation for live viewing on the Client systems. (through use of multiple systems such as transcoding server)
   - From the Rajkot Police, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server.

t. The Recording Server / System shall support camera (analogue and IP cameras) devices from various manufacturers.

u. Failover Support
   - The system shall support automatic failover for recording servers. This functionality shall be accomplished by failover server as a standby unit that shall take over in the event that one of a group of designated recording servers fails. Recordings shall be synchronized back to the original recording server once it is back online.
   - The system shall support multiple failover servers for a group of recording servers.

v. SNMP Support
   - The system shall support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system.
   - The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.

4.2.3.5 Other General Requirements

1. Management/Integration functionality

a. The Surveillance System shall offer centralised management of all devices, servers and users.

b. The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.
c. The Surveillance System should have ability to knit the video streams from multiple cameras, based on the date/time stamp. Every video stream shall have date, time, source camera location, FPS etc. water-marked. These attributes shall be finalised at the System Design time. There shall be a centralised NTP server, from which all devices shall synchronise the date and time.
d. The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
e. The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices.
f. It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
g. It should be possible to integrate social media platforms to Surveillance System to enable Rajkot Police to track and monitor certain trending incident or crime.
h. The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.
i. System should be able to be integrated with Event Management / Incident Management System, if implemented by Rajkot Police in future.

2. System Administration functionality

a. The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system
b. The System Administration Server shall support different logs related to the Management Server
    - The System Log
    - The Audit Log
    - The Alert Log
    - The Event Log

3. Rules

The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:

- Start and stop recording
- Set non-default live frame rate
- Set non-default recording rate
- Start and stop PTZ patrolling
- Send notifications via email
- Pop-up video on designated Client Monitor recipients

4. Client System

a. The Client system shall provide remote users with rich functionality and features as described below.
b. Viewing live video from cameras on the surveillance system
c. Browsing recordings from storage systems
d. Creating and switching between multiple of views.
e. Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
f. Using digital zoom on live as well as recorded video.
g. Using sound notifications for attracting attention to detected motion or events.
h. Getting quick overview of sequences with detected motion.
i. Getting quick overviews of detected alerts or events.
j. Quickly searching selected areas of video recording for motion (also known as Smart Search).

5. Remote Web Client

The web-based remote client shall offer live view of up to 16 cameras, including PTZ control and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.

a. User Authentication – The Remote Client shall support logon using the user name and password credentials

6. Matrix Monitor

a. Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple camera on the system on any monitor
b. The Matrix Monitor feature shall access the H.264/MJPEG/MPEG4 stream from the connected camera directly and not sourced through the recording server

7. Alarm Management Module

a. The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.
b. The alarm management module shall provide interface and navigational tools through the client including;
    - Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
    - Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
c. The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
d. Basic VMS should be capable to accept third party generated events / triggers
e. Based on alarms/alerts, customised/standard alert messages should be published on VMB/PA, after authorisation by a supervisor/operator.

8. Other Miscellaneous Requirements

a. System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and MSI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. Bidder is required to specify any additional hardware / software required for this purpose & the same can be listed in miscellaneous section of the commercial bid. MSI will also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.
b. All the systems proposed and operationalisation of Video Management System should comply with requirements of IT Acts.
c. Any hardware or software required to achieve the functional requirement and technical solution of the overall Project (may not be not specified in the schedule) is to be proposed in the Bid and borne by the MSI.
d. Bidder shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication with the Surveillance System in a secure manner. Rajkot Police may provide such tablets / smart phones to the designated Police Personnel. It will be responsibility of MSI to configure such tablets / Smartphone, for the

Surveillance System being implemented a part of this project, and ensure that all the necessary access is given to these mobile users. Functionalities to be provided through mobile application: Viewing of any video steam from Central VMS, uploading of video / pictures central VMS, Location based GIS Map access, tagging of mobile device/location information for all relevant functionalities.

Rajkot Police reserves the right to appoint any Independent Evaluation Agency at any time during the phases of the project.

4.2.3.6 Fixed Box Cameras

No.	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		
2.	**Model**	<to be provided by the bidder>		
3.	Video Compression	H.264		
4.	Video Resolution	1920 X 1080		
5.	Frame rate	Min. 30 fps		
6.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
7.	Lens Type	Varifocal, C/CS Mount, IR Corrected Full HD		
8.	LensNo.	Auto IRIS 5~50mm/ 8 – 40 mm, F1.4		
9.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)		
10.	IR Cut Filter	Automatically Removable IR-cut filter		
11.	Day/Night Mode	Colour, Mono, Auto		
12.	S/N Ratio	≥ 50 Db		
13.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range		
14.	Audio	Audio Capture		

No.	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
		Capability (G.711, G.726)		
15.	Local storage	Micro SDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.		
16.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP/SMTP, NTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS, ONVIF Profile S		
17.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
18.	Operating conditions	0 to 50°C (temperature), 50 to 90% (humidity)		
19.	Intelligent Video	Motion Detection & Tampering alert		
20.	Alarm I/O	Minimum 1 Input & 1 Output contact for 3rd part interface		
21.	Casing	NEMA 4X / IP-66 rated, IK10		
22.	Certification	UL/EN, CE,FCC		

4.2.3.7 Network Video Recorder

No.	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		

No.	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
2.	**Model**	<to be provided by the bidder>		
3.	Input	8 channel IP camera inputs		
4.	Output	1 VGA, 1 HDMI		
5.	Support for Two-way Talk	1 channel Input, 1 channel Output		
6.	OSD	Camera title, Time, Video loss, Camera lock, Motion detection, Recording		
7.	Video/Audio Compression	H.264 / MJPEG / PCM		
8.	Resolution	1080P (1920×1080) / 720P(1280×720) / D1 (704×576 / 704×480)		
9.	Record Rate	25 FPS@1080P for each channel		
10.	Bit Rate	48~8192Kb/s		
11.	Record Mode	Manual, Schedule(Regular(Continuous), MD, Alarm), Stop		
12.	Record Interval	1~120 min (default: 60 min), Pre-record: 1~30 sec, Post-record: 10~300 sec		
13.	Search Mode	Time/Date, Alarm, MD & Exact search (accurate to second), Smart search		
14.	Playback Functions	Play, Pause, Stop, Rewind, Fast play, Slow play, Next file, Previous file, Next camera, Previous camera, Full screen, Repeat, Shuffle, Backup selection, Digital zoom		
15.	Ethernet	RJ-45 port (10/100/1000M)		
16.	Network Functions	TCP/IP, UDP, DHCP, DNS, IP Filter, PPPOE, DDNS, FTP, Email, Alarm Server		

No.	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
17.	Internal HDD	Minimum 2 HDD slots with capacity up to 4TB with RAID 5 support. Should be provided with appropriate storage to meet the functional requirements.		
18.	USB	Minimum 2 port		
19.	Working Environment	0°C to 50°C / 0% to 90% RH		
20.	Certification	UL/EN, CE, FCC		
21.	Protocol	ONVIF		

4.2.3.7.1 Field Junction Box

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		
2.	**Model**	<to be provided by the bidder>		
3.	Size	Suitable size as per site requirements to house the field equipment		
4.	Cabinet Material	GI with powder coated		
5.	Material Thickness	Min 1.2mm		
6.	Number of Locks	Two		
7.	Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake		
8.	Mounting	On Camera Pole / Ground mounted on concrete base		
9.	Form Factor	Rack Mount/DIN Rail		
10.	Other Features	Rain Canopy, Cable		

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		entry with glands, proper earthing and Fans/any other accessories as required for operation of equipment's within junction box.		

4.2.3.7.2 Poles for Camera

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		
2.	**Model**	<to be provided by the bidder>		
3.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)		
4.	Height	5-10 Meters (or higher), as-per-requirements for different types of cameras & Site conditions		
5.	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)		
6.	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole		
7.	Bottom base plate	Minimum base plate of size 30x30x1.5 cm		
8.	Mounting facilities	To mount RLVD Cameras, ANPR, Speed detection sensors, CCTV		

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		cameras, Traffic Signals, Pedestrian Signals, Switch, etc.		
9.	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.		
10.	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms. Please refer to earthing standards mentioned elsewhere in the document.		
11.	Protection	Lightning arrester shall be provided, to protect all field equipment mounted on pole.		

4.2.3.7.3 Edge Level Switch (at Traffic Junctions)

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		
2.	**Model**	<to be provided by the bidder>		
3.	Type	Managed Outdoor Industrial grade switch		

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
4.	Total Ports	• Minimum 4 10/100/1000/TX PoE/PoE+, 2x SFP Ports (can have 4xSFP Ports in certain locations) • May require higher port density at some locations, depending upon site conditions • May require fiber ports (for devices or for uplinks) at some locations, depending upon site conditions/distances.		
5.	PoE Standard	IEEE 802.3af/ IEEE 802.3at or better		
6.	Protocols	• IPV4,IPV6 • Support 802.1Q VLAN • DHCP support • IGMP • SNMP Management • Should support Loop protection		

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		and Loop detection • Should support Ring protection • End point Authentication • Should support NTP		
7.	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering • Support security group access control list		
8.	PoE Power per port	Sufficient to operate the CCTV cameras/edge devices connected		
9.	Enclosure Rating	IP 30 or equivalent Industrial Grade Rating(to be housed in Junction box)		
10.	Operating Temperature	0 -50 C or better Industrial Grade Rating		
11.	Multicast support	IGMP Snooping V1, V2, V3		

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
12.	Management	Switch needs to have RS-232/USB/RJ45 console port for management via a console terminal or PC,Web GUI NTP, Syslog for log capturing SNMP V1,V2,V3		
13.	Compliance	UL/EN/IEC or equivalent		

4.2.3.7.4 Online UPS for field locations

Sr No	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>		
2.	**Model**	<to be provided by the bidder>		
3.	Capacity	Adequate capacity to cover all above IT Components at respective field locations		
4.	Technology	IGBT based PWM Technology, True Online UPS		
5.	Input Frequency	45 to 55 Hz		

Sr No	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
	Range			
6.	Output Frequency Range	45 to 55 Hz		
7.	Output Voltage	220VAC - 230VAC		
8.	Voltage Regulation	+/-2% (or better) and with built-in Over Voltage Cut off facility in the Device		
9.	Frequency	50 Hz +/- 0.1% (free Run Mode)		
10.	Harmonic Distortion (THD)	< 3% (linear load)		
11.	Output Waveform	Pure Sine wave		
12.	Output Power Factor	0.8 or more		
13.	Battery Backup	Adequate and required battery backup to achieve		

Sr No	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		required uptime of field device as well as SLA of the overall solution..		
14.	Battery Type	Lead acid, Sealed Maintenance Free (SMF)		
15.	General Operating Temperature	0 to 40 Degree Celsius		
16.	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection		
17.	Bypass	Automatic, Manual Bypass Switch		
18.	Certifications	For Safety & EMC as per international standard		
19.	Overall	IP 55,		

Sr No	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
	Protection	Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake		

4.2.3.7.5 Video Management System

The SI shall use the existing Video management system of RSCDL. The VMS platform which will be designed for viewing, recording and replaying acquired video as part of overall project solution. This platform will be based on the Internet Protocol (IP) open platform concept. Major functionalities are described here:

VMS Overview

No.	Description	Bidder Compliance (Yes/No)
1.	VMS shall be used for centralized	

No.	Description	Bidder Compliance (Yes/No)
	management of all field camera devices, video servers and client users.	
2.	VMS server shall be deployed in a clustered server environment or support inbuilt mechanism for high availability and failover.	
3.	VMS shall support a flexible rule-based system driven by schedules and events.	
4.	VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.	
5.	VMS shall support ONVIF compliant internet protocol (IP) cameras.	
6.	The bidder shall clearly list in their proposal the make and models that can be integrated with the VMS, additionally all the offered VMS and cameras must have Open Network Video Interface Forum (ONVIF) compliance. VMS shall be enabled for any standard storage technologies and video wall system integration.	
7.	VMS shall be enabled for integration with any external Video Analytics Systems both server & edge based.	
8.	VMS shall be capable of being deployed in a virtualized server environment without loss of any functionality.	
9.	All CCTV cameras locations shall	

No.	Description	Bidder Compliance (Yes/No)
	be overlaid in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking on the camera location on the graphical map. The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.	
10.	VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.	
11.	VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.	
12.	Whilst live control and monitoring is the primary activity of the monitoring workstations, video replay shall also be accommodated on the GUI for general review and also for pre- and post-alarm recording display.	
13.	The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.	
14.	All CCTV camera video signal inputs to the system shall be provided to various command control centre(s), viewing centre etc., and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.	

No.	Description	Bidder Compliance (Yes/No)
15.	VMS client shall have the capability to work with touch enabled multi-monitor workstations. It shall be capable of displaying videos in up to three (3) monitors simultaneously.	
a.	AVI files	
b.	Motion- Joint Photographic Experts Group (M-JPEG)	
c.	Moving Picture Expert Group-4 (MPEG-4)	
d.	MP4 Export or Latest	
16.	All streams to the above locations shall be available in real-time and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.	
17.	The VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following settings, the specific settings shall be determined according to the encoding device:	
18.	The VMS shall support the following operations:	
a.	Adding an IP device	
b.	Updating an IP device	
c.	Updating basic device parameters	
d.	Adding/removing channels	

No.	Description	Bidder Compliance (Yes/No)
e.	Adding/removing output signals	
f.	Updating an IP channel	
g.	Removing an IP device	
h.	Enabling/disabling an IP channel	
i.	Refreshing an IP device (in case of firmware upgrade)	
j.	Multicast at multiple aggregation points	
19.	The VMS shall support retrieving data from edge storage. Thus when a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage. System should support to view the recordings available over cameras local storage device (such as an SD card), and copy them to the server.	
20.	The VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.	
21.	The VMS shall allow the administrator to distribute camera load across multiple recorders and be able shift the cameras from one recorder to another by simple drag and drop facility.	
22.	VMS shall support automatic failover for recording.	
23.	VMS should also support dual recording or mirroring if required.	

No.	Description	Bidder Compliance (Yes/No)
24.	VMS shall support manual failover for maintenance purpose.	
25.	VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).	
26.	VMS shall support integration with the ANPR application.	
27.	VMS shall support integration with other online and offline video analytic applications.	
28.	VMS shall be able to accept alerts from video analytics built into the cameras, other third party systems, sensors etc.	

Client System

The Client system shall provide remote users with rich functionality and features as described below:

No.	Functionality	Bidder Compliance (Yes/No)
1.	Viewing live video from cameras on the surveillance system.	
2.	Browsing recordings from storage systems.	
3.	Creating and switching between multiple of views.	
4.	Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.	
5.	Using digital zoom on live as well as recorded video.	
6.	Using sound notifications for attracting attention to detected motion or events.	
7.	Getting quick overview of sequences with detected motion.	
8.	Getting quick overviews of detected alerts or events.	

9.	Quickly searching selected areas of video recording for motion (also known as Smart Search).

Remote Web Client

No.	Description	Bidder Compliance (Yes/No)
1.	The web-based remote client shall offer live view of up to 9 cameras, including PTZ control (if applicable) and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.	
2.	User Authentication – The Remote Client shall support logon using the user name and password credentials	

Mobile Client

No.	Description	Bidder Compliance (Yes/No)
1.	The bidder shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication with the Video Management System in a secure manner. It will be responsibility of MSI to configure such tablets / Smartphone with the Surveillance System and ensure that all the necessary access is given to these mobile users.	
2.	Communication with mobile client and server shall be encrypted with Digital Certificate.	

Matrix Monitor

No.	Description	Bidder Compliance (Yes/No)
1.	Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple cameras on the system on any monitor.	
2	The Matrix Monitor feature shall access the	

.	H.264/MJPEG/MPEG4 stream from the connected camera directly and not sourced through the recording server.

Alarm Management Module

No.	Description	Bidder Compliance (Yes/No)
1.	The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.	
2.	The alarm management module shall provide interface and navigational tools through the client including;	
3.	Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.	
4.	Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.	
5.	The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.	
6.	Basic VMS should be capable to accept third party generated events / triggers.	

Management / Integration Functionality

No.	Description	Bidder Compliance (Yes/No)
1.	The Surveillance System shall offer centralised management of all devices, servers and users.	
2.	The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance,	

	Monitoring and Recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.	
3.	The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.	
4.	The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices.	
5.	It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call, etc.	
6.	The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.	
7.	System should be able to be integrated with Event Management / Incident Management System.	

System Administration Functionality

No.	Description	Bidder Compliance (Yes/No)
1.	The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.	
2.	The System Administration Server shall support different logs related to the Management Server. • The System Log • The Audit Log • The Alert Log • The Event Log	
3.	Rules: The system shall support the use of rules to determine	

	when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as: • Start and stop recording • Set non-default live frame rate • Send notifications via email • Pop-up video on designated Client Monitor recipients	

Other Miscellaneous Requirements

No.	Description	Bidder Compliance (Yes/No)
1.	System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and MSI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. Bidder is required to specify any additional hardware / software required for this purpose & the same can be listed in Miscellaneous section of the commercial bid. The bidder will also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.	
2.	All the systems proposed and operationalization of Video Management System should comply with requirements of IT Acts.	
3.	Security Platform shall have strong security mechanism such as the use of advance encryption/digital certificates/ authentication to ensure that only authorized personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.	

4.	System should ensure that once recorded, the video cannot be altered, ensuring the audit trail is intact for evidential purposes.

Major Server components for VMS

Video Management Server(s)	Video Management System Servers will maintain coherent operations between all servers and workstations. It will host Control Center, where the system is administered, and System database. It will monitor one or more Recorder servers on separate dedicated computers, storage devices, IP-compatible devices, and one or more workstation. All networkcommunication will also be is performed via the Video Management servers.
Video Recording Server(s)	The Video Recorder Server will be a dedicated server that will store and processes video with the help of Video Management System
Video Analytics Server (s)	Video Analytics Software will be installed in the Video Analytics Server, Video Analytics is a software product that will analyse live video in real-time to detect, identify, and track objects of interest. It will automatically issue alerts to the appropriate personnel and initiate appropriate follow-up action according to pre-defined rules. This software will also manage sensors; each sensor will monitor a single video feed for security events. The video feeds will be connected over the network to the Video Analytics Server. Sensors on the Video Analytics Server will perform all event detection functions.
Web Server(s)	It will be used to launch the client application remotely through web browsers.
Gateway Server (s) – If required	A Media Gateway server will be used to establish remote connections to review and transcode the video. Standalone Media Gateway servers can also be installed on separate machines. Standalone servers will be recommended for such large systems that will transfer video data to remote clients.

4.2.4 Automatic fare collection system

4.2.4.1 Functional Requirement AFCS

Sr. No.	Requirement	Compliance (Yes/No)	Reference of documentary proof/evidence supported by system screenshot/ MIS/Report/ Brochure etc.

Central Backend AFC System		
1.	Central BackOffice will be the heart of the AFC system where all the AFC functional activities will be performed.	
2.	The Central BackOffice system shall generate the necessary management reports from the fare media transaction information received from the Bus Validators.	
3.	The Central BackOffice system shall hold and download the fare media parameters and fare table information to each validator.	
4.	The Central BackOffice System shall communicate with each device via the wide area network and process the data received to provide overall audit, statistical and operational information.	
5.	The data transferred from the devices to the BackOffice shall include, as a minimum, information such as usage of various equipment's commissioning, various transaction, EOD shift summary, Ridership numbers, shift revenue, fault reports.	
6.	The Central BackOffice shall have facilities to generate and update blacklists for fare media.	
7.	The Central BackOffice shall be able to support applicable fare media replacement and refund applications from devices.	
8.	In case there is a failure in network,	

	station devices independently record all transaction and alarm data for a period of not less than seven days and all data stored will be transmitted to the Central Back office System once the system is fully operational.	
Product Configuration		
9.	Product Configuration Management system should be capable of adding, removing, editing and updating Fare Media for Sales and Usage at transit network.	
10.	Product configuration should be able to configure a transit product with the following parameters such as ID, Name , Expiry date /time , Number of days in week , start and end time , service provider , Route/Stop , Device type ,fare , discounted fare , profile etc..,	
11.	Product configuration should be able to configure a transit product with the following parameters for peak hour/ non-peak hour fare, route/stop, Device type etc..,	
12.	Product configuration Management should be able to create any number of products as per client requirements by changing the business parameters defined in business rules	
13.	Should be able configure fares for single journey tickets, return journey tickets, Group ticket as mentioned in business rules document	

14.	On scheduling to devices, the update should be downloaded and updated in devices locally and status should be updated in system.	
Transaction management		
15.	The Transaction Management system shall acquire and process all the transactions from all fare media issued by client at acceptance infrastructure.	
16.	Transaction Management system should acquire and process all the transactions from all the issuance channels for top-ups, update transit products, refund, renew, reissue cards etc.	
17.	The Transaction Management shall, in future, share the details with the settlement and clearing system of the transactions	
18.	The Transaction Management system shall actively update its Contactless Smart Media Blacklist Table by adding/ removing Contactless Smart cards IDs when the Contactless Smart Media has been blocked physically by conductor.	
19.	Transaction Management should post all the transit transaction performed through batch processing for transactions performed offline.	
20.	Should be capable of checking and handling exception, missing, duplicate, delayed and fabricated data	
System Configuration		

21.	System configuration should allow configuring the devices configuration parameters.	
22.	System configuration should allow updating selected device types, groups, group of devices and individual devices.	
23.	Should be able to select the devices and update the devices for Tariff, users, Terminal parameters, Key, Certificates and software updates.	
Equipment Management		
24.	The Central back office system will include Equipment Management functions which shall allow client to configure new devices	
25.	Equipment Management should allow to tracking the complete lifecycle of devices from Equipment commissioning to faulty replacement / removed	
26.	Equipment Management system should be able to process, manage and display the alarms/alerts raised by the equipment's.	
27.	Equipment management should allow to configure maintenance/technician users, profiles in the system.	
28.	Equipment should allow to generate the reports on equipment's, alerts/alarms, equipment's downtime and incidents life cycle.	
Reconciliation		
29.	The purpose of the functionality is to	

	provide an efficient revenue management system.	
30.	Central system shall have feature for automatic generation of daily, monthly & yearly reports for revenue reconciliation using the revenue data - transactions, audit register and cash amount. Reports shall be generated global, Route wise, operator wise and shift wise.	
31.	The functionality shall have flexibility to take care of any manual entry errors. There shall be provision for entry correction (stating reasons) within a defined period.	
32.	It shall provide a transparent Account of revenue figures. Any discrepancy highlighted in revenue figures reconciliation shall be visible in the detailed reports.	
Key Management		
33.	The Central Backoffice system shall provide a key Management System for the management of keys throughout the lifetime of the Smart Card based AFC system installation and support.	
34.	The Key Management System shall be responsible for the downloading the Public key and revocation list from the Acquirer/Payment schemes.	
35.	The Key Management System shall also be responsible for updating the files to all the devices in the AFC system.	
36.	The Key Management should allow to	

	update the system periodically and whenever required and should have the versioning mechanism to manage the updates	
Reports		
37.	**Daily sales Summary Report:** Summary of all ticketing, financial transactions / cash received or refunded. Route wise, ticket wise	
38.	**Daily ridership summary report:** Summary of transit transaction at buses using various products	
39.	**Shift summary reports:** All ticketing, financial transactions. Each transaction with date and time stamped.	
40.	**Aggregated / Consolidation reports** For matching all Transaction based, Audit registers based and Revenue figures.	
41.	**Individual ticket transaction history**	
42.	**Operator action reports**	
43.	**Log reports**: Chronological report of daily activities. Each event shall have date and time recorded.	
44.	**Equipment inventory: E**quipment installed and removed	
45.	**System reports:** System configuration reports	
Hardware Management		
46.	Geographic area layout based GUI for	

monitoring and controlling	
47. Equipment status, Equipment mode of operation,	
48. Current stock status	
49. Configuration parameters	
Updates Management	
50. Should be able to create an update and assign an version number for all update categories	
51. Should be able to manage all the updates from the backoffice systems for all categories Tariff, parameters, Hotlist, users etc..,	
52. Should be able to automatically schedule updates to devices whether is an updated hotlist available	
53. All the status of the update should be captured in the Central computer	
54. Reports should be generated for all the updates schedules and status of the updates.	
Authentication	
55. All connections to the server from devices should be securely connected.	
56. All data exchange should be encrypted between the server and client	
57. All active connections should be managed by servers	
58. All the configuration with connections should be managed through configuration management	

59.	Should log all credentials of the login details when logging in /off in the AFC system		
60.	Should be securely hosted with access only to Client's user configuration managers		
61.	Should be able to create users and profiles based on the devices and functions to be performed		

4.2.4.2 Technical Specification Handheld Electronic Ticketing Device

Module / Component	Description	Compliance (Yes/No)	Documentary Reference
Processor	32-bit ARM11		
Memory	192MB standard (128MB Flash, 64MB DDR) Micro SD (TF card) up to32GB		
Display	3.5 inch 240 x 320 pixel TFT colour LCD Touch screen		
Keypad	10 numeric / letter keys, 8 function keys Back-lighting		
Printer	Fast thermal printer (18 lps) or faster depending on font size Paper roll width / diameter: 58mm /38mm		
Card Slots	2 SAMs, 1SIM		
Magnetic Card Reader	Track 1 / 2 / 3, bi-directional		
Contactless Card Reader	MasterCard Pay Pass& Visa pay Wave 13.56MHZ,		

	ISO / IEC 14443 Type A/B, Mifare®, NFC
Audio	Speaker
Communication	GPRS / 3G(WCDMA)
Peripheral Ports	1xminiUSB 1 x RS232 1 x power charge
Security	DUKPT/Master / Session/DES/3DES/AES
Battery	Li-ion batteries 1850mAh, 7.4V
Voltage	Input: 100~240VAC, 50Hz / 60Hz, 1.0A Output: 9VDC,2.5A
Physical	Length: 175mm Width: 82mm Height:63mm
Certifications	PCI PTS 3.x MasterCard Pay Pass Visa pay Wave EMV Contactless L1

4.2.4.3 Technical Specification Turnstile and Validator

4.2.4.3.1 Turnstile

Item	Specifications	Compliance (Yes/No)	Documentary Reference
Turnstile type Fare Gate Specification	Tripod Turnstile should offer the best security performance by means of a photocell and IR sensor alarming in case of unauthorized passage attempt.		
Material	Stainless Steel AISI 304		
Orientation	Pass Left or Pass Right		

Tripod	38mm diameter	
Arms	AISI 304	
Function	Passage in both directions, electronically controlled	
	Ticket/Smart card validity check to be implemented via validator and turnstile integration	
	Authorized passage for entry/exit	
	Deduct value from Smart card to be implemented via validator	
	Used ticket validation to be implemented via validator and turnstile integration	
	Alarms for tailgating, fraud, ticket amount display etc.	
Passage width	Passage (Normal): 500 mm(approx.)	
Validator and Turnstile Integrated functionality	Reader/Writer (EMV level 1 & 2 support). The design of the gate arrays should be such that the passenger uses reader placed on the right-hand side while passing through the gate.	
	Reader/Writer for EMV smart cards, mobile NFC media, QR code validators. The design of the gate arrays should be such that the passenger uses reader placed on the right-hand side while passing through the gate.	
	Fare media are checked for validity and updated in accordance	

	with the business rules and fare tables currently in force For QR Coder reader: • Read QR code printed on paper • Read digital QR code from mobile • Read Distance up to 4 cm from plate	
Throughput	At-least 30-35 passengers per minute (PPM)	
Safety Sensor Requirements	System should have pressure lid at cabinet for sensing improper access through climbing over cabinet.	
IR Sensor	Tripod should have one IR sensor below tripod angling downward to detect presence of any person crawling through below the tripod arm or below the gaps of casing	
Photo Sensor	Tripod should have photo sensor. In case of any obstruction/abnormality/trespassing, it should sense & generate alarm for improper transaction.	
Mechanism	Control of the Tripod operation should be achieved by an electro mechanical head mechanism located within the top section of the turnstile casework.	
Normally Closed	The mechanism should be locked until a valid authorization signal is received. It should also be possible to	

	configure the turnstile in normally open mode.	
Power Failure	In the event of an emergency or isolation of the power supply, Tripod should be configured to Fail-Safe i.e. rotates freely or Fail-Lock i.e. locks in the HOME position. Either option should be available in both or one direction.	
Emergency / Fire Alarm	The turnstile should offer an input (0V normally closed) in order to receive an Emergency /Fire Alarm remote command (by others).	
	When this command is active, the control logic should release the rotation of the tripod in both directions. This condition should remain for the duration of the signal being received by the control logic.	
Alarms	If a person attempts to rotate the Tripod without authorization from the reader unit, the control logic should interpret this as an attempt of fraud ("Fraud" alarm).	
Damper	Turnstile should be equipped with Damper functionality.	
Anti-Reversal Device	The anti-reversal device should be used to prevent rotation of the rotary unit in the opposite direction to that of the initial rotation. This means that once the Tripod has been moved in	

	one direction, the device should prevent a reverse movement in the opposite direction.		
MCBF & IP:	1.500.000 cycles (normally closed mode), 2.500.000 cycles (normally open mode)		
	IP: IP 44 or more		
Power Supply	230 Vac 50Hz.		
Operating Temperature	Operating Temperature should be 0 to +45 degrees Celsius.		
Humidity	Humidity RH 95% non-condensing		
Drop arm (optional)	Drop arm: the horizontal arm should drop to create a clear passage for evacuation.		
ISO	OEM should be ISO 9001:2000 & ISO 14001:2004 for development, producing & trading of turnstiles		
Certificate	CE certified		

4.2.4.3.2 Validator

Sr. No.	Particular	Minimum Specification	Compliance (Yes/No)	Documentary Reference
1	Processor	Min 32 Bit		
2	Memory	Flash 4 to 8 MB		
3	Memory	SDRAM 8 to 16 MB		
4	External	Micro SD Card Up		

	memory slot	to 4 GB
5	Contactless Card Reader	13.56 MHz, ISO 14443 Type A/B, Mifare, Ultralight C, DesFire, NFC
6	Barcode Reader	1D and 2D barcode
7	Display	Color 3.2 inches TFT LCD
8	Card Slots	1 SAM Slot
9	Peripheral Ports	1 X RS232 or 1 X USB 1XRS422 /485
10	Buzzer	95 dB
11	Indicators	LEDs (Orange, white , green)
13	External Power Supply	12 to 48V DC
14	Operating supply	5V DC , 500 mAh
15	Physical Reader Dimensions	To be fitted aesthetically into turnstile/flap gates
16	OS	Window / Linux / Android
17	Communication	GSM/GPRS3G, Ethernet 10/100 Mbps, WiFi (optional)

4.2.5 Functional Requirement Smart Bus stops

Sr. No.	Requirement	Compliance (Yes/No)	Reference of documentary proof/evidence supported by system screenshot/ MIS/Report/ Brochure etc.
1	The smart bus stop should have below components 1. Surveillance 2. Smart Lighting 3. LED Passenger Information System 4. Solar roof top 5. Mobile Charging station 6. Seating place for 5-15 people (depending on location and feasibility) 7. Standing place for 5-10 people (depending on location and feasibility)		
2	The bus stop should have provision to display static content such as city public transport map, route information etc.		
3	The bus stop structure frame and seats shall be made of stainless steel, The structure should be smoothly finished (Grade SS304 satin finish) surface with chamfered edges / corners without any protruding parts.		
4	The side panel of the bus stop should be made of clear glass		
5	The Side panels should be mounted 3 inches off the ground		

6	Easy to use dustbins	
7	Smart Bus stop should be inclusive in design - differently-abled, women, children and the elderly requirements should be taken care of.	
8	ICT components such as camera, lighting, PIS should have protective casing to reduce vandalism	
9	Power requirement of the bus stop should be taken care by rooftop solar	
10	The PIS at bus stop shall also display information about arrival/departure of flights and train from Rajkot city	

4.2.6 Technical Specification Smart Parking components

4.2.6.1 Entry Exit Barrier

S. No	Parameter	Minimum Specification	Bidder Compliance	Product Documentation Reference
1	Three phase 0, 37 CV motor			
2	Scaled, self-lubricating motor			
3	Movement transmission is done by ball-bearing-supported connecting rods			
4	Opening/ closing time: from 0,8 secs. to 8 secs. Depending on the mounted arm (standard: 1,2 secs. For			

	an arm of 3m.)			
5	Low maintenance rate: soft start and stop movements without arm oscillations			
6	Emergency stop feature by a photocell or pressure strip (optional)			
7	Optional UPS (Uninterrupted Power Supply) to continue operating when mains supply's fails (max. 100 up/ down movements)			
8	Internal memory of 7 pulses with Automatic reset on down signal loose			
9	Polyester powder painted and oven-dried steel housing			
10	Operating temperature: -20 ºC a +55 ºC			
11	Single phase power supply: 220 Vac. ± 10% 50 Hz (110 Vac. ± 10% 60 Hz. optional)			
12	Operating consumption: 330 w. maximum			
13	The Barrier unit must conform to ISO 9001 Quality Assurance Standard			

14	CE, Ukr - Sepcro certified			
15	Degree of Protection: IP34D			

4.2.6.2 Automatic Ticket Dispenser & Validator at exit

S. No	Parameter	Minimum Specification	Bidder Compliance	Product Documentation Reference
1	Ticket dispenser with an option to record and print entrance time, date and other relevant parameters for a car entrance			
2	Ability to scan QR code or similar technology based mobile tickets & provide access based on data captured in QR code			
3	Automatic/ manual ticket issue activated by car presence detector			
4	Control of vehicle passage sequence, sending ticket code as “cancelled” to the Central Unit in case of abnormal operation			
5	Barrier management			
6	Electronic self-adjusting vehicle presence detector			

	that prevents ticket extraction by pedestrians			
7	User-oriented alphanumerical information display in two languages with TFT monitor			
8	Date and time visualization on display while inactive			
9	Ticket loading container with capacity for 5000 tickets with Ticket level control			
10	Ethernet communications connection to the central unit with Optional RS-422 connection			
11	Pocket terminal connection for maintenance processes			
12	Autonomous operation			
13	Electronically controlled internal heating/ ventilation system			
14	Polyester powder painted and oven-dried steel housing			
15	Operating temperature: -20 ºC a +55 ºC			
1	Protected environment			

6	use (roofed)			
17	Power supply: 220 Vac. ± 10% 50 Hz (110 Vac. ± 10% 60 Hz. optional)			
18	Maximum consumption 70 w (270w with heater option)			
19	Conform ISO 9001 Quality Assurance Standard 25. CE, FCC, IC, CNRTLUS certified			

4.2.6.3 Payment Kiosk

S. No	Parameter	Minimum Specification	Bidder Compliance	Product Documentation Reference
1	System should be able to scan the entry ticket and calculate the charges as per entry time. Accepts payment in cash/coin and returns changes.			
2	Programmable automatic recharge of out-of-stock coins by means of a safe container with an approximate 500 coins capacity			
3	Banknote acceptor for different notes types in any			

	of the 2 insertion directions with two deposits for recycling, storage and change returns (optional) and a capacity of 120 banknotes for cassette			
4	Thermal printer (no printer ribbon required) for receipts, payment vouchers, liquidation and accounts states			
5	Automatically issues liquidation voucher on withdrawal of safety boxes (coins or notes). The voucher specifies the content of box number of coins/ notes of each type and total			
6	Accepts payment through Rajkot mitra Card			
7	Accepts credit card payment			
8	Multilingual information display with 12" TFT monitor			
9	Motorized magnetic ISO lateral strip reader/ recorder			
10	Optional magnetic card reader/collector			

11	Ethernet communications connection to the central unit. Optional RS-422 connection			
12	Pocket terminal connection for maintenance processes			
13	Powerless Operation: Incorporating a UPS to enable the credit pay station to complete operations in progress in the event of a power supply failure			
14	Polyester powder painted and oven-dried steel housing			
15	Operating temperature: -5 ºC a +50 ºC			

4.2.6.4 Parking enforcement application

S. No	Parameter	Minimum Specification	Bidder Compliance	Product Documentation Reference
1	Mobile application to capture information of parking violation			
2	Traffic police should be			

	able to enter vehicle details, location details and picture of violation while reporting the same			
3	System should be able to batch process daily parking violation and send it to e-challan software for e-challan generation.			
4	As an end user, traffic police should be able to retrieve violation reports along with status of e-challan on daily/monthly basis			

4.2.6.5 Parking Variable messaging board

S. No	Parameter	Minimum Specification	Bidder Compliance	Product Documentation Reference
1	Source of light	High intensity LEDs		
2	Colour	True Colour		
3	Brightness:	>8000 cd/m2		
4	Luminance Class:	L-3 as per EN 12966		
5	Contrast Ratio:	R2-R3 as per EN 12966		
6	Beam Ratio:	B-3 as per should be		

		wide angle B6 or B7 or B4		
7	Viewing distance:	>300 meters		
8	Display capability:	Alpha-numeric, Pictorials, Graphical & Video		
9	Display Front Panel:	100% anti-glare		
10	Language:	Multilingual (Hindi/English/Gujarati) and all fonts supported by windows		
11	Auto Dimming:	Auto dimming adjust to ambient light level.		
12	In built sensor:	Photoelectric sensor		
13	. Storage capacity:	Minimum 100 GB		
14	Display area:	Display size of VMD should be 3x2 mtrs.		
15	Number of Lines &Characters:	The number of lines and characters can be customized as per the requirement s(Min. 3 lines & 10 characters)		
16	Brightness & control:	Controlled through software		
17	Display Driving method:	Direct current control driving circuit. Driver card of display applies Direct Current Technology.		

18	Display Style:	Stay on and flashing		
19	Connectivity:	IP based		
20	Access control:	Access control mechanism would be also required to establish so that the usage is regulated.		
21	Integration:	With smart city operations centre and service providers for offering G2C and B2c services.		
22	Construction:	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment.		
23	Battery:	Internal Battery with different charging options (Solar/Mains)		
24	Power:	Automatic on/off operation		
25	Casing:	IP-55 rated for housing		
26	Operating conditions:	0 Degree to 55 degree C		

4.2.6.6 Smart Card Reader

S. No	Parameter	Minimum Specification	Bidder Compliance	Product Documentation

				Reference
1	Display	7" inches or higher scratch resistant multi point capacitive touch screen with minimum WSVGA resolution (1024 X 600). 3.5" QVGA with backlight, TFT-LCD, 260K, 240 x 320		
2	Dimensions (W X H X D)	87 (min.74) x 218 x 56.2 (min.29)mm		
3	Weight	497g to 502 g		
4	CPU/Processor	520MHz		
5	RAM	128MB RAM		
6	Memory	128MB ROM (Optional)		
7	Expansion slot	At least a micro SD slot supporting up to 16 GB memory card		
8	Audio	Good quality Speaker with 1W or higher output for announcements. Speaker, Headset jack		
9	External Keyboard support	Device should support keyboard through USB or Bluetooth interface		
10	Connectivity	Device should support both 3G, GPRS		

		and Wi-Fi, should support GPS feature		
11	USB Port	At least one free USB port shall be available after setting up the entire solution including peripheral devices		
12	Battery	Rechargeable, 3.7V, 4,000mAh, Li-ion. Battery should be minimum 3000 MaH for the hand held terminal (HHT).		
13	Operating system	Should support latest versions of iOS, Android and windows		
14	Certification	RoHS (Restriction of Hazardous substance)CE or UL		
15	Indicators	Status indicator provides ease of use, Indicators for connectivity (presence/absence), signal strength, battery status etc.,		
16	Barcode Reader	Barcode reader capable of reading 1D Laser Class II or 1D&2D CMOS Imager		

17	SIM/ SAM Slots	Minimum 1 SIM and 2 SAM Slots (Security encryption of MI Card) to support secure loading of signed applications		
18	Biometric Sensor	STQC certified Finger Print Module		
19	Smart Card Reader	ISO 7816 Compliant		
20	Printer	Integrated or external. 2" thermal Printer (max. 90mm/sec)		
21	Antenna (mandatory)	Internal		
22	Terminal Management	Device should be remotely manageable in secured mode		
23	Warranty	Suitable Warranty support		
24	Certification	PCI / EMV Certification (Bank Certified)		
25	RFID Reader	Optional, ISO 14443 A/B (MIFARE, Calypso), ISO 15693; ISO 14443 A/B (MIFARE, Calypso), ISO 18092 (NFC), Felica		
26	Radio	• WWAN Radio- Optional, CDMA 1x for		

		Korea SKT, LGT; GSM/GPRS/eGPRS for global • WLAN Radio- IEEE 802.11b/g • WPAN Radio- Bluetooth V2.0+EDR Class II		
27	Capabilities for Transaction and Payment	• MSR- Bi-directional, Track1,2,3, ISO 7810, ISO 7811, ISO 7813 • Contact Payment- EMV Level 1&2, ISO 7816 • Contactless Payment- Optional, EMV Contactless Level 1 & 2 (Master PayPass, Visa Wave) • PIN Transaction- Optional, PCI PED 2.0; APACS Common Criteria; GIE CB Approved		
28	GPS	Optional, Integrated GPS w/ AGPS and DGPS PERFORMANCE CHARACTERISTICS		
29	Environment & Durability	• Operating -20°C to 55°C/ -4°Fto 131°F• Storage- 30°C to 70°C/ -22°Fto 158°F• Humidity- 93% non-		

		condensing Damp heat Cyclic --0perating-40˚C, 95%RH for (12+12 hrs.)), No. of cycles: 2 • Drop/Free Fall Specification- 4ft. / 1.2m drop to steel surface with silicon case, 2drops per 6 sides • Vibration Test should be in packed condition, switched off conditions (10-150Hz, 0.15mm/2g, 10 sweep, cycles/axes) • Bump test should be in packed condition, switched off condition.(1000Bumps, 40g, in vertical position)		

4.3 Cyber Security

This section provides detailed cyber security requirements across various domains:

- Network Security
- Application Security
- Data Security
- IoT Device Security
- Electronic Medical Record Security
- Cyber Security Governance

4.3.1 Network Security

Area	Cyber Security -Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference
Switches	• Switches should be equipped with user authentication and password management procedures • Security settings on different management interfaces (physical and logical) should be enabled • Logging and monitoring should be enabled • Configuration to defy common security attacks like IP spoofing, ICMP redirects • Delegation of privileged use in accordance with job function Session management • Configuration of VLANs and associated protocol • Security Controls around port security, Spanning Tree protocol, VLAN trunking protocol etc. should be enabled • Ensure updated version of IOS / patches are implemented		
Routers	• Routers should be equipped with user authentication and password management procedures • Security settings on different management interfaces (physical and logical) should be enabled • Logging and monitoring should be enabled • Configuration to defy common security attacks like IP spoofing, ICMP redirects • Delegation of privileged use in accordance with job function Routing protocols configured and appropriate security settings • Review of access lists for different		

	network segments (to different outside networks) • Ensure updated version of IOS / patches are implemented		
Firewalls	• Ensure placement of firewall within the network policies and rule sets • Authentication & Authorization mechanism should be enabled • Auditing, logging, monitoring, alerting mechanism should be enabled • Stringent password control and security controls for administrative / management interfaces • Firewall should be configured to defy commonly known security attacks • Configuration of access control and priority of traffic flow Allowed inbound and outbound services • Service proxies, circuit-level gateways, and packet filters should be enabled • VPN configuration and encryption should be enabled • Updated version of OS / patches should be implemented		
Intrusion Prevention / Detection Systems	• Ensure secured placement of devices • Authentication and Authorization mechanism should be enabled • Auditing, logging, monitoring , Incident management should be enabled		

Network Monitoring Software	• Should monitor critical servers of the entire network including the branches for sizing etc. • It should monitor the network components of LAN & WAN, Fault Management, Performance Management of the network and the servers, Inventory Management, automatic discovery of network components etc. • Functional capabilities and effectiveness of NMS software should be reviewed and audited		
Network Architecture Security	• Network should be segregated into various trusted zones, route path and table audit • Security measures should be implemented at the entry and exit points of the network		
Wi-Fi Security	• Secure authentication mechanism through unique user id password should be enabled • Security policies should be deployed at various levels based on the requirement • For Wi-Fi –Access - DoT Guidelines and PEAP (Protected Extensible Authentication Protocol), 3 rd Generation Partnership Projects for Wi-Fi Networks		

4.3.1.1 Operating System and Database security

Area	Cyber Security -Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference

OS Security Configuration	• **Windows** Secure Access Management should be enabled User and group privileges & System and user policies should be enabled Secure remote access polices should be enabled Logging mechanism should be enabled Service packs and hot-fixes should be updated regularly System services and applications Policies and procedures that govern its use Patch and Antivirus update Registry settings, including registry security permissions Profiles and log-in scripts • **UNIX** Secure Access Management should be enabled Secured Network Information System (NIS), Network File System (NFS) should be enabled Ensure control over Cron jobs Security patches should be updated regularly		

Database Security Configuration	• **Oracle** Secure Access Management should be enabled Controlled allocation of privileges and usage of privilege accounts Auditing, logging and monitoring should be enabled Secured DBMS configuration Appropriate policy to monitor deviation - Database activity monitoring (DAM) tools		

4.3.2 Application Security

Area	Cyber Security -Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference
Application Testing	• Security testing should be conducted pre-deployment – functionality, usability, scalability and security • Regular application audit post deployment- functionality, usability, scalability and security		
Backup	• Data storage ,backup and restoration should be enabled as per regulatory and business requirement		
Logging & Audit Trail	• Logging based on data criticality should be enabled on application • Audit trail maintenance and availability as per business and regulatory requirement		

Application Access Management	• Strong access control mechanism should be enabled with need based access • Regular access review should be conducted • Ensure controlled usage of generic and system password		
Password Management	• Strong password management features based on criticality of application		
Interface security	• Encrypted and authenticated data exchange between application (within Smart City or with external components)		
Encryption	• The message exchange between various applications in the smart city should be fully encrypted and authenticated. • Any application outside the Data Centre (DC) should talk to the applications hosted in the datacenter through only predefined APIs. • Centralize control of application-layer encryption and file system encryption • Secure sensitive data across a broad range of platforms and on-premises and PaaS environments • Stop malicious DBAs, cloud administrators, hackers and authorities with subpoenas from accessing valuable data • Streamline large-scale encryption migrations with Batch Data Transformation utility • Required encryption of specific data or database fields at the application, before data is stored • Encrypts data as either NIST approved AES-CBC or Format Preserving Encryption (FPE)		
Patch Management	• Regular security patch updates and hotfixes should be applied using Four Phase approach - Measurement and Assessment,		

	Identification and Classification, Estimation and Preparation and Implementation		
Software License Compliance	• Policy and procedures should be followed for software license compliance • Actions should be defined for non-compliance to software licensing		
Web Application Security –OWASP Top 10-2013	• Threat analysis should be conducted where appropriate tests targeting critical applications, application modules or access methods are identified • Web applications should be scanned at defined frequency for known vulnerabilities		
Configuration Security	• Ensure Minimum Baseline Security Standards (MBSS) for all application		
Application Load Testing	• Load testing should be conducted to identify application's maximum operating capacity as well as any bottlenecks		

4.3.3 Hardware Security

Area	Cyber Security -Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference

Functional Capabilities	• Must support cryptographic offloading and acceleration • Should provide Authenticated multi-level access control • Must have strong separation of administration and operator roles • Capability to support client authentication • Must have secure key wrapping, backup, replication and recovery • Must support unlimited protected key storage • Must support clustering and load balancing • Should support Logical cryptographic separation of application keys • Must support —k of n‖ multi-factor authentication		
Application Program Interfaces (APIs)	• PKCSNo.11, OpenSSL, Java (JCE), Microsoft CAPI and CNG		
Host connectivity	• Dual Gigabit Ethernet ports (to service two network segments)		
Cryptography	• Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA, ECDH • Symmetric algorithms: AES, ARIA, Camellia, CAST, RIPEMD160, HMAC, SEED, Triple DES • Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit) • Full Suite B implementation with fully licensed ECC including Brain pool and custom curves		

Security compliance	• FIPS 140-2 Level 3		
Safety and environmental compliance	• Compliance to UL, CE, FCC part 15 (for Commercial products) • Compliance to RoHS2, WEEE		
Management and monitoring	• Support Remote Administration — including adding applications, updating firmware, and checking the status— from NoC • Syslog diagnostics support • Command line interface (CLI)/graphical user interface (GUI) • Support SNMP monitoring agent		
Physical characteristics	• Standard 1U 19in. rack mount with integrated Smart Card Reader		
Performance	• RSA 2048 Signing performance - 7000 RSA 2048 Key generation performance - 25 • ECC 256 bit Signing performance - 14000 ECC 256 bit key generation performance - 1500		
Custom Application	• Should enable secure execution of custom security-critical application code within the tamper resistant hardware boundary		
Key Generation and Protection	• Ability to generate RSA keys (2048 and 4096) on board on demand and shall be secured by high security module in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules		

	Validation. RSA 2048 key generation performance min 10 keys/second		
Key back up and restoration	• The proposed solution must include the software/hardware to - securely store the keys at DC, at DR and at one remote location and restore them in case of necessity		
No. of Keys to be protected	• The HSM must secure a minimum of 1 lakh keys in accordance with FIPS 140-2 level 3 standards. The licensing and HSM hardware must have no restriction on the number of keys to be protected		
Performance upgrade of HSM	• The performance of HSM should be upgradable on field.		
Instant Key reflection	• Multiple HSMs to be supportable for DR, key backup, key update, and key processes, load balancing and failover. Should support instant key reflection to all the HSMs in the system.		
Logical partitions	• Unlimited logical/cryptographic separation of application keys. all The licenses must be included		

4.3.4 Data Security

Area	Cyber Security -Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference
Data Privacy	• Should ensure adherence to IT Act 2000 in terms of data privacy • Biometric information capture, stored and transmitted should follow Aadhar Act 2016 • Protection of cardholder data , compliance to PCI DSS is mandatory		
Data Exchange	• Security features across data in transit (password protection, device protection, network protection) • Data exchange with external entity as per the legal and regulatory guidelines • Security of data exchanged within internal entities (e.g.. edge device to aggregator) • As per MoUD requisite, all message exchange between various applications should be fully encrypted and authenticated		
General Security	Authentication capabilities: • All systems should require a username and password to access functionality, at a		

	minimum. To enhance authentication capabilities, • The solution should support strong authentication mechanisms (one-time passwords, certificate and biometric-based authentication, etc.).		
	Authorization capabilities: • All functionality should require and enforce proper permissions before performing any actions		
	• Automatic and secure update of software, firmware, etc.: Software/firmware update mechanisms should be available, and updates should be delivered in an automatic and secure way		
	Auditing, alerting, and logging capabilities: • All systems should provide mechanisms for auditing and logging security events. • Logs must also be saved securely against tampering.		
	Anti-tampering capabilities: • Devices should have a mechanism to prevent tampering by unauthorized sources		
	No backdoor/undocumented/hardcoded accounts: • Removing or disabling these accounts should be enforced in the service-level agreement (SLA) to ensure vendors will comply.		

	• Only basic functionality should be enabled by default, and the rest should be enabled depending on the organization's needs		
	Fail safe/close: • In the case of a system malfunction or crash, the system should remain secure and security protections remain enforced.		
	• Solutions should come with a secure configuration by default.		
Electronic card data Security	• The payment gateway provider should be Level 1 compliant with the Payment Card Industry Data Security Standard (PCI DSS) and also offer built-in security such as tokenization		
	• They should have proper encryption on all payment pages, have solid authentication procedures (such as 3D secure pin, One time password authentication etc) , use API's to securely post data from the website etc.		
	• Electronic signatures should be used by each party involved in the transaction		
	• Communication path used to communicate between the parties should be encrypted and secured protocols should be used.		
	• Confidentiality and non-accessibility of the transaction from the internet		
	• Password authentication of all users		
	• Conformation to legal and regulatory requirements		

4.3.5 IoT device security

Area	Cyber Security -Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference
Device Identity Management	• Consolidate, organize, and manage identity relationships for people, devices, and sensors using digital certificates		
IoT Network Security	• MUST support standards-based secure protocols that provide authentication, data confidentiality,data integrity, and replay protection to safeguard any sensitive data in transit. • MUST support a cryptographic authentication mechanism (e.g., public key) for communication between peers • MUST support proper validation of peer credentials. • If they transmit sensitive data, then non-secure protocols MUST require an authorized administrative action to enable. • MUST prevent unauthorized traffic from traversing different interfaces. • Physical interfaces MUST satisfy be disable or MUST satisfy allow only authorized access and be invulnerable to attack. • The Network Operator or IoT Service Provider should perform an assessment of the network services that are needed to enable the IoT Service (voice, data, SMS, etc.) both now and in the future. • Based upon this assessment the Network Operator should operate on the "principle of least		

	privilege" and provision the IoT Service Provider's subscriptions with only those services required for the specific IoT Service. • Network Operators should implement secure subscription management processes for IoT subscriptions that enable critical IoT Services • Network Operators should identify the UICCs used for IoT Services from traditional UICCs used to provide traditional services and, if required by the IoT Service Provider, segregate these appropriately. • Recommendations for IoT using LPWA technologies: a) Whether an IP network layer is implemented over the link layer. b) Whether a secure element is present, and if so, whether it is removable. c) To what extent data integrity is guaranteed. d) Whether any algorithms or key lengths supported by the technology are black-listed or should be deprecated (such as 64-bit encryption keys for GPRS). • For 3GPP LPWA Network Technologies: a) Whether Remote SIM Provisioning (RSP) is supported. b) Which integrity algorithms (EIAx/GIAx) and confidentiality		

	algorithms (EEAx/GEAx) are implemented and permitted. • For LoRaWAN: a) Whether ABP (Activation By Personalisation) or OTAA (Over-The-Air Activation) is implemented, and for OTAA whether an AppKey may be shared between devices. • For All LPWA Devices: a) What form (if any) of security certification has been undertaken.		
IoT Encryption	• Encrypting data at rest and in transit between IoT edge devices and back-end systems using standard cryptographic algorithms, helping maintain data integrity and preventing data sniffing by hackers IoT encryption must be accompanied by equivalent full encryption key lifecycle management processes		
IoT PKI	• Digital certificate and cryptographic key and life-cycle capabilities, including public/private key generation, distribution, management, and revocation • Digital certificates securely loaded onto IoT devices at the time of manufacture and then activated/enabled by third-party PKI software suites		

IoT security analytics	• IoT security analytics will increasingly be required to detect IoT-specific attacks and intrusions that are not identified by traditional network security solutions such as firewalls		
IoT Authentication	• MUST support authentication for administrative access. • MUST support strong authentication for all users including administrators. • MUST require the configuration of unique identification and authentication credentials on first use. • Authentication data MUST be protected against unauthorized disclosure, modification (e.g. FIPS140-2 strength of authentication mechanism requirements and/or OWASP IoT Top 10 authentication requirements). • MUST prevent users from escalating privileges without administrative authorization. • MUST prevent enumeration of user accounts.		
IoT Device Physical Security	• MUST incorporate visible tamper evidence mechanisms. • MUST support mechanisms to prevent unauthorized access to internal components. • MUST support tamper detection mechanisms that sends alert, zeroize private keys anddisable the device itself. •		
Alert & Logging	• MUST support sending an alert on any attempts to upgrade. • Support sending an alert on any attempts to gain administrative access. • support sending an alert when		

	tampering or attack has been detected. • MUST support sending an alert when changing from secure communication and/or interfaces to non-secure communications and/or interfaces. • support sending an alert when changing any setting related to the handling of sensitive data • Support sending an alert upon being reset to factory defaults. • Alert messages MUST be time-stamped.		
Platform Security	• MUST be invulnerable to exploits known within the information security community. • MUST NOT be rendered inoperable by denial of service attacks against which it is capable of defending per industry standard practices. • MUST support a secure boot mechanism including: b) a non-modifiable boot loader, c) verification of the integrity of software/firmware and critical configuration data, d) a manual administrative initiated verification of the integrity of software/firmware and critical configuration data. • MUST support a secure remote upgrade mechanism including: a) authorized initiation and activation of upgrade b) validating authentication and integrity of signed		

	code, c) supporting a rollback in the event of a failed upgrade, d) maintaining configuration and stored data after upgrade, e) reporting version data on authorized administrative request. • MUST support a clock with the following attributes: a) supports synchronization with an authorized time source, b) maintains accuracy within 1 second per day, c) maintains time in the absence of power or synchronization source		

4.3.6 Data at rest security requirements

Area	Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference
Separation of Duty and Privileged User Access Control	• The solution must be able to protect data-at-rest against root/system privileged user account access. It should also protect file level encryption. • Proposed data protection solution must support fine-grained policy to enable administrator to perform activity like file archive and backup without access to the data content itself. • The proposed solution must support a separation of duties (SoD) to meet rigorous compliance rules including PCI		

	DSS, HIPAA/HITECH and government data breach policy. The vendor must provide compliance whitepaper to prove such support capability • Proposed solution must support multi-tenancy using separate domain with configurable policies, data encryption key management and audit log. Must have a seamless SIEM Integration. Must protect the unstructured data (file-shares, files and folders) including big data.		
support Transparent Data Encryption	• The proposed data protection and encryption solution must support transparent data protection on all major operating system include: • Microsoft: Windows Server, 2008, 2012 • Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Oracle RedHat Compatible Kernel and Ubuntu • UNIX: IBM AIX, HP-UX, and Solaris Database • There should not be any changes in the storage space after the encryption. • Proposed data protection solution must be able to secure both structure database information and unstructured files such as PDF, spreadsheet, scripts, images, audio/video recordings and extract-transformation-load batch files • Proposed data security solution should have minimum performance impact to database		

	transactions with not more than 10% performance overhead on transactions. Vendor must provide benchmark report to prove the performance claim • The data transformation should not involve any downtime and live transformation is expected to achieve high Performance Encryption with 100% System Uptime. - Solution must be able to enforces access controls based on – "resources", "processes", and "time based access" so that only the defined resources can be accessed with the defined processes and defined users/groups at any given time - Ability to learn the effect of policies (learn mode) before actual encryption is applied is must. -Not only appliance but agent also needs to be FIPS certified		
Application Encryption and Tokenization	• The data protection solution must support format preserving tokenization • the proposed tokenization and masking solution must provide REST API • The data masking solution must support dynamic masking through policy based masks • The proposed solution should support Teradata V14 and V14.1 database encryption with UDF • The proposed platform should support vault less		

	tokenization • The proposed platform should support vault based tokenization • The proposed platform should support gateway to encrypt data stored on S3 and Box		
Key Management and KMIP	• The proposed encryption and key management solution must be able to support KMIP client • The proposed solution should be certified to support Nutanix KMIP • The proposed solution must provide centralized key management for Oracle and MSSQL TDE master key. • The security administrator console should support 2-factor authentication with RSA. • The data protection solution must provide centralized audit for security administration access, key creation, policy changes, data access log and so on. • The proposed solution must provide application encryption support with Java, C/C++, and .Net API. • The proposed solution support LDAP and Microsoft Active Directory authentication • Support industry proven cryptograph security standard:3DES, AES128, AES256, ARIA128, and ARIA256 and asymmetric key RSA-4096/2048, SHA-256 algorithm The Key management repository		

	must provide virtualization option, with OVF image for deployment option - Hardened Operating System, root account must be disabled, all unnecessary software packages must be removed. A firewall in place that only opens a limited set of required ports		
Installation and Deployment	• Proposed data security and encryption solution must support transparent deployment which does not require application code change. • The proposed data protection solution must support cloud deployment with Amazon AWS, Rackspace • The proposed data protection solution must support deployments including physical, virtual and cloud based servers with minimal administrative overhead. • The proposed data protection solution must support a centralized policy and key management, with highly configurable security and policy enforcement to provide granular access control and audit. • The proposed security repository must support high-availability clustering configuration across Local Area Network (LAN) and across geographies over Wide Area Network(WAN). Vendor must provide network architecture		

	diagram to illustrate the high availability setup.		
High Performance	• The proposed data protection solution must support hardware cryptographic acceleration including • Intel and AMD AES-NI • SPARC encryption • IBM P8 cryptographic coprocessor		
Data Access Audit and Report	• The proposed data protection solution must provide fine-grained auditing records that show system accounts and processes accessing data based on security policy. • The proposed data protection solution must support integration with SIEM solution include: Archsight, Splunk, IBM Qradar, and deliver centralized access audit and monitoring report		
Certification & Validations	• The encryption key manager must be Common Criteria (ESM PP PM V2.1) certified • The encryption key manager should have option with FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level Certified		

4.3.7 Cloud security requirements

Area	Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference
Cloud Setup	• Ensure public facing services are deployed in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer • Security rules should be defined as part of firewall to restrict access • Cloud offering should have built-in user-level controls and administrator logs for transparency and audit control • The Primary DC and the DRC should be in different seismic zones		
Network	• VPN gateway should be enabled for controlled access • Appropriate security rules should be enabled to encrypt outward data flow • IDS, IPS, API Gateways and ELB logs for any activities, access and exceptions carried out in the cloud setup should be enabled • Database logs should be configured to be routed as part of the Logging VPC setup		
API Gateways	• Digital Certificate should be used to secure access to API Gateways • Data flow between external API and internal API Gateway should be encrypted • Logging and monitoring		

	should be enabled		
Web Services	• Web Application Firewall should ensure perimeter security solution for the web services • IPS should be hosted on all the Web servers • Web servers should be configured as per the CIS hardening guidelines and baseline security requirements • Logging and monitoring should be enabled		
OS and DB	• Application access between applications hosted, internal infrastructure and external traffic should be segregated • Database instances should be hardened as per the CIS baselines configuration guidelines in the cloud setup • Logging and monitoring should be enabled		
Secure Code	• Cloud Applications should undergo regular secure code review		
Compliance	• Certification/Compliance: Provisional Empanelment of Cloud Service Offerings CSPs facilities/services shall be certified to be compliant to the following standards: ISO 27001, ISO 27018, ISO 20000-9, ISO/IEC 20000-1 & PCI DSS - The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000		

	• Encryption should be implemented based on data classification (for confidential data)		
	• Incident management should be managed by Cloud Service Provider (CSP)		
	• Data encryption should be implemented for data at rest using departments managed keys, which are not stored in the cloud		
	• CSP should inform all security breach incidents to Smart City management		
	• SLA with CSP should ensure data confidentiality		
	• Sub-contractual risk should be covered by CSP		
	• Location where data resides shall be as per terms and conditions of the "Empanelment of the Cloud Service Provider"		
	• E-Discovery to be included as clause in SLA with CSP		
	• Audit: ensure that the CSP's services offerings are audited and certified by STQC/MeitY		
	• Exit Management Plan should include - Transition of Managed Services & Migration from the incumbent cloud service provider's environment to the new environment shall follow all security clauses		
	• Performance Management of CSP should be done through SLA		

	• Dispute Resolution: Escalation procedure shall be set in the SLA. • Unresolved cases move to mediator, expert panel and then referred to Arbitration		
Data Security	• The Data Centre Facility shall at a minimum implement the security toolset: Security & Data • Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Single Signon, UTM, One Time Passwords, Multi Factor Authentication, Log Analyser / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Web Application Filter for OWASP Top 10 protection, Data Privacy, Data Encryption, Certifications & Compliance		

4.3.8 Cyber Security Governance

Area	Cyber Security -Detail Requirement	Bidder Compliance (Yes/No)	Product Documentation Reference
Third Party Security			
Service Level Agreement	• There should be an agreement about the specific security features of the product/service • There should be a clear understanding that the absence or malfunction of these features could have legal and/or financial consequences for the vendor		

	• Agreement should include continuous (24/7/365) 'reliability tested' support for security incidents related to its products/service • There should be a defined and limited timeframe during which vendors must provide solutions when security flaws are found • There should be a clear understanding that non-compliance could have legal and/or financial consequences to the vendor.		
	• Agreement should include that vendors prove their compliance to security requirements through third-party testing, certifications, etc.		
	• MSI should clearly define controlled sub-contracting		
Vendor Vulnerability record	MSI should assess its vendor vulnerability record by checking: • How does the vendor protect its own infrastructure from attacks and intellectual property leaks? • How does the vendor protect its own infrastructure from attacks and intellectual property leaks? • Does the vendor run regular independent code reviews and penetration tests on its products, networks, and systems? • How does the vendor protect details about its clients, such as design details, product lists, and client contact information? • Does the vendor enforce supply-chain cyber security to prevent the delivery of products with malware, backdoors, etc.? • Does the vendor have a public security vulnerability disclosure		

	and reporting policy and proper contact channels to get the vulnerability reports? • Does the vendor have support teams for security issues/incidents, such as a Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), online support, etc.?		
Secure Development	MSI should assess development process by checking: • How does the vendor test its products and simulate large-scale environments to verify its product's usability? • Does the vendor have a Secure Development Life Cycle (SDLC) program? If so, how long has it been running? • Does the vendor adequately protect its development environment and intellectual property from spying or manipulation? • ensure vendor compliance to remove any backdoors, undocumented and hard cored accounts		
Physically segmented Zones	• The information processing center should be segmented into multiple zones with each zone having a dedicated functionality • The internet facing part of the data center should have a Demilitarized zone where all the customer application servers would be located that are customer facing. Only these servers can access the data from the actual utility application servers on predefined ports		

Physical Entry Control	• The information processing center should be controlled through secured access/biometric access with periodic access review • Guarded/restricted visitor access management		
Environmental Control	• The information processing center should be protected from fire, electrical and water damage		
Equipment Maintenance	• The information processing center should undergo routine maintenance and reporting of all IT equipment		
Power Supply	• The information processing center should have uninterrupted power supply ensuring continuity to business		
Surveillance	• The information processing center should be guarded by trained security guards and CCTV cameras		
Product Management			
Integration	• MSI should evaluate the security impact when integrating a new product to the existing system and deploy specific measures to ensure security (i.e. network segregation, monitoring of specific KPI, etc.).		
Hardening	• All devices and systems deployed in Smart city should be hardened with the ability to be upgraded remotely for firmware through encrypted image files		
Certification	• In smart cities, certification authorities could be available to evaluate products and solutions on behalf of Service Provider. • These certifications could be used to support decision-making, but the testing scope and procedures should be		

	verified.		
Operation and Maintenance			
Monitoring	Monitoring: • MSI should monitor the stability of the services, tracking any suspicious activity, abnormal behavior, performance hooks, or any other service-threatening events by regularly reviewing system audit logs and/or other available mechanisms		
Patching	Patching: • Service Provider and vendors are expected to collaborate on deploying the latest security patches. • Patches should be deployed per the company's patch management policies, taking into account the urgency of the patches. • Patches are expected to be tested in the lab environment first. There are challenges associated with patching IoT devices when compared to traditional enterprise IT systems. Often it is the device firmware that must be updated. When doing so, make sure that the firmware update mechanisms deliver the updates in a secure manner–that is with encryption and a digital signature.		

Regular Assessment	Regular assessment and auditing: • Testing smart services is also expected to run continuously to verify service compliance with the applicable standards and security policies (i.e. make sure encryption remains turned on, authentication enabled, strong passwords set, security settings not changed, etc.). • Being ready to respond is imperative to protecting infrastructure. Testing services is especially relevant after applying new changes to the systems, where simulating a large-scale live environment might not be possible, and testing changes might only be possible in the production environment.		
Logging	Protection of logging environment: • All logs should be safely transmitted and stored. • Logging should occur as close to the end-device as possible, although it may not be possible to collect or routinely forward data at some disadvantaged devices. • In these instances, maintaining situational awareness through data collection at IP propagators such as WiFi or other protocol routers, gateways, and standard network security devices should be evaluated.		
Access Control	Access control • Appropriately monitoring who, when, and how someone has access to smart service systems is critical to prevent unplanned changes, tampering, or		

	downtime, which are not acceptable in smart city environments.		
Threat Intelligence	• Threat intelligence enables an organization to identify regional and worldwide occurrences, such as new, trending, common, and regional attacks. Armed with such information, an organization can update its security posture and parameters as needed to block attacks before they happen. • Cyber-threat intelligence could also be used on a country-level by the government, where certain traffic patterns and source locations could be blocked upon need on the regional Internet gateways, protecting all Service Provider within.		
Reaction and Recovery	• It is important to create detailed procedure manuals or checklists that define compromised. This includes things like certificate revocation, key zeroization, and systems isolation and clean up, as well as how to follow up on the incident in order to understand how the system was compromised and develop plans so that it will not happen again.		
Implementation			
Secure Delivery	• It should have not tampered with, modified, etc. from the time it was shipped from the solution provider. • Binaries should be cryptographically signed, and devices should have not been tampered with.		

Encryption	• All communications should be properly protected against unauthorized eavesdropping, interception, and modification. • Encryption keys must be well protected and kept in a safe place.		
Secure System administration	• Avoid using a single administrator system user to perform all actions on all systems. • Use different administrator users and passwords and grant granular permissions.		
Set strong passwords	• Access to administration interfaces, functionality, etc. should require a user account with a strong password. • Passwords policy must be defined for password strength and duration validity. • To enhance authentication capabilities, use strong authentication mechanisms (one-time password, certificate- or biometric-based authentication, multifactor authentication, etc.) especially any technology that can impact public safety.		
Disable unused functionality and services	• Some solutions have all functionality and services enabled by default. Disabling unused functionality and services reduces the attack surface and prevents possible attacks that abuse weaknesses in those functions and services.		
Remove unnecessary user accounts	• Some solutions come with test/default accounts and passwords that could be used by unauthorized parties to access the systems, if these accounts are not removed. Specific accounts can be created for the implementation process, but		

	these accounts must be removed after the solution is installed and not used for operation purposes. These accounts should be identified in the product and implementation documentations for easy identification and removal.		
Enable auditing of security events	• Constantly monitoring audit logs will help to identify ongoing attacks and breaches.		
Anti-tampering, anti-vandalism	• Devices should be protected against unauthorized physical access for modification, vandalism, or device stealing.		
Testing	• Before implementing specific technology, the same model, version, etc. must have passed security testing.		
	• Penetration testing is a recommended method for verifying the security of smart city products. When faced with real-world attacks, services could misbehave, leak data, or even crash.		
Change Request	• Formal Change Management process shall be established, which covers all types of change-upgrades and modifications to application and software, modifications to business information, emergency 'fixes', and changes to the computers / networks that support the application.		
	• Formal "Request For Change" form shall contain the following detail: Description of change, Change objective or reason for change & users affected		
Change Impact Analysis	• Feasibility Analysis -a. Need for change, b. Impact of change, c. Priority of change should be		

	conducted for all type of changes related to IT infra		
Change Testing	• Changes shall be tested to help determine the expected results (for e.g., deploying the patch into the live environment)		
Change Implementation	• Changes shall be reviewed to ensure that they do not compromise security controls (e.g., by checking software to ensure it does not contain malicious code, such as a Trojan horse or a virus)		
	• Changes to the application shall be performed by skilled and competent individuals who are capable of making changes correctly and securely and signed off by an appropriate business official.		
Change Rollback	• Back-out positions shall be established so that the application can recover from failed changes or unexpected results		
Change Monitoring and Verification	• the change shall be monitored for a few days to ensure that the change has not affected the regular business operations		
Information Security Incident Management			
Information Security Incident	It defined as the act of (or the threat of) occurrence of non-compliance with the security policy, procedure that may result in: • Loss of confidentiality of information assets. • Compromise of integrity of information assets. • Denial of service. • Misuse of service, systems or		

	information assets. • Damage to information assets		
Incident Response Team (IRT)	• Notify IRT in a timely manner of any incident detected/reported that require immediate attention. • Record incident details in preliminary incident report • Initial Diagnosis, Classification and Preliminary Support – IT helpdesk Team • Investigate and analyze incident • Ensure that data and information found during investigation is not tampered • Resolve and Report incident • Incident reporting to *Computer Emergency Response Team (CERT-In) and NCIIPC (National Critical Information Infrastructure Protection Centre)*		
Assessment and Identification	• Derive list of security threats and vulnerabilities Check relevance of new software updates		
Estimation and Preparation	• testing the software update in a production-like environment • Taking approval for patch implementation		
Implementation & Reporting	• Deployment of the approved patches • Monitoring and reporting on the		

	progress of deployment		
Backup and Recovery	• There shall be documented backup and recovery procedures for the following: a. Source codes and/or executables of Application software b. Data files of all application software c. End-user document files like Microsoft Office documents etc. d. Electronic mail e. System software's like operating system, RDBMS etc. f. Parameter and configuration files of networks and network devices		
	• Combination of full and incremental backup or full backup shall be taken based on the criticality of data, servers		
Backup scheduling & media	• Type and frequency of backup and type of backup media to be used shall be depend on: Volume of data, Criticality of data and Recovery time constraints		
Type of backup solution	• Automated backup or Manual Backup		
Backup logs	• Backup logs shall be reviewed to ensure verification of successful completion of backups.		
	• Backup logs shall be stored for a period of 60 days		
Security of Backup Process	• Data on Backup media (tapes, disks etc.) shall be secured against unauthorized access. • Backup media shall be secured against environmental and physical threats. • For all applications, a copy of the backup shall be stored offsite.		

Recovery Testing	• Recovery testing shall be done periodically for all and those applications for which synchronized data backup at DR site is not available to ensure that data can be recovered from the backup media. • Frequency of recovery testing shall be at least every six months.		
Backup Failure	• In case of failure of backup incidence shall be raised and incident management process shall be followed		
Secure Data disposal	• Securely erase data on systems storage. This is a good measure to apply, but destruction of storage may be required to assure the safe, quick disposal of critical data.		
Secure device disposal	• Vendor replacement is also important. While many Service Provider think about the disposal of data correctly, a vendor's maintenance and support personnel could easily access smart service systems to perform regular maintenance activities. If they replace hardware, the vendor could repurpose it at other clients or dispose of it without appropriate security measures. Hardware that is removed from live environments by support personnel is not usually protected. Vendors are expected to provide secure technology disposal as part of their services and maintenance contract with the client organization.		

Avoid reuse	• Avoid repurposing technology by the same organization or third parties. It could leak sensitive design, client, password, or cryptographic information, which could create a threat to production services.		

4.4 Servers

4.4.1 Blade Chassis

No.	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Minimum 6U size, rack-mountable, capable of accommodating minimum 8 or higher hot pluggable blades		
2	Dual network connectivity of 10 G speed for each blade server for redundancy shall be provided		
3	Backplane shall be completely passive device. If it is active, dual backplane shall be provided for redundancy.		
4	Have the capability for installing industry standard flavours of Microsoft Windows, and Enterprise RedHat Linux OS		
5	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE, Oracle VM etc. OEM of the blade chassis and servers offered should in "Validated Configuration" list and certified by OEM to run virtualization.		
6	DVD ROM shall be available in chassis, can be internal or external, which can be shared by all the blades		

	allowing remote installation of software	
7	Minimum 1 USB port	
8	Two hot-plug/hot-swap, redundant 10 Gbps Ethernet or FCoE module with minimum 16 ports (cumulative), having Layer 2/3 functionality. If bidder is offering FCoE based solution, corresponding ports must be present in server as well as storage controller.	
9	Two hot-plugs/hot-swap redundant 16 Gbps Fibre Channel module for connectivity to the external Fibre channel Switch and ultimately to the storage device	
10	Power supplies shall have N+N (Hot Swap/Hot Plug). All power supplies modules shall be populated in the chassis. Required number of PDUs and power cables, to connect all blades, Chassis to Data Centre power outlet.	
12	Hot pluggable/hot-swappable redundant cooling unit	
13	Provision of systems management and deployment tools to aid in blade server configuration and OS deployment	
14	Blade enclosure shall have provision to connect to display console/central console for local management such as troubleshooting, configuration, system status/health display.	
15	Single console for all blades in the enclosure, built-in KVM switch or Virtual KVM features over IP	

16	Dedicated management network port shall have separate path for remote management.	

4.4.2 16 Core Server

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	Processor	16 Cores (E5 Xeon 2600 V4 series)		
4.	Memory	64 GB		
5.	Hard disk drive	3 TB usable post RAID		
6.	Controller	Integrated SAS Raid Controller with RAID1 1with512 MB cache		
7.	Networking features	Total 04 nos of Gigabit LAN ports		
8.	Ports	Minimum of 1 * internal USB 2.0 port		
9.	Server Connectivity to SAN	Support for Dual-Port 8 Gbps FC Host Bus adapter		
10.	OS Support	Red Hat Enterprise Linux 5.7 (32 bit and 64 bit) Red Hat Enterprise Linux 6.0 (32 bit and 64 bit) SUSE LINUX Enterprise Server 11 (32 bit and 64 bit) SUSE LINUX Enterprise Server 10 (32 bit		

		and 64 bit) VMware ESX 4.1 VMware ESXi 5.0		
11.	Warranty	3 year 24x7 4Hour response comprehensive warranty		
12.	Server Management	Should have comprehensive solution for complete monitoring and management of the server health, preferably of the same brand as of the server supplier		

4.4.3 32 Core Server

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	Processor	32 Cores (E5 Xeon 2600 V4 series)		
4.	Memory	128 GB		
5.	Hard disk drive	6 TB usable post RAID		
6.	Controller	Integrated SAS Raid Controller with RAID1 1 with 512MBcache		
7.	Networking features	Total 04 nos of Gigabit LAN ports		
8.	Ports	Minimum of 1 * internal USB 2.0 port		

9.	Server Connectivity to SAN	Support for Dual-Port 8 Gbps FC Host Bus adapter	
10.	OS Support	Red Hat Enterprise Linux 5.7 (32 bit and 64 bit) Red Hat Enterprise Linux 6.0 (32 bit and 64 bit) SUSE LINUX Enterprise Server 11 (32 bit and 64 bit) SUSE LINUX Enterprise Server 10 (32 bit and 64 bit) VMware ESX 4.1 VMware ESXi 5.0	
11.	Warranty	3 year 24x7 4Hour response comprehensive warranty	
12.	Server Management	Should have comprehensive solution for complete monitoring and management of the server health, preferably of the same brand as of the server supplier	

4.4.4 8 Core Server

No.	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	Processor	8 Cores (E5 Xeon 2600 V4 series)		
4.	Memory	32 GB		

5.	Hard disk drive	1 TB usable post RAID	
6.	Controller	Integrated SAS Raid Controller with RAID1 1 with 512MBcache	
7.	Networking features	Total 04 nos of Gigabit LAN ports	
8.	Ports	Minimum of 1 * internal USB 2.0 port	
9.	Server Connectivity to SAN	Support for Dual-Port 8 Gbps FC Host Bus adapter	
10.	OS Support	Red Hat Enterprise Linux 5.7 (32 bit and 64 bit) Red Hat Enterprise Linux 6.0 (32 bit and 64 bit) SUSE LINUX Enterprise Server 11 (32 bit and 64 bit) SUSE LINUX Enterprise Server 10 (32 bit and 64 bit) VMware ESX 4.1 VMware ESXi 5.0	
11.	Warranty	3 year 24x7 4Hour response comprehensive warranty	
12.	Server Management	Should have comprehensive solution for complete monitoring and management of the server health, preferably of the same brand as of the server supplier	

4.4.5 Firewall

No.	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	Physical attributes	• Should be mountable on 19" Rack • Modular Chassis • Internal redundant power supply		
4.	Interfaces	• 4 x GE, upgradable to 8 GE • Console Port 1 number		
5.	Performance and Availability	• Encrypted throughput: minimum 800 Mbps • Concurrent connections: up to 100,000 • Simultaneous VPN tunnels: 2000		
6.	Routing Protocols	• Static Routes • RIPv1, RIPv2 • OSPF		
7.	Protocols	• TCP/IP, PPTP • RTP, L2TP		

	• IPSec, GRE, DES/3DES/AES • PPPoE, EAP-TLS, RTP • FTP, HTTP, HTTPS • SNMP, SMTP • DHCP, DNS • Support for Ipv6	
8. Other support	• 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS	
9. QoS	• QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies.	
10 Management	• Console, Telnet, SSHv2, Browser based configuration • SNMPv1, SNMPv2	

4.4.6 Switch

4.4.6.1 8 Port Industrial Grade access Switch

No.	Parameter	Minimum Specifications	Bidders Compliance (Yes/No)	Product Documentation Reference
Proposed Make, Model with Warranty/AMC : <<pls. specify>>				
1	Ports	8 Port Rack / DIN Rail Mountable Industrial Grade L2 Managed POE/POE+ Switch with: • Minimum 6 10/100/1000 Mbps Ethernet POE/POE+ ports and 2x1G SFP / Combo ports loaded with necessary SFP modules required as per design from day one. • All RJ 45 ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, TX, half-duplex or full duplex and flow control for full-duplex ports.		
2	Switch type	Layer 2		
3	MAC	4k or more		
4	Backplane	Properly sized non-blocking Switching fabric capacity (as per network configuration to meet performance requirements of wire speed switching for the connected devices)		
5	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
6	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.		
7	Layer 2 features	• IEEE 802.1Q VLAN tagging. • 802. 1Q VLAN on all ports with support. • Spanning Tree Protocol as per IEEE 802.1d • Multiple Spanning-Tree Protocol as per IEEE 802.1s		

- Rapid Spanning-Tree Protocol as per IEEE 802.1w
- Self-learning of unicast & multicast MAC addresses and associated VLANs
- Jumbo frames up to 9000 bytes
- Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
- "Port Mirroring" functionality for measurements using a network analyzer.
- Broadcast, Multicast and Unicast storm control on per port basis to prevent degradation of overall system performance occurred due to faulty end stations.
- Switch hardware should support IEEE 802.1ah MAC-in-MAC encapsulation or IEEE 802.1ad Qin Q.
- Should support Ethernet (IEEE 802.3, 10BASE-T)
- Should support Fast Ethernet (IEEE 802.3u, 100BASE-TX)
- Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)
- Must support Ten Gigabit Ethernet (IEEE 802.3ae)
- Software based standards for Network Device
- Must support IEEE 802.1d - Spanning-Tree Protocol
- Should support IEEE 802.1s - Multiple Spanning Tree Protocol
- Must support IEEE 802.1q - VLAN encapsulation
- Should support IEEE 802.3x Flow Control

		• Must support auto-sensing and auto-negotiation (Link Speed/Duplex)	
9	Protocols	• IPV4, IPv6 • Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • DHCP support • Support IGMP Snooping and IGMP Querying • Support Multicasting • Should support Loop protection and Loop detection, • Should support Ring protection	
10	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication	
11	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent	
12	Protocol and Traffic	• Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number	
13	Management	• Switch needs to have console port for management via PC • Must have support SNMP v1,v2 and v3 • Should support RMON feature • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP/HTTP etc. Configuration management through CLI, GUI based software utility and using web interface(optional)	
14	Power	• Switch proposed must have redundant power supply from day one	

15	Compliance	• UL/EN/IEC or equivalent
16	Operating Temperature	• -40°C to 70°C
17	IP Enclosure Rating	• IP 30 or equivalent Industrial Grade Rating

4.4.6.2 24 Port Industrial Grade access Switch

o.	Parameter	Minimum Specifications	Bidders Compliance (Yes/No)	Product Documentation Reference
Proposed Make, Model with Warranty/AMC : <<pls. specify>>				
	Ports	24 Port Rack Mountable Industrial Grade L2 Managed POE/POE+ Switch with : • Minimum 20 10/100/1000 Mbps Ethernet POE/POE+ ports and 4x1G SFP ports loaded with necessary SFP modules required as per design from day one. • All RJ 45 ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, TX, half-duplex or full duplex and flow control for full-duplex ports.		
	Switch type	Layer 2		
	MAC	16k or more		
	Backplane	Properly sized non-blocking Switching fabric capacity (as per network		

		configuration to meet performance requirements of wire speed switching for the connected devices)		
	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.		
	Layer 2 features	• IEEE 802.1Q VLAN tagging. • 802. 1Q VLAN on all ports with support. • Support for minimum 16 k MAC addresses • Spanning Tree Protocol as per IEEE 802.1d • Multiple Spanning-Tree Protocol as per IEEE 802.1s • Rapid Spanning-Tree Protocol as per IEEE 802.1w • Self-learning of unicast & multicast MAC addresses and associated VLANs • Jumbo frames up to 9000 bytes • Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad. • "Port Mirroring" functionality for measurements using a network analyzer. • Broadcast, Multicast and Unicast storm control on per port basis to prevent degradation of overall system performance occurred due to faulty end		

		stations. • Switch hardware should support IEEE 802.1ah MAC-in-MAC encapsulation or IEEE 802.1ad Qin Q. • Should support Ethernet (IEEE 802.3, 10BASE-T) • Should support Fast Ethernet (IEEE 802.3u, 100BASE-TX) • Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab) • Must support Ten Gigabit Ethernet (IEEE 802.3ae) • Software based standards for Network Device • Must support IEEE 802.1d - Spanning-Tree Protocol • Should support IEEE 802.1s - Multiple Spanning Tree Protocol • Must support IEEE 802.1q - VLAN encapsulation • Should support IEEE 802.3x Flow Control • Must support auto-sensing and auto-negotiation (Link Speed/Duplex)		
	Protocols	• IPV4, IPv6 • Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • DHCP support • Support IGMP Snooping and IGMP		

		Querying • Support Multicasting • Should support Loop protection and Loop detection, • Should support Ring protection		
0	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication		
1	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent		
2	Protocol and Traffic	• Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number		
3	Management	• Switch needs to have console port for management via PC • Must have support SNMP v1,v2 and v3 • Should support RMON feature • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP/HTTP etc. Configuration management through CLI, GUI based software utility and using web interface(optional)		
4	Power	• Switch proposed must have redundant power supply from day one		
5	Compliance	• UL/EN/IEC or equivalent		

6	Operating Temperature	• -40°C to 70°C		
7	IP Enclosure Rating	• IP 30 or equivalent Industrial Grade Rating		

4.5 Data Centre

4.5.1 Firewall

No.	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
	Make		<to be provided by the bidder>	
	Model		<to be provided by the bidder>	
1	Physical attributes	Should be mountable on 19" Rack Modular Chassis/Appliance Design Internal redundant power supply		
2	Interfaces	Should have minimum 4X1GE ports and 2X10G port with necessary SFP loaded from day one. Should be scalable to add 2 or more 10G ports in future. Console Port 1 number		
3	Performance and Availability	Encrypted throughput: minimum 20 Gbps Concurrent connections: Minimum 5 million concurrent sessions or more and 300,000 new sessions per second or more Simultaneous VPN tunnels: 2000		

4	Routing Protocols	Static Routes RIPv1, RIPv2 OSPF
5	Protocols	TCP/IP RTP IPSec, DES/3DES/AES FTP, HTTP, HTTPS,SNMP, SMTP DHCP, DNS, Support for IP v4 & IPv6 IPSEC
6	Other support	802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS, Support multilayer firewall protection, Traffic shaping, Bandwidth monitoring
7	QoS	QoS features like traffic prioritisation, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies.
8	Management	Console, SSHv2, Browser based configuration SNMPv1, SNMPv2, SNMPv3
9	Additional Features	Should have inbuilt HDD of minimum 64 GB Should support DDoS protection
10	Certifications	ICSA/NDPP/EAL4

4.5.2 Intrusion Prevention System

This can be offered as separate unit or as a module in firewall

No.	Item	Required Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
	Make		<to be provided by the bidder>	
	Model		<to be provided by the bidder>	
1	Performance	Should have an aggregate throughput of no less than 200Mbps Total Simultaneous Sessions – 500,000		
2	Features	IPS should have Dual Power Supply IPS system should be transparent to network, not default gateway to Network IPS system should have Separate interface for secure management IPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.		
3	Real Time Protection	Web Protection Mail Server Protection Cross Site Scripting SNMP Vulnerability Worms and Viruses Brute Force Protection SQL Injection Backdoor and Trojans		
4	Stateful	TCP Reassembly IP Defragmentation		

	Operation	Bi-directional Inspection Forensic Data Collection Access Lists
5	Signature Detection	Should have provision for Real Time Updates of Signatures, IPS Should support Automatic signature synchronization from database server on web Device should have capability to define User Defined Signatures
6	Block attacks in real time	Drop Attack Packets Reset Connections Packet Logging Action per Attack
7	Alerts	Alerting SNMP Log File Syslog E-mail
8	Management	SNMP v1, v2, v3 HTTP/HTTPS SSHv2, Console
9	Security Maintenance	IPS Should support 24/7 Security Update Service IPS Should support Real Time signature update IPS Should support Provision to add static own attack signatures System should show real-time and History reports of Bandwidth