



Kolkata Port Trust

KOLKATA PORT TRUST

**Supply, Installation, Commissioning, and Maintenance
of RFID Systems at Kolkata Dock System, Kolkata Port
Trust**

Request for Proposal

Volume I: Technical and Functional Requirement

Document Reference No: **Plg/165/RFID/11667**

Date: 18th April 2017

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

Table of Contents

1.	INTRODUCTION	4
1.1.	<i>About Kolkata Port Trust</i>	4
1.2.	<i>Purpose of this Document</i>	4
1.3.	<i>Project Background</i>	4
1.4.	<i>Project Objectives.....</i>	5
2.	IMPLEMENTATION SCOPE	6
2.1.	<i>Overall Scope of the work</i>	6
2.2.	<i>Broad set of activities under the scope of this project</i>	8
2.3.	<i>Detailed Scope of Work:</i>	11
2.4.	<i>Organisation Scope</i>	35
2.5.	<i>Solution Scope</i>	35
2.6.	<i>Process Scope:</i>	35
2.7.	<i>Functional Scope:</i>	36
2.8.	<i>Installation Scope</i>	36
2.9.	<i>Report Generation.....</i>	36
2.10.	<i>Project Phases</i>	36
2.11.	<i>Governance Model for O & M support</i>	37
2.12.	<i>Service Level Agreement (SLA).....</i>	37
2.12.1.	<i>Service Level Agreement Framework</i>	37
2.12.1.1.	<i>Timely Delivery</i>	38
2.12.1.2.	<i>Down Time.....</i>	38
2.12.1.3.	<i>Average Pass Generation Time (PGT).....</i>	40
2.12.1.4.	<i>Average Monthly Pass Generation Failure (PGF)</i>	41
2.12.1.5.	<i>Average Pass Verification Time (PVT)</i>	42
2.12.1.6.	<i>Average Monthly Pass Verification Failure (PVF)</i>	43
2.12.1.7.	<i>Average Resolution Time</i>	44
2.12.2.	<i>Quality Management.....</i>	45
2.13.	<i>Status Reports</i>	45
2.14.	<i>Project Timelines:</i>	46
2.15.	<i>Project Governance Structure</i>	46
2.15.1.	<i>Steering Committee</i>	46

2.15.2. Project Management Team	47
2.16. Facilities Provided by KoPT to the successful bidder	47

1. Introduction

1.1. About Kolkata Port Trust

Kolkata Dock System (KDS), Kolkata Port Trust (KoPT) – KDS-KoPT is a premier dock system of Kolkata Port in eastern India under the administrative control of the Ministry of Shipping, Government of India, commanding approximately 4576 acres of land and handling vessels and cargo to cater to the demand of a vast hinterland. KDS, KoPT primarily carries out vessel and cargo operation and handles around 15 million tonnes of cargo (which primarily includes container, break bulk cargo, etc.) and around 1450 vessels annually.

Under KDS, KoPT there are two impounded dock systems viz. Kidderpore Dock (KPD) and Netaji Subhash Dock (NSD) with 21 Multipurpose Berths, 5 Dedicated Berths for Containers, 1 Dedicated Berth at NSD for Liquid Bulk and 1 Passenger Terminal. In addition, there are 6 riverine Oil Jetties at Budge Budge. Cargo is also handled at various anchorages at deep-drafted locations viz. Sandheads, Sagar, Diamond Harbour, etc.

1.2. Purpose of this Document

The objective of this document is to solicit bids from the interested parties, hereinafter called as bidder or Service Provider (Service Provider), who can demonstrate their organizational, technical and financial capabilities for the **“Supply, Installation, Commissioning and Maintenance of RFID system at Kolkata Port Trust on OPEX Model and provide Operations and Maintenance (O&M) support for a period of 07 years from the date of Go-Live”**.

1.3. Project Background

Kolkata Dock System (KDS), Kolkata Port Trust (KoPT) is a premier dock system of Kolkata Port in eastern India under the administrative control of the Ministry of Shipping,

Government of India. KDS, KoPT primarily carries out vessel and cargo operation and handles around 15 million tonnes of cargo (which primarily includes container, break bulk cargo, etc.) and around 1450 vessels annually. Under KDS, KoPT there are two impounded dock systems viz. Kidderpore Dock (KPD) and Netaji Subhash Dock (NSD) with 21 Multipurpose Berths which includes dedicated berths for Containers, Liquid Bulk and Passenger Terminal.

Due to the increased threat to the ports from various corners which had necessitated the need of enhanced surveillance and security at the port area, KoPT decided to implement a Radio Frequency Identification (RFID) based Port Access Control System based on Government of India formulated "National Maritime Agenda 2010-20" in which RFID was identified as a key technology for Port Sector security and efficiency enhancement.

Presently, KDS, KoPT uses various Information & Communication Technology (ICT) enabled solutions to handle its day-to-day management and operational activities. An established optic fiber network covering all major locations / buildings act as the backbone for information flow (KDS-NET). The proposed RFID based access control solution is envisaged to be seamlessly integrated with the existing ICT environment at KDS, KoPT.

Existing Permit System at KDS, KoPT: The Docks are a prohibited area with certain areas restricted under ISPS Plan and physical access into this area is administered through issuance of Dock Entry Permits falling under various categories. Presently, at KDS, KoPT, permits are generated using integrated application software deployed at seven (7) Permit Generating Counters in different offices of KDS which includes Budge Budge also. A permit request is submitted by the user. After due verification of credentials and payment, the permit issuance approval is issued by Port authorities. Photo enabled permits are generated through this system and printed. Verification is carried out by CISF/PSO personnel at designated gates of KDS, KoPT.

1.4. Project Objectives

KoPT is implementing the RFID based Port Access Control System (PACS) to achieve the following broad objectives:

- Enhance operational efficiency through reduced labour intensive workflow processes
- To have systematic and secured entry, movement & exit of men and vehicles
- Augment and strengthen the security at all the gates and within port premises
- To automate and speed up movement and activity within ports
- To generate visibility of activities within and around gates/port area
- To control the access/movement to authorized time & zones
- To track every movement of vehicle across the port
- To trace each movement and alert on anonymous pattern of activity
- To record all movements of individuals & vehicles to create verifiable historical audit trail
- To prevent revenue leakage and any malpractices at the gates
- To comply with the International Ship and Port Facility Security (ISPS) code

2. Implementation Scope

2.1. Overall Scope of the work

The selected Service Provider shall have the following overall scope of work:

- Conduct a Detailed Functional Requirement study, System Requirements Study and System Design
- Obtain prior approvals from KoPT authorities on Design/ Requirements documents before initiating actual implementation work to ensure alignment to project objectives/ requirements
- Supply, installation, implementation, configuration, customization, integration and testing of RFID Based Access Control System together with relevant system software(s) at the 08 Gates of Netaji Subhash Dock (NSD) and the 06 Gates of Kidderpore Dock.
- Procurement, installation, configuration and commissioning of central servers for hosting the RFID based Access Control System at KoPT in Data Centre

- Procurement, installation, configuration and commissioning of central servers for hosting the proposed RFID based Access Control System in the Disaster Recovery Center.
- Implement the RFID solution using the existing KDS-KoPT network wherever available. Else, procure, install, configure and commission a wired and wireless network to connect all the required pass issuance counters, gates and port premises. Feasibility and requirement study should cover the network requirement study also.
- Create and maintain comprehensive master database for the RFID based Access Control System.
- Testing of the application developed and deployed and taking sign-off from the KoPT.
- Change Management and Capacity Building including Training of users for effective use of the system
- Comprehensive Operation and Maintenance of the entire RFID based Access Control System infrastructure including networking, if done by the Service Provider, for a period of 07 (Seven) years, from the date of Go-live. The maintenance includes RFID based security solution maintenance, IT infrastructure maintenance, network maintenance, system administration, security administration, database administration, end-user problem resolution and staffing the sufficient resources.
- Setting up and O&M support of a total Ten (10) pass issuance counters, which includes manning the counters, at Subhash Bhawan, Kidderpore Dock, Port Security Office and Budge Budge during the 1st year of operations.
- O&M support of only 3 counters, at any of the above four locations, which includes manning the counters, from the 2nd year onwards till the completion of contract.

- KoPT reserves the right to increase or decrease the number of counters being operated based on requirements and payment towards the same shall be made by KoPT on a pro-rata basis.
- Place a Project Management Team or Core team at the site consisting of following:
 - 02 Technical resources i.e. 1 Project Manager and 1 Solution Architect
 - Place sufficient manpower at pass issuance counter such that the respective SLA criterion is fulfilled. The pass issuance counters are to be operated 24 x 7 x 365 days.
 - Deploy sufficient Operational team members for supporting the Project Management team and pass issuance counters for smooth and continuous operation of the counters.
 - Payment towards OPEX shall be made based on the SLA and service delivery.
- Carry out one time enrolment of users and issuance of printed permanent RFID cards to them
- Documentation of the RFID based Access Control System Project

2.2. Broad set of activities under the scope of this project

- Supply, installation, commissioning of hardware (Boom Barrier, Flap Barriers, Photo capturing web/digital cameras, computers and servers, digital label printers, RFID cards, LPRs, Readers, Long Range RFID Readers, 32" LED screens, Application for tracking GPS enabled device/ modems for tracking vehicles, SMS Gateway, CISF cabins and other accessories as per BOQ as provided in Annexure V) and System software (Operating system, Database) and Application Software (Personalization Software, with features like Time and Attendance management, Data logs, Enrolments & renewal software with built-in Visitor Management System for issue of port entry permits, vehicle passes, tracking the IN/Out movement of Visitors and Vehicles, GIS& GPS based vehicle tracking software etc.) Software should have the facility to be customized to meet the specific requirements & reporting system of Port.

- Setup, Operate and manage enrolment counters with adequate number of photo capturing web/digital cameras, computers and servers, Digital printers, RFID reading and/ or writing devices 32" LED screens and other accessories, and software (operating system and applications) for issue of dock entry permits to visitors and vehicle so that the complete infrastructure is in sound and good working conditions.
- Supply and Issue of Contactless Mifare cards as per requirement. The cards supplied shall be with the holder and lanyard.
- Supply of consumables like Print Heads , cartridges , cleaning cartridges, and other consumables required for printing on RFID cards
- Maintaining the RFID Access control System and complete solution throughout the year on around the clock basis (365 x 24x7) during the currency of contract.
- Personal Computers shall be provided at different locations for operation of Access Control System for various verification and online approval.
- The Port Access Control System and solution should be maintained in such a way that there is minimal downtime and minimal breach of SLAs
- The works mentioned are illustrative and not exhaustive and bidder may have to carry out any other works related to access control system, issue of permits, vehicle tracking system and other components which are not explicitly included above but are implied by nature. The entire system shall be operated round the clock.
- Technical manpower resources including IT support executive, repair technicians, etc. shall be provided by the Service Provider.
- The complete permit issuance process should be online. The details shall be updated to the central server through the network connectivity provided by the Port.
- The service provider shall supply, install and commission the entire infrastructure required at Data Centre, which is planned to be set up at Subhash Bhavan and Disaster Recovery Centre which is planned to be set up at HQ.

- Even though Port provides the network, the vendor should consider network failures and design the system in such a way to have minimum or no downtime. Failure of network should not be claimed as reason for breach of SLA.
- Service Provider will be responsible for insurance of all the manpower & hardware/network supplied and installed by vendor for risk coverage (accidental hazards, death and disability of person, other hazards which may occur due to trespassing vehicles and/or natural adverse climatic calamities-War, Fire, Cyclone, Salinity problems at shore).
- Necessary interfacing with Port LAN/WAN. It shall be the responsibility of the service provider to arrange for equipment that would be necessary for interconnectivity/cabling between the switches at the gate end , Flap Barrier, Boom Barrier, etc. and server.
- Installation of Access Control Server at a central location and connection of all access control equipment with central server.
- The Access Control System Solution should be an integrated solution with the entire data including the photographs, biometrics, and data logging to be stored on central server.
- It will be responsibility of the vendor to provide and fix the shelters for Card Readers, Flap Barriers exposed to open weather and Cabins for setting up of system at gates. All associated civil works for fixing and installation of flap barriers/tripod and boom barrier has to be carried out by the successful vendor.
- All system components should be certified by UL or any other reputed Indian / foreign certifying agency to ensure product reliability and product quality. Any operating system software or application software, which will be part of the system, shall come with proper and legal licenses. Such licenses shall be procured in the name of Kolkata Port Trust, or as informed by KoPT, from day one.
- Final testing and commissioning of complete system including training, submission of reports, drawings, login & passwords and database design etc.
- Post implementation on-site support and maintenance.
- All other items in the scope of system implementation.

2.3. Detailed Scope of Work:

2.3.1. Detailed Functional Requirement study, System Requirements Study and System Design

- Project Preparation
 - A detailed project charter including the detailed project plan indicating all activities, with resources required, their roles and responsibilities and time schedule of deliverables needs to be prepared at the start of the project and submitted to KoPT for approval.
 - The project charter should also contain detailed project description, approach and methodology, milestones, deliverables, project organization, roles and responsibilities, project risks and mitigation plans, dependencies etc.
 - The project charter should include a detailed program for installing and implementing the RFID based Access Control System covered under this RFP.
 - Service Provider shall form a project team comprising the following key positions:
 - Project Manager
 - Solution Architect
 - Project Management Team should be deployed at the project site from the beginning of the requirement gathering/ SRS study phase.
 - The Service Provider shall not change any member of the Project Team during the entire implementation of the project. However, in the unlikely event of a change being required, the procedure for replacement of personnel shall be followed as per the agreement mutually signed by the parties.
- Requirements Gathering:
 - A high-level analysis of the existing processes has already been done and functional requirements have been identified. The indicative Functional Requirements as envisaged for this project are referred in the **Annexure I** of Volume I of the RFP document.

- Service Provider needs to go through the document, and shall consult with KoPT authority wherever necessary, to obtain more details/ clarity on the requirements of the project and have to get a sign-off separately for the Functional Requirements. The Service Provider shall conduct a detailed Functional Requirements study and prepare a FRS document accordingly.
- The Service Provider shall conduct detailed discussions with KoPT officials (or its representatives) and do subsequent analysis to ensure that each of the requirements captured during the FRS stage are covered in the requirements analysis and are later incorporated in the RFID based Access Control System.
- The Service Provider shall carry out a detailed survey of the Port area and shall identify a suitable method for the creation of Geo-spatial Map of the Port area for GPS based vehicle tracking software. KoPT will provide the maps of the Port area as input data to the Service Provider wherever available. In case maps are not available then the Service Provider shall define alternate method of generating the Geo-spatial database of the port area where the vehicle tracking system is implemented.
- Activities conducted as part of this task will result in the project deliverable “RFID based Access Control System - Functional Requirements & Software Requirement Specifications” (SRS) document, which shall detail the requirements of the complete solution up to the granular/ ground level.
- System Design
 - The Service Provider shall prepare a comprehensive Systems Architecture and design documents for the RFID based Access Control System after conducting a comprehensive analysis of the requirement. This design should include Solution Architecture, Hardware Deployment Architecture, Network Architecture and Security Architecture etc. for the RFID based Access Control System.

- The Architecture document should give the complete architecture of the proposed RFID based Access Control System. The documents including, but not limited to the following, shall be submitted for sign-off:
 - Application Functional architecture
 - Format of all input screens including data entry requirements
 - Format of all reports that would be generated by the system
 - Access control mechanisms, data security and audit trails to ensure that databases are not tampered with or modified by unauthorized users.
- Build a complete audit trail of all transactions using transaction log reports and store them in database, so that errors in data, intentional or otherwise, can be traced and reversed.
- Design and Implementation of the System Architecture: The Service Provider shall be entirely responsible for the architecture of the system implemented to satisfy all features, functions, performance and security as described in this document including sizing of the required hardware. System architecture description provided in this document is for reference only. The Service Provider should ensure all possible and required improvements.
- The Service Provider shall provide Plans for User Acceptance Tests (UAT) and System Integration Tests (SIT) including Performance Tests (PT) to KoPT and/or its designated Third Party Audit Agency (TPAA) and make the necessary changes to system configuration to optimize performance as per recommendations of KoPT and/or TPAA.
- The Service Provider shall be responsible for making sure that all the above considerations are adequately met. The Service Provider shall deliver an architecture document covering the above aspects.
- The Service Provider shall make necessary arrangement for management reports, dashboards, business intelligence tools, SMS gateway, Online payment gateway, online e-wallet and Data migration in line with the expectations of users provided in the functional requirements.

2.3.2. Supply, installation, implementation, configuration, integration and testing of RFID Based Access Control System together with relevant system software

- The Service Provider shall deploy a dedicated team experienced in installation, configuration, integration, testing, implementation and deployment of the proposed RFID Based Access Control System at KoPT
 - Configuring the third party built-in applications, development of interfaces wherever and whenever necessary.
 - Service Provider shall ensure that the proposed RFID Based Access Control System provides adequate interfacing mechanisms (both at the application and data level) with a view to future integration. Such interfaces shall follow industry standards such as Application Programming Interface (API's) and web services.
 - Service Provider shall supply and install the application and related software, integration tools, along with the customized source code and requisite perpetual licenses for RFID based security application. The tentative Bill of Material is provided in **Annexure V**.
 - Service Provider shall design the hardware configuration in line with contemporary principles and ensure that it comprises various servers including database, application, web servers etc.
 - Service Provider shall consider stakeholder inputs when they are finalizing all processes including user interfaces, mode of data entry, storage and retrieval, output reports, queries and the application design as a whole.
 - The system must have easy-to-use user interfaces, perform tasks with minimum clicks, quick links (maximum select options and provide suitable short-cuts) wherever possible along with Help screens.
 - The system shall provide services through online also so that the visitors need not to visit the counter for availing the services like applying for permit, renewal of permit, collection of pass fee etc.
 - Service Provider shall create and manage all necessary master files for the proposed RFID based Access Control System.
 - Service Provider shall create and manage the complete set of Geo-spatial database required for the vehicle tracking system. KoPT will provide the

maps of the port area wherever available. If not available, service provider shall collect the data through alternate source and shall be acceptable to the KoPT.

- The layout of the Port area along with the number of gates and volume of traffic for the year 2013, 2014 and 2015 is provided in Annexure-I. The furnished figures are only indicative information for providing the volume of traffic.
- Service Provider to provide a Network Monitoring Software (NMS) to KoPT for monitoring all the devices connected on IP related to RFID project being implemented. Necessary configuration of all such components needs to be done by Service Provider so that all IP based components are visible on NMS for monitoring. The NMS should provide alerts for such components that are offline or down. NMS should be capable of providing reports of all such downtime with date and time and also calculate the total downtime.
- PACS software should have the feature to calculate the total time taken for each pass issuance. Pass issuance time will be calculated from the time issue process was initiated by the pass issuance resource till the time pass was printed. Software should be able to provide system generated monthly reports on such pass issuance time.
- PACS application should provide a system generated monthly report of the number of transactions failed.
- PACS application should provide a system generated monthly report on the total time taken by the application to verify a pass.
- PACS application should provide a system generated monthly report on the total number of passes that were not read.
- Service Provider to provide an online issue ticketing tool for raising and addressing of issues by users. The tool should be capable to provide reports based on various parameters like no. of issues raised, issues resolved, open issues, average time taken for resolution, etc.

- Service Provider to setup a command control centre at Subhash Bhawan to centrally monitor the traffic movements and should have following indicative features:
 - View of each gate should be consolidated on the central display device at Command centre.
 - Feature to pull-up individual gates for scrutiny based on requirements
 - Feature to remotely zoom cameras if required
 - Feature to alert officials at the gates on requirement
- A 32" LED monitor to be installed in the chamber of the Traffic Manager, KoPT for viewing the activities like Access Control and Vehicle Tracking within Dock. Necessary client software to view the activities in real time mode should be supplied.
- Compliance to Standards
 - Service Provider shall ensure bilingual (English & Hindi) support and other relevant standard formats for display, Printing and transmission of data.
 - Service Provider must ensure that the technology components adhere to flexibility, interoperability, usability, availability, manageability, security and integration standards
 - Service Provider shall ensure adherence to all relevant standards as defined and notified by regulatory bodies.
- Deployment Architecture
 - Service Provider shall ensure deployment of servers and commissioning of application at the Data Center which would be setup by Service Provider at Subhash Bhawan at KoPT premises and Disaster Recovery Center which would be setup by Service Provider at Head Quarters.. The deployment of application shall follow and comply with contemporary principles of Information Security Management System (ISMS) i.e. ISO 27001. Service Provider shall ensure the deployment of management and monitoring tools like Project Management, Application Performance

Monitoring, Version Control (software as well as document), issue tracking tools etc.

- Testing and Hosting
 - Service Provider shall conduct all tests as a part of standard Software Testing Life Cycle (STLC). The detailed Testing requirements are elaborated in the subsequent sections of this RFP.
 - Service Provider shall facilitate Port or its nominated agencies to conduct User Acceptance Testing, Application Security testing (vulnerability testing and penetration testing) and Infrastructure Security
 - It is the responsibility of the Service Provider to get the complete RFID infrastructure including PACS solution, implemented in KoPT, audited by Cert-In empanelled agencies and produce the compliance reports every year to KoPT during the currency of the contract.

2.3.3. Setting up of Data Centre at Subhash Bhavan, KoPT and Procurement, installation, configuration and commissioning of central servers for hosting the RFID based Access Control System at Data Centre

- Service Provider shall be responsible for setting up of Data centre at Subhash Bhawan, KoPT for hosting RFID based Access Control System
- KoPT will provide the space; power (General Power) for setting up of Data Centres (DC and DR). The Data Centres shall be set-up by the service provider as per industry best practice for similar type of organization.
- Service Provider shall be responsible for Installation, configuration and commissioning of Central servers for hosting RFID based Access Control System at the Data Centre (DC)
- Service Provider shall ensure that adequate skilled technical and qualified staffs are available to operate and manage the DC at desired levels.
- The servers should be able to scalable enough to accommodate future requirements that may arise due to scaling-up of operations/ load. All hardware including, but not limited to the servers procured, shall be branded and reputed.

- It must be noted that all system hardware and perpetual software licenses shall be on the name of Kolkata Port Trust from day one.

2.3.4. Procurement, installation, configuration and commissioning of central servers for hosting the proposed RFID based Port Access Control system in the Disaster Recovery Centre (DRC)

- Service Provider shall be responsible for setting up of Disaster Recovery centre at Kolkata Port Trust Head Quarter Building at 15, Strands Road, Kolkata.
- Service Provider shall be responsible for Installation, configuration and commissioning of central servers for hosting RFID based Access Control System at Disaster Recovery Centre (DRC) **Kolkata Port Trust Head Quarter Building at 15, Strands Road, Kolkata..**
- The proposed DRC shall act as a Business Continuity Centre in case of failure of DC. Service Provider shall make all necessary configurations so that the DRC shall serve as business continuity in case of Data Centre failure.
- Service Provider shall ensure that adequate skilled technical and qualified staff is available to operate and manage the DRC at desired levels.
- The recommended servers should be able to accommodate possible scaling up requirements in the future. All hardware including, but not limited to the servers procured, shall be branded and reputed.
- It must be noted that all system hardware and software licenses shall be on the name of Kolkata Port Trust from day one.
- The proposed DRC shall act a business continuity centre. In case of failure of the Data Centre, the application at the DRC shall take over without causing any interruption to the operations and should be made available and operational within 30 minutes from the time of failure of DC.

2.3.5. Procurement, installation, configuration and commissioning of wired and wireless network to connect all Pass issuance counters, operational gates and all other locations in the project

- Service Provider will establish its own reliable and fail-safe network/ IT infrastructure for operationalization of RFID solution. Service Provider can use the existing KDS-NET network and make necessary last-mile connectivity (using KDS-NET as backbone) between the gates and various zones of KDS-KoPT shall be established using OFC/ wireless connectivity, including connectivity at all pass issuance counters.
- Service Provider shall draw out and specify detailed specifications for the network that needs to be used for the RFID based Access Control System to perform satisfactorily
- The Networking requirement is for the list of locations as specified in Annexure I of volume I of the RFP document.
- Service Provider shall ensure that the recommended network shall be able to accommodate scaling up requirements of the KoPT in future.
- Service Provider shall carryout the installation as per the instructions defined in the Annexure III of Volume I of the RFP Document.
- Service Provider shall provide, install, configure and commission required client side computing infrastructure comprising of hardware and software, handheld terminals, etc.

2.3.6. Create and migrate the complete master database required for the functioning of the RFID based Access Control System.

- The master database is a critical component of the system. This should store unique datasets which are to be used across application.
- Master Data is a single source of basic data used across multiple systems, applications, and/or processes.
- Service Provider shall identify and provide the set of master data required for the functioning of the proposed RFID based Access Control System and shall create the master data. Port will provide the required data to Service Provider in the format that is available with the port.

- Service Provider shall examine the existing applications and shall migrate the master data from the existing applications into RFID based Access Control System.

2.3.7. Create and manage the complete Geospatial database required for tracking the vehicles.

- Geo-spatial database is the base data required for any vehicle tracking system.
- Service Provider shall identify and define an appropriate co-ordinate system for the Geo-spatial database and creation of the GPS tracking application.
- KoPT will provide the maps related to Port, wherever available, as input data for the creation of Geo-spatial database. Service Provider shall define the method of conversion of maps into Geo-Spatial database. However, Service Provider shall be responsible for the accuracy of the Geo-spatial data
- Wherever the maps are not available, Service Provider shall identify the alternate means of creation of data (Ground Survey, DGPS survey, Satellite Imagery based survey etc.) and generate the data.
- The data shall be managed by the Service Provider through the project period. If any changes are made on ground, the same shall be updated in the Geo-spatial database.
- Design, develop and deploy an application that can depict the position and movement of the vehicles within the port area.
- Supply of the GPS enabled Vehicle tracking devices/modems are not in the scope of the bidder. However, Service Provider will be responsible for providing GPS enabled Vehicle tracking devices/modems to the concerned users on actual payment basis if the users require so. Hence, to have uniformity, specification of the GPS devices/modems should be specified in bid/ offer document. GPS devices should function based on both Wi-fi connectivity and/ or SIM based connectivity. Concerned users, if desire, may arrange for the said devices on their own based on the mentioned specification by Service Provider. Service Provider

should develop the GPS tracking application which is compatible with all standard GPS devices available in the market.

2.3.8. Testing of the application developed and deployed and taking sign-off from the Port

Service Provider shall perform the following tests, as required, before Go-Live of the Application. The broad testing and commissioning requirements are provided in the Annexure IV.

2.3.8.1. Acceptance Test and Approvals

This section covers the minimum requirements for system's functional and performance testing, mechanical, electrical, electronic testing of hardware and computer software, testing of discreet components making up the Works as well as the entire Works operating as a whole, at the Service Provider's factory as well as on site. Also covered are the minimum requirements for the commissioning and acceptance of the Works by the Port Authority on site as well as all test equipment and develop systems required to be provided by the Service Provider to be incorporated into the Works. These will involve at least the following:

- a) Submission of interface details for the various items of equipment that rely on other Service Providers to provide supporting structures and cable entries,
- b) Development and Set up of equipment prototypes in India / suitable location, which should cover all the individual system processes and, if ready for demonstration the integrated functioning of all system components as a whole (PAT)
- c) System functionality and performance testing to verify conformance of the system to specification. This will take the form of factory acceptance testing of random sample of every component of the system working independently and integrated into the whole system (FAT).
- d) Installation approvals and equipment unit testing (Benchmarking).
- e) System Site Acceptance Testing (SAT)
- f) Performance Guarantee Testing (PGT)

- g) The development of all the above test procedures shall always remain the responsibility of the Service Provider. These test procedures must clearly identify the steps to be followed to prove the system including the cross referencing against the Approved Technical Specifications document and shall be comprehensive. The agreed procedure must be followed precisely. However, KoPT Authority may vary these procedures should unexpected results emerge from the testing.

2.3.8.2. General Requirements for Testing

The Service Provider shall be required to supply all test equipment and permanent site test equipment and tools, where necessary.

2.3.8.3. Location for performing tests

All tests listed under this section shall be performed only in India.

2.3.8.4. Test Equipment

The Service Provider shall provide all the required test equipment and materials necessary to carry out the functional and operational tests of the total Works as deemed necessary by KoPT Authority during factory tests at the Service Provider's works, and during testing and commissioning of the Works on site. Pre-requisites and Test equipment list shall be part of respective Test procedure (PAT/FAT/SAT/PGT).

2.3.8.5. Prototype Approval Process

The prototype approval process shall be as follows:

a. Paper Design

The Service Provider shall develop the paper design of all the items requiring prototype approval and submit them to the KoPT Authority for approval. The Port Authority shall evaluate and add or alter the document and return to the Service Provider with all required amendments noted.

The format for the same shall be as per the process defined in the introduction part of this chapter.

b. Prototype Approval

Before the prototype approval tests are to be carried out, the Service Provider shall submit to the KoPT Authority the method statement of each

type of test, for approval at least 6 weeks in advance. Also, the complete responsibility of getting the document approved at least 2 weeks in advance before PAT, is that of Service Provider. KoPT Authority shall carry out the testing of all components of the Works in such a way as to guarantee the actual functionality of the equipment to meet the claimed specifications. These tests shall simulate normal operating conditions for the components being tested. The equipment that shall be tested shall include all aspects of the equipment to be supplied.

On completion of the test, the Port Authority shall notify the Service Provider of any unacceptable aspects of the prototype and the Service Provider shall correct such unacceptable works. If the remarks on prototype provided are of critical nature, then the whole prototype shall be tested again before proceeding to the next milestone. If not, then the remarks shall be verified as part of FAT.

Once the prototype testing has been completed and is acceptable to the KoPT Authority, the KoPT Authority shall issue an acceptance certificate for the prototype, which is "Prototype Test" acceptance.

c. Modifications to the Approved Prototype

The Service Provider may find it necessary for the approved prototypes to be altered as the Works progress. Should this be necessary, the Service Provider shall apply to KoPT Authority for a new approval as described above.

d. System Development Progress Reporting

The Service Provider shall note that they are bound to provide hardware and software progress reports as the works proceeds. These reports shall always contain the status of progress as against the Compliance Statement and the original schedule. These fortnightly reports shall be in the English language for project management purposes and shall include, but not be limited to the following:

e. Hardware

At the commencement of the Supply, the Service Provider shall provide a schedule of all equipment requiring prototype approval and the

manufacturing, supply and delivery programme for all items of equipment. This shall be submitted to the Port Authority for approval. The Service Provider shall issue a fortnightly report on the status of the approvals, manufacture, supply and delivery as part of the review reports.

f. Software

The Service Provider shall submit reports on the progress of any modifications and configurations to the software. This shall be submitted as part of the review reports.

g. Project Progress Meeting

The Service Provider shall present the monthly progress achieved on the documentation / development part from the date of signing of the agreement until material / software delivery to site. This shall be done in person with Project Manager and at least one software technical personnel.

h. Equipment Interface Schedules

The Service Provider shall develop a schedule to identify each and every physical interface between KoPT Authority and Service Provider as described in this document. This schedule shall provide the status of the approval and acceptance of these interfaces and design requirements as part of the design review meeting minutes.

2.3.8.6. Factory Acceptance Testing

Note: In case the factory premises of the Service Provider is outside India, such Service Provider shall produce the successful commissioning/functioning certificate of their solution at the time of SAT.

Testing of the system is required to validate the deliverables and to minimize the risks of non-conformance. The following is the testing framework to be followed to achieve Acceptance of the RFID based access control System. The testing conducted at the Service Provider's / Factory premises before delivery of the system to site is referred to as Factory Acceptance Testing. Tests undertaken on site once the system has been integrated into the whole is referred to as Site Acceptance Testing. The Service Provider is required to comply with the requirements of the Specifications and to develop all the test procedures

necessary for the issuance of the Acceptance Test clearance certificates and for the issue of the Taking over Certificate on site. This section of the document serves as a framework to focus the testing effort to achieve system acceptance. The Service Provider shall develop the test procedures to satisfy these acceptance criteria at least 6 weeks in advance. Also, the complete responsibility of getting the document approved at least 2 weeks in advance before FAT, is that of Service Provider. This shall include hardware acceptance criteria as well as hardware and software configuration. The test procedures shall be issued to KoPT Authority for assessment to ensure that all aspects of the system have been covered under the test procedures. KoPT Authority shall reserve the right to vary tests should it be established that certain conditions requiring validation have not been covered. During the execution of the test, KoPT Authority will evaluate the results of the tests to verify whether the results prove the requirements for acceptance. This will require certain functional and performance tests.

2.3.8.7. Test Zones

The RFID based access control system must be separated in to areas of focus, referred to as test zones. These zones are representative of functional areas and may cross hardware boundaries. The Service Provider shall submit his proposals for the test zones to KoPT Authority for acceptance and these approved zones will serve as the basis for testing. KoPT have a number of divisions of functionality, which must be covered in the test procedures.

2.3.8.8. Required to Prove

Each test shall have an expressed purpose of proving an expected result. This result is referred to as the "Required to Prove" objective and will be given below in the paragraph titled RTP in each section. The Service Provider must propose and KoPT Authority shall accept this requirement with reference to the URS and Functional Specifications. Where the Service Provider has omitted a specific testable function or condition, KoPT Authority shall advise the Service Provider, giving the reference to the specifications and the RFP to be satisfied. Service Provider shall develop these test procedures, defining the inputs and the

procedures required to satisfy these requirements.

2.3.8.9. Boundary Testing

The test procedures shall identify all the system boundaries where irregularities may occur and these must be tested for all valid and possible cases, i.e. roll over of counters, month-ends, year-ends, reset points, etc. This process shall form a separate section of SAT document.

2.3.8.10. Limit Testing

The test procedures shall identify all the system limits (exceptional conditions) where irregularities may occur and these must be tested for all valid and possible cases, etc. and explicitly documented as limitations. This process shall form a separate section of SAT document.

2.3.8.11. Hardware

Each item out of complete list of equipment to be supplied and installed shall be inspected and verified for compliance to the Specifications.

2.3.8.12. Configuration

The hardware and software configuration shall be assessed for correctness of set-up for compliance to the requirements.

2.3.8.13. Performance Testing

- a) At Factory Acceptance Testing, the performance testing covers the individual system processes as well as the integration of all system components as a whole. The Service Provider shall be required to satisfy the performance criteria of the specifications under the maximum system loading stresses. KoPT Authority will identify these conditions and the Service Provider shall design the tests to satisfy the requirements.
- b) Maximum system loading shall satisfy but not be limited to at least the 1 years data in the database with an average of 50,000 transactions per day and all corresponding entries

2.3.8.14. Installation Approvals

- a) The installation method statement shall be submitted by the Service Provider at least 6 weeks in advance. Also, the complete responsibility of getting the document approved at least 2 weeks in advance before start of actual installation is that of Service Provider.

- b) Due to non-availability of time, if KoPT Authority so decides to skip this process, the Service Provider shall be notified regarding the same. This does not however relieve the Service Provider from not following the said process as the comments can still be given as part of SAT.
- c) The installation of equipment on site shall be subject to the benchmark approval process as described below.

2.3.8.15. Works Requiring Benchmark Approval

Each type of installation procedure shall be subject to the Benchmark approval process. This shall include the installation of one complete lane in all aspects including booth equipment. In addition, any type of installation work being carried out for the first time on site shall be subject to the benchmark approval process. This will include but not be limited to the installation of cables, cable terminations, cable joints where these are permitted and the mounting of system peripherals.

2.3.8.16. Benchmark Approval Process

a) Notice

The Service Provider shall notify KoPT Authority prior to any new works being carried out. This notice shall be in an agreed manner giving KoPT Authority sufficient time to be in attendance to witness such installation procedures. If KoPT Authority is unable to be present to witness the procedure, the Service Provider shall be notified and an alternative date shall be agreed to. This date shall not be later than two working dates after the date requested by the Service Provider. If KoPT Authority is still unable to be present at the installation of the benchmark works, the Service Provider may proceed with the benchmark and shall hold the works in a state enabling KoPT Authority to inspect the works, provided that the works is not left in a state that exposes persons or property to any dangers.

b) Installation Method Statements

The Service Provider shall submit with the request for the installation of a benchmark, a copy of the method statement to be followed for the

execution of the works. The method statement shall record the materials required, any special tools, the steps to be followed and any testing procedures.

c) Bench Mark Approval

On completion of the Bench Mark installation, KoPT Authority shall notify the Service Provider of any unacceptable procedures, materials or test results and the Service Provider shall correct such unacceptable works. Once the benchmark installation has been completed and is acceptable to KoPT Authority, KoPT Authority shall issue an acceptance certificate for the works subject to the benchmark, recording clearly the identification of the works being accepted. Once this benchmark acceptance certificate has been issued, all works of a similar nature may be installed in accordance with the benchmark acceptance certificate.

d) Inspection of Installation works

KoPT Authority will carry out inspections of the installation works as and when these are completed on site. If any works are found to be non-conformant to the approved benchmark installation, KoPT Authority shall issue a notice to the Service Provider identifying the non-conformity and the Service Provider shall immediately attend to the works. KoPT Authority may, should it be beneficial to the progress of the works in KoPT Authority's opinion, issue notices of non-conformity for work-in-progress.

e) Acceptance of Completed Works

Once an item of work has been completed, the Service Provider shall notify KoPT Authority requesting an inspection of the installation. KoPT Authority shall inspect the works and issue an Installation Acceptance Certificate accepting the quantity of the works. This acceptance shall serve as a step towards gaining Site Acceptance of the Works to facilitate the issue of the Taking over Certificate in terms of the Conditions of Contract.

f) Modifications to the Benchmark

Any works carried out on the benchmark without the written approval of KoPT Authority shall automatically invalidate this benchmark and the Service

Provider shall be required to reapply for a benchmark approval as described above.

2.3.8.17. Site Acceptance Testing

- a) All equipment installed on the site shall be subjected to testing to ensure that the devices are functional and the quality characteristics of the equipment meet the requirements. KoPT Authority reserves the right to carry out subsets of the full functional testing on selected items of the system.
- b) The Service Provider shall submit the SAT Procedure at least 6 weeks in advance. Also, the complete responsibility of getting the document approved at least 2 weeks in advance before SAT is that of Service Provider.
- c) The following is the testing framework to be followed to achieve Site Acceptance of the RFID System. Any testing not fully completed at the Factory Acceptance Testing or requiring retesting, shall have been completed before Site Acceptance Testing is permitted to start. The purpose of Site Acceptance Testing is to confirm that the system operates in terms of the specifications in its integrated configuration, to facilitate the Hand Over of the system. KoPT Authority may instruct the Service Provider to carry out certain functional testing as Site Acceptance Testing to verify the correct functionality in the integrated environment. The Service Provider is expected to take every opportunity to effect the testing of the system using available site users and should these not be available, the Service Provider shall arrange for such users to be available on site to carry out the testing.

2.3.8.18. Unit Testing

The Service Provider shall develop unit tests for each zone identified in the Factory Acceptance Testing. These tests shall validate the system functionality in the integrated environment, as an example, the data transfer from one level of the system to another, such as blacklists and balance tables. The tests at SAT shall be undertaken at the normal operating stress levels of the system.

2.3.8.19. Full Functional Tests

Each system and subsystem must be completely functionally tested with set of tests to verify the correct operation of peripherals, set-up and configuration

tables and downloaded parameters.

2.3.8.20. Hardware Installation

Each item of equipment shall be checked for correct installation and shall be inspected and verified for compliance to the Specifications.

2.3.8.21. Performance Testing

Performance testing shall cover the individual system processes as well as the integration of all system components as a whole. Each performance criteria in the specifications shall be identified and tested for the defined conditions. The Service Provider shall be required to design these tests and prove that compliance to KoPT Authority.

2.3.8.22. System Dry Run Testing

Where site traffic is available to test the system prior to commissioning, the Service Provider shall make use of this traffic to verify system functionality and performance.

2.3.8.23. Data Validation

- a) The Service Provider shall prove that all raw data generated at gate/ pass section/ workstations level is registered by the system in correct, complete and consistent manner.
- b) The Service Provider shall prove that all data processed by the system is correct, complete and consistent. The methods used by the Service Provider shall be demonstrated to KoPT Authority and the onus is on the Service Provider to prove the validity of the data to KoPT Authority.

2.3.8.24. Report Validation

The Service Provider shall prove the validity of the information in each and every system generated report. This shall mean that the basis of verification shall be raw data generated in the gate / pass section and the Supervisor actions only. The contents of the report shall be matched with live script to generate the same report in the presence of KoPT Authority with all requisite formula to verify correctness of the report provided to KoPT Authority. This shall be demonstrated to KoPT Authority and the onus is on the Service Provider to prove the validity of the information to KoPT Authority.

2.3.8.25. Commissioning

- a) Once Site Acceptance Testing has been concluded and the Service Provider has attended to and remedied all reported defects, the system shall be ready to be commissioned and taken into operation.
- b) Failure by the Service Provider to complete the Works and to have remedied all reported defects by the Prescribed Date for commissioning shall result in the application of the defined penalties for delay.

2.3.9. Change Management and Capacity Building including Training of users for effective use of the system

- a) The Service Provider shall submit the detailed Training schedule and contents in Microsoft Power point format covering all modules / aspects of training at least 6 weeks in advance. Also, the complete responsibility of getting the document approved at least 2 weeks in advance before start of training is that of Service Provider.
- b) The Service Provider shall provide training to designated/ nominated staff members of KoPT in the use and maintenance of the items, features and systems of the RFID based access control system, such that the trained personnel shall become fully conversant with the contents of the equipment, its operation and equipment manuals. Service Provider needs to identify the different user segments within KoPT for designing the type and content of training to be imparted and prepare a training calendar accordingly. A generic training session covering the overall functioning of the solution should be provided to all the nominated staffs. Besides the generic session, each training session should cover the specific requirements of each department viz. Training for Traffic department users should primarily be focussed on the workflow of pass approval, issuance and complete operations while training for the CISF/ PSO officials may be focussed towards the gate level operations, security aspects and its enforcements.
- c) The training shall be in-depth series of sessions, which shall comprise of both classroom type training as well as practical training.
- d) The training shall be specific for both classes of personnel, being Operational and Maintenance personnel.
- e) Training process – Operational personnel

The training process shall comprise the following minimum requirements for Operational personnel:

- A. A start up training program detailing the purpose, usage and functionality of the integrated system(s). (Theory and Practical training)
- B. A training program detailing the operation and administration of each level of operations of the equipment, component, sub-system and integrated system. (Theory and Practical training). The equipment / user manuals shall be referenced and utilized during the training session.
- C. At the end of each training session, objective tests shall be given for each user-group and the users shall be graded accordingly. The test procedure and questionnaire set shall be made available to KoPT Authority by Service Provider as part of Training schedule submission. The test results shall be made available to KoPT Authority after grading by Service Provider. If the results are not satisfactory, the Service Provider shall redo the training module with a different trainer.

2.3.9.1. Training process – Maintenance personnel

The training process shall comprise the following minimum requirements for Maintenance personnel:

- 1) A start up training program detailing the purpose, usage and functionality of the integrated system/s. (Theory and Practical training)
- 2) A training program detailing functions and specific features of each sub-system and its associated equipment components. (Theory and Practical training)
- 3) A training program detailing the operation, administration and maintenance of each level of operations of the equipment, component, sub-system and integrated system. (Theory and Practical training). The equipment manuals shall be referenced and utilized during the training session.

At the end of each training session, objective tests shall be given for each user-group and the users shall be graded accordingly. The test procedure and questionnaire set shall be made available to KoPT Authority by Service Provider as part of Training schedule submission. The test results shall be made available to KoPT Authority after grading by Service Provider. If the results are not satisfactory,

the Service Provider shall re do the training module with a different trainer

2.3.10.Operation and Maintenance of the entire RFID based Access Control System for a period of 07 (Seven) years from the date of Go-live.

- a. The maintenance includes RFID based Access Control solution maintenance, IT infrastructure maintenance, network maintenance, system administration, security administration, database administration, end-user problem resolution and staffing sufficient resources.
- b. On successful completion of the implementation or the Final Go-Live, the Service Provider must extend Post Implementation Support (including warranty) till the end of the contractual period which is 07 (Seven) years from the date of Go Live.
- c. The Service Provider needs to provide the operational and maintenance support for the systems that are implemented and being used before Go Live. The other details of operational support are provided in Annexure VII of volume I the RFP document.
- d. The Service Provider must provide manpower for each of the 10pass issuance counters in the 1st year and 03 pass issuance counters from the 2nd year onwards including pass approval request submission counter if the same is different from the issuance counter.
- e. The Service Provider must provide a centralized Helpdesk and Incident Management Support with sufficient staff till the end of contractual period.
- f. KoPT will provide Office space, telephone line and other minimum amenities to the Service Provider at Subhash Bhawan office of KoPT in Kolkata. The proposed Helpdesk shall be operational during the general shift only.
- g. The Service Provider must provide centralized Technical Support for the O&M period from the date of Go-Live. The Centralized Technical support team will be Onsite in the Subhash Bhawan office of KoPT in Kolkata.
- h. During the operations and maintenance phase, the Service Provider should:
 - Ensure that all necessary measures are taken for the smooth operation of the RFID based access control system
 - Ensure adherence to baseline performance SLA matrix as defined in volume III of this RFP

2.3.11. Carry out one time enrolment of users and issuance of printed permanent RFID cards to the users

- a. Service Provider shall carry out enrolment and issuance of one time printed RFID cards to users.
- b. Service Provider shall collect the primary information that includes particulars with respect to the persons/vehicle which would act as a master data.
- c. Service Provider shall issue RFID cards to the users after collecting the requisite fee for the issuance of RFID card/after getting the approval from the KoPT Officials.
- d. Service Provider shall issue the high quality cards with permanent print on the card with photo and other details as specified by KoPT Officials.
- e. Service Provider shall setup temporary counters depending on the rush at the counters and shall issue the passes.
- f. Service Provider shall make the different options of collection of primary information. The options include through portal, collected from the sponsors, collected from the existing applications etc.
- g. The issued card shall have a life of at least 07years in terms of usability of the card. The bidder shall replace the card free of cost in case the card becomes dysfunctional during the period of contract due to any reason except physical damage to the card.

2.3.12. Documentation of the RFID based Access Control System Project

- a. The documentation plan shall be prepared to define the specific documents to be delivered, their intent and content, the schedules for preparation, review, submittal, validation when necessary, and revision and update. The numbering system to be used to identify and track the documentation and to permit their configuration control shall be proposed by the Service Provider and approved by KoPT Authority.
- b. Documents relating to proprietary or commercially available hardware and software shall be identified. If such documents do not fulfil the intent of the deliverable documentation specified below, the plan shall describe how the deficiency will be eliminated.
- c. When document review is in progress, document modifications against all

comments made in the previous versions shall be highlighted and any other modifications apart from this shall be explicitly brought to the notice of the Port Authority. The comments and responses shall be part of the document itself and the final approved document shall contain the complete history. Upon approval of KoPT Authority, the Service Provider shall update the final version of the document.

- d. Documentations shall be project specific and shall include:
 - 1) Equipment manuals (technical and user)
 - 2) Component manuals (technical and user)
 - 3) Installation methods and manuals (Hardware and software)
 - 4) Operations / User manuals (separate for each level of operations)
 - 5) Maintenance manuals
 - 6) Test procedures
 - 7) Revised documentation based on As-built
 - 8) And any other documents as required by the Port Authority.
- e. All documents shall be provided in both hard and electronic format (Microsoft compliant) and editable format.
- f. All drawings shall be provided in both hard and electronic format (AutoCAD compliant) and editable format.
- g. The Detailed documentation scope is provided in Annexure VI.

2.4. Organisation Scope

The present organizational scope includes the Kolkata Dock System of Kolkata Port Trust and all its offices.

2.5. Solution Scope

The indicative solution is given in the Annexure – I. The bidder shall design an appropriate solution based on the requirements gathered during the System Requirements Study.

Bidder shall configure all required business processes, define business rules, establish controls, establish workflows, configure Information Systems/ Reports, configure Archival rules, backup mechanism and empower Port team inducting proper training.

2.6. Process Scope:

An indicative list of processes with broad workflow is provided in the Annexure I. However, the bidder may propose any changes in the processes based on the experience of best practices adopted across the Globe, but Port reserves the right of acceptance of the proposed changes in the process.

2.7. Functional Scope:

An indicative list of Functional requirements is provided in Annexure I.

2.8. Installation Scope

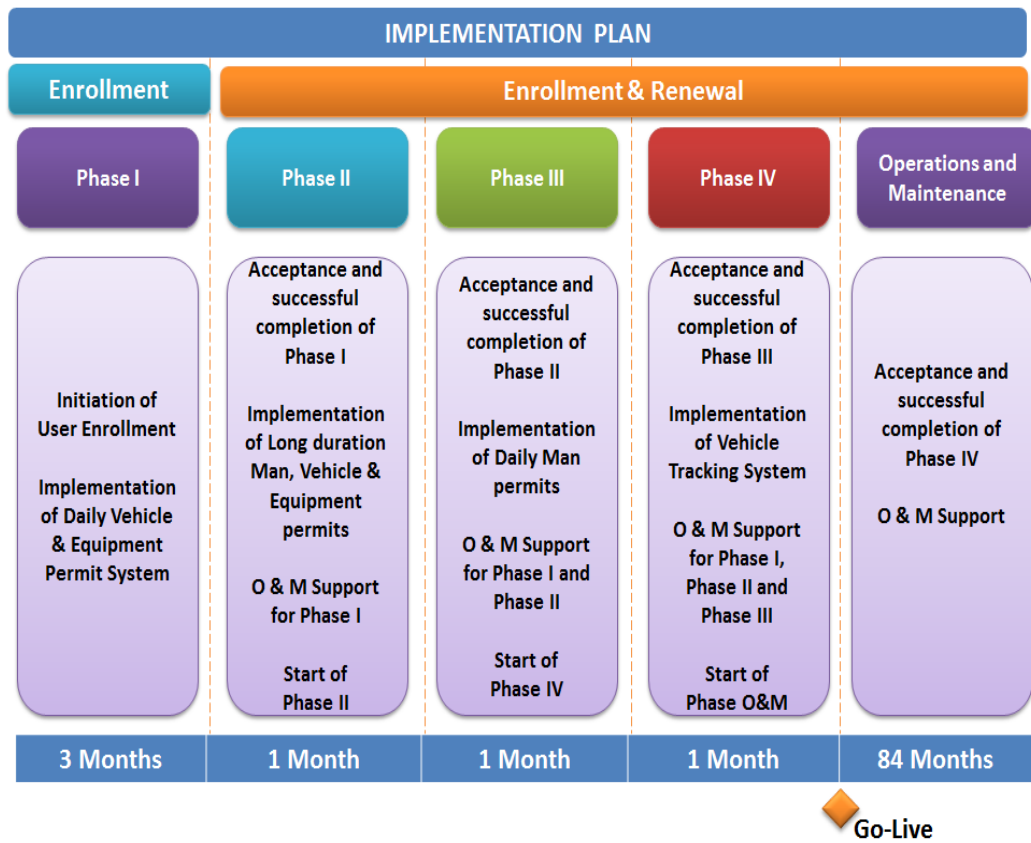
An indicative installation scope is provided in the Annexure III.

2.9. Report Generation

An indicative report generation scope is provided in Annexure I.

2.10. Project Phases

- It is proposed to implement the project in the following four phases:
 - Phase I : Implementation of Daily Vehicle & Equipment Permit System
 - Phase II: Implementation of Long duration Man, Vehicle and Equipment permits
 - Phase III: Implementation of Daily man permits
 - Phase IV: Implementation of Vehicle Tracking System



- It is proposed to retain the manual pass issuance system also in parallel to the RFID based access control system till the new system got accepted and sign-off is given to have Business Continuity.
- **Go-Live** is the date on which the RFID based Access Control System is completely operational at all the locations as per the requirements of the RFP and all the acceptance tests are successfully concluded as per the satisfaction of KoPT.

2.11. Governance Model for O & M support

- Bidder should propose a detailed Governance Model for the O & M activities. The governance structure should ensure smooth on-going operations of support to KoPT's business processes and day-to-day working.

2.12. Service Level Agreement (SLA)

2.12.1. Service Level Agreement Framework

Service Level Agreement (SLA) is the contract between KoPT and the bidder. SLA defines the terms of the Successful bidder's responsibility in ensuring the timely delivery of the deliverables/ services and the correctness of the same based on the

agreed performance indicators as detailed in the Agreement. This section defines various Service Level Indicators which will be considered by KoPT in the Service Level Agreement with Successful bidder.

The successful bidder has to comply with Service Level Agreements (SLAs) given below to ensure adherence to project timelines, quality and availability of services.

Penalties shall not be levied on the successful bidder in the following cases:

- There is a Force Majeure event effecting the SLA which is beyond the control of the successful bidder
- During the first three (03) months after system Go-live as this period will be treated as stabilization period.

2.12.1.1. Timely Delivery

Definition	Timely delivery of deliverables would comprise of software application and all documents that are to be submitted as part of the project deliverables.
Service Level Requirement	All the deliverables defined in the contract have to be submitted On-time on or before the date as mentioned in the contract with no delay.
Measurement of Service Level Parameter for LD	To be measured in Number of Business Days of delay from the date of submission as defined in the project contract.
LD for non-compliance of SLA Requirement	<p>Delay of every Business Day would attract Liquidated Damages (LD) per day as per the following –</p> <p>i. For non-delivery of Documents = No. of days of delay from the scheduled date of submission of documents X Per day LD</p> <p>The LD per day is INR 5,000.</p>

2.12.1.2. Down Time

Definition	<p>“Downtime” means the time during which the system is not available for working to users. This will not include the Scheduled Downtime.</p> <p>The reason for the downtime may be non-function of software, network, hardware and any other infrastructure and also non-availability of the infrastructure required.</p> <p>“Scheduled Downtime” means those times where successful bidder notified KoPT of periods of Downtime at least five days prior to the commencement of such Downtime.</p>				
Service Level Requirement	<p>The uptime of the system should be 98.5% measured in a month. Service Provider shall provide a Server generated monthly report on the system uptime. Service Provider to provide a Network Monitoring Software (NMS) to KoPT for monitoring all the devices connected on IP related to the RFID project. Necessary configuration of all such components needs to be done by Service Provider so that monitoring can be done using NMS.</p>				
Measurement of Service Level Parameter	<p>The percentage of uptime is measured as</p> $\frac{(Total\ Scheduled\ Time - Unscheduled\ Downtime)}{Total\ Scheduled\ Time} \times 100$ <p>The downtime will be measured as the time difference between the breakdown of the system and restoration of the system.</p> <p>For billing purpose the total downtime for a given month will be calculated.</p>				
LD for non-compliance of SLA Requirement	<p>The following penalties are charged for the non-compliance with the SLA requirements.</p> <table border="1" data-bbox="563 1794 1305 2024"> <tr> <td data-bbox="563 1794 890 1973">Downtime</td> <td data-bbox="890 1794 1305 1973">Penalty as percentage of the total invoiced amount for that month.</td> </tr> <tr> <td data-bbox="563 1973 890 2024">Compliance with SLA</td> <td data-bbox="890 1973 1305 2024">0%</td> </tr> </table>	Downtime	Penalty as percentage of the total invoiced amount for that month.	Compliance with SLA	0%
Downtime	Penalty as percentage of the total invoiced amount for that month.				
Compliance with SLA	0%				

	<98.5% and ≥97.0%	2%
	<97.0% and ≥95.0%	5%
	<95.0% and ≥90.0%	10%
	<90.0% and ≥ 80.0%	25%
	<80.0%	100%

2.12.1.3. Average Pass Generation Time (PGT)

Definition	The average time take to issue a pass to Vehicle/Individual. The average time is measured over a period one month.	
Service Level Requirement	Average time take for issue of pass to vehicle <60 Sec Average time take for issue of pass to individual <75 Sec PACS software should have the feature to calculate the total time taken for each transaction of pass issuance. Pass issuance time will be calculated from the time issue process was initiated by the pass issuance resource till the time pass was printed. Software should be able to provide system generated monthly reports on such pass issuance time.	
Measurement of Service Level Parameter	It is measured in terms of average time taken to issue a pass to a vehicle/Individual. $\frac{\textit{(Total time taken to issue passes in a quarter)}}{\textit{Total passes issues in a quarter}}$ For billing purpose the Average PGT for a given month will be calculated.	
LD for non-compliance of SLA Requirement	The following penalties are charged for the non-compliance with the SLA requirements.	
	PGT for Vehicle	Penalty as percentage of the total invoiced amount for that month.

	Compliance with SLA	0%
	>60 Sec and \leq 70 Sec	2%
	>70 Sec and \leq 80 Sec	5%
	>80 Sec and \leq 90 Sec	10%
	>80 Sec	25%
	PGT for Individual	Penalty as percentage of the total invoiced amount for that month.
	Compliance with SLA	0%
	>75 Sec and \leq 90 Sec	2%
	>90 Sec and \leq 100 Sec	5%
	>100 Sec and \leq 110 Sec	10%
	>110 Sec	25%

2.12.1.4. Average Monthly Pass Generation Failure (PGF)

Definition	The average number of times the system failed to generate the pass after uploading all the required information. The failure to generate the pass may be due to any factor. The average failures are measured over a period of one Month.
Service Level Requirement	Average monthly pass generation failures <30. PACS application should provide a system generated monthly report of the number of transactions failed.
Measurement of Service Level Parameter	<p>It is measured in terms of average failures to generate pass.</p> $\frac{\textit{(Total number of failed pass generations)}}{30}$ <p>For billing purpose the Average PGF for a given month will be calculated.</p>

LD for non-compliance of SLA Requirement	The following penalties are charged for the non-compliance with the SLA requirements.	
	PGF	Penalty as percentage of the total invoiced amount for that month.
	Compliance with SLA	0%
	>30 and \leq 40	2%
	>40 and \leq 60	5%
	>60 and \leq 100	10%
	>100	25%

2.12.1.5. Average Pass Verification Time (PVT)

Definition	The average time taken by Vehicle/Individual to verify a pass at a reader. The average time is measured over a period one month.	
Service Level Requirement	Average time take for verification of pass of vehicle and individual <2 Sec. PACS application should provide a system generated monthly report on the total time taken by the application to verify a pass.	
Measurement of Service Level Parameter	<p>It is measured in terms of average time take to verify a pass of a vehicle/Individual.</p> $\frac{\textit{(Total time taken to verify passes in a quarter)}}{\textit{Total passes verified in a quarter}}$ <p>For billing purpose the average PVT for a given month will be calculated.</p>	
LD for non-compliance of SLA Requirement	The following penalties are charged for the non-compliance with the SLA requirements.	
	PVT for Vehicle and individual	Penalty as percentage of the total invoiced amount for that month.

	Compliance with SLA	0%
	>2 Sec and ≤ 4 Sec	2%
	>4 Sec and ≤5 Sec	5%
	>5 Sec and ≤6 Sec	10%
	>6 Sec	25%

2.12.1.6. Average Monthly Pass Verification Failure (PVF)

Definition	The average number of times the system failed to verify the pass after uploading all the required information. The failure to verify the pass may be due to any factor. The average failures are measured over a period one Month.											
Service Level Requirement	Average monthly pass verification failures <5. PACS application should provide a system generated monthly report on the total number of passes that were not read.											
Measurement of Service Level Parameter	<p>It is measured in terms of average failures to verify pass.</p> $\frac{\textit{(Total number of failed pass verifications)}}{30}$ <p>For billing purpose the Average PGF for a given month will be calculated.</p>											
LD for non-compliance of SLA Requirement	<p>The following penalties are charged for the non-compliance with the SLA requirements.</p> <table border="1"> <tr> <td>PVF</td> <td>Penalty as percentage of the total invoiced amount for that month.</td> </tr> <tr> <td>Compliance with SLA</td> <td>0%</td> </tr> <tr> <td>>5 and ≤7</td> <td>2%</td> </tr> <tr> <td>>7 and ≤8</td> <td>5%</td> </tr> <tr> <td>>8 and ≤10</td> <td>10%</td> </tr> </table>		PVF	Penalty as percentage of the total invoiced amount for that month.	Compliance with SLA	0%	>5 and ≤7	2%	>7 and ≤8	5%	>8 and ≤10	10%
PVF	Penalty as percentage of the total invoiced amount for that month.											
Compliance with SLA	0%											
>5 and ≤7	2%											
>7 and ≤8	5%											
>8 and ≤10	10%											

	>10	25%
--	-----	-----

2.12.1.7. Average Resolution Time

Definition	Defined as Average Time taken to resolve component complaint / query is resolved after it is reported to Service Provider Support team. The average failures are measured over a period one Month.												
Service Level Requirement	Average time for resolution of issue <4 Hours All the queries resolution times are applicable during business hours only. Service Provider to provide an online issue ticketing tool for raising and addressing of issues by users. The tool should be capable to provide reports based on various parameters like no. of issues raised, issues resolved, open issues, average time taken for resolution, etc.												
Measurement of Service Level Parameter	It is measured in terms of average time taken for resolving the issues in a month. <i>(Total time taken for resolving issues in a month)</i> <i>Total Number of Issues reported in that month</i> For billing purpose the Average PGF for a given month will be calculated.												
LD for non-compliance of SLA Requirement	The following penalties are charged for the non-compliance with the SLA requirements. <table border="1"> <thead> <tr> <th>Average Resolution Time</th> <th>Penalty as percentage of the total invoiced amount for that month.</th> </tr> </thead> <tbody> <tr> <td>Compliance with SLA</td> <td>0%</td> </tr> <tr> <td>>5 Hrs and \leq 7Hrs</td> <td>2%</td> </tr> <tr> <td>>7 Hrs and \leq 8 Hrs</td> <td>5%</td> </tr> <tr> <td>>8 Hrs and \leq 10 Hrs</td> <td>10%</td> </tr> <tr> <td>>10 Hrs</td> <td>25%</td> </tr> </tbody> </table>	Average Resolution Time	Penalty as percentage of the total invoiced amount for that month.	Compliance with SLA	0%	>5 Hrs and \leq 7Hrs	2%	>7 Hrs and \leq 8 Hrs	5%	>8 Hrs and \leq 10 Hrs	10%	>10 Hrs	25%
Average Resolution Time	Penalty as percentage of the total invoiced amount for that month.												
Compliance with SLA	0%												
>5 Hrs and \leq 7Hrs	2%												
>7 Hrs and \leq 8 Hrs	5%												
>8 Hrs and \leq 10 Hrs	10%												
>10 Hrs	25%												

2.12.2. Quality Management

A Quality Assurance process shall be there which will provide independent assurance that work efforts conform to defined processes and are operating within the parameters and policies defined for an engagement.

The Quality Metrics that will be calculated and reported on a Monthly basis

- i. SLA Compliance
- ii. Issue resolution

These Metrics shall be analysed by Port

2.13. Status Reports

Status reporting would be done on a weekly and monthly basis through different reports. The table below lists out few of the reports. Other than these, there would be weekly/monthly status review by Bidder and Port. The reports will be sent by Bidder's Manager to Port representative nominated for this project.

Report Name	Frequency
SLA report on Response Times	Monthly
SLA report on Resolution Times according to call priority	Monthly
Call Resolution Time (turnaround time) trend report-month wise	Monthly
Call Category Report – type of problem, priority, number of calls, average resolution time. -	Monthly
Call Status Sheet – open calls at beginning of week, new calls received, calls closed, calls open, call closing balance at end of week	Weekly
Classification of incidents – by priority -	Weekly/ Monthly
Root Cause Analysis, for example : for priority 1 calls or for SLA non-adherence, or any exceptional situation	Event driven
Process Improvement Report – After the Go-Live	As and when required

Submission of the backup database in softcopy	Monthly
---	---------

This is not an exhaustive list and some more reports may be required or some existing may be deleted as and when the need is identified.

2.14. Project Timelines:

The overall implementation of the proposed RFID based Access Control system shall be completed as per the phases defined in the earlier section. However, requirements gathering, preparation of SRS and Design Document shall be carried out at the beginning of the project for the entire project. The functional phasing shall be as per the phasing defined in the earlier sections. The Service Provider needs to adhere to the duration and a tentative schedule as specified in the table below:

S. No	Activity	Duration (Months)												
		1	2	3	4	5	6	7	8	9	10	11	12	84
1	SRS Preparation	█												
2	Development of Phase I Application		█	█										
3	Approval of Phase I and Development of Phase II				█									
4	Approval of Phase II and Development of Phase III					█								
5	Approval of Phase III and Development of Phase IV						█							
6	O&M Support							█	█	█	█	█	█	█

2.15. Project Governance Structure

2.15.1. Steering Committee

- The Steering Committee is composed of Heads of Departments / Divisions level personnel of KDS of KoPT, chaired by Deputy Chairman, KDS.
- Bidder shall nominate a Senior Executive level to participate in the steering committee meeting to review the project progress and to take decisions escalated for resolution from the Steering Committee.

- Bidder shall provide the name, designation, position and role of the executive nominated for participating in Steering Committee Meetings.
- Bidder shall propose the name in the Steering Committee of such official who is a part of the resident team at the project site

2.15.2. Project Management Team

- Service Provider shall propose a lean Project Management team consisting of officials from Service Provider's side which can include members from resident team.
- The Project Management Team shall be headed by Official of KoPT or officials indicated by the KoPT.
- The Project Management Team or the core team proposed by the Service Provider shall be a resident team and the complete team shall report at the project site from the SRS study stage itself.

2.16. Facilities Provided by KoPT to the successful bidder

KoPT will provide the following facilities to the successful bidder to the establishment of the project office and other infrastructure.

- Existing KDS-Net backbone (OFC) may be used by the vendor. Proposed project should use existing established fibre network wherever it is healthy to cover all proposed locations, berths, buildings for successful connectivity. All last mile network connectivity in terms of cabling is the responsibility of the Service Provider.
- KoPT will provide free of cost raw power 1-Phase (220V A.C. +/-10%50Hz (A.C Incoming supply 190-270 V, Single Phase,50Hz +/-2.5Hz)) at nearby source/building requiring installation of electrical equipment connect with the project. All last mile electrical connectivity in terms of cabling is the responsibility of the Service Provider
- Proposed project should be based on the existing movement plan/traffic plan assigned to vehicles (enclosed) by Traffic dept.
- Central Control & Monitoring will be done at Subhash Bhavan. A 32" LED monitor to be installed in the chamber of the Traffic Manager, KoPT for viewing the activities like Access Control and Vehicle Tracking within Dock. Necessary client

software to view the activities in real time mode should be supplied by the vendor.

- KoPT network is available as backbone and Service Provider is expected to utilize the same. Connectivity to be established wherever KoPT network is not available/not healthy. Service Provider may conduct a detailed survey to understand the requirement for connectivity.
- Wireless / Wi-Fi is to be established wherever wired is not feasible.
- RFID gate infrastructure like, lane, dividers, security rooms, lighting, A.Cs, furniture, etc. wherever applicable are in Service Provider scope in consultation with KoPT.

===== END OF DOCUMENT=====



Kolkata Port Trust

KOLKATA PORT TRUST

**Supply, Installation, Commissioning, and Maintenance
of RFID Systems at Kolkata Dock System, Kolkata Port
Trust.**

Request for Proposal

Volume II: Commercial and Bidding Terms

Document Reference No: **Plg/165/RFID/11667**

Date: 18th April 2017.

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

TABLE OF CONTENTS

1.	PURPOSE AND STRUCTURE OF THE RFP	5
1.1	PURPOSE OF THE RFP	5
1.2	STRUCTURE OF THE RFP	5
2.	BIDDING PROCESS DETAILS	6
3.	RFP ISSUING AUTHORITY	6
4.	TENTATIVE CALENDAR OF EVENTS AND EVENT LOCATION:	8
5.	GENERAL INSTRUCTIONS TO BIDDERS	9
5.1	AVAILABILITY AND COST OF THE RFP DOCUMENTS	9
5.2	BID PROCESSING FEE	10
5.3	ACKNOWLEDGEMENT	11
5.4	EARNEST MONEY DEPOSIT	12
5.5	PRE-BID MEETING	13
5.6	BIDDER INQUIRIES AND KOPT'S RESPONSES	13
5.7	SITE VISIT OPPORTUNITY FOR THE BIDDERS	14
5.8	SUPPLEMENTARY INFORMATION / CORRIGENDUM / AMENDMENT TO THE RFP	14
5.9	BID PREPARATION COSTS	15
5.10	KOPT'S RIGHT TO TERMINATE THE PROCESS	15
5.11	ACCEPTANCE OF PART / WHOLE BID / MODIFICATION – RIGHTS THEREOF	15
5.12	AUTHENTICATION OF BIDS	16
5.13	INTERLINEATIONS IN BIDS	16
5.14	CONSORTIUM BIDS	16
5.15	VENUE & DEADLINE FOR SUBMISSION OF BID	17
5.16	LATE BIDS	17
5.17	GENERAL CONDITIONS OF CONTRACT (GCC):	17
5.18	CONDITIONS UNDER WHICH THIS RFP IS ISSUED	18
5.19	RIGHTS TO THE CONTENT OF THE BID	18
5.20	MODIFICATION AND WITHDRAWAL OF BID	19
5.21	NON-CONFORMING BIDS	20
5.22	DISQUALIFICATION	20
5.23	CONFLICT OF INTEREST	21
5.24	ACKNOWLEDGEMENT OF UNDERSTANDING OF TERMS	22
6.	BID SUBMISSION INSTRUCTIONS	22
6.1	MODE OF SUBMISSION	ERROR! BOOKMARK NOT DEFINED.
6.2	LANGUAGE OF BID	24
7.	BID OPENING AND EVALUATION PROCESS	25
7.1	BID OPENING SESSIONS	25
7.2	OVERALL EVALUATION PROCESS	26
7.3	EVALUATION OF PRE-QUALIFICATION BIDS	26
7.4	EVALUATION OF TECHNICAL BID	27

7.5	EVALUATION OF COMMERCIAL BID.....	28
7.6	PRE-QUALIFICATION EVALUATION CRITERIA.....	30
7.7	TECHNICAL EVALUATION CRITERIA	32
7.7.1	MANDATORY COMPLIANCE CRITERIA.....	32
7.8	TECHNICAL BID.....	33
7.9	COMMERCIAL BID.....	35
8.	AWARD OF CONTRACT	41
8.1	AWARD CRITERIA.....	41
8.2	KOPT’S RIGHT TO ACCEPT/ REJECT ANY OR ALL BIDS.....	41
8.3	NOTIFICATION OF AWARD	41
8.4	CONTRACT FINALIZATION AND AWARD	41
8.5	SIGNING OF CONTRACT	41
8.6	SUGGESTIONS ON THE DRAFT CONTRACT.....	42
8.7	FAILURE TO AGREE WITH THE TERMS AND CONDITIONS OF THE RFP	42
9.	PAYMENT TERMS AND SCHEDULE	43
9.1	PERFORMANCE BANK GUARANTEE.....	43
9.2	LIQUIDATED DAMAGES	43
9.3	PAYMENT SCHEDULES AND MILESTONES	44
	ANNEXURE A: BID FORMATS	46
	<i>Form A.1: RFP acknowledgement letter.....</i>	<i>46</i>
	<i>Form A.2 : Proposal Cover Letter.....</i>	<i>48</i>
	<i>Form A.3: Power of Attorney for signing of Application/ Bid.....</i>	<i>50</i>
	<i>Form A.4: Earnest Money Deposit (EMD) Covering Letter.....</i>	<i>52</i>
	<i>Form A.5: Conflict of Interest.....</i>	<i>53</i>
	<i>Form A.7: Request for Clarification</i>	<i>54</i>
	ANNEXURE B: PRE-QUALIFICATION BID FORMATS.....	55
	<i>Form B.1 : Pre-Qualification Bid Response Check List.....</i>	<i>55</i>
	<i>Form B.2: General Details of the Organization</i>	<i>56</i>
	<i>Form B.3: Relevant Project Experience for RFID Project</i>	<i>58</i>
	<i>Form B.4: Self-declaration on the Blacklisting (Each bidder in case of consortium).....</i>	<i>59</i>
	ANNEXURE C: TECHNICAL BID FORMATS	62
	<i>Form C.1: Technical Response Check list</i>	<i>62</i>
	<i>Form C.2: Undertaking On Pricing of Items of Technical Response.....</i>	<i>63</i>
	<i>Form C.3: Undertaking on Compliance, Sizing of Infrastructure and Service Level Compliance</i>	<i>64</i>
	<i>Form C.4: Undertaking on Work Environment and Personnel.....</i>	<i>65</i>
	<i>Form C.6: Undertaking on Patent Rights.....</i>	<i>68</i>
	<i>Form C.7: Non-Malicious Code Certificate.....</i>	<i>69</i>
	<i>Form C.8: Undertaking on Support to Third Party Audits and Certification.....</i>	<i>70</i>
	<i>Form C.9: Profiles of the resources proposed for the project.....</i>	<i>71</i>
	ANNEXURE D: COMMERCIAL BID FORMATS	72
	<i>Form D.1: Commercial Bid Cover Letter.....</i>	<i>72</i>
	<i>Form D.2: Pricing Summary</i>	<i>75</i>
	<i>Form D.3: Item wise pricing for CAPEX as per the Bill of Material:.....</i>	<i>76</i>
	<i>Form D.4 : Item wise pricing for OPEX as per the Bill of Material:</i>	<i>76</i>
	<i>Form D.5: Performance Bank Guarantee Format</i>	<i>79</i>

1. Purpose and Structure of the RFP

1.1 Purpose of the RFP

The purpose of this RFP is to solicit bids from the interested parties, hereinafter called as bidder or Service Provider, who can demonstrate their organizational, technical and financial capabilities for implementation of RFID based Access Control system for Kolkata Port Trust. The Service Provider will be responsible for Supply, Installation, Commissioning and Maintenance of RFID based Access Control system at Kolkata Port KoPT, and maintains the application for a period of 07 (Seven) years from the date of Go-Live.

1.2 Structure of the RFP

The Request for Proposal or RFP for selection of Service Provider is segregated into the following three volumes:

Volume I: Scope of Services

Volume I of RFP intends to bring out all the details with respect to functional, non-functional, technical requirements, and implementation model along with details on scope of work required from the Service Provider that KoPT deems necessary to share with the potential bidders.

Volume II: Commercial and Bidding Terms

Volume II of the RFP details the General Terms & Conditions with respect to the bid process management including the evaluation criteria and bid submission forms to be adopted for the proposed project.

Volume III – Draft Master Services Agreement (MSA)

Volume III of the RFP details out the Draft Master Services Agreement for the proposed engagement and outlines the contractual, legal terms & conditions applicable for the proposed engagement.

This volume is Volume II of the RFP.

2. Bidding Process Details

The RFP is not an offer by KoPT but an invitation to receive proposals from eligible and interested bidders in respect of the above-mentioned project. The RFP does not commit KoPT to enter into a binding agreement in respect of the project with the potential bidders. Potential bidders are referred to as “Bidders” in this document.

3. RFP Issuing Authority

This RFP is issued by Kolkata Port Trust (KoPT) to the bidders and is intended to select the competent Service Provider for the implementation of RFID based Port Access Control System at KoPT. KoPT’s decision with regard to the selection of Service Provider through this RFP shall be final and the KoPT reserves the right to reject any or all the bids without assigning any reason.

Sl. No	Item	Description
1.	Organization	KOLKATA PORTTRUST, KOLKATA
2.	Tender No. and Date	Plg/165/RFID/11667 18/04/2017
3.	Mode of tender	e-Procurement System (Online Part I – Techno-Commercial Bid and Part II – Price Bid through https://www.mstcecommerce.com/epr/ochome/kopt of MSTC Ltd.) The intending bidders are required to submit their offers electronically through e-tendering portal. No physical tender is acceptable by KOLKATA PORT TRUST.
4.	e-Tender No.	KoPT/Kolkata Dock System/PnR/1/17-18/ET/29
5.	Name Of Work	Supply, Installation, Commissioning, and Maintenance of RFID based Port Access Control System at Kolkata Dock System, Kolkata Port Trust
6.	Period Of Completion	As per the schedule provided in Volume I
7.	Tender Type	Open
8.	Tender Document Fee	Rs 10,000 /-(Rupees Ten Thousand only)

Sl. No	Item	Description
9.	Transaction fee to MSTC	Rs 15,000/- (Rupees Fifteen Thousand only) + taxes as applicable
10.	Estimated Cost of Contract	Rs14.40 crores
11.	EMD	Rs. 24,40,000/- (Rupees Twenty Four Lakhs Forty Thousand Only). Out of this, Rs.10,00,000/- (Rupees Ten lakh Only) should be paid in the form of DD/Pay Order/ Bankers' Cheque and remaining amount of Rs. 14,40,000/- (Rupees Fourteen Lakhs Forty Thousand only) may be accepted in the form of Bank Guarantee issued by an Indian nationalized / scheduled bank.
12.	Officer Inviting Bids	Joint Director(P&R)
13.	Bid Opening Authority	Tender Committee
14.	Address	Office of the Joint Director (P&R Division); Kolkata Port Trust 15, Strand Road, Kolkata 700001, West Bengal, India.
15.	Contact Details KoPT	<p>a. Mrs. Rebecca Das Joint Director (P&R) KOLKATA DOCK SYSTEM Ph. No. 033 – 22107365 E-mail: jt.dir.pr@kolkataporttrust.gov.in</p> <p>b. Mr. Naba Dey Roy Sr. Dy. Director (EDP) KOLKATA DOCK SYSTEM Ph. No. 033 – 71003464 E-mail: nabadeyroy@kolkataporttrust.gov.in</p>

Sl. No	Item	Description
		c. Mr. Naba Kumar Sarkar Dy. Director (EDP) KOLKATA DOCK SYSTEM Ph. No. 033 – 71003465 E-mail: nksarkar@kolkataporttrust.gov.in
16.	Contact Details - MSTC	1. Shri S Mukherjee, DM(e-Commerce) – smukherjee@mstcindia.co.in 2. Ms S Maity, AM(e-Commerce) – smaity@mstcindia.co.in Google hangout ID- (for text chat)- mstceproc@gmail.com

4. Tentative Calendar of Events and event location:

The following table enlists important milestones and timelines for completion of bidding activities:

S. No	Key Activities	Date
1.	Release of Request For Proposal (RFP)	18-04-2017
2.	Date of NIT available for download	18-04-2017
3.	Last date for Submission of Written Queries / Clarification by bidders	02-05-2017 till 3 pm
4.	Pre- Bid Meeting (offline) and Venue	03-05-2017 at 11 am in the Conference hall located on the 2 nd floor of Kolkata Port Trust office at 15, Strand Road, Kolkata 700001, West Bengal, India
5.	Issue of response to bidder Queries / clarification	05-05-2017
6.	Last Date for download of RFP Document	17-05-2017 till 2 pm

7.	Last Date for Submission of EMD and Bid Document Fee	17-05-2017 till 3 pm
8.	Date of Start of online submission of bids	04-05-2017
9.	Last Date for Submission of Bids	17-05-2017 till 3 pm
10.	Submission of Original copies of Bid Security (Physical Copy), Power of attorney, if any	17-05-2017 at 3.30 pm
11.	Opening of Techno-Commercial (Pre-qualification and Technical- Bid) Bids on e-procurement platform	17-05-2017 at 3.30 pm
12.	Evaluation of the Pre-qualification and Technical- Bid on e-procurement platform	From 17-05-2017 at 3.30 pm onwards
13.	Opening the Price Bid on e-procurement platform	Will be informed later
14.	Contract Finalization and Award	Will be informed later

5. General Instructions to Bidders

5.1 Availability and cost of the RFP Documents

- For the detailed tender notice, please visit website <https://www.mstcecommerce.com/eprochome/kopt>. For participation in e-tender please visit e-tender website <https://www.mstcecommerce.com/eprochome/kopt>. The bidders are expected to purchase the tender documents as per the details mentioned below.
- Cost of Tender documents is as mentioned in the section 3.
- The Request for Proposal documents (in three volumes) can be obtained in person from the address mentioned in the section 3 on any working day by paying the cost of bid document through non-refundable crossed Demand Draft, drawn on any nationalized/scheduled bank in favour of Kolkata Port Trust, payable at Kolkata (or) through ECS (RTGS/NEFT) in favour of Kolkata Port Trust, Kolkata Dock System directly into the designated bank account. The details of the bank for RTGS/NEFT are
 - Name of Bank & Branch: State Bank of Mysore, IFB Branch, Kolkata
 - Beneficiary Name : Kolkata Port Trust

c) Beneficiary Account No.: 54027971277

d) IFSC Code: SBMY0040259

Payment for tender document is exempted for Micro and Small Enterprises (MSE) with NSIC registered organizations in case of Single Point Registration covering all components of the said tender. Copy of valid NSIC Certificate for MSEs along with DIC's (District Industries Centre) Certificate has to be submitted along with the bid. Relevant documentation needs to be submitted along with the bid to substantiate the claim for exemption of tender document fee failing which, bidder's bid will be liable for rejection.

4. The tender document can also be downloaded from the web site provided in the section 3. In case the tender documents are downloaded from the website, then the bidder shall submit the cost of tender document along with his bid on or before the last date for submission of bid.
5. The bids submitted by the bidder without purchasing the RFP document will be summarily rejected. Also, the relevant bids submitted online will not be opened.
6. The bid documents purchased by the bidders from KoPT are not transferable. In case of consortium, any member of the respective consortium can purchase the bid document.
7. *Concerned bidder must ensure that the remitting bank positively enters their name and System Generated E - Tender no. in the 'Sender to Receiver' column at the time of making payment by RTGS/NEFT.*

5.2 Bid Processing Fee

- a) The Bid Processing fee (non-refundable) as mentioned in section 3 is to be paid/transferred online through NEFT/RTGS in favour of MSTC Limited. The Bank details, format etc., for transferring Transaction fee by RTGS to MSTC is detailed below :
 - a) Bank Details : Axis Bank, Shakespeare Sarani Branch
 - b) Account Details : Axis Bank A/c.No.005010200057840
 - c) IFSC Code No. : UTIB0000005.
- b) "The bidders shall enter the transaction fee details by using the "Transaction Fee Entry" Link under "My Menu" in the bidder login. The bidders have to select the particular tender in which they want to participate against the transaction fee by clicking on the tick box at the right and then Clicking on the "Submit" Button at the

bottom of the page. Then the page appears where the bidders are required to fill up the transaction details, namely the UTR No, Date of Transaction and the Remitting Bank in the given fields and then click on the “Confirm” Button”.

- c) The bidders should submit the transaction fee well in advance before the last date of submission of tender as they will be activated for bid submission only after receipt of transaction fee by MSTC Limited. The following are the contact details of the MSTC Limited
- Fax No. : 033- 22831002
 - Email ids: sanjibpoddar@mstcindia.co.in, arindam@mstcindia.co.in, rpradhan@mstcindia.co.in, smukherjee@mstcindia.co.in.
- d) Bidders may please note that the transaction fee should be deposited by debiting the account of the bidder only; transaction fee deposited from or by debiting any other party’s account will not be accepted.
- e) Transaction fee is non-refundable.
- f) In case of failure to access the payment towards Transaction fee for any reason, the bidder, in term, will not have the access to online e-tender.
- g) In case of failure to access the payment towards cost of tender document and/ or EMD for any reason, the bidder, in turn, will not have the access to online e-tender and no correspondence in this respect will be entertained and KoPTwill not be responsible for any such lapses on this account. Bidder(s) are advised to make remittance of tender fee and/ or EMD through ECS (RTGS/NEFT) well in advance and verify completion of transaction in respect of tender fee and EMD.
- h) Concerned bidder must ensure that the remitting bank positively enters their name and System Generated E - Tender no. in the ‘Sender to Receiver’ column at the time of making payment by RTGS/NEFT.

5.3 Acknowledgement

The bidders are requested to acknowledge the receipt of the complete set of RFP documents by handing over acknowledgement receipt to the RFP issue authority as per the Form A.1 by hand, e-mail or Fax to the address mentioned in Section 3 or in case of online bid submission, upload the form along with the technical cover on the online procurement portal of KoPT.

5.4 Earnest Money Deposit

1. Bidders shall transfer/ submit an amount as mentioned in Section 3, as EMD.
2. In case of DD/Pay Order/Banker's Cheque should in favour of Kolkata Port Trust payable at Kolkata.
3. In case of RTGS/NEFT should in favour of Kolkata Port Trust and the details are mentioned in Section 5.1.
4. In case of Bank Guarantee, the same should be in favour of Kolkata Port Trust as per the format given in Annexure B – Form B.6.
5. EMD payment is exempted for Micro and Small Enterprises (MSE) with NSIC registered organizations in case of Single Point Registration covering all components of the said tender. Copy of valid NSIC Certificate for MSEs along with DIC's (District Industries Centre) Certificate has to be submitted along with the bid. Relevant documentation needs to be submitted along with the bid to substantiate the claim for exemption of EMD failing which, bidder's bid will be liable for rejection.
6. Unless forfeited pursuant to point 9 of this clause, Bid Security/EMD, if any, will be returned on following occasions, without any interest, as promptly as possible, and within 30 days of receipt of written request from the bidder for the return of bid security:
 - a) All Bidders upon annulment of the bidding pursuant to "Authority's Right to Accept any Bid or Reject any or all Bids";
 - b) Bidders refusing a request to extend the period of validity of their bids;
 - c) The successful Bidder once it has signed the Contract Agreement, KoPT may, at the Selected Bidder's option, adjust the amount of EMD in the amount of PBG to be provided by him in accordance with the provisions of the Bidding Document;
 - d) The unsuccessful Bidders at the same time as in (c), that is, when they are informed about the successful establishment of the contract with the successful Bidder.
7. No interest shall be payable by KoPT to the Bidder(s) on the bid security amount for the period of its currency.

8. The bid without adequate bid security, as mentioned above, will be liable for rejection without providing any further opportunity to the bidder concerned.
9. The bid security may be forfeited:
 - i. If a bidder withdraws its bid during the period of bid validity
 - ii. In case of a successful bidder, if the bidder fails to sign the contract in accordance with terms and conditions
 - iii. If any of the bidders modify their bid during the validity period.
 - iv. On submission of any forged documents

5.5 Pre-Bid meeting

6. The KoPT will conduct a Pre-Bid meeting, tentatively scheduled as per the schedule given in section 4 above. The representatives of the interested organizations may attend the pre-bid conference at their own cost. The purpose of the pre-bid meeting is to provide bidders with information regarding the RFP and the proposed requirements in reference to this RFP. It will also provide each bidder with an opportunity to seek clarifications regarding any aspect of the RFP and the project. The venue for the Pre-bid meeting is the bid issuer's address provided in Section 3.

6.1 Bidder Inquiries and KoPT's responses

1. All enquiries from the bidders relating to this RFP must be submitted in writing exclusively to the contact person notified by KoPT in section 3 in the format specified in *Form A.7 Request for Clarification*. A copy of the bidder enquiries should also be emailed to the bid issuer's email address provided in the Section 3. The mode of delivering written questions would be through post or email. KoPT will not be held responsible for ensuring receipt of such bidders' email inquiries. Telephone calls will not be accepted for clarifying the queries.
2. After the RFP is issued to the bidder, KoPT shall accept written questions/inquiries from the bidders who downloaded/purchased the RFP document. KoPT will endeavour to provide a complete, accurate, and timely response to all questions to all the bidders through corrigendum(s). However, KoPT makes no representation or warranty as to the completeness or accuracy of any response, nor does KoPT undertake to answer all the queries that have been posed by the bidders.

3. All clarifications/ responses given by KoPT for bidder queries will be published on the website / Procurement Portal given under Section 3 and will form part of NIT/ RFP. No separate mails/ clarifications/ responses shall be sent to individual bidder queries. Any email communications sent by bidders to KoPT must be sent to the email address provided in Section 3.

6.2 Site Visit Opportunity for the Bidders

KoPT will facilitate for a site visit to port area to the bidders who are interested and have downloaded the tender documents. This could potentially help them understand the requirements. A maximum of 2 technical persons from each bidder will be allowed to visit the site. The date and time may be decided mutually after the Pre-bid meeting date. All bidders who are submitting the bid in response to this tender shall be deemed to have inspected the entire project site prior to submitting their bid.

6.3 Supplementary Information / Corrigendum / Amendment to the RFP

1. If KoPT deems it appropriate to revise any part of this RFP or to issue additional data to clarify an interpretation of the provisions of this RFP, it may issue supplements to this RFP. Such supplemental information, including but not limited to, any additional conditions, clarifications, minutes of meeting, and official communication over email/post will be communicated to all the bidders by publishing on the KoPT's procurement website given under Section 3. Any such supplement/corrigendum/amendment shall be deemed to be incorporated by this reference into this RFP.
2. The letters seeking clarifications sent either to all the bidders or to specific bidder as the case may be during the evaluation of technical and commercial proposal shall also be deemed to be incorporated by this reference in this RFP.
3. At any time prior to the deadline (or as extended by KoPT) for submission of bids, KoPT, for any reason, whether at its own initiative or in response to clarifications requested by prospective bidder, may modify the RFP document by issuing amendment(s). All such amendments will be published on the KoPT's procurement website given under Section 3. All such amendment(s) will be binding on all the bidders.

4. In order to allow bidders a reasonable time to take the amendment(s) into account in preparing their bids, KoPT, at its discretion, may extend the deadline for the submission of bids.

6.4 Bid Preparation Costs

7. The bidder is responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings / discussions / presentations, preparation of bid in providing any additional information required by KoPT to facilitate the evaluation process, and in negotiating a definitive Service Agreement (Master Service Agreement provided in Volume III of this RFP) and all such activities related to the bid process. This RFP does not commit KoPT to award a contractor to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award of the contract for implementation of the project.

7.1 KoPT's Right to terminate the Process

1. KoPT may terminate the RFP process at any time without assigning any reason. KoPT makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone.
2. This RFP does not constitute an offer by KoPT. The bidder's participation in this process may result in KoPT selecting the bidder to engage in further discussions and negotiations towards execution of a contract. The commencement of such negotiations does not, however, signify a commitment by KoPT to execute a contract or to continue negotiations.
3. The KoPT has the right to terminate this discussions and negotiations process without assigning any reason and no costs will be reimbursed to the participating bidders.

7.2 Acceptance of part / whole bid / modification – Rights thereof

8. KoPT reserves the right to modify the technical specifications /quantities / requirements / tenure mentioned in this RFP including addition / deletion of any of the item or part thereof after pre-bid and the right to accept or reject wholly or partly bid offer, or, without assigning any reason whatsoever. No correspondence in this regard shall be

entertained. KoPT also reserves the unconditional right to place order on the whole or part bid quantity to successful bidder.

8.1 Authentication of Bids

The original and all copies of the bid shall be typed or written in indelible ink and signed by the Bidder or a person duly authorized to bind the Bidder to the Contract. A certified true copy of the corporate sanctions/approvals authorizing its authorized representative to sign/act/execute documents forming part of this proposal including various RFP documents and binding contract shall accompany the bid. All pages of the bid, except for un-amended printed literature, shall be initialed and stamped by the person or persons signing the bid.

8.2 Interlineations in Bids

The bid shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by the Bidder, in which case such corrections shall be initialed by the person or persons signing the bid.

8.3 Consortium Bids

Considering the high levels of expertise and specialized skills needed to carry out the project, a group of Companies are allowed to come together and bid for this project as a consortium. However, the following must be noted with respect to consortium bids:

- i. The number of consortium members cannot exceed **two**, including the Prime Bidder.
- ii. The primary responsibility for discharging of the project responsibilities under the agreement would be that of the Prime Bidder only.
- iii. Only Prime Bidder will submit the bids. However, a tri-party agreement shall be executed/ signed between the KoPT, Prime bidder and consortium partner in case the tender is awarded to a consortium.
- iv. The Prime Bidder as well as consortium bidder shall be registered in **India** only

- v. The technical bid shall contain the details of arrangements between the Prime Bidder and other member of the consortium, in the form of an *inter-se* agreement between them.
- vi. The turnover of the Prime bidder shall be considered for pre-qualification evaluation.
- vii. The technical qualifications of all the members of a consortium shall be considered for evaluation. In case, consortium member leaves the prime bidder during the currency of the contract, it is the responsibility of the prime bidder to either fulfill the contractual obligation himself or bring in another consortium member whose qualification matches the criteria stated in the NIT.
- viii. Notwithstanding anything contained in this agreement, all the members of the Consortium of Companies, entrusted with the responsibilities of the Project, shall be jointly and severally responsible to KoPT in respect of meeting the financial liabilities of the Service Provider arising out of the Project.

8.4 Venue & Deadline for submission of bid

1. Bid documents are to be submitted online as mentioned in section 6.1.
2. **Last Date & Time of submission:** Before the date and time stipulated in schedule given in section 4
3. KoPT may, in exceptional circumstances and at its discretion, extend the deadline for submission of bids by issuing an addendum. All such addendums will be published on the website / Procurement Portal given under Section 3. In such a case of extension, all rights and obligations of KoPT and the bidders previously subject to the original deadline will thereafter be subject to the deadline as extended.

8.5 Late Bids

9. Bids received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained.

9.1 General Conditions of Contract (GCC):

General Conditions of Contract, Forms and Agreements as sanctioned by the Board of Trustees of KoPT for the Port of Kolkata is hosted at

www.kolkataporttrust.gov.in(<http://www.kolkataporttrust.gov.in/showfile.php?layout=1&lang=1&lid=1342>). Only those Clauses, Forms or Formats, which are not covered elsewhere in this Tender Document, shall be applicable. Also, for the sake of interpretation of the contents of the Annexures, the terms contained in the main tender document (other than Annexures) including the General Conditions of Contract, Forms and Agreements shall prevail.

9.2 Conditions under which this RFP is issued

1. This RFP is not an offer and is issued with no commitment. KoPT reserves the right to withdraw the RFP and change or vary any part thereof at any stage. KoPT also reserves the right to disqualify any bidder, should it be so necessary at any stage for any reason whatsoever.
2. Timing and sequence of events resulting from this RFP shall ultimately be determined by KoPT.
3. No oral conversations or agreements with any official, agent, or employee of KoPT shall affect or modify any terms of this RFP and any alleged oral agreement or arrangement made by a bidder with any department, agency, official or employee of KoPT shall be superseded by the definitive agreement that results from this RFP process. Oral communications by KoPT to bidders shall not be considered binding on KoPT, nor shall any written materials provided by any person other than KoPT.
4. Neither the bidder nor any of the bidder's representatives shall have any claims whatsoever against KoPT or any of their respective officials, agents, or employees arising out of, or relating to this RFP or these procedures (other than those arising under a definitive service agreement with the bidder in accordance with the terms thereof).
5. All bidders, until the contract is awarded and the successful bidder, up to one year during the currency of the contract shall not, directly or indirectly, solicit any employee of KoPT to leave KoPT or any other officials involved in this RFP process in order to accept employment with the organization, or any person acting in concert with the bidder, without prior written approval of KoPT.

9.3 Rights to the Content of the bid

All the bids and accompanying documentation submitted as bids against this RFP will

become the property of KoPT and will not be returned after opening of pre-qualification proposals. If any bidder does not qualify in pre-qualification evaluation, the technical proposal shall not be evaluated. KoPT is not restricted in its rights to use or disclose any or all of the information contained in the proposal and can do so without compensation to the bidders. KoPT shall not be bound by any language in the proposal indicating the confidentiality of the proposal or any other restriction on its use or disclosure. KoPT has the right to use the services of external experts to evaluate the bids submitted by the bidders and share the content of the bid either partially or completely with the experts for evaluation with adequate protection of the confidentiality information of the bidder.

9.4 Modification and Withdrawal of Bid

1. No Bid shall be modified, substituted or withdrawn by the Bidder on or after the Bid Due Date. Entire bid security shall be forfeited if any of the bidders modify or withdraw their bid during the bid validity period.
2. Any alteration/ modification in the Bid or additional information supplied subsequent to the Bid Due Date, unless the same has been expressly sought for by the KoPT, shall be disregarded.
3. The tender/ bid submission process is according to the e-Procurement process. The procedure for modification, substitution and withdrawal of bids shall be as specified in the e-Procurement website mentioned in the section 3 of this RFP. Hence, bidders are advised to go through such procedures stated in the online procurement portal of KoPT.
4. The Bidder may modify, substitute or withdraw its Bid after submission, provided the same is done before the last date of bid submission or that written notice of the modification, substitution or withdrawal is received by the KoPT prior to the last date and time for submission of Bid. However, after the last date of bid submission, the EMD amount will be forfeited in case of modification, substitution or withdrawal of bid and such modified/ substituted bid will not be considered for evaluation.

9.5 Non-Conforming Bids

A bid may be construed as a non-conforming bid and ineligible for consideration:

1. If it does not comply with the requirements of this RFP.
2. If a bid appears to be “canned” presentations of promotional materials that do not follow the format requested in this RFP or do not appear to address the particular requirements of the proposed solution, and any such bidders may also be disqualified

9.6 Disqualification

A bid is liable to be disqualified in the following cases:

- a) Bid submitted without tender document fee, Bid Processing fee and EMD or has not been credited/ transferred online to the designated account stated in the RFP. A mere attempt to transfer the required funds shall not be construed as payment.
- b) Bid not submitted in accordance with the procedure and formats prescribed in this document/ NIT/ RFP or submitted without required documents stipulated in this NIT/ RFP or treated as non-conforming proposal;
- c) During validity of the Bid, or its extended period, if any, the bidder increases his quoted prices;
- d) After last date of bid submission, bidder modifies/ withdraws the bid
- e) The bidder qualifies the bid with its own conditions or assumptions;
- f) Bid is received in incomplete form;
- g) Bid is received after due date and time;
- h) Bid is not accompanied by all the requisite documents;
- i) A commercial bid submitted with assumptions or conditions.
- j) If the bidder provides any assumptions in the commercial bid or qualifies the commercial bid with its own conditions, such bids will be rejected even if the commercial value of such bid is the lowest (best value);
- k) If bidder provides quotation only for a part of the project;
- l) Information submitted in technical proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period of the contract if any;

- m) Commercial bid/ details is enclosed/ uploaded along with technical proposal;
- n) Bidder tries to influence the proposal evaluation process by unlawful/corrupt/fraudulent means at any point of time during the bid process;
- o) If multiple bids are received from the same company, all such bids are liable to be rejected.
- p) Bidder fails to deposit the Performance Bank Guarantee (PBG) or fails to enter into a contract within 30 working days of the date of notice of award or within such extended period, as may be specified by KoPT;
- q) Bidders may specifically note that while evaluating the bids, if it comes to KoPT's knowledge expressly or implied, that some bidders may have colluded in any manner whatsoever or otherwise joined to form an alliance resulting in delaying the processing of bid, then the bidders so involved are liable to be disqualified for this tender as well as for a further period of three years from participation in any of the tenders floated by KoPT;
- r) If the EMD, pre-qualification bid, technical bid and the entire documentation (including but not limited to the soft/electronic copies of the same, presentations during technical evaluation, clarifications provided by the bidder) submitted along with EMD, Pre-qualification and technical bid are found to contain any information on price, pricing policy, pricing mechanism or any information indicative of the commercial aspects of the bid;
- s) Bidders or any person acting on its behalf indulges in corrupt and fraudulent practices; and
- t) In case bidder fails to meet any of the bidding requirements as indicated in this RFP

9.7 Conflict of Interest

Bidder shall furnish an affirmative statement as to the absence of, actual or potential conflict of interest on the part of the Bidder or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with KoPT. Additionally, such disclosure shall address any and all potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of the Bidder to complete the requirements

as given in the RFP. Please use form given in Form A.5 (Undertaking on Conflict of Interest) for making declaration to this effect.

9.8 Acknowledgement of Understanding of Terms

By submitting a bid in response to this tender, each bidder shall be deemed to acknowledge having carefully read and understood all sections of this RFP, including all forms, schedules, annexure hereto, and all existing terms, conditions and limitations.

10. Bid Submission Instructions (Important instructions for E – tender)

Bidders are requested to read the terms & conditions of this tender before submitting your online tender. Bid must be direct, concise, and complete. All information not directly relevant to this RFP should be omitted. KoPT will evaluate bidder's bid based on its clarity and the directness of its response to the requirements of the project as outlined in this RFP.

Bidders shall furnish/ upload the required information on their pre-qualification, technical and commercial proposals in the formats provided in the RFP. Any deviations in format the tender will be liable for rejection.

1.	<p>Process of E-tender :</p> <p>A) Registration: The process involves vendor's registration with MSTC e-procurement portal which is free of cost. Only after registration, the vendor(s) can submit his/their bids electronically. Electronic Bidding for submission of Technical Bid as well as Commercial Bid will be done over the internet. The Vendor should possess Class III signing type digital certificate. Vendors are to make their own arrangement for bidding from a PC connected with Internet. MSTC is not responsible for making such arrangement. (Bids will not be recorded without Digital Signature).</p> <p>SPECIAL NOTE: THE TECHNICAL BID AND THE COMMERCIAL BID HAS TO BE SUBMITTED ON-LINE AT https://www.mstcecommerce.com/eprhome/kopt</p> <p>1). Vendors are required to register themselves online with https://www.mstcecommerce.com → e-Procurement → PSU/Govt depts → Select KoPT Logo → Register as Vendor -- Filling up details and creating own user id and password → Submit.</p> <p>2). Vendors will receive a system generated mail confirming their registration in their email which has been provided during filling the registration form. In case of any clarification, please contact KoPT / MSTC, (before the scheduled time of the e- tender).</p> <p>B) System Requirement:</p> <ul style="list-style-type: none"> i) Windows 7 or above Operating System ii) IE-7 and above Internet browser. iii) Signing type digital signature
----	--

	<p>iv) Latest updated JRE 8 (x86 Offline) software to be downloaded and installed in the system.</p> <p>To disable “Protected Mode” for DSC to appear in The signer box following settings may be applied.</p> <ul style="list-style-type: none"> • Tools => Internet Options =>Security => Disable protected Mode If enabled- i.e, Remove the tick from the tick box mentioning “Enable Protected Mode”. • Other Settings: Tools => Internet Options => General => Click On Settings under “browsing history/ Delete Browsing History” => Temporary Internet Files => Activate “Every time I Visit the Webpage”. <p>To enable ALL active X controls and disable ‘use pop up blocker’ under Tools→Internet Options→ custom level (Please run IE settings from the page https://www.mstcecommerce.com once)</p>
2.	The Techno-commercial Bid and the Price Bid shall have to be submitted online at https://www.mstcecommerce.com/eprochome/kopt Tenders will be opened electronically on specified date and time as given in the Tender.
3.	All entries in the tender should be entered in online Technical & Commercial Formats without any ambiguity.
4.	<p>Special Note towards Transaction fee:</p> <p>The vendors shall pay the transaction fee using “Transaction Fee Payment” Link under “My Menu” in the vendor login. The vendors have to select the particular tender from the event dropdown box. On selecting NEFT, the vendor shall generate a challan by filling up a form. The vendor shall remit the transaction fee amount as per the details printed on the challan without making change in the same. On selecting Online Payment, the vendor shall have the provision of making payment using its Credit/ Debit Card/ Net Banking. Once the payment gets credited to MSTC’s designated bank account, the transaction fee shall be auto authorized and the vendor shall be receiving a system generated mail.</p> <p>Transaction fee is non-refundable.</p> <p>A vendor will not have the access to online e-tender without making the payment towards transaction fee.</p> <p>NOTE</p> <p>Bidders are advised to remit the transaction fee well in advance before the closing time of the event so as to give themselves sufficient time to submit the bid.</p>
5.	Information about tenders / corrigendum uploaded shall be sent by email only during the process till finalization of tender by KoPT. Hence the bidders are required to ensure that their corporate email I.D. provided is valid and updated at the time of registration of vendor with MSTC. Vendors are also requested to ensure validity of their DSC (Digital Signature Certificate).
6.	E-tender cannot be accessed after the due date and time mentioned in NIT.
7.	<p>Bidding in e-tender :</p> <ol style="list-style-type: none"> a) Vendor(s) need to submit necessary EMD, Tender fees and Transaction fees (If ANY) to be eligible to bid online in the e-tender. Tender fees and Transaction fees are non refundable. No interest will be paid on EMD. EMD of the unsuccessful vendor(s) will be refunded by the tender inviting authority. b) The process involves Electronic Bidding for submission of Technical and Commercial Bid. c) The vendor(s) who have submitted transaction fee can only submit their

	<p>Technical Bid and Commercial Bid through internet in MSTC website https://www.mstcecommerce.com → e-procurement → PSU/Govt depts → Login under KoPT → My menu → Auction Floor Manager → live event → Selection of the live event</p> <p>d) The vendor should allow running JAVA application. This exercise has to be done immediately after opening of Bid floor. Then they have to fill up Common terms/Commercial specification and save the same. After that click on the Technical bid. If this application is not run then the vendor will not be able to save/submit his Technical bid.</p> <p>e) After filling the Technical Bid, vendor should click ‘save’ for recording their Technical bid. Once the same is done, the Commercial Bid link becomes active and the same has to filled up and then vendor should click on “save” to record their Commercial bid. Then once both the Technical bid & Commercial bid has been saved, the vendor can click on the “Final submission” button to register their bid</p> <p>f) Vendors are instructed to use <i>Attach Doc button</i> to upload documents. Multiple documents can be uploaded.</p> <p>g) In all cases, vendor should use their own ID and Password along with Digital Signature at the time of submission of their bid.</p> <p>h) During the entire e-tender process, the vendors will remain completely anonymous to one another and also to everybody else.</p> <p>i) The e-tender floor shall remain open from the pre-announced date & time and for as much duration as mentioned above.</p> <p>j) All electronic bids submitted during the e-tender process shall be legally binding on the vendor. Any bid will be considered as the valid bid offered by that vendor and acceptance of the same by the Buyer will form a binding contract between Buyer and the Vendor for execution of supply.</p> <p>k) It is mandatory that all the bids are submitted with digital signature certificate otherwise the same will not be accepted by the system.</p> <p>l) Buyer reserves the right to cancel or reject or accept or withdraw or extend the tender in full or part as the case may be without assigning any reason thereof.</p> <p>m) No deviation of the terms and conditions of the tender document is acceptable. Submission of bid in the e-tender floor by any vendor confirms his acceptance of terms & conditions for the tender.</p>
8.	Any order resulting from this open e-tender shall be governed by the terms and conditions mentioned therein.
9.	No deviation to the technical and commercial terms & conditions are allowed.
10.	The tender inviting authority has the right to cancel this e-tender without assigning any reason thereof.
11.	Vendors are requested to read the vendor guide and see the video in the page https://www.mstcecommerce.com/eprhome to familiarize them with the system before bidding.

10.1 Language of bid

The bid and all correspondence and documents shall be written in English.

11. Bid Opening and Evaluation Process

11.1 Bid opening sessions

1. Total transparency will be observed while opening the bids.
2. KoPT reserves the rights at all times to postpone or cancel a scheduled bid opening.
3. The KoPT will open all bids, in the presence of Bidders' representatives who choose to attend, at the time, on the date and at the place specified in the section 3 of this RFP or as updated through amendment/ corrigendum. Bidders' representatives shall sign a register as proof of their attendance.
4. Only bids that are opened and read out at bid opening shall be considered further.
5. Bids shall be opened one at a time, reading out the name of the Bidder and whether there is a modification; the presence or absence of a EMD, etc..
6. The commercial bids of all technically qualified bidders will be opened in the presence of the bidders who are present at the time of opening of the commercial bid. The bidders' names, the bid prices, the prices of any alternative (if alternatives have been requested or permitted) any discounts, bid deviations, and such other details as the KoPT may consider appropriate, will be announced by the KoPT at the time of financial bid opening. Any bid price, discount or modification that is not read out and recorded at bid opening will not be considered for bid evaluation, irrespective of the circumstances.
7. KoPT shall go ahead and open the bid of the bidders even if there is no representative of the bidder present.
8. In the event of the specified date of bid opening being declared a holiday for KoPT, the Bids shall be opened at the same time and location on the next working day.
9. During bid opening, preliminary scrutiny of the bid documents will be made to determine whether they are complete, whether required bid security and/ or tender document fee has been furnished, and whether the bids are generally in order. Bids not conforming to such preliminary requirements will be prima facie rejected.

10. The EMD will be opened by KoPT for evaluation, in the presence of bidders' representatives who may choose to attend the session on the specified date, time and address. EMD envelope of the bidders will be opened on the same day and time, on which the Pre-Qualification bid is opened, and bids not accompanied with the requisite EMD or whose EMD is not in order shall be rejected. In case EMD amount and/ or tender document fee are transferred online, the receipt of the same shall be verified as per e-Procurement process guidelines. Bids shall be considered for further evaluation only if there is a successful credit in the bank account or as per the norms laid out by KoPT.

11.2 Overall Evaluation Process

1. A tiered evaluation procedure will be adopted for evaluation of bids, with the pre-qualification evaluation being completed before technical evaluation and technical evaluation being completed before the commercial bids are opened and compared.
2. KoPT will assess the bidders' capabilities against the pre-qualification criteria. Only those bidders' who meet / exceed the pre-qualification criteria shall proceed for technical evaluation.
3. KoPT will review the technical bids of the qualified bidders to determine whether the technical bids are substantially responsive as per the requirements specified in the RFP. Bids that are not substantially responsive are liable to be disqualified.
4. KoPT may seek inputs from their professional, external experts, agencies in the bid evaluation process.
5. The bidders who meet all the mandatory technical criteria shall qualify for the commercial evaluation stage.
6. The commercial bids for the technically qualified bidders will then be opened and reviewed to determine whether the commercial bids are substantially responsive as per the requirements specified in the RFP.

11.3 Evaluation of Pre-Qualification bids

The evaluation of the Pre-Qualification bids will be carried out in the following manner:

1. The bidders' Pre-Qualification bid in the bid document will be evaluated as per the requirements specified in the RFP and adopting the pre-qualification criteria spelt out in this RFP. The Bidders are required to submit all required documentation in support of the pre-qualification criteria specified for evaluation.
2. KoPT may seek additional information and clarifications from any or all of the Bidders on the Pre-Qualification bid. Any of the additional information or clarifications submitted by the Bidder on the pre-qualification bid should not have any commercial implications.

11.4 Evaluation of Technical bid

The evaluation of the Technical bids will be carried out in the following manner:

1. The bidders' technical bid proposed in the bid document is evaluated as per the requirements specified in the RFP and adopting the evaluation criteria spelt out in this RFP. The Bidders are required to submit all required documentation in support of the evaluation criteria as per the format given in the RFP for technical evaluation.
2. KoPT may seek additional information and clarifications from any or all of the Bidders on the Technical bid. Any of the additional information or clarifications submitted by the Bidder on the technical bid should not have any commercial implications.
3. **Proposal Presentations:** The Bid Evaluation Committee ("Committee") may invite each pre-qualified bidder to make a presentation to KoPT at a date, time and venue decided by KoPT. The purpose of such presentations would be to allow the bidders to present their proposed solutions to the committee and orchestrate the key points in their bids. Bidders should also attempt to provide a live demonstration, on the presentation day, of all such equipment (RFID related equipment) that is being proposed as a part of the solution. This is to facilitate the users with a better insight on the proposed solution and its functioning.
4. The committee may seek oral clarifications from the bidders. The primary function of clarifications in the evaluation process is to clarify ambiguities and uncertainties arising out of the evaluation of the bid documents. Oral clarifications provide the opportunity for the committee to state its

requirements clearly and for the bidder to more clearly state its bid. The committee may seek inputs from their professional and technical experts in the evaluation process.

5. Following will be the technical evaluation methodology:
 - a) Verify compliance of the bidder's technical bid against the compliance criteria.
 - b) Only those bidders, who fulfil the mandatory technical compliance criteria, mentioned in section 7.7 and 7.8 and the Technical Specification Requirements (RFP, Annexure II), will qualify for the evaluation of their Commercial bids.
 - c) The result of the technical evaluation stage shall be uploaded on the procurement portal for viewing of all bidders.
 - d) The technically qualified bidders will be informed of the date and venue of the opening of commercial bids through online or through a written communication.

11.5 Evaluation of Commercial Bid

1. The Commercial Bids of only the technically qualified bidders will be opened for evaluation.
2. Since the payments to the Bidder will be made over a period of 7 years, the Discounted Cash Flow (DCF method) method will be used to compare different payment terms, including progressive stage payments so as to bring them to a common denomination for determining lowest bidder.
3. Detailed modalities for applying DCF technique are as below:
 - a) Net Present Value (NPV) will be used for evaluation of the Commercial Offer. The Net Present Value of a contract is equal to the sum of the present values of all the cash flows associated with it. The formula for calculating NPV of a Commercial Offer is illustrated below.
 - b) KoPT will evaluate bids by adopting DCF method with a discounting rate in consonance with the SBI Prime Lending Rate (SBIPLR) of 13.85% (effective

from 01.04.2017) (as published on SBI website –<https://www.sbi.co.in>).The DCF is defined in the Glossary of Management and Accounting Terms, published by the Institute of Cost and Works Accountants of India. DCF method would be used for evaluation of bids.

c) Standard software for example 'Excel', 'Lotus 1-2-3' or any other spread sheet which comes preloaded as part of a personal computer will be used for NPV calculation.

d) The NPV will be calculated using the formula below:

NPV will be calculated as

NPV = PCC + cUHF + cHF + (NPV of MCC for 84 months) + (NPV of MOC for 84 months) where,

- o Quoted Total CAPEX cost (TCC) –include cost of 4,200 HF RFID cards
- o Paid CAPEX Cost (PCC)=60% of Estimated Capex Cost or 60% of quoted Capex Cost, whichever is lower.
- o Cost of 20,000 UHF RFID cards (cUHF)
- o Cost of 50,000 HF RFID cards (cHF)
- o Monthly Capex Cost (MCC) = (TCC – PCC)/84
- o Monthly OPEX cost (MOC)
- o NPV of MCC for 84 months = $\sum MCC / (1 + r)^i$ where,
 - $i = 1, 2, 3, \dots, 84$ months
 - $r =$ Monthly Discounting Rate calculated as $((1 + \text{annual discounting rate})^{1/12} - 1)$
- o *(MCC) is the monthly amount calculated after deducting the amount paid to the service provider from the total Capital Cost quoted (refer to Form D.2) and divided with 84 in the respective month "i"*
- o NPV of MOC for 84 months = $\sum MOC / (1 + r)^i$ where,
 - $i = 1, 2, 3, \dots, 84$ months
 - $r =$ Monthly Discounting Rate calculated as $((1 + \text{annual discounting rate})^{1/12} - 1)$
- o *(MOC) is the monthly amount quoted under the Services Provided during contract period (7 Years) (refer Form D.2) in the respective month "i"*

4. The bidder who has quoted the lowest NPV as per above calculation will be adjudged as the Lowest bidder for the tender and will be awarded the work.
5. Even though the cost of UHF and HF RFID cards is included in the commercial evaluation, this cost will not be considered in the contract value of the project.
6. The Contract Value for the purpose of this project will be the sum of :
 - Total CAPEX cost (TCC)
 - Monthly OPEX Cost (MOC) * 84 months

11.6 Pre-Qualification Evaluation Criteria

The Responses received will be evaluated based on the criteria as specified below.

1.	The Bidder (all the members of the consortium, in case of consortium) should be a company registered in India under Indian Companies Act 1956 as evidenced by the Certificate of Incorporation issued by the Registrar of Companies, India. The company should be primarily providing IT / ICT / IteS operations in India for at least the last five financial years for the year ending 31 st December, 2016 as evidenced by the Memorandum of Association and certificate of Commencement of Business respectively..
2.	The Bidder (the Prime Bidder in case of consortium) should have an average annual turnover of not less than INR 4.32 Crores for each of the last three financial years ending 31 st March 2016.
3.	<p>Bidder (the Prime Bidder or member of the consortium in case of consortium) must have successfully completed similar work(s)² or Part completed ongoing similar works (executed value of completed works/Part completed on going similar works during last Seven (07) years ending last day of month previous to the one in which applications are invited should be either of the following.</p> <p style="margin-left: 40px;">a. Three similar completed works/Part completed on going similar works (Executed value of completed work/Part completed on going similar works) each costing not less than</p>

	<p>amount equal to 40% of the estimated cost (or)</p> <p>b. Two similar completed works/ Part completed on going similar works (Executed value of completed works/Part completed on going similar works) each costing not less than amount equal to 50% of the estimated cost (or)</p> <p>c. One similar completed work/ Part completed on going similar works (Executed value of completed work/Part completed on going similar works) costing not less than amount equal to 80% of the estimated cost</p>
4.	The bidder (all the members in case of consortium) must have valid Service Tax Code No., ESI Reg. No, EPF Reg. No.,
5.	Bidder should submit Original Manufacturer Authorization Form (MAF) from all hardware manufacturers & software system providers authorizing to bid specific to this tender. MAF should be on the original letterhead of the OEM.OEMs of Hardware (or) Software may support multiple bidders.
6.	The Bidder (all the members in case of consortium) should not be blacklisted by Central/ State Government Ministry/ Department/ PSU/ Government Company. Bidder also should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry/ Department/ PSU/ Government Company. The Bidder shall submit a self-declaration in the respective company letter head, signed by authorized signatory.

Notes:

- In case of on-going long duration projects that includes operations and maintenance services in scope, the bidder should have successfully completed 01 year of the project after Go-Live phase in the project.*
- Similar Work** means *“Supply , Installation, Integration, Commissioning and maintenance at least a period of 01 year after commissioning of system like*

- a. *ERP/Access Control/Biometric/Visitor Management System/ Attendance/Access Control Readers/Long Range Readers/Smart Card System (OR)*
 - b. *Companies who have successfully executed e-Governance projects under Aadhar/RSBYJ/Driving license/Financial Inclusion are also eligible to bid.*
3. *Only Project Citations in- progress ongoing long duration / completed in the last 7 financial years will be considered for evaluation.*

11.7 Technical Evaluation Criteria

11.7.1 Mandatory Compliance Criteria

The bidders shall meet all the mandatory compliance criteria mentioned below. Failure in meeting the mandatory compliance criteria will result in technical disqualification of the bidder.

Mandatory Compliance	
The technical response must meet all the following mandatory compliance requirements. Failure to meet any one or more of the following criteria will result in the disqualification of the technical bid response.	
Part I: Bid Cover Letter	
1.	Bid/ Proposal Cover Letter as per Form A.2 of Volume – II of RFP (Submitted as part of the Pre-qualification bid)
Part II: Undertakings from the Bidder	
1.	Submission of <i>Undertaking on Pricing of Items of Technical Response</i> in the format prescribed in this RFP (Form C.2)
2.	Submission of <i>Undertaking on Compliance, Sizing of Infrastructure, and Service Level Compliance</i> in the format prescribed in this RFP (Form C.3)
3.	Submission of <i>Undertaking on Work Environment and Personnel</i> in the format prescribed in this RFP (Form C.4)
4.	Submission of <i>Undertaking on Changes to the Contract Clauses</i> in the format prescribed in this RFP (Form C.5)
5.	Submission of <i>Undertaking on Absence of Litigation</i> in the format prescribed in this RFP (Form C.6)

6.	Submission of Integrity Pact as per format given in the General Conditions of Contract and Consortium Agreement executed between the consortium members clearly explaining the roles, responsibilities, liabilities, etc. that would be discharged by members of the consortium for the project
Part III: Undertakings from the OEM or Licensee of the proposed product	
7.	Submission of <i>Undertaking on Patent Rights</i> in the format prescribed in this RFP (Form C.7)
8.	Submission of <i>Undertaking on Non-malicious Code Certificate</i> in the format prescribed in this RFP (Form C.8)
9.	Submission of <i>Undertaking on Support to Third Party Audits and Certification</i> in the format prescribed in this RFP (Form C.9)

11.8 Technical Bid

The technical bid must not contain any pricing information.

The technical bid shall contain the following:

1. Part I: Undertakings from the Bidder as mentioned in section 7.7.1

2. Part II: Project Team

- a. Attachment 1 to Part II: Details of the list of the key personnel of the project team that will be permanently based out of the Project Office till project completion.
- b. Attachment 2 to Part II: Proposed profiles for the below key personnel. Use the format provided in Form C.12 Profiles of the resources proposed for the project. Experience and qualification of the key resources are listed below:
 - i. Project Manager:
 - Graduate
 - 10+ years of experience
 - Experience in handling RFID based implementation will be preferred
 - Experience in Public Sector / Government Projects
 - Should have handled 3 IT projects

- PMP/ PRICE2 is preferred
- ii. Solution Architect:
 - Graduate
 - 15+ years of experience
 - 10 years of relevant experience
 - Experience in solution RFID based projects is preferred
- iii. IT support desk:
 - Graduate with CCNA or diploma of minimum 1 year in hardware and software
 - 1-3 years of experience
 - Installation, configuration and support of IT equipment (PC, laptops, printers etc.)
 - Understanding in troubleshooting Internet Connectivity, LAN /WAN related Issues
 - Identify and escalate priority issues to the concerned team
 - Log Tickets in the call-logging tool on behalf of users
 - Multi-tasking capabilities
 - Should be fluent in English, Hindi and Bengali
 - Willing to work in shifts
 - Excellent verbal & written communication
- iv. Operations executive:
 - Graduate with CCNA or diploma of minimum 1 year in hardware and software
 - 1-3 years of experience
 - Experience in coordinating IT projects
 - Coordination with multiple functional teams
 - E-savvy & have good command over written/ spoken English , Hindi & Bengali
 - Willing to work in shifts

3. Part III – Assumptions: List out all the assumptions made by the bidder in the preparation of the bid response. However, the assumptions shall not have any

commercial impact, shall not be binding on the KoPT and such assumptions cannot be basis for any Change Requests during the project duration.

4. Part IV – Optional Supplementary Information: Additional information directly relevant to the scope of services provided in the Volume I of the RFP may be submitted to accompany the proposal. In submitting additional information, please mark it as supplemental to the required response. However, it is clearly understood that the additional services or supplementary information will not be considered for evaluation purposes.

5. Part V: Technical Specifications Compliance

Bidder shall provide a detailed compliance of specifications of the proposed products with the specifications mentioned in the RFP, Annexure II document. Any deviations to the required specification shall result in rejection of bid. However, bidder is free to offer a product which exceeds the required specification and the same shall not be treated as a deviation.

-

11.9 Commercial Bid

1. The price should be quoted on total CAPEX and monthly OPEX basis.
2. It is mandatory to provide prices inclusive of all taxes (excluding Service Tax), duties and levies. All the taxes of any nature whatsoever shall be borne by the Bidder. In case Excise Duty is applicable, the same should be clearly indicated so that KoPT can avail the CENVAT credit.
3. "TAXES & DUTIES: - The rate quoted by the tenderer should be considered to complete the work in all respect and should include all taxes, octroi, surcharge etc. (except service taxes) payable to Government or any other concern and no extra payment, whatsoever will be entertained by the Trustees' under any circumstances.
4. As KoPT is not a Registered Body Corporate, it is not liable to pay service tax under 'Reverse Charge Mechanism' as per Service Tax Law.
5. Service Tax, if leviable, will be paid extra by the Trustees as applicable. The bidder shall not include Service Tax in his rates. In case Service Tax is payable, the Contractor will be required to submit necessary bill / challans / invoice in accordance with Service Tax Rules and the Contractor needs to be registered with the Central Excise/Service Tax Authority as the case may be, and copy of the

same shall be submitted to KoPT. On demand, the successful bidder will have to submit documents regarding payment of Service Tax.

6. CENVAT CRITERIA: In the event of cenvatable bought out items, if any ,the contractor is required to ensure that invoices are drawn in the name of contractor and it should be marked " account KOLKATA PORT TRUST" as per cenvat credit rules and regulations. KoPT would provide the Service Tax Registration No. for availing Cenvat Credit. As far as possible items to be procured from first/second stage dealer and maintain the above formalities to the extent possible so that KoPT can avail the cenvat credit.
7. However, Service Tax as applicable on the amount of liquidated damage as well as other recovery i.e. damage, penalty, land rent, etc. shall be deducted from contractors' bill at applicable rates and the same will not be reimbursed by KoPT."
8. KoPT shall pay the eligible monthly payment including service tax that will be paid as extra at actuals.
9. Bill of Quantity is indicative and arrived to facilitate RFID systems at all operational gates for a period of 07 years. However, owing to requirements, if additional quantities of components need to be supplied, the same would be supplied at the rate quoted in the price bid by the bidder during the currency of the contract.
10. Entire RFID solution/ systems including all associated equipment supplied by the Service Provider as part of the contract shall remain the property of KoPT.
11. The charges towards entry/permits for each vehicle, persons etc. will be fixed and collected by KoPT officials.
12. Statutory recoveries (WB VAT, Income Tax) will be recovered wherever applicable as per the rules in force (presently WBVAT@5%,I.T@2%)
13. Service Tax shall be reimbursed for item wherever applicable to the firm as per the prevailing rates subject to documentary proof of Service Tax registration.
14. VAT/CST will be absorbed by the firm.
15. No financial commitment at this stage on either side is given. Above BOQ is an indicative list. However actual quantity may vary as per the site conditions

16. The prices quoted in the Commercial bid shall be valid and firm for the entire period of the contract, including any extensions.
17. The Commercial bid should be submitted as per the format provided in the Form D.2, Form D.3 and Form D.4 (Formats for the Commercial Bid Response):
 - a. Commercial bid Covering Letter as per the format provided in Form D.1- Commercial Bid Cover Letter
 - b. Prices and Price Information
 - i. The Bidder shall quote a price for all the components, the services of the solution to meet the requirements of KoPT as listed in the Volume – I of this RFP.
 - ii. Prices shall be quoted entirely in Indian Rupees.
 - iii. No adjustment of the price quoted in the Commercial bid shall be made on account of any variations in costs of labour and materials, currency exchange fluctuations with international currency or any other cost component affecting the total cost in fulfilling the obligations under the contract.
 - iv. The price quoted in the Commercial Bid shall be the only payment, payable by the KoPT to the successful Bidder for completion of the contractual obligations, by the successful Bidder under the Contract, subject to the terms of payment specified as in the proposed commercial bid or the one agreed between KoPT and the Bidder.
 - v. The prices, once offered, must remain fixed and must not be subject to escalation for any reason whatsoever within the period of the validity of the bid and the contract. A bid submitted with an adjustable price quotation or conditional bid may be rejected as non-responsive.
 - vi. Bidder should provide all prices as per the prescribed format given in Form D.2 and Form D.3 (Formats for the Commercial Bid Response). Bidder should not leave any field blank. In case the field is not applicable, Bidder must indicate “0” (zero) in all such fields.
 - vii. If the rate for a line item is left blank it would be considered as zero and no payment would be made to the respective item.

- viii. It is mandatory to provide prices inclusive of all taxes, duties and levies. All the taxes of any nature whatsoever shall be borne by the Bidder. The bidder needs to quote only the applicable Service Taxes as extra
 - ix. The bid amount shall be inclusive of packing, forwarding, transportation, insurance, delivery, installation charges and any other charges as applicable.
 - x. All costs incurred due to delay of any sort, shall be borne by the Bidder.
 - xi. KoPT reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated within specified time frames.
18. Bidders should submit the price bid as per the format provided online in the e-Procurement portal.
19. The Bidder is expected to price all the items and services as per the Bill of Quantity at Annexure-V for successful implementation of the project and subsequent operations & maintenance in line with SLA.
20. KoPT may seek clarifications from the Bidder on the Technical bid. Any of the clarifications by the Bidder on the technical proposal should not have any commercial implications. The Commercial Bid submitted by the Bidder should be inclusive of all the items in the technical bid and should incorporate all the clarifications provided by the Bidder on the technical bid during the evaluation of the technical offer.
21. Unless expressly indicated in this RFP, bidder shall not include any technical information regarding the services in the commercial bid. Additional information directly relevant to the scope of services provided in the Volume – I of the RFP may be submitted to accompany the bid. In submitting additional information, please mark it as supplemental to the required response. However, this information will not be considered for evaluation purposes.
22. The bidder is expected to provide all the assumptions related to the bid in the technical bid itself and not in the Commercial bid. A commercial bid with any assumptions or conditions will be disqualified.

23. Taxes

- a. The KoPT or its nominated agencies shall deduct taxes, levies, cess, duties etc. from the amounts due and payable to the Implementing Agency wherever applicable and pay the balance amount after deduction of such taxes. The Service Provider shall pay for all other taxes in connection with this Agreement, SLA, scope of work and any other engagement required to be undertaken as a part of this Agreement, including, but not limited to, property, sales, use, excise, value-added, goods and services, consumption and other similar taxes or duties.
- b. The KoPT or its nominated agencies shall provide the Service Provider with the TDS certificate towards deduction of taxes on payments under this Agreement. The Service Provider agrees to reimburse and hold the KoPT or its nominated agencies harmless from any deficiency including penalties and interest relating to taxes that are its responsibility under this paragraph. For the purposes of this Agreement, taxes shall include taxes incurred on transactions between and among the KoPT or its nominated agencies, the Service Provider and third party subcontractors.
- c. If, after the date of this Agreement, there is any change of rate of levy under the existing applicable laws of India with respect to taxes and duties due to any statutory notification/s, which are directly payable by the KoPT for providing the services i.e. service tax or any such other applicable tax from time to time, which increase or decreases the cost incurred by the Service Provider in performing the Services, then the remuneration and reimbursable expense otherwise payable by the KoPT under this Agreement, shall be increased or decreased accordingly by correspondence between the Parties hereto. However, in case of any new or fresh tax or levy imposed after submission of the bid the Service Provider shall be entitled to reimbursement on submission of proof of payment of such tax or levy.

24. Correction of Errors

- a. Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted figures will be entertained after the

bids are submitted to KoPT. All corrections, if any, should be initialed by the authorized signatory signing the proposal form before submission, failing which the figures for such items may not be considered. In case of online bid submission, no correction is allowed in the commercial bid.

- b. In case of discrepancy between the amounts mentioned in figures and in words, the amount in words shall govern.

12. Award of Contract

12.1 Award Criteria

KoPT will award the Contract to the successful bidder whose bid has been determined to be substantially responsive, technically qualified and has been determined as the lowest value bid as per the commercial evaluation details provided under Section 7.5.

12.2 KoPT's Right to Accept/ Reject Any or All bids

KoPT reserves the right to accept or reject any bid, and to annul the tendering process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the reasons / grounds for KoPT action.

12.3 Notification of Award

Prior to the expiration of the validity period, KoPT will notify the successful bidder in writing or by email, that its bid has been accepted. The notification of award will constitute the formation of the contract. The successful bidder will be required to furnish the Performance Bank Guarantee within 30 days of the date of notice of award.

12.4 Contract Finalization and Award

The contract will be awarded to the bidder whose NPV (as explained in section 7.5) is the lowest in comparison to all other bidders.

12.5 Signing of Contract

The successful bidder shall provide the Letter of Acceptance along with "Performance Bank Guarantee" and certified true copies of its constitutional documents and board resolutions authorizing the execution, delivery and performance of this Agreement by the Service Provider to the KoPT within 30 days of Notice of Award. The submission of the above documents is conditions precedent for signing the Agreement. The Agreement (MSA) is provided in Volume III of the RFP.

KoPT shall have the right to annul the award in case there is a delay of more than 15 days from the fulfillment of conditions precedent in signing of Agreement, for any reasons attributable to the successful bidder.

12.6 Suggestions on the Draft Contract

- a. A Master Service Agreement (MSA) including the standard terms and all the other terms specific to the implementation of the Project is circulated as Volume III of this RFP. KoPT reserves the right to revise the contract.
- b. It is expected that the bidder will be able to execute this contract without any modifications, in case they are selected for doing so.
- c. The bidder is requested to indicate as per the form specified in the Form A.6, the changes the bidder desires to have and the reason for the same. This is only a solicitation of suggestions for change. However, it is neither guaranteed that these requests for changes will be accepted in the final contract nor this process should be construed as any commitment from KoPT to consider those suggestions.
- d. However, it is clearly understood that the changes the bidder desires to have will not be the basis for affecting any changes in the Commercial bid already submitted by the bidders. The bidder should not suggest any change that has financial or commercial implications during the execution of the contract and is against the basic spirit of procuring the services for the implementation of the project
- e. The bidder is also requested not to base the commercial quote on the assumptions that the suggestions for changes to the draft contract will be accepted by KoPT

12.7 Failure to agree with the Terms and Conditions of the RFP

Failure of the successful bidder to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, KoPT will also invoke the BG, PBG (if the PBG is submitted) and forfeit the EMD of the successful bidder in case of default.

13. Payment Terms and Schedule

13.1 Performance Bank Guarantee

A Performance Bank Guarantee (PBG) of 10% of contract value would be furnished by the successful bidder in the form of a Bank Guarantee as per the format provided in this RFP from Scheduled Indian Banks. The PBG should be furnished within 30 working days from the date of notice of award and should be valid up to 180 days beyond the duration of contract.

In case any claims or any other contract obligations are outstanding, the Service Provider (successful bidder) will extend the Performance Bank Guarantee as asked by KoPT till such time the Service Provider settles all claims and completes all contract obligations. The Performance Bank Guarantee will be subject to encashment by the KoPT, in case, conditions regarding adherence to delivery schedule, conditions regarding warranty, settlement of claims and other provisions of the contract are not fulfilled by the Service Provider.

In case the contract is extended, the PBG has to be valid for 180days beyond the extended period.

13.2 Liquidated Damages

In the event of the Bidder's failure to submit the Bond, Guarantees and Documents and supply the solution / equipment as per schedule specified in this RFP, KoPT may at its discretion withhold any payment until the completion of the contract. The KoPT may also deduct from the payment due to the Bidder as agreed, liquidated damages to the tune of 0.5% from the corresponding milestone payment of the delayed / undelivered services for every week of delay or part of a week, subject to the maximum value of the Liquidated Damages being not more than 10% of the value of corresponding milestone payment of the delayed / undelivered services. This right to claim any liquidated damages shall be, without prejudice to other rights and remedies, available to KoPT under the contract and law.

13.3 Payment Schedules and Milestones

All the payments will be done to the selected Service Provider by the KoPT after successfully completion of the milestone and acceptance of deliverable by the KoPT.

1. No advance/mobilization payment will be made by KoPT
2. Payment to the Service Provider will start after the Go-Live period and system stabilization period.
3. Following payment milestones shall be applicable for the project:
 - o 60% of the Estimated Capex Value (ECV) or 60% of the Total CAPEX Cost (TCC) quoted by the Service Provider, whichever is lesser, will be paid on the declaration of successful Go-Live of project.
 - o Balance of the Total CAPEX cost (Total CAPEX cost – (60% of ECV or TCC, whichever is lesser)) quoted by the Service Provider will be paid as Equated Monthly Installments (EMI) for 07 years.
 - o Monthly OPEX cost quoted by the Service Provider will be paid on a monthly basis
 - o Total Equated Monthly Installment (EMI) for the Service Provider will be the sum of:
 - Monthly installment of balance of CAPEX cost for 07 years
 - Monthly OPEX cost quoted by the Service Provider
 - o Payment towards OPEX shall be made based on the SLA and service deliverable as per the RFP.
 - o KoPT will not make any payment towards RFID Cards provided for its internal requirement, as the same is included in the estimate (CAPEX). Payment towards RFID cards provided to Port users shall be directly collected by the Service Provider from the users at the quoted rate.
 - o If required, Additional RFID cards will be provided to meet port's internal requirements by Service Provider and charges for registration and issuing additional cards & passes will be paid by KoPT as per the quoted rates on actual basis.
4. Payments for the monthly Operations and Maintenance phase will be made at the end of that respective month after satisfactory delivery of the services.

5. Payment of the equated Monthly payment (EMI) is linked to the compliance with the SLA metrics.
6. Actual EMI amount payable is the payment due to the Service Provider after any SLA related deductions.
7. If the contract period is extended then the payment will be only for the term that is extended and all other terms and conditions remains the same.
8. The liability of the KoPT during such extended period is limited to the quoted monthly OPEX cost payable on a monthly basis for the extended period.

Annexure A: Bid Formats**Form A.1: RFP acknowledgement letter****(Company Letterhead)**

[Date]

To,

The Joint Director (P & R)

Kolkata Dock System

15 Strand Road, 6th Floor,

Kolkata – 700001

Sub: Acknowledgement of Request for Proposal (RFP) for Implementation of RFID based Access Control system at KoPT

Dear Sir,

This is to notify you that we have received the complete set of RFP documents circulated by your organization for the implementation of RFID based Access Control system at KoPT.

The following persons will be the authorized representatives of the company for all the future correspondence till the completion of the bidding process, between the KoPT and our organization.

	Primary Contact Person	Secondary Contact Person
Name		
Title		
Company name		
Address		
Phone No.		
Mobile No.		
Fax No.		

Email		
--------------	--	--

We understand that it will be the responsibility of our organization to keep the KoPT informed of any changes in this list of authorized persons and we fully understand that the KoPT shall not be responsible for non-receipt or non-delivery of any communication and/or any missing communication in the event reasonable prior notice of any change in the authorized person(s) of the company is not provided to the KoPT.

Information relating to the examination, clarification and any other processes concerning the RFP and selection shall not be disclosed to any person(s) not officially concerned with such process until the process is over. Undue use of confidential information related to the process by us may result in rejection of our proposal.

Dated this Day of **2017**

(Signature) (In the capacity of)
(Name)

Duly authorized to sign the Tender Response for and on behalf of:

(Name and Address of Company)

Seal/Stamp of bidder

Witness Signature:

Witness Name:

Witness Address:

Form A.2 : Proposal Cover Letter
[Company Letter Head]

[Date]

To,

The Joint Director (P & R)

Kolkata Dock System

15 Strand Road, 6th Floor,

Kolkata – 700001

Dear Sir,

Ref: Request for Proposal – Implementation of RFID based Access Control system at KoPT

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in the RFP for the implementation of RFID based Port Access Control system at KoPT, and to meet such requirements and provide such services as set out in the RFP.

We attach hereto the bid response as required by the RFP, which constitutes our proposal.

We undertake, if our proposal is accepted, to adhere to the implementation plan put forward in RFP or such adjusted plan as may subsequently be mutually agreed between us and the KoPT or its appointed representatives.

If our proposal is accepted, we will obtain a Performance Bank Guarantee in the format given in the RFP document issued by a schedule bank in India, acceptable to the KoPT, for a sum of 10% of the contract value as specified in the RFP for the due performance of the agreement.

We agree for unconditional acceptance of all the terms and conditions set out in the RFP document and also agree to abide by this tender response for a period of **180days** from the date fixed for bid opening and it shall remain binding upon us with full force and virtue. Until within this period a formal Agreement is prepared and executed, this tender response, together with your written acceptance thereof in your notification of award, shall constitute a binding agreement between us and KoPT.

Form A.3: Power of Attorney for signing of Application/ Bid

Know all men by these presents, We..... (name of the firm and address of the registered office) do hereby irrevocably constitute, nominate, appoint and authorize Mr./ Ms. (name), son/daughter/wife of and presently residing at, who is presently employed with us and holding the position of , as our true and lawful attorney (hereinafter referred to as the "Attorney") to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to submission of our application for Request for Proposal and submission of our response for the implementation of RFID based Port Access Control system initiated by the KoPT, including but not limited to signing and submission of all applications, bids and other documents and writings, participate in Pre-bid and other conferences and providing information/ responses to the Authority, representing us in all matters before the Authority, signing and execution of all contracts including the Agreement and undertakings consequent to acceptance of our bid, and generally dealing with the Authority in all matters in connection with or relating to or arising out of our response for the said Project and/ or upon award thereof to us and/or till the entering into Agreement with the KoPT.

AND, we hereby agree to ratify and confirm and do hereby ratify and confirm all acts, deeds and things lawfully done or caused to be done by our said Attorney pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Attorney in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

IN WITNESS WHEREOF WE, THE ABOVE NAMED
PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON THISDAY OF
....., 2017

For
(Signature, name, designation and address)

Witnesses:

1.

(Notarised)

2.

Accepted

.....

(Signature)

(Name, Title and Address of the Attorney)

Notes:

- The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required, the same should be under common seal affixed in accordance with the required procedure.
- Also, wherever required, the Respondent should submit for verification the extract of the charter documents and documents such as a resolution/ power of attorney in favour of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Respondent.

**Form A.4: Earnest Money Deposit (EMD) Covering Letter
(Company letter head)**

[Date]

To

The Joint Director (P & R)

Kolkata Dock System

15 Strand Road, 6th Floor,

Kolkata – 700001

Dear Sir,

Sub: EMD/Bid Security – Implementation of RFID based Port Access Control System

The following are the details of the Earnest Money Deposit as requested in the RFP document for the implementation of RFID based Access Control system.

Sl. No		Details	Details
1.	EMD in the form of		
2.	In favor of		
3.	Amount		
4.	Date		
5.	Name of the Bank		
6	Valid Up to		

Yours faithfully,

Designated Contact Person

Designation

Company Seal

**Form A.5: Conflict of Interest
(Company letter head)**

[Date]

To

The Joint Director (P & R)

Kolkata Dock System

15 Strand Road, 6th Floor,

Kolkata – 700001

Dear Sir,

Sub: Undertaking on Conflict of Interest regarding Implementation of RFID based Port Access Control System at KoPT

I/We do hereby undertake that there is absence of, actual or potential conflict of interest on the part of the bidder or any prospective sub-contractor due to prior, current, or proposed contracts, engagements, or affiliations with KoPT.

I/We also confirm that there are no potential elements (time-frame for service delivery, resource, financial or other) that would adversely impact our ability to complete the requirements as given in the RFP.

We undertake and agree to indemnify and hold the KoPT harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees and fees of professionals, reasonably) by the KoPT and/or his representatives, if any such conflict arises later.

Yours faithfully,

Authorized Signatory

Designation

Company Seal

Form A.6: Request for Clarification**(Company letter head)**

[Date]

To

The Joint Director (P & R)

Kolkata Dock System

15 Strand Road, 6th Floor,

Kolkata – 700001

Dear Sir,

Sub : Request for Clarifications

BIDDER'S REQUEST FOR CLARIFICATION			
Name of Organization submitting request		Name & position of person submitting request	Full formal address of the organization including phone, fax and email points of contact
			Tel:
			Fax:
			Email:
S. No	Bidding Document Reference(s) (section number/page)	Content of RFP requiring Clarification	Points of clarification required
1			
2			

Yours faithfully,

Authorized Signatory

Designation

Company Seal

Annexure B: Pre-qualification Bid Formats

Form B.1 : Pre-Qualification Bid Response Check List

Bid Response Checklist		Submitted in the Bid Response (Y / N)	Reference (Page Number of the Bid Response)
Part – I			
1.	General Details of the Organization as per Form B.2		
2.	Financial Details of the Organization as per Form B.3		
Part – II			
3.	Relevant Project Experience as per Form B.4		
Part –III			
4.	Original Manufacturer Authorization Form		
Part – IV			
5.	Self-declaration that not black listed as per the Form B.5		

Form B.2: General Details of the Organization

Details of the Organization	
Name of organization	
Nature of the legal status in India	
Legal status reference details	
Nature of business in India	
Date of Incorporation	
Date of Commencement of Business	
Number of full time IT professionals on its payroll	
Address of the Headquarters	<i><<street and mailing addresses, phone, fax and email>></i>
Address of the Registered Office in India	<i><<street and mailing addresses, phone, fax and email>></i>
Address of the Branch Office in India (if responsible for work under this contract)	<i><<street and mailing addresses, phone, fax and email>></i>
Other Relevant Information	
Mandatory Supporting Documents: <ul style="list-style-type: none"> a) Certificate of Incorporation from Registrar Of Companies(ROC) b) Certificate of Commencement of Business c) Memorandum of Association 	

Form B.3 : Financial Details of the Organization (Prime bidder in case of consortium)

Financial Information			
	FY 2013-14	FY 2014-15	FY 2015-16
Revenue (in INR crores)			
Profit Before Tax (in INR crores)			
Revenue from IT services and system integration services (in INR crores)			
Net Worth			
Other Relevant Information			
<p>Mandatory Supporting Documents:</p> <p>a. Auditor Certified financial statements for the last three financial years ending 31st March 2016; 2013-14, 2014-15 and 2015-16</p> <p>b. Certification by the company auditors supporting the revenue break-up for IT Services and System Integration Services</p>			

Form B.4: Relevant Project Experience for RFID Project

Project Experience for RFID Projects	
General Information	
Name of the project	
Client for which the project was executed	
Contact details / Address of the client	
Current Status	
Project Details	
Description of the project	
Scope of Services / Business Processes addressed by the Application Developed / Maintained by the Bidder	
Other Details	
Total Duration of the project (no. of months, start date, completion date)	
Total cost of the project	
Total cost of the services provided by the Bidder	
Any Other Relevant Information	
Project Capability Demonstration	
Complete details of the scope of the project shall be provided to indicate the relevance to the pre-qualification criterion (which is part of minimum qualification criteria).	

Form B.5: Self-declaration on the Blacklisting (Each bidder in case of consortium)

(Company letterhead)

[Date]

To,

The Joint Director (P & R)

Kolkata Dock System

15 Strand Road, 6th Floor,

Kolkata – 700001

Dear Sir,

Dear Sir,

Ref: Request for Proposal for implementation of RFID based Access Control system

We confirm that we are not blacklisted by Central/ State Government Ministry/ Department/ PSU/ Government Company. We also confirm that we're not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry/ Department/ PSU/ Government Company.

Dated this Day of **2017**

(Signature)

(In the capacity of)

(Name)

Duly authorized to sign the Tender Response for and on behalf of:

(Name and Address of Company) Seal/Stamp of bidder

Form B.6: Bank Guarantee format for submission of EMD

(The Bank shall fill in this Bank Guarantee form in accordance with the instructions indicated. To be executed on Rs 100/- non-judicial stamp paper)

(Bank's Name and Address of Issuing Branch or Office)

Beneficiary: _____ (Name and Address of Employer/Board)

Date : _____

Tender Guarantee No: _____

We have informed that *<name of the Bidder>* (hereinafter called "the Bidder") has submitted to you its Tender dated (hereinafter called "the Tender") for the execution of "RFID based Port Access Control System" under Invitation for Tenders No.*<Tender reference number>*. Furthermore, we understand that, according to your conditions Tenders must be supported by an Earnest Money Deposit (EMD).

At the request of the Bidder, we, *<name of Bank>* irrevocably undertake to pay you any sum or sums not exceeding in total an amount of *<amount in figures and words>* upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the Tender conditions, because the Bidder:

- a) Has withdrawn its Tender during the period of Tender validity specified by the Bidder in the Form of Tender; or
- b) Having been notified of the acceptance of its Tender by the Employer / Board during the period of Tender Validity, (i) fails or refuses to execute the form of Agreement, if required or (ii) fails or refuses to furnish the performance guarantee, in accordance with the instructions to Bidders.

This guarantee will expire unless otherwise extended or informed by the Employer/ Board:

- a) If the Bidder is the successful Bidder, upon our receipt of copies of the contract signed by the Bidder and the performance guarantee issued to you upon the instructions of the Bidder; or
- b) If the Bidder is not the successful Bidder, upon the earlier of:

- i. Our receipt of a copy of your notification to the Bidder of the name of successful Bidder; or
- ii. Twenty eight days after the expiration of the Bidder's Tender validity or any extended period thereof;

Consequently, any demand for payment under this guarantee must be received by us at the office on or before that date.

[Signature (s)]

[|Authorisation letter from the issuing bank that the signatory of this BG is authorized to do so should also be enclosed]

Annexure C: Technical Bid Formats

Form C.1: Technical Response Check list

Bid Response Checklist		Submitted in the Bid Response (Y / N)	Reference (Page Number of the Bid Response)
Part – I Undertakings from the Bidder			
1.	Undertaking on Pricing of Items of Technical Response in the format prescribed in this RFP (Form C.2)		
2.	Undertaking on Compliance, Sizing of Infrastructure, and Service Level Compliance in the format prescribed in this RFP (Form C.3)		
3.	Undertaking on Work Environment and Personnel in the format prescribed in this RFP (Form C.4)		
4.	Undertaking on Changes to the Contract Clauses in the format prescribed in this RFP (Section Form C.5)		
5.	Undertaking on Absence of Litigation in the format prescribed in this RFP (Form C.6)		
6.	Undertaking on Patent Rights in the format prescribed in this RFP (Form C.7)		
7.	Undertaking on Non-malicious Code Certificate in the format prescribed in this RFP (Form C.8)		
8.	Undertaking on Support to Third Party Audits and Certification in the format prescribed in this RFP (Form C.9)		
9.	Submission of Integrity Pact as per format given in the General Conditions of Contract and submission of Consortium Agreement executed between the consortium members		
Part – II: Project Team			
10.	Attachment 1 to Part II		
11.	Attachment 2 to Part II		
Part – III: Assumptions			
12.	Assumptions, if any		
Part – IV: Optional Supplementary Information			
13.	Optional Supplementary Information, if any		
Part V: Technical Specifications Compliance			
14.	Submission of Technical Specification Compliance as per RFP Annexure II		

Form C.2: Undertaking On Pricing of Items of Technical Response

(Company letterhead)

[Date]

To,
The Joint Director (P & R)
Kolkata Dock System
15 Strand Road, 6th Floor,
Kolkata – 700001

Sub: Undertaking on Clarifications sent to KoPT

Dear Sir / Madam,

I/We do hereby undertake that Commercial bid submitted by us is inclusive of all the items in the technical bid and is inclusive of all the clarifications provided/may be provided by us on the technical bid during the evaluation of the technical offer. We understand and agree that our Commercial bid is firm and final and that any clarifications sought by you and provided by us would not have any impact on the Commercial bid submitted by us.

Yours faithfully,

Authorized Signatory
Designation

**Form C.3: Undertaking on Compliance, Sizing of Infrastructure and Service Level
Compliance**

(Company letterhead)

[Date]

To,
The Joint Director (P & R)
Kolkata Dock System
15 Strand Road, 6th Floor,
Kolkata – 700001

Sub: Undertaking on Compliance, Sizing of Infrastructure and Service Level

Dear Sir / Madam,

1. I/We as Service Provider (SP) do hereby undertake that we have proposed and sized the infrastructure and all software (including licenses) based on information provided by KoPT in its RFP document and in accordance with the Service Level requirements and minimum specifications provided and assure KoPT that the sizing is for all the functionality envisaged in the RFP document.
2. I/We as Service Provider do hereby undertake that the proposed compute, storage (primary and backup) and memory at the Data Centre and Disaster Recovery Site as per our sizing will be sufficient to meet the project's requirements.
3. I/We as Service Provider (SP) do hereby undertake that we shall monitor, maintain, and comply with the service levels stated in the RFP to provide quality service to KoPT.

4. Any augmentation of the proposed solution or storage or sizing of any of the proposed solutions (software, hardware) or resources in order to meet the requirements and/or the requisite Service Level requirements given by KoPT will be carried out at no additional cost to KoPT.

Yours faithfully,

Authorized Signatory
Designation

Form C.4: Undertaking on Work Environment and Personnel

(Company letterhead)

[Date]

To,
The Joint Director (P & R)
Kolkata Dock System
15 Strand Road, 6th Floor,
Kolkata – 700001

Sub: Undertaking on Work Environment and Personnel

Dear Sir / Madam,

1. I/We as Service Provider (SP) do hereby understand that the onsite team of Service Provider operating out of KoPT premises will be provided only with seating space. Any other requirements such as desktops, software will be Service Provider's responsibility.
2. I/We as Service Provider do hereby undertake that those persons, whose profiles were part of the basis for evaluation of the bids and have been identified as "Key Personnel" of the proposed team for the project, shall be deployed at the project site during the Project as per our bid submitted in response to the RFP.
3. We undertake that any of the identified "Key Personnel" shall not be removed or replaced without the prior written consent of KoPT.

4. Under exceptional circumstances, if the Key Personnel are to be replaced or removed, we shall put forward the profiles of personnel being proposed as replacements, which will be either equivalent or better than the ones being replaced. However, whether these profiles are better or equivalent to the ones being replaced will be decided by KoPT. KoPT will have the right to accept or reject these substitute profiles.

5. We also undertake to staff the Project with competent team members in case any of the proposed team members leave the Project either due to voluntary severance or disciplinary actions against them.

6. We acknowledge that KoPT has the right to seek the replacement of any member of the Project team being deployed by us, based on the assessment of KoPT that the person in question is incompetent to carry out the tasks expected of him/her or found that person does not really possess the skills /experience/qualifications as projected in his/her profile or on the ground of security concerns or breach of ethics.

7. In case we assign or reassign any of the team members, we shall be responsible, at our expense, for transferring all appropriate knowledge from personnel being replaced to their replacements within a reasonable time.

Yours faithfully,

Authorized Signatory
Designation

Form C.5: Undertaking on Absence of Litigation

(Company letterhead)

[Date]

To,
The Joint Director (P & R)
Kolkata Dock System
15 Strand Road, 6th Floor,
Kolkata – 700001

Sub: Undertaking on Absence of Litigation

Dear Sir,

I/We as Service Provider (SP) do hereby confirm that no claim, litigation, proceeding, arbitration, investigation, inquiry or order from any regulatory authority, or material controversy is pending, on-going or is contemplated which would have a material adverse effect on our ability to enter into the Agreement or provide the Services to KoPT on this Project.

Yours faithfully,

Authorised Signatory
Designation

Form C.6: Undertaking on Patent Rights

(Company letterhead)

[Date]

To,
The Joint Director (P & R)
Kolkata Dock System
15 Strand Road, 6th Floor,
Kolkata – 700001

Sub: Undertaking on Patent Rights

Dear Sir / Madam,

1. We as Service Provider (SP) do hereby undertake that none of the deliverables being provided by us is infringing on any patent or intellectual and industrial property rights as per the applicable laws of relevant jurisdictions having requisite competence.
2. We also confirm that there shall be no infringement of any patent or intellectual and industrial property rights as per the applicable laws of relevant jurisdictions having requisite competence, in respect of the equipment, systems or any part thereof to be supplied by us. We shall indemnify KoPT against all cost/claims/legal claims/liabilities arising from third party claim in this regard at any time on account of the infringement or unauthorized use of patent or intellectual and industrial property rights of any such parties, whether such claims arise in respect of manufacture or use. Without prejudice to the aforesaid indemnity, we shall be responsible for the completion of the supplies including spares and uninterrupted use of the equipment and/or system or any part thereof to KoPT and persons authorized by KoPT, irrespective of the fact of claims of infringement of any or all the rights mentioned above.
3. If it is found that it does infringe on patent rights, We absolve KoPT of any legal action.

Yours faithfully,
Authorized Signatory
Designation

Form C.7: Non-Malicious Code Certificate

(Company letterhead)

[Date]

To,
The Joint Director (P & R)
Kolkata Dock System
15 Strand Road, 6th Floor,
Kolkata – 700001

Sub: Non-Malicious Code Certificate

Dear Sir,

1. We hereby certify that the software being offered / developed as part of the contract does not and will not contain any kind of malicious code that would activate procedures to:
 - a. Inhibit the desired and the designed function of the equipment / solution.
 - b. Cause damage to the user or his equipment / solution during the operational exploitation of the equipment / solution.
 - c. Tap information regarding network, network users and information stored on the network that is classified and / or relating to National Security.
2. There are / will be no Trojans, Viruses, Worms, Spywares or any malicious software on the system and in the software offered or software that will be developed.
3. Without prejudice to any other rights and remedies available to KoPT , we are liable under Information Technology Act, 2000 and Indian Penal Code 1860 in case of physical damage, loss of information and those relating to copyright and Intellectual Property rights (IPRs), caused due to activation of any such malicious code in offered / developed software.

Yours faithfully,

Authorised Signatory
Designation

Form C.8: Undertaking on Support to Third Party Audits and Certification

(Company letterhead)

[Date]

To,
The Joint Director (P & R)
Kolkata Dock System
15 Strand Road, 6th Floor,
Kolkata – 700001

Sub: Undertaking on Support to Third Party Audits and Certification

Dear Sir / Madam,

1. I/We as Service Provider (SP) understand that third party audits may be carried out on deliverables, processes, applications, infrastructure, and all aspects of the project. Also, third party certification will also be carried out for the final acceptance of each phase in the project.
2. I/We understand that the responsibility to engage and ensure successful third party audit by CERT-In or Govt. empanelled agency and certification of RFID solution lies with the Service Provider.

Yours faithfully,

Authorized Signatory
Designation

Form C.9: Profiles of the resources proposed for the project

Summary of Profiles	
Role	Name of the Proposed Resource

A separate undertaking with the format as below with all the names of the proposed profiles should be provided.

Format for the Profiles: <<Role being proposed for>>	
Name of the person	
Current Organization	
Current Designation / Job Title	
Current job responsibilities	
Proposed Role in the Project	
Proposed Responsibilities in the Project	
Academic Qualifications (include the degree, academic institution, and year of graduation):	
Total number of years of experience	
Relevant Experience & Key Responsibilities (Provide the details of the projects such as project name, customer name, key project features, duration of the project, and status of the project)	

Certificate:

I, the undersigned, certify that to the best of my knowledge and belief, the proposed CVs correctly describes the qualifications and experience of the respective resource. I understand that any willful misstatement described herein may lead to disqualification of the bid.

Names of the proposed profiles:

1.

2.

3.

Signature:

Date:

[Signature of authorized representative] Day/Month/Year

Full name of authorized representative:

Annexure D: Commercial Bid Formats

Form D.1: Commercial Bid Cover Letter

(Company letterhead)

[Date]

To,
The Joint Director (P & R)
Kolkata Dock System
15 Strand Road, 6th Floor,
Kolkata – 700001

Dear Sir,

Ref: RFP for Selection of Service Provider for implementation of RFID based Port Access Control System at KoPT

Having examined the RFP Document, bid clarifications, Amendments thereof, the receipt of which is hereby duly acknowledged, we, the undersigned offer to provide the services, as required and outlined in the RFP. In order to meet such requirements and to provide services as set out in the RFP document, following is our quotation summarizing our Commercial Bid.

We attach hereto the Commercial bid as required by the Bid document, which constitutes our bid.

We undertake, if our bid is accepted, to carry out the services as put forward in the RFP or such modified requirements as may subsequently be agreed mutually between us and the KoPT or its appointed representatives.

We will obtain necessary Performance Bank Guarantees in the formats given in the bid document issued by a bank in India, acceptable to the KoPT and furnish them within the time frames set out in the RFP.

We agree for unconditional acceptance of all the terms and conditions in the bid document and we also agree to abide by this bid response for a period of 180 days from the date of bid opening and it shall be valid bid till such period with full force and virtue. Until within this period a formal contract is prepared and executed, this bid response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between the KoPT and us.

We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to the KoPT is true, accurate, and complete.

We agree that you are not bound to accept the lowest or any bid response you may receive. We also agree that you reserve the right in absolute sense to reject all or any if the products/ service specified in the bid response without assigning any reason whatsoever.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company/ agency/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this Day of **2017**

(Signature)

(In the capacity of)

Duly authorized to sign the Bid Response for and on behalf of:

(Name and Address of Company)

Seal/Stamp of Service Provider

Form D.2: Pricing Summary

S.No.	Description	Unit	Total amount in Rupees (Inclusive of all applicable taxes excluding Service Tax)
	Total CAPEX Cost (Sum of Form D.3)	Project	
	Monthly OPEX Cost (Sum of Form D.4)	Monthly	
	Cost of UHF RFID cards	20,000 cards	
	Cost of HF RFID cards	50,000 cards	

Applicable Taxes

1	Applicable Taxes for Monthly Variable Cost	
	Service Tax	Service Tax as applicable to be paid as extra at actuals.

Form D.3: Item wise pricing for CAPEX as per the Bill of Material:

Sl. No	BoM Components	Unit Pricing (inclusive of Taxes)
1	Item 1	
2	Item 2	
3	Item 3	
4	Item 4	
5	Itemn	

Note:

1. The complete RFID infrastructures including system hardware and software licenses shall be on the name of Kolkata Port Trust from day one.

Form D.4 :Item wise pricing for OPEX as per the Bill of Material:

Sl. No	BoM Components	Unit Pricing (inclusive of Taxes)
1	Man month rate of Technical resources – Project Manager	
2	Man month rate of Technical resources – Solution Architect	
3	Man month rate for Pass issue resource person	
4	Man month rate for Operational resource person	
5	<i>Any other item.....</i>	

Notes:

1. NPV will be calculated as per the clause 11.5 using a monthly discounting rate calculated as below:

$$\text{Monthly Discounting Rate (r)} = ((1 + \text{annual discounting rate})^{(1/12)} - 1)$$

2. Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted figures will be entertained after the proposals are submitted to the KoPT. All corrections, if any, should be initialed by the

- person signing the proposal form before submission, failing which the figures for such items may not be considered.
3. It is mandatory to provide prices inclusive of all taxes, duties and levies. All the taxes of any nature whatsoever shall be borne by the Bidder. The bidder needs to quote only the applicable Service Taxes as extra.
 4. The bid amount shall be inclusive of packing, forwarding, transportation, insurance, delivery, installation charges and any other charges as applicable.
 5. Prices shall be quoted entirely in Indian Rupees.
 6. The above table is comprehensive cost for bid evaluation purpose. Actual payment terms and conditions are as referred in Section Payment Schedules and Milestones.
 7. The prices quoted (including the man-power costs, additional compute & Storage capacity) in the Commercial bid shall be valid for the entire period of the contract.
 8. Correction of Errors:
 - a. In case of discrepancy between the amounts mentioned in figures and in words, the amount in words shall govern.
 9. If the rate for a line item is left blank it would be considered as zero and no payment would be made for the respective item during the contract duration.
 10. Bidder shall not include any technical information regarding the item/ services in the commercial proposal.
 11. The Bidder is expected to price all the items and services required for successful implementation of the project and subsequent operations & maintenance in line with SLA.
 12. All costs incurred due to delay of any sort, shall be borne by the Bidder.
 13. The bidder is expected to provide all the assumptions related to the proposal in the technical proposal itself and not in the Commercial bid. A Price bid with any assumptions or conditions will be disqualified.
 14. No adjustment of the price quoted in the Commercial bid shall be made on account of any variations in costs of labour and materials, currency exchange fluctuations with international currency or any other cost component affecting the total cost in fulfilling the obligations under the contract.

15. The price quoted in the Commercial bid shall be the only payment, payable by the KoPT to the successful Bidder for completion of the contractual obligations by the successful Bidder under the Contract, subject to the terms of payment specified as in the proposed commercial bid or the one agreed between the KoPT and the Bidder after negotiations.
16. The prices, once offered, must remain fixed and must not be subject to escalation for any reason whatsoever within the period of the validity of the proposal and the contract. A proposal submitted with an adjustable price quotation or conditional proposal may be rejected as non-responsive.

Form D.5: Performance Bank Guarantee Format

[Date]

From:

Bank _____

To,

The Joint Director (P & R)

Kolkata Dock System

15 Strand Road, 6th Floor,

Kolkata - 700001

Dear Sir / Madam,

WHEREAS _____ [Name and address of Agency] (hereinafter called "the Contractor") vide letter ref. _____ dated _____ has accepted Kolkata Port Trust's Letter of Award ref. _____ dated _____ for "_____{Details of work awarded}_____" (hereinafter called the "Contract").

AND WHEREAS it has been stipulated by KoPT in the said letter that the Contractor shall furnish a Bank Guarantee for the sum specified therein as security for compliance with his obligations in accordance with the terms & conditions of empanelment.

AND WHEREAS we have agreed to give the Contractor such a Bank Guarantee:

NOW THEREOF we hereby affirm that we are the Guarantor and responsible to you, on behalf of the Contractor up to a total of Rs. _____/- (Rupees _____) only, such sum being payable in the types and proportions of currencies in which the Contract Price is payable, and we undertake to pay you, upon your first written demand and without cavil or argument, any sum or sums within the limits of Rs. _____/- as aforesaid without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

1. We hereby waive the necessity of your demanding the said debt from the

Contractor before presenting us with the demand.

2. We further agree that no change or addition to or other modification of the terms of the service provider or of the works to be performed thereunder or of any of the Contract documents which may be made between you and the Service Provider shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification.
3. We undertake to pay to the KoPT any money so demanded notwithstanding any dispute or disputes raised by the Contractor in any suit or proceeding pending before any Court or Tribunal relating thereto our liability under this present being absolute and unequivocal. The payment so made by us under this bond shall be a valid discharge of our liability for payment there under and the Contractor shall have no claim against us for making such payment.
4. The liability of the Bank under this Guarantee shall not be affected by any change in the constitution of the Contractor or of the Bank.
5. This guarantee shall also be operable at our _____ branch at New Delhi, from whom, confirmation regarding the issue of this guarantee or extension/ renewal thereof shall be made available on demand. In the contingency of this guarantee being invoked and payment thereunder claimed, the said branch shall accept such invocation letter and make payment of amounts so demanded under the said invocation.
6. This bank guarantee shall be valid from
7. Notwithstanding anything contained herein:
 - (i) Our liability under this Bank Guarantee shall not exceed Rs. _____/-
 - (ii) The Bank Guarantee shall be valid up to.....
 - (iii) We are liable to pay the Guarantee amount or any part thereof under this Guarantee only and only if you serve upon us a written claim or demand on or before

Name:

Date:

Designation:

Employee Code Number:

Mobile Telephone

Number: Name of issuing bank branch _____

Address _____

Telephone number _____

E-mail: _____

Name of bank branch at _____

Address _____

Telephone number _____

E-mail: _____

Name of controlling bank branch _____

Address _____

Telephone number _____

E-mail: _____

=====END OF THE REPORT=====



Kolkata Port Trust

KOLKATA PORT TRUST

Supply, Installation, Commissioning, and Maintenance of RFID Systems at Kolkata Dock System, Kolkata Port Trust

Request for Proposal

Volume III: Draft contractual terms and Service Level Agreement

Document Reference No: **Plg/165/RFID/11667**

Date: 18th April 2017.

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

TABLE OF CONTENTS

1.	SCHEDULE I : CHANGE CONTROL SCHEDULE	60
2.	SCHEDULE II : EXIT MANAGEMENT SCHEDULE.....	63
3.	SCHEDULE III : AUDIT, ACCESS AND REPORTING SCHEDULE.....	70
4.	SCHEDULE IV : GOVERNANCE SCHEDULE	74
5.	SCHEDULE V : INVOICING AND SETTLEMENT SCHEDULE	78
6.	SCHEDULE VI : TERMS OF PAYMENT SCHEDULE.....	79
7.	SCHEDULE VII : CHANGE CONTROL NOTICE	80
8.	SCHEDULE VIII : SCOPE OF WORK	83
9.	SCHEDULE IX : SERVICE LEVELS	84

1. INTRODUCTION

1.1. ABOUT Kolkata Port Trust

Kolkata Dock System (KDS), Kolkata Port Trust (KoPT) – KDS, KoPT is a premier dock system of Kolkata Port in eastern India under the administrative control of the Ministry of Shipping, Government of India, commanding approx. 4576 acres of land and handling vessels and cargo to cater to the demand of a vast hinterland. KDS, KoPT primarily carries out vessel and cargo operation and handles around 15 million tonnes of cargo (which primarily includes container, break bulk cargo, etc.) and around 1450 vessels annually.

Under KDS, KoPT there are two impounded dock systems viz. Kidderpore Dock (KPD) and Netaji Subhash Dock (NSD) with 21 Multipurpose Berths, 5 Dedicated Berths for Containers, 1 Dedicated Berth at NSD for Liquid Bulk and 1 Passenger Terminal. In addition, there are 6 riverine Oil Jetties at Budge Budge. Cargo is also handled at various anchorages at deep-drafted locations viz. Sandheads, Sagar, Diamond Harbour, etc.

1.2. LIST OF DOCUMENTS COMPRISING THE RFP

The Request for Proposal or RFP (this document) for selection of Service Provider is segregated into the following three volumes:

Volume I: Scope of Services

Volume I of RFP intends to bring out all the details with respect to functional, non-functional, technical requirements, and implementation model along with details on scope of work required from the Service Provider that Board deems necessary to share with the potential bidders.

Volume II: Commercial and Bidding Terms

Volume II of the RFP details the General Terms & Conditions with respect to the bid process management including the evaluation criteria and bid submission forms to be adopted for the proposed project.

Volume III – Draft Master Services Agreement (MSA)

Volume III of the RFP details out the Draft Master Services Agreement for the proposed engagement and outlines the contractual, legal terms & conditions applicable for the proposed engagement.

This volume is the Volume III of the RFP.

2. SERVICE AGREEMENT

Following section outlines the key service level requirements for RFID Based Access Control System, which needs to be ensured by the Service Provider (SP) during the Operations and Maintenance period. These performance requirements shall be strictly imposed and a third party audit/certification agency may be deployed for certifying the performance of the SP against the target performance metrics as outlined in this volume of the RFP. Certification shall be done by a third party audit agency appointed as per RFP. The Service Level monitoring shall be performed/reviewed on a monthly basis. During the Contract period, it is envisaged that there could be changes to the Service Level, in terms of addition, alteration or deletion of certain parameters, based on mutual consent of both the Parties i.e. the Board and Service Provider.

2.1. SERVICE LEVEL OBJECTIVES

The following Service Level Objectives have been identified for governing the Service Level in RFID Based Port Access Control System (RFID PACS) Project.

- System should have all the required features to fulfil the project objectives
- System should always be available to the users
- System should be easy to use and
- System should be responsive enough for the user to work without time delays/ interruptions
- Users should always get the right kind of support as and when it is required to perform their work

2.2. SERVICE LEVEL DEFINITION AND MEASUREMENT

The definition and measurement of Service Level is provided in Schedule IX of the Agreement in this Volume of the RFP. The Service Level specifies the expected levels of service to be provided by the SP to the various stakeholders of the Project.

The following points clarify the manner in which the Service Level metrics operate:

- a. A set of parameters has been identified as key to ensuring the desired performance level of RFID Based Port Access Control System.

- b. The table lists out the performance level, method of measurement and how penalties shall be levied
- c. All payments to SP shall be after deduction of penalties as per the Service Level metrics.

2.3. RFID BASED PORT ACCESS CONTROL SYSTEM SERVICE LEVEL METRICS

The Service Level metrics that define the Service Levels, the method of measurement of each Service Level and the penalties for not meeting the Service Levels are specified in Schedule IX of the Agreement, in this Volume III of the RFP. The SP shall comply with the Service Levels specified in the said Schedule IX

2.4. SERVICE LEVEL MONITORING

The aforementioned Service Level parameters shall be measured on a daily/weekly/monthly/quarterly basis as per the individual Service Level parameter requirements, through appropriate Service Level Measurement tools to be designed by the SP for the purpose and audited by a third party for accuracy and reliability, if required by the Board. If the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of the board or an agency designated by him, then the board will have the right to take appropriate corrective actions including termination of the contract. It is to be noted that if the Penalty applicable in four consecutive months during the currency of the Contract exceeds 20% of the Equated Monthly Installment (EMI) in each Month; then the board shall have the right to terminate the Contract.

The Service Levels defined in Schedule IX of the Agreement, shall be reviewed on an annual basis by the Board after taking the advice of the SP and other agencies appointed by the Board. Changes in Service Level would be made by the Board after consultation with the SP.

3. DRAFT SERVICES AGREEMENT

Board intends to sign the Agreement with the successful bidder for Supply, Installation, Commissioning and Maintenance of RFID Based Access Control System and subsequent operation & maintenance of the RFID Based Access Control System.

Given below is a draft of the Agreement. Schedule IX of the Agreement provides a draft Service Level. The Board may propose changes required to this draft and shall be communicated to all the bidders before the bid closing date.

3.1. AGREEMENT

THIS AGREEMENT(hereinafter referred to as the “**Agreement**”, as defined hereinafter) is made on this ____ day of ____ 2017, by and between:

The Board of Trustees of the Port of Kolkata, a body corporate under Major Port Trust Act, 1963, having its office at _____ (hereinafter referred to as ‘**Board**’, which expression unless repugnant to the context or meaning thereof, shall mean and include its successors, administrators, assign) represented by its Board Of Trustee of Kolkata Port Trust, of the FIRST PART;

AND

____<name of the company>____, a company registered under the Indian Companies Act, 1956 having its registered office at ____<address>____ and place of business at ____<address>____(hereinafter referred to as “**Service Provider (SP)**”, which expression, unless repugnant to the context or meaning thereof, shall mean and include its successors or permitted assigns) represented through its ____<designation of authorized person>____, who is duly authorized by the SP to execute this Agreement, of the SECOND PART.

WHEREAS

- A. Board intends to enable and augment the RFID Based Access Control System Project involving supply, installation, commissioning and maintenance with the ultimate objective of creating a highly secured environment at the Port.
- B. Board carried out selection process for selecting a suitable Service Provider for implementing the Project, through the process of competitive bidding, pursuant to the “RFP” (as defined hereinafter);

- C. SP has been selected as the successful bidder to undertake the RFID Based Access Control System Project involving the development of the total RFID Based Access Control System solution and maintenance to achieve the defined objectives;
- D. Board intends to engage the SP to undertake and implement the RFID Based Access Control System Project on the terms and conditions set forth below.
- E. SP in pursuance of its proposal undertakes to implement the RFID Based Access Control System Project stated herein above.

NOW THEREFORE, IN VIEW OF THE MUTUAL PROMISES AND CONSIDERATION SET OUT HEREIN, IT IS HEREBY AGREED BETWEEN THE PARTIES:

Board and SP (Board and SP shall independently be called as “**Party**” and jointly as “**Parties**”) have agreed to enter into this Agreement to govern the manner in which the SP will design, develop, implement and manage the solution and deliver the services specified under this Agreement and in accordance with roles and responsibilities of AND, and its nominated agencies and the SP as set forth in this agreement.

1. ARTICLE 1 - DEFINITIONS AND INTERPRETATION

1.1 DEFINITIONS

a. In this Agreement, unless the context requires otherwise:

- i. **“Agreement”** means this agreement together with all the Schedules and the contents and specifications of all the volumes of the Request for Proposal (RFP) and in all the attached schedules and any addendums, corrigendum issued and shall include any modifications, alterations, additions or deletions thereto agreed between the Parties in writing after the date hereof in terms of this Agreement. In the event of a conflict between this Agreement and the Schedules, the terms of the Agreement shall prevail;
- ii. **“Applicable Laws”** includes all applicable statutes, enactments, acts of legislature or parliament laws, ordinances, rules, by-laws, regulations, notifications, guidelines, policies, directions, directives and orders of KoPT and any governmental authority, tribunal, board, court or other quasi-judicial authority;
- iii. **“Project”** means RFID Based Access Control System Project involving the Supply, Installation, Commissioning and Maintenance as per the terms and conditions laid in the RFP and provision of Board-related services in conformance to the Service Level;
- iv. **“Bespoke Software”** means the software designed, developed, tested and deployed by the SP for the purposes of rendering the Services to the users of the Project and includes the source code along with associated documentation, which is the work product of the development efforts involved in the Project and the improvements and enhancements effected during the term of the Project, but does not include the third party software products (except for the customization components on such products), proprietary software components and tools deployed by the SP, and which, i.e., the bespoke software, shall be solely owned by the Board;
- v. **“Confidential Information”** means all information including Project Data, Project Proprietary Information whether in written, oral, electronic or other format,

technical, financial and business affairs, customers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party in the course of or in connection with this Agreement (including without limitation such information received during negotiations, location visits and meetings in connection with this Agreement);

- vi. **“Control”** means possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of any entity, whether through the ownership of voting securities, by contract or otherwise;
- vii. **“Customization”** means the process of making Modifications, Enhancements, developing interfaces and making changes to any COTS software that may be used as part of the solution to meet the requirements of Board as specified in this Agreement;
- viii. **“Deliverables”** means the products, infrastructure and services agreed to be delivered by the SP in pursuance of the Agreement as elaborated in Volume I of the RFP in relation to the Implementation Phase and the Operations and Maintenance Phase and includes all documents related to the solution, user manual, technical manual, design, process and operating manuals, service mechanisms, policies and guidelines and source code and all its modifications;
- ix. **“Effective Date”** means the date on which the Agreement is executed by both the Parties.
- x. **“Implementation Phase”** means the period between the Effective Date and the Go-Live Date;
- xi. **“O&M Service Level”** means the service and other performance criteria which will apply to the Services during the Operation and Maintenance Phase as set out in Schedule IX;
- xii. **“Operation and Maintenance Phase”** means the period commencing from the Go-Live Date till the expiry of the Term or early termination of this Agreement;

- xiii. **“Intellectual Property Rights”** means and includes all rights in the Bespoke Software, its improvements, upgradations enhancements, modified versions that may be made from time to time, database generated, compilations made, source code and object code of the Bespoke Software, the said rights including designs, copyrights, trademarks, patents, trade secrets, moral and other rights therein;
- xiv. **“Material Breach”** means breach that has an effect on (a) the ability of SP to perform/discharge any of its duties/obligations under and in accordance with the provisions of the Agreement; and/or (b) the legal validity, binding nature or enforceability of the Agreement;
- xv. **“Performance Bank Guarantee”** shall mean the guarantee provided by a Nationalized Bank to Board on behalf of the SP for the amount specified in Volume II of the RFP;
- xvi. **“Project Data”** means all proprietary data of the PROJECT generated out of Project operations and transactions, documents and related information including but not restricted to user data which the SP obtains, possesses or processes in the context of providing the Services to the users pursuant to this Agreement and the Service Level;
- xvii. **“Project Location”** shall include all such Board sites that will require setup of RFID Based Access Control System solution.
- xviii. **Project Implementation”** means Project Implementation as per procedure prescribed in Volume I of the RFP;
- xix. **“Go-Live”** means the date on which the proposed RFID Based Access Control System is completely operational as per the functional, technical and operational requirements specified in the Volume I of the RFP and all the acceptance tests & certifications as defined in the Volume I of the RFP are successfully concluded to the satisfaction of Board.
- xx. **“Proposal”** shall mean proposal no. [●] dated[●] submitted by the SP for undertaking to implement the Project;

- xxi. **"Proprietary Information"** means processes, methodologies and technical and business information, including drawings, designs, formulae, flow charts, data and computer programs already owned by, or granted by third parties to a Party hereto prior to its being made available under this Agreement;
- xxii. **"RFP" or "Request for Proposal"** means the documents containing the Technical, Functional, Commercial and Legal Specifications for the implementation of the Project, issued in 3 volumes (referred to as Volume I, Volume II, Volume III and Annexures) and includes the clarifications, explanations and amendments issued by Board from time to time.
- xxiii. **"Replacement SP"** means any third party that the Board may appoint to replace the SP upon expiry of the Term or otherwise termination of this Agreement to undertake the Services or part thereof;
- xxiv. **"Service Level"** means the level of service and other performance criteria which will apply to the Services as set out in the Service Level, in Schedule IX;
- xxv. **"Services"** means the services delivered to the users of Project, as defined in the Volume I of the RFP, using the tangible and intangible assets created, procured, installed, managed and operated by the SP including the tools of information and communications technology and includes but is not limited to the list of services specified in Article 2.1 herein;
- xxvi. **"End Users"** means the users who use the software and services;
- xxvii. **"Schedules"** shall mean schedules attached to this Agreement;
- xxviii. **"Third Party Systems"** means Systems (or any part thereof) in which the Intellectual Property Rights are owned by a third party and to which SP has been granted a license to use and which are used in the provision of Services;
- xxix. **"Working Day"** means any day on which any of the Board unit will be functioning, including gazetted Holidays, restricted holidays or other holidays, Saturdays and Sundays

1.2 INTERPRETATIONS

- a. References to any statute or statutory provision include a reference to that statute or statutory provision as from time to time amended, extended, re-enacted or consolidated and to all statutory instruments made pursuant to it.
- b. Words denoting the singular shall include the plural and vice versa and words denoting natural persons shall include firms and corporations and vice versa. A word denoting a gender includes all genders.
- c. Unless otherwise expressly stated, the words "herein", "hereof", "hereunder" and similar words refer to this Agreement as a whole and not to any particular Article, Schedule. The term Articles, refers to Articles of this Agreement. The words "include" and "including" shall not be construed as terms of limitation. The words "day" and "month" mean "calendar day" and "calendar month" unless otherwise stated. Where, because of a difference in time zone, the calendar day or calendar month in one Country differs from another Country, then the calendar day or calendar month shall be deemed to be the calendar day or calendar month applicable to India. The words "writing" and "written" mean "in documented form", whether electronic or hard copy, unless otherwise stated. Any reference to attorneys' fees shall include reasonable fees of the professional assistants of such attorneys.
- d. The headings and use of bold type in this Agreement are for convenience only and shall not affect the interpretation of any provision of this Agreement.
- e. References to Clauses, Sub-Clauses, Paragraphs, Article, Schedules and Annexures are to clauses, sub-clauses, paragraphs, article, schedules and annexures to this Agreement.
- f. References to a 'company' shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established.
- g. References to a 'person': person shall be construed to include any individual, partnerships, firms, companies, corporations, joint ventures, trusts, associations, organizations, executors, administrators, successors, agents, substitutes and any permitted assignees or other entities (whether or not

having a separate legal entity). A reference to a group of persons is a reference to all of them collectively, to any two or more of them collectively and to each of them individually.

- h. Any reference to a 'day' (including within the phrase 'business day') shall mean a period of 24 hours running from midnight to midnight.
- i. References to a 'business day' shall be construed as a reference to a day (other than a Sunday) on which Board Office in Kolkata are generally open for business;
- j. References to times are to Indian Standard Time;
- k. A reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time;
- l. Any reference at any time to any Agreement, deed, instrument, license or document of any description shall be construed as reference to that Agreement, deed, instrument, license or other document as amended, varied, supplemented, modified or novated at the time of such reference;
- m. Any contract, consent, approval, authorization, notice, communication, Information or report required under or pursuant to this Agreement from or by any Party and/or any other authority shall be valid and effectual only if it is in writing under the hands of duly authorized representative of such Party or authority, as the case may be, in this behalf and not otherwise;
- n. Unless otherwise stated, any reference to any period commencing "from" a specified day or date and "till" or "until" a specified day or date shall include either such days or dates;
- o. A reference to knowledge of a person includes Information that a reasonable person in the circumstances of that person would have known by reasonable inquiry;

In interpreting this Agreement no rule of construction applies to the disadvantage of a party because that party or its legal advisor was responsible for the preparation of this Agreement.

1.3 STRUCTURE

- a. This Agreement shall operate as a legally binding services agreement specifying the master terms which apply to the Parties under this Agreement and to the provision of the Services by the SP to the End Users of the Project under the duly executed Service Level.
- b. In respect of any future Service Levels entered into between the Parties, each of the Parties shall observe and perform the obligations set out herein.
- c. In the event of a change of Control of the SP during the currency of this Agreement. SP shall promptly notify Board of the same and in the event that the net worth of the surviving entity is less than that of SP prior to the change of Control, Board may within 30 days of his/ her becoming aware of the change in Control, require a replacement of existing Performance Bank Guarantee furnished by the SP from a guarantor acceptable to the Board (which shall not be SP or any of its associated entities). If such a guarantee cannot be obtained within 30 days of the Board becoming aware of the change in Control, he/ she may exercise its right to terminate the Service Level within a further 30 days by written notice, to become effective when specified in such notice. Pursuant to termination, the consequences of termination as set out in Article 5.2 hereinafter will become effective. The internal reorganization of the SP shall not be deemed an event of a change of Control for purposes of this Article unless the surviving entity is of less net worth than the predecessor entity.
- d. The Project engagement which includes Project Implementation will be governed by the acceptance and testing criteria which will have the Board and/or a technically competent agency or agencies for conducting the acceptance and testing certifications in the manner herein below:
 - i. Board may nominate a technically competent agency/person for conducting acceptance testing and certification.
 - ii. The agency/person may lay down a set of guidelines following internationally accepted norms and standards for testing and certification

in all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and subsystems, coding, testing, business process description, documentation, version control, change control, security, service oriented architecture, performance in relation to compliance with Service Level, metrics, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and this Agreement.

- iii. The agency/person will be involved with Project early in the development stage to ensure that the guidelines are being followed and to avoid large scale modifications pursuant to testing done after the application is fully developed.
- iv. The agency/person nominated by Board can engage professional organizations for conducting specific tests on the software, hardware, networking, security and all other aspects.
- v. The agency/person will establish appropriate processes for notifying the SP of any deviations from the norms, standards or guidelines at the earliest instance after taking cognizance of the same to enable the SP to take corrective action.
- vi. Such an involvement of and guidance by the agency/person will not, however absolve the SP of the fundamental responsibility of designing, developing, installing, testing and commissioning the various components of the Project to deliver the services in perfect conformity with the Service Level.

1.4 CONDITIONS PRECEDENT

Subject to express terms to the contrary, the rights and obligations of the Parties in respect of this Agreement shall be effective only upon fulfillment of all the conditions precedent set out in this Article (“**Conditions Precedent**”). However, the Board, may at any time at its sole discretion waive fully or partially any of the

aforesaid conditions precedent for the SP. The following conditions precedent needs to be fulfilled by the SP within 15 days from the Effective Date (**“Conditions Precedent Fulfillment Date”**):

- a. SP shall have been given a work order for provision of the Services under the Agreement;
- b. SP shall have provided the Performance Bank Guarantee and other guarantees/ payments to Board as specified in RFP;
- c. SP shall have provided the Board certified true copies of its constitutional documents and board resolutions authorizing the execution, delivery and performance of this Agreement with Board.

1.4.1 NON-FULFILLMENT OF CONDITIONS PRECEDENT

- a. In the event that any of the Conditions Precedent has not been fulfilled within Conditions Precedent Fulfillment Date, and the same has not been waived by the Board fully or partially, this Agreement shall stand terminated as of that date, at the sole option of the Board.
- b. Notwithstanding anything contained to the contrary, in the event of termination of this Agreement, on account of non-fulfillment of any of the Conditions Precedent to be fulfilled by the SP, the Board shall not be liable in any manner whatsoever to the SP and the Board shall forthwith invoke the Performance Bank Guarantee and forfeit the guaranteed amount. Such termination and invocation shall be without prejudice or other rights of the Board under law.
- c. In the event that vacant possession of any of the facilities or any Project Data has been delivered to the SP prior to the fulfillment of all of the Conditions Precedent for the Implementation, upon the termination of this Agreement such possession shall immediately revert to the Board, free and clear from any encumbrances or claims.
- d. Instead of terminating this Agreement as provided in Article 1.4.1 (a) above, the Board may, at its sole discretion, extend the time for fulfilling the Conditions Precedent and the RFID Based Access Control System Project Implementation milestones set out in the RFP document on such terms and conditions as it may deem fit. It is clarified that any extension of time shall be subject to imposition of

agreed liquidated damages on the SP in accordance with Article 4.4 linked to the delay in achieving the Implementation Service Levels.

2. ARTICLE 2 – SCOPE OF RFID BASED ACCESS CONTROL SYSTEM PROJECT

2.1. SCOPE OF AGREEMENT

This Agreement shall govern the provision of the contractual professional services, listed hereunder and more fully described in the RFP, in conformance with the Service Level, to all the End users of the RFID Based Port Access Control System Project.

Services to be provided by the SP under the Agreement:

The RFID Based Port Access Control System project broadly covers the following activities:

- Supply, installation, commissioning of hardware (Boom Barrier, Flap Barriers, Photo capturing web/digital cameras, computers and servers, digital label printers, RFID cards, LPRs, Readers, Long Range RFID Readers, 32" LED screens, Application for tracking GPS enabled device/ modems for tracking vehicles, SMS Gateway, CISF cabins and other accessories as per BOQ as provided in Annexure V) and System software (Operating system, Database) and Application Software (Personalization Software, with features like Time and Attendance management, Data logs, Enrolments & renewal software with built-in Visitor Management System for issue of port entry permits, vehicle passes, tracking the IN/Out movement of Visitors and Vehicles, GIS & GPS based vehicle tracking software etc.) Software should have the facility to be customized to meet the specific requirements & reporting system of Port.
- Setup, Operate and manage enrolment counters with adequate number of photo capturing web/digital cameras, computers and servers, Digital printers, RFID reading and/ or writing devices 32" LED screens and other accessories, and software (operating system and applications) for issue of dock entry permits to visitors and vehicle so that the complete infrastructure is in sound and good working conditions.
- Supply and Issue of Contactless Mifare cards as per requirement. The cards supplied shall be with the holder and lanyard.

- Supply of consumables like Print Heads , cartridges , cleaning cartridges, and other consumables required for printing on RFID cards
- Maintaining the RFID Access control System and complete solution throughout the year on a round the clock basis (365 x 24 x 7) during the currency of contract.
- Personal Computers shall be provided at different locations for operation of Access Control System for various verification and online approval.
- The Port Access Control System and solution should be maintained in such a way that there is minimal downtime and minimal breach of SLAs
- The works mentioned are illustrative and not exhaustive and bidder may have to carry out any other works related to access control system, issue of permits, vehicle tracking system and other components which are not explicitly included above but are implied by nature. The entire system shall be operated round the clock.
- Technical manpower resources including IT support executive, repair technicians, etc. shall be provided by the Service Provider.
- The complete permit issuance process should be online. The details shall be updated to the central server through the network connectivity provided by the Port.
- The service provider shall supply, install and commission the entire infrastructure required at Data Centre, which is planned to be set up at Subhash Bhavan and Disaster Recovery Centre which is planned to be set up at HQ.
- Even though Port provides the network, the vendor should consider network failures and design the system in such a way to have minimum or no downtime. Failure of network should not be claimed as reason for breach of SLA.
- Service Provider will be responsible for insurance of all the deployed manpower for risk coverage (accidental hazards, death and disability of person, other hazards which may occur due to trespassing vehicles and/or natural adverse climatic calamities-War, Fire, Cyclone, Salinity problems at shore).
- Necessary interfacing with Port LAN/WAN. It shall be the responsibility of the service provider to arrange for equipment that would be necessary for interconnectivity/cabling between the switches at the gate end , Flap Barrier, Boom Barrier, etc. and server.

- Installation of Access Control Server at a central location and connection of all access control equipment with central server.
- The Access Control System Solution should be an integrated solution with the entire data including the photographs, biometrics, and data logging to be stored on central server.
- It will be responsibility of the vendor to provide and fix the shelters for Card Readers, Flap Barriers exposed to open weather and Cabins for setting up of system at gates. All associated civil works for fixing and installation of flap barriers/tripod and boom barrier has to be carried out by the successful vendor.
- All system components should be certified by UL or any other reputed Indian / foreign certifying agency to ensure product reliability and product quality. Any operating system software or application software, which will be part of the system, shall come with proper and legal licenses. Such licenses shall be procured in the name of Kolkata Port Trust, or as informed by KoPT, from day one.
- Final testing and commissioning of complete system including training, submission of reports, drawings, login & passwords and database design etc.
- Post implementation on-site support and maintenance.
- All other items in the scope of system implementation as mentioned in section 2 of RFP volume I.

2.2. Interpretation of the Scope of Work

- (i) The Board retains the right of the final say in the interpretation of the scope of the Project. The possible variations to the processes from the way they are specified in the scope of work should not be considered as deviations or extensions to the original process specifications.
- (ii) Sign-off on the Deliverables by Board does not necessarily indicate the complete approval of the Deliverables. All the responsibilities with respect to operations and maintenance of the existing applications, infrastructure or requirements in the RFP or Board processes will be the responsibility of the SP. Any gap that is

found in a deliverable with respect to the above, even after the sign-off, will have to be addressed by the SP without any additional cost to Board.

- (iii) The performance of the ultimate system can be achieved by different combinations of the equipment and network components. The final acceptance of the integrated solution and infrastructure components should be as per the performance requirements and will be the determining factor but not the specifications of the infrastructure alone.

2.3. COMMENCEMENT AND DURATION OF THIS AGREEMENT

Subject to Clause 1.4 (Conditions Precedence), this Agreement shall come into effect on the Effective Date and shall continue till the completion of 07 years from the date of Go-Live, unless terminated earlier in accordance with the terms of this Agreement (**"Term"**).

2.4. SCOPE AND PROVISION OF THE SERVICES

- a. The provision of Services to the End user with certainty and speed is the essence of the Agreement between the Parties.
- b. The SP represents that it is a competent and efficient provider of a variety of information technology and Geospatial services. SP will keep abreast of the relevant technical, managerial and operational requirements applicable to the provision of the services and best practices in this area and will share their knowledge with the Board, regarding matters which would assist the Board, in its use of the Services, provided that SP shall not be obligated to share other client information or Confidential Information of SP not relevant to this Agreement.
- c. The Services shall be performed by the SP pursuant to terms under the Service Level.
- d. The SP shall perform the Services (a) in a good professional manner commensurate with professional industry and technical standards which are generally in effect for international projects and innovations pursuant thereon similar to those contemplated by this Agreement, (b) so as to comply with the applicable Service Levels and (c) in accordance with the terms set out in this Agreement

- e. The Parties shall ensure that the range of the Services under the Service Level shall not be varied, reduced or increased except by the prior written agreement of Board in accordance with the Change Control Schedule. Save, for the express terms of the Terms of Payment Schedule, Board and its users shall be obliged to purchase any particular category of Services that may become necessary as per the Change Control Schedule from the SP, without the need to go for a separate procurement process.
- f. In providing the Services, SP shall ensure not to cause any unnecessary disruption to the Board's normal business operations.
- g. No Party to this Agreement will at any time perform, or omit to perform, any act which they are aware, at the time of performance, will place the other Party in default under any insurance policy, mortgage or lease, governing activities at any location provided by the Board.

2.5. APPROVALS AND REQUIRED CONSENTS

- a. The Parties will cooperate reasonably to obtain, maintain and observe all relevant and customary regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "**Approvals**") necessary for the SP to provide the Services. The costs of such Approvals shall be borne by the SP.
- b. Both parties will give each other all co-operation and information reasonably required to meet their respective obligations under this Agreement.
- c. Board shall use reasonable endeavors to assist SP obtain the Approvals. In the event that any Approval is not obtained, the SP and the Board will co-operate with each other in achieving a reasonable alternative arrangement as soon as reasonably practicable for the Board, to continue to process its work with as minimal interruption to its business operations as is commercially reasonable until such Approval is obtained, provided that the SP shall not be relieved of its obligations to provide the Services and to achieve the Service Levels until the Approvals are obtained if and to the extent that the SP's obligations are dependent upon such Approvals.

2.6. USE AND ACQUISITION OF ASSETS

During the Term of the Agreement, the SP shall:

- a. take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components used for the Project and other facilities leased / owned by the KoPT exclusively in terms of the delivery of the Services as per this Agreement (hereinafter the **“Assets”**) in proportion to their use and control of such Assets which will include all upgrades/ enhancements and improvements to meet the current needs of the Project; and
- b. Keep all the tangible Assets in as good and serviceable condition and/or the intangible Assets suitably upgraded subject to the relevant standards as stated in the RFP as at the date the SP uses the Assets and during the entire Term of the Agreement; and
- c. Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of the Assets and provided to the SP will be followed by the SP and any person who will be responsible for the use of the Assets; and
- d. Take such steps as may be properly recommended by the manufacturer of the Assets and notified to the SP or as may, in the reasonable opinion of the SP, be necessary to use the Assets in a safe manner; and
- e. To the extent that the Assets are used by the SP, keep the Assets suitably housed and in conformity with any statutory requirements from time to time applicable to them; and
- f. Procure permission from the Board and any persons duly authorized by him/ her to enter any land or premises on which the Assets are for the time being sited so as to inspect the same, subject to any reasonable third party requirements; and
- g. Not knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or contrary to law; and
- h. Use the Assets exclusively for the purpose of providing the Services as appropriate; and

- i. Not sell, offer for sale, assign, mortgage, pledge, sub-let or lend out any of the Assets; and
- j. Use the Assets only in accordance with the terms hereof and those contained in the Service Level; and
- k. Obtain and/ or maintain standard forms of comprehensive insurance policy and any other insurance for the personnel; and
- l. Transfer the ownership of all the Assets (not already with the Board, including but not limited to the project documentation which is the work product of the development efforts involved in the Project) to KoPT from day one and subject to the acceptance of the same by Board upon testing and/ or audit , to the Board in accordance with the terms of this Agreement; and
- m. To ensure the integration of the software with hardware to be installed and the current Assets in order to ensure the smooth operations of the entire solution architecture to provide efficient services to all the users of Project in an efficient and speedy manner; and
- n. To provide a well-prepared documentation for user manual, a clear plan for training, educating and hand holding the users and shall form part of handholding phase until bringing up to speed; and
- o. Train the team identified by Board in accordance with the terms of RFP; and
- p. An approval (i.e. sign off) from Board at each stage is essential to close each of the above considerations.
- q. If Board needs to be shifted to a different location within the same city or an adjacent city, the SP shall be responsible for all the re-installation, configuration and setting up of the servers and all other software, network and hardware equipment at no extra cost to the Board. The cost of transportation for relocation shall be borne by Board.

2.7. ACCESS TO SP OR ITS NOMINATED AGENCIES TO Board LOCATION

- a. For so long as the SP provides Services from any Project location on a non-permanent basis and to the extent necessary for the SP to provide the Services and at no cost to the SP, Board, shall, subject to compliance by the SP with any safety and security guidelines which may be notified by the Board to the SP in writing, provide the SP with:
- (i) reasonable access, in the same manner granted to Board employees, to Board locations during the working hours of Board; and
 - (ii) Access to office equipment as mutually agreed and other related support services in project location and at other Board locations, if any, as may be reasonably necessary for the SP to perform its obligations hereunder and under the Service Level.
- b. Locations and items shall be made available to the SP on an "as is, where is" basis by the Board as per the time schedule agreed upon between the parties. The SP agrees to ensure that its employees, agents and contractors use these locations solely for performing the bona fide Project activities and do not use the location, services and items :
- (i) for the transmission of any material which is defamatory, offensive or abusive or of an obscene or menacing character; or
- In a manner which constitutes a violation or infringement of the rights of any person, firm or company (including but not limited to rights of copyright or confidentiality).

3. ARTICLE 3 - MANAGEMENT PHASE

3.1. GOVERNANCE

The review and management process of this Agreement shall be carried out in accordance with the Governance Schedule (Schedule IV of this Agreement) and shall cover all the management aspects as set out in the RFP.

3.2. USE OF SERVICES

- a. Board, or its nominated agencies will undertake and use the Services in accordance with the terms of this Agreement for such usage and mutually agreed by the Parties from time to time.
- b. Board, or its nominated agencies will use the Deliverables resulting from the Services provided by or on behalf of the SP.

3.3. CHANGES

Unless expressly dealt with elsewhere in this Agreement, any changes under or to this Agreement or under shall be dealt with in accordance with the Change Control Schedule (Schedule I of this Agreement).

3.4. SECURITY AND SAFETY

- a. The SP will comply with the directions issued from time to time by the Board and the standards related to the security and safety as stated in RFP Volume I, insofar as it applies to the provision of the Services. Notwithstanding anything contained herein, the obligation of the SP to adhere to standards related to security and safety as have been agreed, shall be absolute.
- b. Each Party to the Agreement shall also comply with RFID Based Security Project's information technology security and standards policies in force from time to time at each location.
- c. The SP shall report forthwith in writing to the Board all identified attempts (whether successful or not) by unauthorized persons (including unauthorized persons who are employees of the SP) either to gain access to or interfere with the RFID Based Access

Control System Project's data, facilities or Confidential Information in addition to taking necessary steps to preventing or minimizing any material loss or damage.

- d. The SP shall upon reasonable request by the Board or its nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.
- e. The Parties shall promptly report in writing to each other any act or omission which they are aware, could have an adverse effect on the proper conduct of safety and information technology security at the Board.
- f. Any private, proprietary or classified information of the disclosing Party which has to be made available by the receiving Party to a third party , shall be submitted to such a third party subject to terms of the Agreement and with such restrictions that are superior if not similar to those set out in this Agreement.

3.1 CO-OPERATION

- a. Except as otherwise provided elsewhere in this Agreement, each Party ("Providing Party") to this Agreement undertakes promptly to provide the other Party ("Receiving Party") with all such information and co-operation which the Receiving Party reasonably requests, provided that such information and co-operation:
 - (i) is reasonably required by the Receiving Party in order for it to comply with its obligations under this Agreement; and
 - (ii) is not Confidential Information; and
 - (iii) is capable of being provided by the Providing Party.

4. ARTICLE 4 - FINANCIAL ISSUES

4.1. TERMS OF PAYMENT

- a. In consideration of the Services and subject to the provisions of this Agreement, the Board shall pay the SP for the Services rendered in pursuance of this Agreement, in accordance with the Terms of Payment Schedule (Schedule VI of this Agreement).
- b. All payments are subject to set-offs on account of liquidated damages payable by the SP pursuant to Article 4.4. .
- c. Except as otherwise provided for herein or as agreed between the Parties in writing, the Board shall not be required to make any payments in respect of the Services other than those covered by the terms of payment as stated in the Terms of Payment Schedule (Schedule VI of this Agreement) .

4.2. INVOICING AND SETTLEMENT

The provisions of the Invoicing & Settlement Schedule (Schedule V of this Agreement) shall apply.

4.3. TAX

- a. The Board shall be entitled to deduct taxes from the amounts due and payable to the SP as per the Applicable Laws. The SP shall pay for all other taxes in connection with the Agreement including, but not limited to property, sales, use, excise duty, value-added, goods, consumption and other similar taxes or duties. Any service tax paid by SP under Agreement shall be reimbursed by Board only if such service tax is stated separately in the invoice and actually paid by SP to the Government Department by submitting documentary evidence to Board as a proof of Service Tax payment. The Board shall provide SP with the original/ copy of tax receipt of any withholding taxes paid for RFID Based Access Control System Project payments under the Agreement. The SP agrees to reimburse and hold the Board harmless from any deficiency (including penalties and interest) relating to taxes that are its responsibility under this Article. For purposes of this Agreement, taxes shall include taxes incurred on transactions between and among the Board, SP and third party subcontractors.

- b. The Parties shall cooperate to enable each other to accurately determine their tax liability and to minimize such liability to the extent legally permissible. In connection therewith, the Parties shall provide each other with (i) any resale certificates, (ii) any relevant information regarding use of out-of-state materials, equipment or services and (iii) any exemption certificates or information reasonably requested by the other Party.

4.4. LIQUIDATED DAMAGES:

In the event of the Bidder's failure to submit the Bond, Guarantees and Documents and supply the solution / equipment as per schedule specified in this RFP, Board may at its discretion withhold any payment until the completion of the contract. The Board may also deduct from the payment due to the Bidder as agreed, liquidated damages to the sum of 0.5% of the contract price of the corresponding milestone payment of the delayed / undelivered services for every week of delay or part of a week, subject to the maximum value of the Liquidated Damages being not more than 10% of the value of corresponding milestone payment of the delayed / undelivered services. This right to claim any liquidated damages shall be without prejudice to other rights and remedies available to Board under the contract and law.

5. ARTICLE 5 - BREACH, RECTIFICATION& TERMINATION

5.1. In the event that the SP is in Material Breach of its obligations under this Agreement, Board may terminate this Agreement upon notice to the other Party. It is clarified that the right to terminate this Agreement shall be without prejudice to other rights and remedies available to the non-defaulting Party in law and/or under contracts, including the right to invoke the Performance Bank Guarantee. Any notice served pursuant to this Article shall give reasonable details of the Material Breach, which could include the following events and the termination will become effective:

- (i) If there is Breach which translates into default in providing Services by the SP as per this Agreement, continuously for more than one week, then the Board, will serve a seven days' notice for curing such Material Breach. In case the Material Breach continues after the notice period, the Board will have the option to terminate the Agreement.
- (ii) in case, for reasons prima facie attributable to the SP, there is a delay of more than 2 months in the RFID Based Access Control System Project Implementation by the SP, the Board may terminate this Agreement after affording an opportunity to the SP to explain the circumstances leading to such a delay. Further, the Board may also invoke the Performance Bank Guarantee of the SP.

5.2. Where a change of control of the SP has occurred whereby the SP-company has merged, amalgamated or been taken over, due to which the majority shareholding of the SP has been transferred to another entity, the Board can by a 60 days written notice, terminate this Agreement and such notice shall become effective at the end of the notice period.

5.3. TERMINATION ON OTHER GROUNDS

Without prejudice to any other rights and remedies available to the Board, the Board may serve written notice to the SP at any time to terminate this Agreement with immediate effect in the following events:

- a. In the event of change of Control of the SP;

- b. In the event SP has merged, amalgamated such that the net worth of the surviving entity is less than that of the SP prior to such merger or amalgamation.
- c. In the event of a reasonable apprehension of bankruptcy, the SP shall inform the Board of any such development, whereupon the Board may, at its sole discretion, terminate the Agreement. Notwithstanding anything mentioned above, if the Board reasonably apprehends the bankruptcy of the SP, the Board may, at its sole discretion, terminate the Agreement immediately.
- d. In the event any member of senior management or any personnel of the SP working in the RFID Based Access Control System Project is involved in any commission of offence involving criminal conspiracy or moral turpitude with punishment for more than 6 months, the Board shall have the right to terminate the Agreement forthwith.
- e. If it is brought to the notice of Board that the SP is indulging in any kind of malpractice or indulging in activities that compromises the ISPS Access Control Code or causing or likely to cause any damage to the Board by using the Agreement, the Board shall have the right to terminate the Agreement forthwith .
- f. If the performance of the system/services is degraded significantly at any given point in time during the Agreement and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of Board or an agency designated by them, then Board will have the right to take appropriate corrective actions including termination of the Agreement. It is to be noted that if the Penalty applicable in four consecutive months during the currency of the Agreement exceeds 20% in each month; then Board shall have the right to terminate the Agreement.
- g. Fraud by the SP - Board reserves its right to initiate criminal action against the SP for fraud or misappropriation, under the applicable laws besides stringent penalties and Board shall have the right to initiate action for termination of Agreement if Board finds it necessary to do so.

5.4. EFFECTS OF TERMINATION

- a. In the event that the Board, , terminates this Agreement pursuant to Article 5.1 and depending on the event of default, compensation will be decided in accordance with the terms of Payment Schedule (Schedule VI of this Agreement).
- b. Upon termination of this Agreement, the Parties will comply with the Exit Management Schedule (Schedule II of this Agreement).

5.5. PERFORMANCE BANK GUARANTEE

- a. Without prejudice to the powers of Board to terminate the Agreement as mentioned in Articles 5.1 and 5.2, the Board shall have the power to invoke the Performance Bank Guarantee, either in full or in part, in case of occurrence of any of the events specified above.
- b. In the event any portion of the Performance Bank Guarantee is en-cashed pursuant hereto, then immediately following such encashment, the SP shall cause the relevant bank to replenish the Performance Bank Guarantee to its full amount. In the event the Performance Bank Guarantee is not replenished to its full amount within one (1) month of its encashment, Board shall have the right to en-cash the entire Performance Bank Guarantee and terminate the Agreement.

5.6. FRAUD BY SP'S PERSONNEL

Board reserves its right to initiate civil as well as criminal action against the agents/ employees of the SP for fraud or misappropriation, besides claiming damages and indemnification. The management of the SP would also be made liable for action in case of fraud, under the Applicable Laws and without prejudice to other rights and obligations available to the Board, it may terminate the Agreement, if it deems fit in its sole discretion.

6. ARTICLE 6 - PROTECTION AND LIMITATIONS

6.1. WARRANTIES

- a. The SP warrants and represents to the Board that:
 - (i) it has full capacity and authority and all necessary approvals to enter into and to perform its obligations under this Agreement;
 - (ii) this Agreement is executed by a duly authorized representative of SP;
 - (iii) it shall discharge its obligations under this Agreement under Article II with due skill, care and diligence and meet the Service Levels;
 - (iv) there are no actions, suits or proceedings pending or to its best knowledge, threatened against or affecting it before any court, administrative body or arbitral tribunal which might materially and adversely affect its ability to meet or perform any of its obligations under this Agreement;
 - (v) it has the financial standing and capacity to undertake the RFID Based Access Control System Project in accordance with the terms of this Agreement;
 - (vi) the execution, delivery and performance of this Agreement will not conflict with, result in the breach of, constitute a default under, or accelerate performance required by any of the terms of its memorandum of association and articles of association or any Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;
 - (vii) it has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any government authority which may result in any Material Adverse Effect on its ability to perform its obligations under this Agreement no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;
 - (viii) it has complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal

liabilities which in the aggregate have or may have a Material Adverse Effect on its ability to perform its obligations under this Agreement;

- (ix) no representation or warranty by it contained herein or in any other document furnished by it to the Board or its nominee including the Proposal or to any Government Authority contains or will contain any untrue or misleading statement of material fact or omits or will omit to state a material fact necessary to make such representation or warranty not misleading;
- (x) no sums, in cash or kind, have been paid or will be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for securing the Agreement or entering into this Agreement or for influencing or attempting to influence any officer or employee of the Board in connection therewith;
- (xi) the SP is experienced in managing and providing works similar to the Services;
- (xii) the Services will be provided and rendered by appropriately qualified, trained and experienced personnel;
- (xiii) the SP has and will have all necessary licenses, approvals, consents of third parties and all necessary technology, hardware and software to enable it to provide the Services;
- (xiv) the Services will be supplied in conformity with all Applicable Laws, enactments, orders and regulations;
- (xv) the SP will use its reasonable endeavors to ensure that the equipment, software and hardware supplied and/or used in the course of the provision of the Services, are updated, new, operational and functional; and
- (xvi) if SP uses in course of provision of the Services, components, equipment, software and hardware manufactured by any third party which are embedded in the Deliverables or are essential for the successful use of the Deliverables, it will pass through third party manufacturer's warranties relating to those components, equipment, software and hardware to the extent possible. In the event that such warranties cannot be enforced by the Board, the SP will

enforce such warranties on behalf of the Board and pass on to the Board, the benefit of any other remedy received in relation to such warranties.

- b. Warranties regarding RFID Based Access Control System:- Without limiting the warranty obligations set out in the RFP, the SP warrants that:
- i. RFID Based Access Control System shall conform to technical specifications prescribed in RFP and this Agreement and shall perform according to the said technical specifications. The SP further warrants that the RFID Based Access Control System shall be of the latest version, non-refurbished, unused and recently manufactured. It shall not be nearing end of sale/ end of support.
 - ii. RFID Based Access Control System shall be free from all encumbrances and defects / faults arising from design, material, manufacture or workmanship or from any act or omission of the SP that may present a snag/fault, under normal use of the same.
- c. Representations and warranties of the Board: The Board represents and warrants to the SP that:
- i. It has full power and authority to execute, deliver and perform its obligations pursuant to the Agreement.
 - ii. It has taken all necessary action to authorize the execution, delivery and performance of the Agreement.
- d. In the event that any occurrence or circumstance comes to the attention of either Party that renders any of its aforesaid representations or warranties untrue or incorrect, such Party shall immediately notify the other Party of the same. Such notification shall not have the effect of remedying any breach of the representation or warranty that has been found to be untrue or incorrect nor shall it adversely affect or waive any right or obligation of either Party under the Agreement.
- e. Notwithstanding what has been stated elsewhere in this Agreement and the Schedules attached herein, in the event the SP is unable to meet the obligations of implementation of the RFID Based Security Project and/or provide the Services and any related scope of work as stated in this Agreement, the Board will, *inter-alia*,

have the option to invoke the Performance Bank Guarantee after serving a written notice of fifteen days on the SP. Such right of the Board shall be without prejudice to any other rights or remedies available under law or contract.

6.2. INDEMNITY

- a. Subject to Article 6.2(b) below, SP (the "Indemnifying Party") undertakes to indemnify the Board (the "Indemnified Party") from and against all losses, claims or damages including but not limited to those caused on account of bodily injury, death or damage to tangible personal property and otherwise caused by its negligence/ fraud/willful misconduct, arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's performance or non-performance under this Agreement or the Service Level.
- b. The indemnities set out in Articles 6.2 shall be subject to the following conditions:
 - (i) the Indemnified Party, as promptly as practicable, informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;
 - (ii) the Indemnified Party may at its option (but shall not be obliged to) at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the defense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such defense;
 - (iii) if the Indemnifying Party does not assume full control over the defense of a claim as provided in this Article, the Indemnified Party may at its option participate in such defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of such defense will be included in the indemnity claim against the Indemnifying Party;

- (iv) the Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;
- (v) all settlements of claims subject to indemnification under this Article will: (a) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant for all liability in respect of such claim; and (b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;
- (vi) the Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favor of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings.

6.3. LIMITATION OF LIABILITY

- a. SP's aggregate liability for damages shall be capped at 100% of the value of the Agreement.
- b. There shall be no limitation of liability in case of (i) any damages for bodily injury (including death) and damage to real property and tangible personal property and/or (ii) the intellectual property infringement claims as per Article 6.1.
- c. This Agreement does not grant or create any rights, benefits, claims, obligations or causes of action in, to or on behalf of any person or entity (including any third party) other than those between the respective Parties to this Agreement.
- d. Any claim or series of claims arising out or in connection with this Agreement shall be time barred and invalid if legal proceedings are not commenced by the relevant Party against the other Party within a period of 18 months from the date when the cause of action first arose or within such period as may be permitted by applicable law without the possibility of contractual waiver or limitation.
- e. The Board shall be entitled to claim the remedy of specific performance under this Agreement. Nothing herein shall preclude Board from seeking interim or permanent equitable or injunctive relief. It is clarified that any action for seeking of equitable or

injunctive relief by the Board shall not act as a waiver for its rights to claim or pursue any remedy of monetary damages.

- f. Notwithstanding anything mentioned in this Agreement, Board expressly agrees that SP shall not be liable to Board for lost profits or other financial loss of any type or description including any special, incidental, indirect or consequential damages, whether or not SP has been advised of the possibility of such damages.
- g. Risk of Loss: SP shall bear the risk of loss on Assets up to the time they are being used by SP.
- h. Notwithstanding what has been stated elsewhere in this Agreement and the Schedules attached herein, Board shall not be liable to SP for any indirect or consequential damages.

6.4. FORCE MAJEURE

- a. Neither Party to this Agreement shall be liable to the other for any loss or damage which may be suffered by the other to the extent and for the duration of any cause beyond the reasonable control of the Party ("**Force Majeure**") due (directly) to events such as but not limited to acts of God not confined to the premises of the Party claiming the Force Majeure, flood, drought, lightning or fire, earthquakes, , acts of government or other competent authority, war, terrorist activities, military operations, riots, epidemics, civil commotions etc. No failure, delay or other default of any contractor or sub-contractor to either Party shall entitle such Party to claim Force Majeure under this Article.
- b. The Party seeking to rely on Force Majeure shall promptly, within 2 days, notify the other Party of the occurrence of a Force Majeure event as a condition precedent to the availability of this defense with particulars detail in writing to the other Party and shall demonstrate that it has and is taking all reasonable measures to mitigate the events of Force Majeure.
- c. In the event the Force Majeure substantially prevents, hinders or delays the SP's performance of Services necessary for the operation of RFID Based Access Control System Project's critical business functions for a period in excess of 5 days, the Board may declare that an emergency exists. However, when the situation arising

out of Force Majeure comes to an end in the assessment of the Board, the following conditions shall apply:

- i. **Prior to commencement of operations:** If the event of Force Majeure occurs prior to commencement of operations and continues for a period in excess of ten days, then the Board will grant a period of 7 days after expiry of such period of 10 days, to the SP to resume normal activities under this Agreement. In case the default continues, then the Board may discuss the issue with the SP and revise the existing timelines for the RFID Based Access Control System Project. If the SP does not complete the implementation of the RFID Based Access Control System Project in accordance with the revised timelessness, the Board will have the option to invoke the Performance Bank Guarantee and/or terminate this Agreement.
 - ii. **Post commencement of operations:** If the event of Force Majeure occurs post commencement of operations and continues for a period in excess of five days, then the Board will grant a period of 7 days after expiry of such period of 5 days, to the SP to resume normal services under this Agreement. In case the default continues, the Board may grant an extension of time to the SP for rectifying the situation. However, the Board, or its nominee will deduct for each day of the extension period a percentage proportionate to the number of days and the affected areas/s from the next payable amount as per terms of the Article 4.4 (ii). If there is any further delay despite the extended period, the Board will have the option to invoke the Performance Bank Guarantee and/or terminate the Agreement.
- d. All payments pursuant to termination due to Force Majeure event shall be in accordance with the Terms of Payment Schedule (Schedule VI of this Agreement).
 - i. Notwithstanding the terms of this Article, the failure on the part of the SP under the Agreement to implement any disaster contingency planning and back-up and other data safeguards in against natural disaster, fire, sabotage or other similar occurrence shall not be an event of Force Majeure.

6.5. DATA PROTECTION AND USE

- a. In the course of providing the Services the SP may be compiling, processing and storing proprietary RFID Based Access Control System Data with respect to the users.
- b. The SP and each user are responsible for complying with its respective obligations under the applicable data protection laws and regulations governing the RFID Based Access Control System Project Data.
- c. As a processor of RFID Based Port Access Control System Data, the SP will process RFID Based Access Control System Data in accordance with the terms of this Agreement.
- d. The SP shall not transfer any RFID Based Port Access Control System Data to any entity unless otherwise authorized by the Board in this regard.
- e. Upon reasonable written request from a Party, the other Party will provide the requesting Party with such information that it has regarding the RFID Based Access Control System, Data and its processing which is necessary to enable the requesting party to comply with its obligations under the applicable data protection law or regulation.

6.6. AUDIT, ACCESS AND REPORTING

- a. The Parties shall comply with the Audit, Access and Reporting Schedule provided in Schedule III.
- b. The SP shall, on request, allow access to the Board and its nominees to all information which is in the possession or control of the SP, which relates to the provision of the Services as set out in the Audit, Access and Reporting Schedule and is reasonably required to comply with the terms of the Audit, Access and Reporting Schedule.

7. ARTICLE 7 - INTELLECTUAL PROPERTY

7.1. INTELLECTUAL PROPERTY

- a. Except to the extent otherwise expressly agreed by the Parties to the Agreement in writing, nothing contained in this Agreement shall or will be construed or deemed to grant to the SP or its respective affiliates/nominees any right, title, license or other interest in, to or under (whether by estoppels, by implication or otherwise) any logo, trademark, trade name, service mark or similar designations owned by the Board in

relation to the RFID Based Access Control System Project or any confusingly similar designations.

- b. For all the reusable components whose source code and IPR vest with the original owner, the licenses for such COTS applications shall be in the name of KoPT/ Board from day one. The Board shall retain exclusive intellectual property rights to the bespoke software, customized enhancements of the COTS application, forms and the compilations of the RFID Based Access Control System Project to which the Board has sovereign rights and nothing herein shall or will be construed or deemed to grant to the SP any right, title, license, sub-license, proprietary right or other claim against or interest in, to or under (whether by estoppels, by implication or otherwise) to the aforesaid rights.
- c. Without limiting the generality of Article 7.1(a) and except to the extent otherwise expressly agreed by the Parties to this Agreement in writing, nothing contained in this Agreement shall or will be construed or deemed to grant to the SP any right, title, license or other interest in, to or under (whether by estoppels, by implication or otherwise) any logo, trademark, trade name, service mark or similar designations of Board or RFID Based Access Control System Project or its respective affiliates/nominees or any confusingly similar designations of Project .
- d. Subject to any sole or exclusive rights granted by the Board to a third party prior to the Effective Date, the Board grants to the SP solely in their performance of Services for RFID Based Access Control System Project , non-exclusive, limited, paid-up, royalty-free license during the Term of this Agreement, but not the right to sub-license, to use the RFID Based Access Control System Project Data including the right to copy, perform, display, execute, reproduce, modify, enhance and improve the RFID Based Access Control System Project Data to the extent reasonably necessary or useful for the provision of Services hereunder.
- e. SP shall not use the RFID Based Access Control System Project Data to provide services for the benefit of any third party, as a service bureau.
- f. SP shall indemnify, defend and hold harmless and their respective officers, employees, successors and assigns, from and against any and all losses arising from

claims by third parties that any Deliverables (or the access, use or other rights thereto) created by SP pursuant to this Agreement, or any equipment, software, information, methods of operation or other intellectual property (or the access, use or other rights thereto) provided by SP or sub-contractors to the SP pursuant to this Agreement (i) infringes a copyright enforceable in India, (ii) infringes a patent issued in India, or (iii) constitutes misappropriation or unlawful disclosure or use of another Party's trade secret under the laws of India (collectively, "**Infringement Claims**"); provided, however, that this will not apply to any Deliverables (or the access, use or other rights thereto) created by (A) Board ; (B) third parties (i.e., other than SP or SP's sub-contractors) at the direction of Board.

- g. The Board shall have no liability or obligation to SP or any other Party under Article 7.1(e) above to the extent the Infringement Claim is based upon any use of the equipment, software, information, methods of operation or other intellectual property (or the access, use or other rights thereto) for the benefit of any Party (including any use by SP or its nominees outside the scope of the Services) other than for Project.
- h. Notwithstanding any provisions of this Agreement to the contrary, the foregoing remedies constitute the Parties' sole and exclusive remedies and each Party's entire liability, with respect to Infringement Claims.
- i. If SP uses in the course of the provision of the Services any Third Party System it will use all commercially reasonable endeavours to pass through to the Board such third party's warranties relating to such Third Party Systems. In the event that such warranties cannot be passed through to or enforced by the Board, the SP will enforce such warranties on Board's behalf and account to Board for so doing.
- j. All rights, title and interest in and to, and ownership in, Proprietary Information of RFID Based Access Control System Project which is provided to SP, and all modifications, enhancements and other derivative works of such RFID Based Access Control System Project Proprietary Information ("**Project Proprietary Information**"), as a result of Services rendered by the SP hereunder shall remain solely with the Board from day one. SP shall be entitled to use such Project Proprietary Information

only during the Agreement Term and only for the purposes of providing the Services or to the extent necessary for SP's normal operational, repair and maintenance purposes related to the Services. The Board shall retain exclusive ownership of all Intellectual Property Rights related to Project Proprietary Information.

- k. All rights, title and interest in and to, and ownership in, Proprietary Information of SP, which is provided to the Board, and all modifications, enhancements and other derivative works of such SP Proprietary Information ("SP Proprietary Information"), shall remain solely with SP. The SP will upon the award of the Project in its favor, declare the status of all the SP Proprietary Information along with documentary support sufficient to establish its sole legal rights in the aforesaid Proprietary Information to the Board. This Proprietary Information shall refer to that which has been owned by the SP prior to commencement of the Agreement. Additionally, any software that may be acquired from third parties during the term of the agreement and that which may be developed by the SP during the course of the Agreement specifically for Project shall also not be considered as SP Proprietary Information by the Project. The Board shall be entitled to use such SP Proprietary Information only in connection with the Services or to the extent necessary for Project's normal operational, repair and maintenance purposes related to the Services. To the extent that the SP Proprietary Information is incorporated within the Deliverables, SP and its employees engaged hereby grant to the Board a worldwide, perpetual, irrevocable, non-exclusive, transferable, paid-up right and license to use, copy, modify (or have modified), transport to Project facilities, and prepare from them, use and copy derivative works for the benefit of and internal use of Project such SP Proprietary Information from day one. The Board's rights pursuant to the preceding sentence include the right to disclose such SP Proprietary Information to third party contractors solely for use on Project provided that all such third party contractors execute, deliver and comply with any customary confidentiality and nondisclosure agreements reasonably required by the Board.
- l. With respect to ownership of the Deliverables, the Parties agree that the following shall apply:

- (i) All the deliverables provided to Board by SP during the course of its performance under this Agreement, which includes but is not limited to Bespoke Software as defined in this Agreement, in which, subject to the foregoing provisions of this Article, all right, title and interest in and to such Deliverables, shall, as between SP and Board, immediately upon creation vest in Board. To the extent that the SP Proprietary Information is incorporated within the Deliverables, SP and its employees engaged hereby grant to Board a worldwide, perpetual, irrevocable, non-exclusive, transferable, paid-up right and license to use, copy, modify (or have modified), transport to Board at facilities and locations provided by Board, and prepare from them, use and copy derivative works for the benefit of and internal use of RFID Based Access Control System Project, of such SP Proprietary Information.
 - (ii) If SP proceeds to apply for, or assign to any third party, any patent rights relating to SP Proprietary Information referred to in the above clause, SP will ensure that Board's rights as provided herein are preserved.
- m. The Board hereby grants to SP a non-exclusive right and license to access and use the Project Proprietary Information solely for the purpose of providing Services to Board. Such right and license shall terminate upon the expiration or termination of this Agreement.
- n. Upon the expiration or any termination of this Agreement, SP shall undertake the actions set forth below in this Article to assist the Board to procure replacement services equivalent to Services provided hereunder.
 - (i) The SP undertakes to negotiate in good faith with the Board and any relevant Replacement SP in respect of commercial terms applying to all SP Intellectual Property Rights and which the Board and any relevant Replacement SP require to enable them to provide or receive services substantially equivalent to the Services hereunder.
 - (ii) In respect of SP's usage of third party Intellectual Property Rights, SP undertakes to assist the Board to secure such consents or licenses from such

third parties as are necessary to enable Project to receive services substantially equivalent to the Services hereunder. The obligations of the SP under this Article shall be considered part of the services performed by the SP under the Exit Management Services.

8. ARTICLE 8 – MISCELLANEOUS

8.1. CONFIDENTIALITY

- a. The SP recognizes that during the term of this Agreement, sensitive data will be procured and made available to it, its Sub contractors and agents and others working for or under the SP. Further, the SP also recognizes that any improper and unauthorized disclosure or usage of the data by any such recipient may constitute a

breach of applicable laws causing harm not only to the Board but also to the company whose data is used but also to its shareholders, directors and other officers. The SP, its Subcontractors and agents shall demonstrate utmost care, sensitivity and strict confidentiality in respect of all such information. Any breach of this Article will result in the Board and its nominees receiving a right to seek injunctive relief and damages without any limit, from the SP and/or also seek termination.

- b. SP agrees as to any Confidential Information disclosed by a Party to this Agreement (the “**Discloser**”) to the other Party to this Agreement (the “**Recipient**”):
- (i) to take such steps necessary to protect the Discloser’s Confidential Information from unauthorized use, reproduction and disclosure as the Recipient takes in relation to its own Confidential Information of the same type, but in no event less than reasonable care; and
 - (ii) to use such Confidential Information only for the purposes of this Agreement or as otherwise expressly permitted or expressly required by this Agreement or as otherwise permitted by the Discloser in writing; and
 - (iii) not, without the Discloser’s prior written consent, to copy the Confidential Information or cause or allow it to be copied, directly or indirectly, in whole or in part, except as otherwise expressly provided in this Agreement, or as required in connection with SP’s use as permitted under this Article, or as needed for the purposes of this Agreement, provided that any proprietary legends and notices (whether of the Discloser or of a Third Party) are not removed or obscured; and
 - (iv) Not, without the Discloser’s prior written consent, to disclose, transfer, publish or communicate the Confidential Information in any manner to any person except as permitted under this Agreement.
 - (v) Limit access to such Confidential Information and materials to those of its directors, partners, advisers, agents or employees who are directly involved in the consideration/evaluation of the Confidential Information and bind

each of its directors, partners, advisers, agents or employees so involved to protect the Confidential Information and materials in the manner prescribed in this Agreement; and

- (vi) Upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of Confidential Information, promptly inform the Discloser of such disclosure in writing and immediately return to the Discloser all such Information and materials, in whatsoever form, including any and all copies thereof.

c. The restrictions of this Article shall not apply to Confidential Information that:

- (i) is or becomes generally available to the public through no breach of this Article by Recipient; and
- (ii) was in the Recipient's possession free of any obligation of confidence prior to the time of receipt of it by the Recipient hereunder; and
- (iii) is developed by the Recipient independently of any of Board's Confidential Information; and
- (iv) is rightfully obtained by the Recipient from third parties authorized at that time to make such disclosure without restriction; and
- (v) is identified in writing by the Discloser as no longer proprietary or confidential; or
- (vi) is required to be disclosed by law, regulation or Court Order or under the Right to Information Act, or to be furnished to the Parliament and/or its Committees, provided that the Recipient gives prompt written notice to the Discloser of such legal and regulatory requirement to disclose so as to allow the Discloser reasonable opportunity to contest such disclosure.

d. To the extent that such disclosure is required for the purposes of this Agreement, Recipient may disclose Confidential Information to:

- (i) its employees, agents and independent contractors and to any of its affiliates and their respective independent contractors or employees; and

- (ii) its professional advisors and auditors, who require access for the purposes of this Agreement, whom the relevant Party has informed of its obligations under this Article and in respect of whom the relevant Party has used commercially reasonable efforts to ensure that they are contractually obliged to keep such Confidential Information confidential on terms substantially the same as set forth in this Article. The Recipient may also disclose Confidential Information to any entity with the Discloser's prior written consent.
- e. The provisions of this Article shall survive the expiration or any earlier termination of this Agreement.
- f. Confidential Information shall be and remain the property of the Discloser and nothing in this Article shall be construed to grant Recipient any right or license with respect to the Discloser's Confidential Information otherwise than as is expressly set out in this Agreement.
- g. Subject as otherwise expressly provided in this Agreement all Confidential Information in tangible or electronic form under the control of the Recipient shall either be destroyed, erased or returned to the Discloser promptly upon the earlier of: (i) the written request of the Discloser or, (ii) termination or expiry of this Agreement. Notwithstanding the forgoing, Recipient may retain, subject to the terms of this Article, a reasonable number of copies of the Party's Confidential Information solely for confirmation of compliance with the confidentiality obligations of this Agreement.
- h. Both Parties agree that monetary damages would not be a sufficient remedy for any breach of this Article by the other Party and that the Board and SP, as appropriate, shall be entitled to equitable relief, including injunction and specific performance as a remedy for any such breach. Such remedies shall not be deemed to be the exclusive remedies for a breach by a Party of this Article, but shall be in addition to all other remedies available at law or equity to the damaged Party including the right to terminate this Agreement.

- i. In connection with the Services, SP may from time to time undertake one or more quality assessment reviews for the purpose of improving Project. In order for such reviews to be frank and candid, for the greatest benefit to Board and SP, they shall be kept confidential to the greatest extent possible. The Parties agree that any documentation created in connection with such quality assessment reviews shall be Confidential Information of SP which is licensed to RFID Based Access Control System project for any internal use except that in no event shall such documentation or the results of such reviews be discoverable or admissible (or used for any purpose) in any arbitration or legal proceedings against SP related to this Agreement or the Services.

8.2. PERSONNEL

- a. Personnel assigned by SP to implement the RFID Based Access Control System Project and perform the Services shall be employees of the SP, and under no circumstances will such personnel be considered employees of the Board. The SP shall have the sole responsibility for supervision and control of its personnel and for payment of such personnel's entire compensation, including salary, withholding of income taxes and social security taxes, worker's compensation, employee and disability benefits and the like and shall be responsible for all employer obligations under all Applicable Laws and the Board shall have no direct or indirect liability or obligation, to pay any charges, claims or wages of any of employee, agents, contractors and subcontractors of the SP.
- b. The SP shall use its best efforts to ensure that sufficient personnel of the SP are employed to perform the Services, and such personnel have appropriate qualifications to perform the Services. The Board shall have the right to require the removal or replacement of any SP personnel performing work under this Agreement. In the event that the Board requests that any SP personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule but not later than 3 working days.
- c. The SP shall also be responsible to train employees of the Board at no additional cost, with regard to the Services being provided by the SP as and when required by

the Board during the Term of this Project. The parameters of the training required for these employees of the Board shall be communicated by the Board to the SP periodically and shall be in accordance with the latest procedures and processes available in the relevant areas of work.

- d. In the event the Board identifies any personnel of SP as "Key Personnel", then the SP shall not remove such personnel without the prior written consent of the Board under this Agreement.
- e. Except as stated in this Article, nothing in this Agreement will limit the ability of SP to freely to assign or reassign its employees; provided that SP shall be responsible, at its expense, for transferring all appropriate knowledge from personnel being replaced to their replacements. The Board shall have the right to review and approve SP's plan for any such knowledge transfer. SP shall maintain the same standards for skills and professionalism among replacement personnel as in personnel being replaced.
- f. Each Party shall be responsible for the performance of all its obligations under this Agreement and shall be liable for the acts and omissions of its employees and agents in connection therewith.
- g. Liability for the actions of the Personnel and Subcontractors
 - i. The SP agrees to be responsible for managing the activities of its personnel or the personnel of the subcontractors and shall be accountable for both.
 - ii. The SP shall be the principal employer of the employees, agents, contractors, subcontractors etc engaged by it and shall be liable for all the acts, deeds or things, whether the same is within the scope of instructions or outside the scope of instructions set out in the Agreement.
 - iii. The SP agrees to hold the Board, its successors, assignees employees, representatives and administrators fully indemnified and harmless against loss or liability, claims actions or proceedings, if any, that may arise from whatsoever nature caused to the Board through the action of the SP's employees, agents, contractors, subcontractors, etc.

- h. Under no circumstance the Board can be made as a party to any of the third party claims arising under this Agreement involving SP and such third party. The SP would protect and hold harmless the Board from any such third party claim.

8.3. INDEPENDENT CONTRACTOR

Nothing in this Agreement shall be construed as establishing or implying any agency, partnership or joint venture between the Parties to this Agreement and, except as expressly stated in this Agreement, nothing in this Agreement shall be deemed to constitute any of the Parties as the agent of any other Party or authorizes either Party (i) to incur any expenses on behalf of the other Party, (ii) to enter into any engagement or make any representation or warranty on behalf of the other Party, (iii) to pledge the credit of or otherwise bind or obligate the other Party, or (iv) to commit the other Party in any way whatsoever without in each case obtaining the other Party's prior written consent.

8.4. SUB-CONTRACTORS

SP shall not subcontract (to other parties not forming part of proposed consortium, if any) any work related to the implementation of RFID Based Access Control System Project to be performed under this Agreement without the Board's explicit prior written consent.

8.5. ASSIGNMENT

- a. The Board may assign this Agreement in whole or as a part of a reorganization, restructuring, consolidation, merger etc.
- b. The SP shall not assign this Agreement or its rights and duties under this Agreement either in whole or in part without the prior written consent of the Board, and any attempted assignment or delegation without such consent will be void. It is understood that transfer of [25%] or more voting share capital of SP by one transaction or a series of transaction in favour of any person or a group of persons shall, *inter-alia*, be considered and deemed to be an assignment/ transfer of this Agreement and shall require prior written consent of the Board.

8.6. TRADEMARKS, PUBLICITY

Neither Party may use the trademarks of the other Party without the prior written consent of the other Party. Except as required by law or the rules and regulations of each stock exchange upon which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either alone or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement or the business of the Parties without prior reference to and approval in writing from the other Party, such approval not be unreasonably withheld or delayed.

8.7. NOTICES

- a. Any notice or other document, which may be given by either Party under this Agreement, shall be given in writing in person or by pre-paid recorded delivery post or by facsimile transmission.
- b. In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below:

Board

Address:

Tel:

Fax:

Email:.....

Service Provider:

Address:

Tel:.....

Fax:.....

Email:.....

- c. Any notice or other document shall be deemed to have been given to the other Party (or, if relevant, its relevant associated company) when delivered (if delivered in person) if delivered between the hours of 9.00 am and 5.30 pm on a working day at the address of the other Party set forth above or if sent by fax, provided the copy fax is accompanied by a confirmation of transmission, or on the next working day thereafter if delivered outside such hours, and 7 days from the date of posting (if by letter).
- d. Either Party to this Agreement may change its address, telephone number, facsimile number and nominated email for notification purposes by giving the other reasonable prior written notice of the new information and its effective date.

8.8. VARIATIONS AND FURTHER ASSURANCE

- a. No amendment, variation or other change to this Agreement shall be valid unless authorized in accordance with the change control procedure as set out in the Change Control Schedule and made in writing and signed by the duly authorized representatives of the Parties to this Agreement.
- b. Each Party to this Agreement agrees to enter into or execute, without limitation, whatever other agreement, document, consent and waiver and to do all other things which shall or may be reasonably required to complete and deliver the obligations set out in this Agreement.

8.9. SEVERABILITY AND WAIVER

- a. If any provision of this Agreement, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the remainder of the provisions in question which shall remain in full force and effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid or unenforceable provision a valid and enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the illegal, invalid or unenforceable provision or part provision.

- b. No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement of any right, remedy or provision of this Agreement shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of such right, remedy or provision. Without limiting the foregoing, no waiver by a Party of any breach by the other Party of any provision hereof shall be deemed to be a waiver of any subsequent breach of that or any other provision hereof.

8.10. COMPLIANCE WITH LAWS AND REGULATIONS

Each Party to this Agreement accepts that its individual conduct shall (to the extent applicable to it) at all times comply with all applicable laws, rules and regulations. For the avoidance of doubt, the obligations of the Parties to this Agreement are subject to their respective compliance with all applicable laws and regulations.

8.11. ETHICS

SP represents, warrants and covenants that it has given no commitments, payments, gifts, kickbacks, lavish or expensive entertainment, or other things of value to any employee or agent of Board, or its nominated agencies in connection with this agreement and acknowledges that the giving of any such payment, gifts, entertainment, or other things of value is strictly in violation of Board's standard policies and may result in cancellation of this Agreement.

8.12. ENTIRE AGREEMENT

This Agreement, all schedules appended thereto and the contents and specifications of all the Volumes of the RFP constitute the entire agreement between the Parties with respect to their subject matter, and supersede all prior or contemporaneous negotiations, written or oral understandings and agreements, between the Parties regarding such subject matter. If there is any aspect of the Project not covered by any of the provisions of the Agreement and the Proposal, reference shall be made by the Parties to the other bid documents, inter alia including the documents issued by

the Board and also including addendums, clarifications given in writing in the pre-bid meetings and the written submissions made by the SP but not otherwise.

8.13. SURVIVABILITY

The termination or expiry of this Agreement for any reason shall not affect or terminate or prejudice (a) any right or obligation arising out of or accruing under this Agreement attributable to events or circumstances occurring prior to such termination or expiry; (b) the provisions of this Agreement that by their nature are intended to survive the its termination or expiry.

9. ARTICLE 9 - DISPUTES

9.1. DISPUTE RESOLUTION

- a. Any dispute arising out of or in connection with this Agreement shall in the first instance be dealt with in accordance with the escalation procedure as set out in the Governance Schedule.
- b. Any dispute or difference whatsoever arising between the parties to this Agreement out of or relating to the construction, meaning, scope, operation or
- c. effect of this Agreement or the validity of the breach thereof, which cannot be resolved through the application of the provisions of the Governance Schedule, shall be referred to a sole arbitrator to be appointed by mutual consent of both the Parties herein. If the Parties cannot agree on the appointment of an arbitrator within a period of one month from the notification by one party to the other of existence of such dispute, then the arbitrator shall be nominated in accordance with the provisions of the Arbitration and Conciliation(Amendment) Act, 2015as amended from time to time and the award made thereunder shall be final and binding upon the Parties hereto, subject to legal remedies available under the Applicable Law. The arbitration proceedings will be held at Kolkata West Bengal.
- d. Each Party shall bear its own cost of preparing and presenting its case. The cost of arbitration including the fees and expenses of the arbitrator shall be shared equally by the Board and the SP. Pending the submission of and/or decision on a dispute, difference or claim or until the arbitral award is made the Parties shall continue to perform all of their obligations under the Agreement without prejudice to a final adjustment in accordance with such award.

10. ARTICLE 10 - AMENDMENT

The Parties acknowledge and agree that amendments to this Agreement shall be made through mutual agreement between the parties in writing in accordance with the procedure this Agreement is executed and signed.

IN WITNESS WHEREOF the Parties have by duly authorized representatives set their respective hands and seal on the date first above written in the presence of:

WITNESSES:

1. (Name, Designation, Organization, and Signature)

2. (Name, Designation, Organization, and Signature)

Board

[SERVICE PROVIDER]

Signed

Signed

Authorized Signatory

For and on behalf of the

For and on behalf of the

Board of Trustees for the Port of Kolkata

_____ (Company

name) _____

By: _____ (signature) _____

By: _____ (signature) _____

____ (Name and designation) _____

____ (Name and designation) _____

An authorized signatory duly nominated
pursuant to Board Resolution No. _____
dated _____ of the [SP]

1. SCHEDULE I : CHANGE CONTROL SCHEDULE

A. PURPOSE

This Schedule applies to and describes the procedure to be followed in the event of any proposed change to the Agreement, Project Implementation Phase, and Operation and Management Service Level. Such change shall include, but shall not be limited to, changes in the scope of services provided by the SP and changes to the terms of payment as stated in the Terms of Payment Schedule (Schedule VI of this Agreement).

The Board and the SP recognize that frequent change is an inevitable part of delivering services and that a significant element of this change can be accomplished by re-organizing processes and responsibilities without a material effect on the cost. The SP will endeavor to the best of its ability and in accordance with prevailing market practices, to effect change without an increase in the terms of payment as stated in the Terms of Payment Schedule and the Board will work with the SP to ensure that all changes are discussed and managed in a constructive manner.

B. CHANGE CONTROL NOTE ("CCN")

- a. Change requests in respect of the Agreement, the Project Implementation, or the Operation and Management Service Level will emanate from the Parties' respective Project Manager who will be responsible for obtaining approval for the change and who will act as its sponsor throughout the Change Control Process and will complete Part A of the CCN attached as Schedule VII hereto. CCNs will be presented to the other Party's Project Manager who will acknowledge receipt by signature on the CCN.
- b. The SP and the Board, while preparing the CCN, shall consider the change in the context of the following parameter, namely whether the change is beyond the scope of Services including ancillary and concomitant services required and as detailed in RFP and is suggested and applicable only after the testing, commissioning and certification of the Project Implementation as set out in this Agreement.

C. QUOTATION

- a. The SP shall assess the CCN and complete Part B of the CCN. In completing Part B of the CCN the SP shall provide as a minimum: a description of the change which should also provide Name of functionality/feature being changed, current functionality/feature (prior to change), new functionality/feature (post change);
 - i. a description of the change;
 - ii. a list of deliverables required for implementing the change;
 - iii. a timetable for implementation;
 - iv. an estimate of the timelines or effort of any proposed change;
 - v. the unit of measure to cost the change;
 - vi. an estimate of any proposed change;
 - vii. any relevant acceptance criteria;
 - viii. an assessment of the value of the proposed change;
 - ix. Material evidence to prove that the proposed change is not already covered within the scope of the Project;
 - x. Description of the circumstances which influenced the origin of this change.
 - xi. Alternative options possible to address the change if any and the implications of these alternative options.
 - xii. Detailed break up of various categories of activities to be performed for implementing a proposed change along with details on where re-usable components are used to reduce the efforts.
 - xiii. Details on software change estimation method used for the calculation of change effort estimation to provide information on how change is classified in various categories, what all items that require efforts and how efforts are estimated.
 - xiv. Underlying Assumptions.

- xv. Any other details that Board would require to assess the effort estimated provided by the SP.
- a. Prior to submission of the completed CCN to the Board, or its nominated agencies, the SP will undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, the SP shall consider the materiality of the proposed change in the context of the Agreement, the Project Implementation, Operation and Management Service Level affected by the change and the total effect that may arise from implementation of the change.
- b. Materiality criteria will be established by the Board and the SP's Project Manager. Changes requiring no escalation of authority can be implemented. Discussion and agreement as to materiality will be held in accordance with the Governance Schedule (Schedule IV of this Agreement).

D. COSTS

Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided the SP meets the obligations as set in the CCN. In the event the SP is unable to meet the obligations as defined in the CCN then the cost of getting it done by third party will be borne by the SP.

E. REPORTING

Change requests and CCNs will be reported monthly to each Party's Project Managers who will prioritize and review progress.

F. OBLIGATIONS

The SP shall be obliged to implement any proposed changes once approval in accordance with above provisions has been given, with effect from the date agreed for implementation and within an agreed timeframe.

2. SCHEDULE II : EXIT MANAGEMENT SCHEDULE

1. PURPOSE

- a. This Schedule sets out the provisions, which will apply prior to the expiry of the Agreement or termination of the Agreement, the Project Implementation, Operation and Management Service Level is initiated.
- b. It sets out the provisions which will ensure that Board will be able to offer the services to its Stakeholders without any interruptions on expiry or termination of the Agreement.
- c. Continuity and performance of the Services at all times including the duration of the Agreement and post expiry of the Agreement is a critical requirement of the Board. It is the prime responsibility of SP to ensure continuity of service at all times of the Agreement including exit management period and in no way any facility/service shall be affected/degraded. Further, SP is also responsible for all activities required to train and transfer the knowledge to the Replacement SP to ensure similar continuity and performance of the Services post expiry of the Agreement. SP will be required to carry out a gap analysis of the facilities and arrangements made by the Replacement SP and specifically inform Board. It sets out the mechanisms for Exit Management Services the SP is to provide on termination or prior to expiration of the Agreement to allow the orderly and efficient transition of the Services to Board or its nominee.
- d. It sets out the mechanisms for managing the knowledge enablement services the SP has to provide to allow Board to create an understanding of the operations and technology of the systems for itself or its nominees or any designated agencies.
- e. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

2. TRANSFER OF ASSETS

- a. The ownership of all assets viz. IT hardware, software, perpetual licenses or products and all associated components purchased/ installed/ developed, as part of this agreement for fulfilment of the scope of services of the project, shall be in the name of KoPT/ Board from day one. SP shall submit an comprehensive list of assets to KoPT and will keep updating the asset list from time to time.

- b. The Board shall be entitled to serve notice in writing on the SP at any time during the exit management period as detailed hereinabove requiring the SP and/or its sub-contractors to provide the Board with a complete and up to date list of the Assets within 30 days of such notice. The Board shall then be entitled to serve notice in writing on the SP at any time prior to the date that is 30 days prior to the end of the exit management period requiring the SP to cease usage of all the Assets to the Project.
- c. **In case of Agreement being terminated by Board**, Board reserves the right to ask SP to continue running the Project operations for a period of 6 months after termination orders are issued. Such period can be extended if the handover of assets is not complete and/or not done to the satisfaction of the Board. In case of successful handover to the satisfaction of Board is achieved before the period of 6 months after termination orders, Board reserves the right to relieve SP of the obligation to run Project operations earlier than the period of 6 months.
- d. Upon service of a notice under this Article the following provisions shall apply:
 - (i) The Board shall take over the assets without any payments to the SP on the last day of the exit management period.
 - (ii) Payment to the outgoing SP shall be made to the tune of last set of completed transactions, subject to requirements under this Agreement and for any Capex component that has been accepted by Board but is pending for payment.
 - (iii) The task of SP with reference to the Exit Management is deemed to be complete only when the Board issues a satisfactory completion certificate for the Exit Management.

3. COOPERATION AND PROVISION OF INFORMATION

During the exit management period:

- a. the SP will allow the Board access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the Board to assess the existing services being delivered;

- b. promptly on reasonable request by the Board, the SP shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with the Agreement, the Project Implementation, and the Operation and Management Service Level relating to any material aspect of the Services (whether provided by the SP or sub-contractors appointed by the SP). The Board shall be entitled to copy all such information. Such information shall include details pertaining to the services rendered and other performance data. The SP shall permit the Board and/or any Replacement SP to have reasonable access to its employees and facilities as reasonably required by the Board to understand the methods of delivery of the services employed by the SP and to assist appropriate knowledge transfer.

4. CONFIDENTIAL INFORMATION, SECURITY AND DATA

- a. The SP will promptly on the commencement of the exit management period supply to the Board the following:
 - (i) information relating to the current services rendered and performance data relating to the performance of sub-contractors in relation to the services;
 - (ii) documentation relating to Project's Intellectual Property Rights;
 - (iii) Project data and confidential information;
 - (iv) documentation relating to sub-contractors;
 - (v) all current and updated Project data as is reasonably required for purposes of Project or its nominated agencies transitioning the services to its Replacement SP in a readily available format specified by the Board;
 - (vi) all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable Project or its nominated agencies, or its Replacement SP to carry out due diligence in order to transition the provision of the Services to Project or its nominated agencies, or its Replacement SP (as the case may be).

- b. Before the expiry of the exit management period, the SP shall deliver to the Board all new or up-dated materials from the categories set out in Article above and shall not retain any copies thereof.
- c. Before the expiry of the exit management period, unless otherwise provided under the Agreement, the Board shall deliver to the SP all forms of SP confidential information, which is in its or its nominees or its users' possession or control.

5. EMPLOYEES

- a. Promptly on reasonable request at any time during the exit management period, the SP shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the Board a list of all employees (with job titles) of the SP dedicated to providing the services at the commencement of the exit management period;
- b. Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the SP to the Board or its nominees, or a Replacement SP ("**Transfer Regulation**") applies to any or all of the employees of the SP, then the Parties shall comply with their respective obligations under such Transfer Regulations.
- c. To the extent that any Transfer Regulation does not apply to any employee of the SP, Board or its Replacement SP may make an offer of employment or contract for services to such employee of the SP and the SP shall not enforce or impose any contractual provision that would prevent any such employee from being hired by the Board or any Replacement SP.

6. TRANSFER OF CERTAIN AGREEMENTS

On request by the Board, the SP shall effect such assignments, transfers, licenses and sub-licenses as the Board may require in favor of the Board, or its Replacement SP in relation to any equipment, lease, maintenance or service provision agreement between SP and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the Board or its Replacement SP.

7. RIGHTS OF ACCESS TO PREMISES

- a. At any time during the exit management period, where Assets pertaining to the RFID Based Access Control System Project are located at the SP's premises, the SP will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) the Board, and/or any Replacement SP in order to make an inventory of the Assets.
- b. The SP shall also give the Board or its nominated agencies, or any Replacement SP right of reasonable access to the SP's premises and shall procure the Board or its nominated agencies and any Replacement SP rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the Agreement as is reasonably necessary to migrate the services to the Board or its nominated agencies, or a Replacement SP.

8. GENERAL OBLIGATIONS OF THE SERVICE PROVIDER

- a. The SP shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the Board or its nominated agencies or its Replacement SP and which the SP has in its possession or control at any time during the exit management period.
- b. For the purposes of this Schedule, anything in the possession or control of any SP, associated entity, or sub-contractor is deemed to be in the possession or control of the SP.
- c. The SP shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

9. EXIT MANAGEMENT PLAN

- a. The SP shall provide the Board with a recommended Exit Management Plan ("**Exit Management Plan**") which shall deal with at least the following aspects of exit management in relation to the Agreement as a whole and in relation to the RFID Based Access Control System Project Implementation and the Operation and Management Service Level.

- (i) A detailed program of the transfer process that could be used in conjunction with a Replacement SP including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
 - (ii) plans for the communication with such of the SP's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project's operations as a result of undertaking the transfer;
 - (iii) (if applicable) proposed arrangements for the segregation of the SP's networks from the networks employed by Project and identification of specific security tasks necessary at termination;
 - (iv) Plans for provision of contingent support to Board and Replacement SP for a reasonable period after transfer.
- b. The SP shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.
 - c. Each Exit Management Plan shall be presented by the SP to and approved by the Board or its nominated agencies.
 - d. The terms of payment as stated in the Terms of Payment Schedule include the costs of the SP complying with its obligations under this Schedule.
 - e. In the event of termination or expiry of Agreement, Project Implementation, or Operation and Management Service Level, each Party shall comply with the Exit Management Plan.
 - f. During the exit management period, the SP shall use its best efforts to deliver the Services.
 - g. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.
 - h. Exit Management Plan shall be furnished in writing to the Board or its nominated agencies within 90 days from the Effective Date of this Agreement.

3. SCHEDULE III : AUDIT, ACCESS AND REPORTING SCHEDULE

A. PURPOSE

This Schedule details the audit, access and reporting rights and obligations of the Board and the SP under the Agreement,

B. AUDIT NOTICE AND TIMING

- a. As soon as reasonably practicable after the Effective Date, the Parties shall use their best endeavors to agree to a timetable for routine audits during the Project Implementation Phase and the Operation and Management Phase. Such timetable may be reviewed every 3 months on the sole discretion of Board. During the Implementation Phase, the Board and thereafter during the Operation Management Phase, the Board shall conduct routine audits in accordance with such agreed timetable and shall not be required to give the SP any further notice of carrying out such audits.
- b. The Board may conduct non-timetabled audits at his/ her own discretion if he/ she reasonably believes that such non-timetabled audits are necessary as a result of an act of fraud by the SP, a security violation, or breach of confidentiality obligations by the SP, provided that the requirement for such an audit is notified in writing to the SP a reasonable period time prior to the audit (taking into account the circumstances giving rise to the reasonable belief) stating in a reasonable level of detail the reasons for the requirement and the alleged facts on which the requirement is based. If the SP considers that the non-timetabled audit was not appropriate, the matter shall be referred to the escalation procedure as set out in the Governance Schedule (Schedule IV of this Agreement).
- c. Provided always that the Board shall endeavor to conduct such audits with the lowest levels of inconvenience, disturbance in normal operations and disturbance practicable being caused to the SP.
- d. In addition to the above, there will be audits conducted by statutory bodies (e.g. CAG) as and when they are required to do it. Notwithstanding any condition given in the Agreement, SP will have to provide these statutory bodies access to all the

facilities, infrastructure, documents and artifacts of the Project as required by them and approved by the Board, in writing.

- e. The audit and access rights contained shall survive the termination or expiration of the Agreement.

C. ACCESS

The SP shall provide to the Board access to employees, subcontractors, suppliers, agents and third party facilities, including leased premises used, if any, documents, records and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections. The Board shall have the right to copy and retain copies of any relevant records. The SP shall co-operate with Board in effecting the audits.

D. AUDIT RIGHTS

- a. The Board shall have the right to audit and inspect suppliers, agents and third party facilities, including leased premises used for providing Services, if any, Primary Site, Back-up site, documents, records, procedures and systems relating to the provision of the services, but only to the extent that they relate to the provision of the services, as shall be reasonably necessary to verify:
 - (i) The security, integrity and availability of all Project data processed, held or conveyed by the SP on behalf of Project and documentation related thereto;
 - (ii) That the actual level of performance of the services is the same as specified in the Service Level;
 - (iii) That the SP has complied with the relevant technical standards, and has adequate internal controls in place; and
 - (iv) The compliance of the SP with any other obligation under the Agreement

E. AUDIT RIGHTS OF SUB-CONTRACTORS, SUPPLIERS AND AGENTS

- a. The SP shall perform the same audit and access provisions as defined in this Schedule with sub-contractors, suppliers and agents who supply labor, services, equipment or materials in respect of the services. The SP shall inform the Board prior to concluding any sub-contract or supply agreement of any failure to achieve the same rights of audit or access.
- b. **REPORTING:** The SP will provide monthly reports to the Board regarding any specific aspects of the Project and in context of the audit and access information as required by the Board.

F. ACTION AND REVIEW

- a. Any change or amendment to the systems and procedures of the SP, or sub-contractors, where applicable, arising from the audit report shall be agreed within thirty (30) calendar days from the submission of the said report.
- b. Any discrepancies identified by any audit pursuant to this Schedule shall be immediately notified to the Board or the appropriate Project Manager and the SP Project Manager who shall determine what action should be taken in respect of such discrepancies in accordance with the terms of the Agreement.

G. TERMS OF PAYMENT FOR COST OF AUDIT

The SP and its sub-contractors, if any, shall bear their own costs of any audits and inspections. The terms of payment are inclusive of any costs of the SP and the sub-contractor, for all reasonable assistance and information provided under the Agreement by the SP pursuant to this Schedule. The cost of solution audit needs to be borne by the Service Provider.

H. RECORDS AND INFORMATION

For the purposes of audit in accordance with this Schedule, the SP shall maintain true and accurate records in connection with the provision of the services and the SP shall handover all the relevant records and documents upon the termination or expiry of the Agreement.

4. SCHEDULE IV : GOVERNANCE SCHEDULE

A. PURPOSE

The purpose of this Schedule is to (i) establish and maintain the formal and informal processes for managing the relationship between the Board and the SP (including the outputs from other Schedules to this Agreement; (ii) define the principles that both Parties wish to follow to ensure the delivery of the Services; (iii) ensure the continued alignment of the interests of the Parties; (iv) ensure that the relationship is maintained at the correct level within each Party; (v) create the flexibility to revise and maintain the relationship and this Agreement during the Term; (vi) set out the procedure for escalating disagreements; and (vii) enable contract administration and performance management.

B. GOVERNANCE STRUCTURE

- a. The Program Governance Structure to be put in place by Board will have the following units:
 - i. Steering Committee (SC)
 - ii. Program Management Team (PMT)

The composition of each of the above units will be in line with the approach described in the RFP or as decided by Board.

- b. **Project Manager:** The relationship under this Agreement will be managed by the Project Manager appointed by each Party, who will provide the interface between the executive management of the respective Parties. In the event that either Party wishes to substitute its Project Manager it will do so in the manner in which the original appointment is made and notify the other Party of such substitution as soon as reasonably practicable but at the latest within fourteen days of the substitution.
- c. The Project Managers shall have responsibility for maintaining the interface and communication between the Parties.
- d. Board will appoint a Project Management Team within 2 weeks of the Effective Date.

- e. The Project Management Team (PMT) of the RFID Based Access Control System project has been constituted to monitor day to day progress of the project and provide approvals and suggestions for smooth Implementation and Operations of the project and Officers from Board and Other expert are the members of the Team. The PMT will meet formally on, at least, a weekly basis at a time and location to be agreed between them. These meetings will cover, as a minimum, the following agenda items: (i) consideration of monthly Performance Reports; (ii) consideration of matters arising out of the Change Control Schedule; (iii) issues escalated in accordance with the escalation procedure as set out in this Schedule; (iv) matters to be brought before the Operations Committee in accordance with the Agreement and the Schedules; (v) any matter brought before the PMT by the SP under this Article; and (vi) any other issue which either Party wishes to add to the agenda.
- f. In the event that there is any material factor which affects the delivery of the Services or the terms of payment as stated in the Terms of Payment Schedule (Schedule VI of this Agreement), the Parties agree to discuss in the PMT any appropriate amendment to the Agreement or any Service Level Agreements or Statement of Works including any variation to the terms of payment as stated in the Terms of Payment Schedule. Any variation so agreed shall be implemented through the change control procedure as set out in the Change Control Schedule (Schedule I of this Agreement).

C. GOVERNANCE PROCEDURES

- a. The SP shall document the agreed structures in a procedures manual.
- b. The agenda for each meeting of the SC and PMT shall be set to reflect the discussion items referred to above and extraordinary items may be added either with the agreement of the Parties or at the request of either Party. Copies of the agenda for meetings of the PMT, along with relevant pre-reading material, shall be distributed at least two days in advance of the relevant meeting.
- c. All meetings and proceedings will be documented; such documents to be distributed to both Parties and copies shall be kept as a record. All actions, responsibilities and accountabilities arising out of any meeting shall be tracked and managed.

- d. The Parties shall ensure as far as reasonably practicable that the SC and PMT shall resolve the issues and resolve the objectives placed before them and those members representing that Party are empowered to make relevant decisions or have easy access to empowered individuals for decisions to be made to achieve this.
- e. The Parties will proceed in good faith so that the SC and PMT shall resolve the issues and smoothen the performance of the Project.

D. LIAISON BETWEEN THE SUB CONTRACTORS

The SP shall participate in the meetings with other sub-contractors, approved by Board and coordinate the receipt and delivery of the Services in a regular program of liaison between the Project Manager, Board or any other representative of Board and each of the sub-contractors.

E. ARBITRATION

- a. The parties agree to attempt to resolve all disputes arising under the Agreement, equitably and in good faith. To this end, the parties agree to provide frank, candid and timely disclosure of all relevant facts, information and documents to facilitate discussions between them/their representatives or senior officers
- b. The Parties shall first submit any dispute or disagreement between the Parties arising out of or relating to and/or in connection with this Agreement or Statement of Work which is not a material breach as stated in Article V of this Agreement (a "**Disputed Matter**") to the Board. In case the Disputed Matter remains unresolved, the same shall be then submitted to SC.
 - i. In order formally to submit a Disputed Matter to the aforesaid fora, one Party ("**Claimant**") shall give a written notice ("**Dispute Notice**") to the other Party. The Dispute Notice shall be accompanied by (a) a statement by the Claimant describing the Disputed Matter in reasonable detail and (b) documentation, if any, supporting the Claimant's position on the Disputed Matter.
 - ii. The other Party ("**Respondent**") shall have the right to respond to the Dispute Notice within 7 days after receipt of the Dispute Notice. In the event that the fora are unable to resolve the Disputed Matter within a further period of 7

days, it shall refer the Disputed Matter to next level of the dispute resolution for action.

- iii. All negotiations, statements and/or documentation pursuant to these Articles shall be without prejudice and confidential (unless mutually agreed otherwise).
- iv. If the Disputed Matter is having a material effect on the operation of the Services (or any of them or part of them) the Parties will use all their respective reasonable endeavors to reduce the elapsed time in reaching a resolution of the Disputed Matter.

5. SCHEDULE V : INVOICING AND SETTLEMENT SCHEDULE

- a. In respect of its remuneration for the Services the SP shall be eligible to receive payments in accordance with the Terms of Payments Schedule (Schedule VI of this Agreement). Subject to the specific terms of each Service Level Agreement, the SP submit its invoices in accordance with the following principles:
 - (i) The Board shall be invoiced by the SP for the Services. Generally and unless otherwise agreed in writing between the Parties, the SP shall raise an invoice as per the terms of payment as stated in this Schedule.
 - (ii) Any invoice presented in accordance with this Article shall be in a form agreed with the Board.
- b. Invoices shall be accurate and all adjustments to or changes in the terms of payment as stated in the Terms of Payment Schedule shall be applied to the next payment invoice. The SP shall waive any charge for a Service that is not invoiced within six months after the end of the month in which the terms of payment as stated in the Terms of Payment Schedule relating to such Service are authorized or incurred, whichever is later.
- c. Payments invoiced shall be made within 45 days of the receipt of invoice by the Board subject to adjustments if any for the previous performance.
- d. The Board shall be entitled to delay or withhold payment of any invoice or part of it delivered by the SP under this Schedule where the Board disputes such invoice or part of it provided that such dispute is bona fide. The withheld amount shall be limited to that which is in dispute. The disputed amount shall be settled in accordance with the escalation procedure as set out in the Governance Schedule (Schedule IV of this Agreement). Any exercise by the Board under this Article shall not entitle the SP to delay or withhold provision of the Services.
- e. The SP shall pay all their sub-contractors in a timely fashion in accordance with a mechanism, which will not prejudice the objective of Project.
- f. If any amount is due and payable by the SP to Board, the same shall be recoverable as arrears of land revenue, in addition to other avenues legally available under this agreement.

6. SCHEDULE VI : TERMS OF PAYMENT SCHEDULE

- a. The Board shall not be liable to make any advance payments.
- b. The payments shall be made after the successful completion and submission of the deliverables
- c. The Payments shall be made as per the following payment milestones

<Insert the Payment milestone at the time of signing of agreement>

- d. **Event of exit of SP on expiry of full term:** SP shall handover the complete assets provided exclusively by Board for project operations including hardware, software and licenses, etc. back to the Board on SP's exit or completion of agreed project term. The handing over/ transfer shall not entitle the SP for any payments on such transfers. The Board shall retain the Performance Bank Guarantee for a period of 180 days or until identification of the replacement SP whichever is later during the Exit Management period. Subsequently, the Performance Bank Guarantee shall be released provided an agency appointed by Board will certify and Board accepts that the handing over procedure as stated in Exit Management Schedule has been duly complied with. In the event that the compliance is not completed, the Performance Bank Guarantee shall be invoked and the amount appropriated and forfeited.
- e. **Event of premature exit of SP:** In the event of premature termination of the Agreement prior to the completion of the Term by the SP, the Board shall forfeit the Performance Bank Guarantee (PBG). In such case SP shall handover the complete assets provided exclusively by Board including hardware, software and licenses to Board.
- f. Board will not pay any costs of SP's conduct of business, except the payments stated in this Schedule.
- g. There will be no payments by Board to SP to compensate for loss of business or wrong calculations. Costs of any investments to ensure SP delivery will be borne by SP.
- h. It is clarified here that there will be no payment upon handover of the Assets pursuant to the expiry or earlier termination of the Agreement.

7. SCHEDULE VII : CHANGE CONTROL NOTICE

Change Control Note		CCN Number:
Part A: Initiation		
Title:		
Originator:		
Sponsor:		
Date of Initiation:		
Details of Proposed Change		
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)		
Authorized by Board	Date:	
Name:		
Signature:		
Received by the SP	Date:	
Name:		
Signature:		
Change Control Note	CCN Number:	

Part B : Evaluation

(Identify any attachments as B1, B2, and B3 etc.)

Changes to Services, charging structure, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.

Brief Description of Solution:

Impact:

Deliverables:

Timetable:

Charges for Implementation:

(including a schedule of payments)

Other Relevant Information:

(including value-added and acceptance criteria)

Authorized by the

SP

Date:

Name:

Signature:	
Change Control Note	CCN Number :
Part C : Authority to Proceed	
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)	
Approved Rejected Requires Further Information (as Follows, or as Attachment 1 etc.)	
For Board and its nominated agencies	For the SP
Signature	Signature
Name	Name
Title	Title
Date	Date

8. SCHEDULE VIII : SCOPE OF WORK

<Fill the Scope of the work from the RFP at the time of signing the Agreement>

9. SCHEDULE IX : SERVICE LEVELS

The following Service Levels shall be adhered by the SP during the implementation and O & M of the RFID Based Access Control System.

<<Insert the SLA at the time of signing of the agreement>>

Note:

1. The Service Level measurement tool designed & developed by SP shall be tested and certified for its accuracy, reliability and completeness by a 3rd Party before it is deployed.

=====END OF THE DOCUMENT=====



Kolkata Port Trust

KOLKATA PORT TRUST

**Supply, Installation, Commissioning, and Maintenance
of RFID Systems at Kolkata Dock System, Kolkata Port
Trust.**

Request for Proposal

Annexure I: Functional Scope

Document Reference No: **Plg/165/RFID/11667**

Date: 18th April 2017.

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

Table of Contents

1.	FUNCTIONAL SCOPE:	5
1.1.	ENROLLMENT OF USERS AND ISSUANCE OF RFID CARDS:	6
1.2.	RFID BASED PASSES TO PORT EMPLOYEES AND ALL INDIVIDUALS SEEKING ENTRY INSIDE THE PORT E.G., WORKERS, DRIVERS, KHALASIS, VISITORS (GUESTS, PASSENGERS, ETC.), CONTRACTORS AND GENERAL PORT USERS (STEVEDORES, SHIPPING AGENTS, C&F) ETC.	7
1.3.	AUTOMATED ENTRY/EXIT OF VEHICLES WITH GATE BARRIERS:	7
1.4.	AUTOMATED ENTRY/EXIT OF INDIVIDUALS WITH FLAP-BARRIER/TURNSTILES.....	8
1.5.	LED VISUALS OF USERS & VEHICLES FOR CISF & GATE SECURITY	9
1.6.	AUTOMATIC VEHICLE IDENTIFICATION WITH RFID TAGS ON VEHICLE WINDSHIELD/ ANY APPROPRIATE POSITION	9
1.7.	PASS HOLDER PHOTO CAPTURING & RECORDING FOR EACH ENTRY & EXIT	9
1.8.	ONLINE WEB BASED PASS ISSUE REQUEST SYSTEM	10
1.9.	SIMPLIFIED APPROVAL SYSTEM WITH EMAIL, SMS, & MOBILE ALERTS TO SCRUTINIZER OR PORT AUTHORITY	10
1.10.	PROVISION FOR ONLINE PAYMENT GATEWAY.....	10
1.11.	MOBILE BASED OTP AUTHENTICATION	11
1.13.	HANDHELD TERMINAL (HHT) FOR MOBILE SPOT CHECKING AS WELL AS SPEEDY MOVEMENT AT THE GATES.....	12
1.14.	LIVE CONTROL ROOM FOR ROUND-THE-CLOCK MONITORING	12
1.15.	DISTRIBUTED ARCHITECTURE	12
1.16.	MASTER DATABASE	13
1.17.	ARCHIVAL & RETRIEVAL SYSTEM.....	13
1.18.	BACKUP & DISASTER RECOVERY	13
1.19.	INTEGRATION APIS.....	14
1.20.	FRONT AND BACK IMAGE CAPTURE OF THE CONTAINER.....	14
1.21.	CENTRALIZED DATA POOLING, REPORTS, INTEGRATION AND MULTIPORT INTEROPERABILITY AT IPA LEVEL	14
1.22.	RFID BASED WORK PERMITS FOR MEN AND MATERIAL.....	15
1.24.	VALIDITY OF VARIOUS RFID PERMITS/ PASSES:	16
2.	INDICATIVE PASS ISSUANCE PROCESS:	17
2.1.	THE USER PASSES ARE BROADLY CATEGORIZED INTO.....	17
2.2.	THE VEHICLE AND EQUIPMENT PASSES ARE BROADLY CATEGORIZED INTO DAILY AND YEARLY:	17
2.3.	STEPS IN ISSUING RFID PASS/ DE-TAGGING:	17
3.	PORT ACCESS CONTROL SYSTEM (PACS):	21
3.1.	HIGH LEVEL DESIGN	22
3.2.	BUSINESS PROCESSES:.....	23
3.3.	HIGH LEVEL SERVER ARCHITECTURE.....	24
3.4.	DETAILED SYSTEM ARCHITECTURE	24
3.5.	SYSTEM SOFTWARE:	26
3.6.	FUNCTIONAL ARCHITECTURE OF RFID BASED PORT ACCESS CONTROL SYSTEM:	26
3.7.	IMPLEMENTATION POINTS:	28
3.8.	GATE TYPES IN KOPT	29
3.9.	GATE FUNCTION	29
3.10.	APPLICATION TO TRACK GPS ENABLED TRACKING WITHIN PORT PREMISES	30
3.11.	DATA TRANSFER PROTOCOL.....	33

3.12.	THE SYSTEM SHOULD	33
3.13.	ADDENDUM POINTS:	34
3.14.	ADDITIONAL FUNCTIONAL REQUIREMENTS	35
3.15.	SYSTEM IMAGE STORAGE DEVICE	36
3.17.	LICENSING	36
3.18.	DATABASE MANAGEMENT SYSTEM	37
3.19.	DATA NETWORK	37
3.20.	REMOTE ACCESS	37
3.21.	HARDWARE AND SOFTWARE CONTROL SYSTEM	37
3.22.	HELP MENU	37
3.23.	SECURITY SYSTEM	37
3.24.	WORKSTATIONS MANAGEMENT	38
3.25.	INTERFACES	38
3.26.	DATA MANAGEMENT AND INTEGRITY	38
3.27.	RFID PACS MANAGER FUNCTIONS	43
3.28.	REPORT VALIDATION	45
4.	KOLKATA PORT TRUST LAYOUT	46
5.	PORT DETAILS FOR RFID PACS	47
6.	HISTORIC TRAFFIC/ PERMIT DATA:	47

1. Functional Scope:

The proposed RFID PACS will be an integrated intelligent system comprising of the following tentative subsystems and features/ functions:

- a. Enrollment of user and issuance of RFID cards to the users
- b. RFID based permits/ passes to workers, drivers, khalasis, employees, visitors (guests, passengers, etc.), contractors, hawkers on ships and port user (stevedores, shipping agents, C&F)
- c. Automated entry/exit of vehicles with Gate Barriers
- d. Automated entry/exit of individuals with flap-barrier/turnstiles
- e. LED visuals of users & vehicles for CISF & Gate Security
- f. Automatic Vehicle Identification with RFID tags on vehicle windshield
- g. Automatic License Plate Capturing System and Recording
- h. Pass holder photo capturing & recording for each entry & exit
- i. Online web based Pass Issue Request System
- j. Provision for online payment through a payment gateway
- k. Simplified Approval System with Email, SMS, & Mobile alerts to Scrutinizer
- l. Pass issuance and pass request Collection Counters/ centres
- m. OTP based Authentication
- n. Application software for GPS based Internal Tracking of Vehicle within the Port premises.
- o. RFID based port work permits for men and material
- p. Handheld Terminal for Mobile Spot Checking, as well as speedy movement at the gates
- q. Live Control Room for Round-the-clock Monitoring
- r. Distributed Architecture
- s. High Availability Master Database
- t. Archival & Retrieval System

- u. Backup & DR
- v. Integration APIs
- w. Kiosk based Automatic RFID Pass Renewal System
- x. Offline image processing and anomaly alerts with matching and comprehensive results
- y. Supply of required hardware networking for successful installation and commissioning
- z. Centralized data pooling, reporting, integration and multiport interoperability at IPA level

1.1. Enrolment of Users and Issuance of RFID Cards:

- Service provider shall carry-out a one-time user enrolment process for those users who wish to procure a permanent RFID Card
- Service provider shall make use of the existing master data of users for issuing the Permanent RFID Cards. The legacy data shall be migrated into the new system.
- Service provider shall carry a one-time registration/ enrolment process for all users
- New user registration may done at the registration counters.
- Service Provider shall collect the primary information that includes particulars with respect to the persons/vehicle which would act as a master data.
- Service Provider shall issue RFID cards to the users after collecting the requisite fee for the issuance of RFID card/after getting the approval from the KoPT Officials.
- Service Provider shall issue the high quality cards with permanent print on the card with photo and other details as specified by KoPT Officials.
- Service Provider shall setup additional centres depending on the rush at the counters and shall issue the passes.
- Service Provider shall make the different options of collection of primary information. The options include through portal, from the sponsors, from the existing applications etc.
- The issued card shall have a life of at least 7 years and shall be replaced in case

the card becomes dysfunctional within 7 years from the date of issuance of card to the users

- There shall be option of collection of information in bulk from the various sponsors and issuance of RFID Cards to the users.

1.2. RFID based passes to Port employees and all individuals seeking entry inside the port e.g., workers, drivers, khalasis, , visitors (guests, passengers, etc.), contractors and general port users (stevedores, shipping agents, C&F) etc.

- RFID Passes will be issued to **all individuals seeking entry inside the port including Port employees..**
- ID cards issued to Port employees (both Permanent and Contractual) are colour coded for easy identification of their class. RFID permits to be issued to Port employees should also be following the same colour coding pattern including details like Name, photograph, accessible area, duration, etc. as the RFID permit/pass would eventually replace the existing ID cards for attendance management. Service Provider should consult the KoPT authorities for understanding the process **including details to be made available on RFID pass/ permit before issuance of such passes.**
 - Port cannot be accessed without an RFID card and valid permit.
 - Each RFID card will be unique identified with Chip Serial Number (CSN) and with a system generated unique ID for each person/vehicle
 - The data in the RFID card will be encrypted
 - The RFID pass will determine the time limit and the area that the pass holder can access. RFID pass will also have permitted area short-codes for easy identification by CISF/ PSO based on which the user would be allowed entry to such area(s). Service Provider should consult the Port authorities for understanding the process in detail.

1.3. Automated entry/exit of vehicles with Gate Barriers:

- Vehicles with authorized passes will be allowed entry by automatic/ controlled opening of the gate barrier when the vehicle permit and driver permit are flashed on the RFID reader

- As the driver's cabin height of heavy vehicles and light motor vehicles etc. are different, placement of RFID card reader(s) needs to be made such that flashing of card at the reader is easy for all types of vehicle drivers.
- The Gate barrier will open under 3-4 seconds from closed state
- The Gate barrier will also have sensors to ensure that it does not fall on standing vehicle
- Presently, each of the Port gate has a physical gate which would act as the 1st point of check by CISF/ PSO for users/ vehicles accessing the port premises. On preliminary verification, the physical gate would be opened for the vehicle to come inside and wait before the boom barrier for further verification of permit/ documents and cargo/ containers. Hence, the boom barrier is to be placed inside the physical gate. Once detailed verification of permit/ documents and cargo/ container is done, the boom barrier should open. In all ideal situation and depending on space availability at each gate, a boom barrier is to be erected in such a manner that 1-2 cargo/ container vehicles can be accommodated between the physical gate and boom barrier. Service Provider should consult the KoPT authorities for understanding the process in detail.
- Boom barrier, when in non-operational state, if struck by Trailer / other equipment, should have the feature / facility to move/swing horizontally to prevent breakage of the Boom Barrier
- Each vehicle lane will have bullet cameras for monitoring purpose
- 3 cameras will be installed in each vehicle lane for capturing images/ video of driver and front & back of the vehicle
- Due to the lack of space at the gates, some of the gates are used both for the entry and exit through a single lane and at some of the gates one either entry or exit.
- Service Provider should mount cameras in such a manner or make provisions at each gate such that it can withstand vibrations, high speed winds, rains, dust, etc.

1.4. Automated entry/exit of individuals with flap-barrier/turnstiles

- Authorized Pass holders are allowed access into the Port gates through flap-barrier / turnstiles
- On successful authentication of the RFID pass, the flap-barrier/ turnstile will

retrieve/ open instantaneously

- The flap-barriers/turnstile will restrict multiple person entry on a single pass
- A single 360 degree view camera for each pedestrian gate for monitoring entry and exit lanes simultaneously.
- The 360 degree camera should be positioned at such a location that monitoring of entry as well as exit of pedestrians is possible.
- Service Provider should mount cameras in such a manner or make provisions at each gate such that it can withstand vibrations, high speed winds, rains, dust, etc.

1.5. LED visuals of users & vehicles for CISF & Gate Security

- CISF/ PSO personnel standing at the gate will see authorized person & vehicle image on the PC display screen
- If an expired pass or a blocked pass is flashed on the RFID Access Control readers then the LED display will immediately indicate such unauthorized access to the CISF/ PSO officials. In such scenario, the boom barrier/ flap barrier/ turnstile should not open.
- LED displays should be appropriately placed/ mounted such that visibility is not hampered due to sunlight, height, etc. for which necessary provision needs to be done while placement of LED display.

1.6. Automatic Vehicle Identification with RFID tags on vehicle windshield/ any appropriate position

- All temporary & permanent vehicles using the Port will be given an RFID cards which can be fixed on windshield or placed at an appropriate position
- Vehicle & owner identification details will be recorded in the RFID database
- The vehicles entry/exit and the movement details will be recorded for security purposes

1.7. Pass holder photo capturing & recording for each entry & exit

- For each entry and exit into & out of the Port Gates, the time as well as photo image of the RFID pass holder will be captured

- The captured image is stored along with the timestamp, gate, & lane entry information
- Any attempt by unauthenticated attempts will also be recorded with photo image
- For capturing the image/ photo of the vehicle's driver, camera would be mounted at an appropriate place and height.

1.8. Online web based Pass Issue Request System

- Pass Issue request can be placed by registered firms from the comfort of their office
- Using an OTP key, they will be able to login to the system and place a request
- On approval (after physical verification of original supporting documents) by the concerned port authority, the sponsor/ user can collect the RFID permit card(s) from the issuance counter
- Sponsor can either request for bulk permit through a flat file or through a pre-defined format.
- Service Provider should integrate a suitable SMS gateway which shall cater to the present as well as future needs of the project.

1.9. Simplified Approval System with Email, SMS, & Mobile alerts to Scrutinizer or Port Authority

- Pass Issue request placed online by registered companies can be accessed by the Port Authority through Port portal
- The request placed by companies will also have option of alert by email, SMS, mobile alert
- As per the Port policy, the system can(may) also be configured to set the policy framework for pass issue

1.10. Provision for online payment gateway

- Online payment gateway option will be provided for Port users to make payment directly to the Port for pass issue and other related activities
- The Port users should be able to make the payment from any bank of their convenience

- Net banking, Debit card, Credit card, etc. will be made available.
- Transaction charges for using payment gateway should be displayed/ informed to the user before processing of payment for user's information.
- Amount collected online should be settled with KoPT on a T + 1 basis or as per requirement from KoPT. The amount shall be settled to the bank account indicated by Port authorities.
- In case where payment from the user is debited but payment confirmation is not received, the payment gateway should refund the complete amount to the user's bank account from which the amount was debited.
- In case of multiple debits from the user's bank account, payment gateway should refund such extra amount debited back to the user's bank account.
- Reconciliation statement for all transactions/ settlements should be provided/ made available in the MIS for verification by the Port authorities.
- KoPT will pay to the ePayment service provider, if any charges are to be paid to ePayment Service Provider.

1.11. Mobile based OTP Authentication

- The access to Port Access Control System will be highly secured with a mobile based OTP authentication for key processes.
- All users including CFS/ICDs, Authorized Pass Issue Centers, Registered Companies, etc. will access the system after keying in OTP based authentication key. OTP should be valid for a particular session or process.
- Service Provider should integrate a suitable SMS gateway which shall cater to the present as well as future needs of the project.

1.12. Development of application for the GPS based vehicle tracking system.

The application should have essential features as follows:

- Application should, on a real-time basis, track and monitor the movement of vehicles within port premises
- Location of vehicles will be displayed on the application using GIS maps for tracking
- Alert/ notification will be generated for un-authorized activities like over stay,

vehicle moving into restricted zones, etc.

- Highlight congestion areas for authorities to take corrective measures
- The system should also be integrated with the application that is going to be deployed by the Kolkata Police for tracking the vehicles outside the port area.

1.13. Handheld Terminal (HHT) for Mobile Spot Checking as well as speedy movement at the gates

- CISF and Port Authorized personnel will be provided with HHT terminal which will be connected via Wi-Fi/GSM /Ethernet to Port Access Control Database.
- Service Provider to create Wi-fi connectivity near all such locations where HHTs are to be used by officials
- Spot checks can be carried out by reading the RFID passes of users and RFID tags on vehicle
- In case of congestion at the gates, HHT can double up as authentication device for faster movement of traffic

1.14. Live Control Room for Round-the-clock Monitoring

- Control room will be established by the Service Provider to monitor the gates 24/7
- Visual view of traffic position at the gates will be displayed
- Unauthorized access or anomalous movement will be highlighted
- Dashboard display of various parameters with real-time updates

1.15. Distributed Architecture

- The system will be highly distributed for better performance and decentralized activities
- The high level of Gate Automation demands that each gate be installed with a local server with an instance of data replication
- The server at each gate will be connected to a Central Server in the Data centre
- The Central Server should be of a high-end configuration to handle transactions/online requests from CFS/ICDs, Authorized Centers, etc.

- The Central Servers of all Major Ports will be connected to Master Server in IPA for which the provision needs to be made by the Service Provider

1.16. Master Database

- Master database with information on all users, vehicles, policies, etc. with active fail over to be configured
- Master Database should be robust to support large scale online requests & approvals and under no circumstances due to transaction load, the server/database should lag.
- Mirroring of Master Database will be implemented
- Replication of Master tables will be available at the Gates & Pass Issue Sections
- Existing master data that is in use currently by the existing port applications shall be migrated into the PACS system

1.17. Archival & Retrieval System

- The transaction data generated by the actions such as RFID pass issue, gate authentication, image capturing, vehicle identification, etc. will be available in the active database for a specific period
- The data is then rolled over to active archival system which will have capacity to hold data for 5 years.
- The archival data should be in multiple copies with adequate back ups
- Archival data should be actively searchable and available for retrieval anytime

1.18. Backup & Disaster Recovery

- Port Access Control Software will have real time fail over as well as DR server
- DR Server will be located separately from Central/ main/ primary Server. Main server will be setup at Subhash bhawan, KoPT, Kolkata
- Service Provider needs to establish a Disaster Recovery centre at the Kolkata Port Trust Headquarters at 15, Strands Road, Kolkata.
- DR Server will have instance of Master Data that is not any older than 2hours from the live data server

1.19. Integration APIs

- Seamless integration and Multi-level APIs will be provided by PACS supplier/ Service Provider for integration with other systems or legacy systems already existing or proposed ERP solution, solutions from other departments, etc. in KoPT.
- Standard XML & Web Services will be available
- Data format and communication protocol will be open for future integrations

1.20. Front and back image capture of the container

- Cameras are to be mounted for capturing front and back of the container/ vehicle
- An additional camera will be mounted at an appropriate place and height for capturing the image/ photo of the vehicle driver.
- Once a vehicle loaded with the container arrives at the gates, the cameras will capture the image of the container from front and back along with driver's image using the 3rd camera.
- Back side Camera should cover the back of vehicle including the vehicle number
- The picture analysis tool of the system should be able to analyse the image and identify simple situations like the door of the container is open/not closed properly, the container is broken, etc.

1.21. Centralized data pooling, reports, integration and multi port interoperability at IPA level

- The data generated by the transaction and activities at each port needs to be centrally pooled in a comprehensive database
- A comprehensive Management information systems (MIS) needs to be built for benefits of Ministry Of Shipping (MOS), Kolkata Port Trust and IPA authorities
- Provision should be available for generating ad-hoc reports based on requirements
- Integration and interoperability at central level with system of different authorities such as Kolkata Police, NIC, NIA, UIDAI, ICDs, Customs, Terminals,

Private Ports, PSUs, Government of India Institutions, and State Government Institutions etc. should be enabled

- Seamless interoperability of systems across the major Ports
- Integration and seamless interoperability between major Ports and nearby small Ports and Terminals

1.22. RFID based work permits for men and material

- RFID based work permits to men and material to execute contract works to all contractors to enter work area with authorized material as per the work order/agreement entered/issued by KoPT till validity of order/agreement.
- The Port area could be broadly classified into following where entry would be required which may be revised from time to time:
 - a) NSD
 - b) NSDD
 - c) NSD LOCK
 - d) KPD – I
 - e) KPDD
 - f) KPD LOCK
 - g) KPD-II
 - h) PWBB
- Also, under the ISPS Plan, certain areas within the Certified Docks are deemed as restricted and entry is accordingly regulated. RFID permits/ cards are also to be superscribed accordingly.
- Presently, entry/ access to Port area is managed through issuance of permit generated using integrated application software developed at seven (7) permit generating counters in different offices of KDS which includes Budge Budge also. Photo enabled permits are generated through this system and printed. Verification is carried out by CISF/ PSO personnel at designated gates of KDS, KoPT.

1.23. Types of Port Entry Permits:

- There are different types of passes issued by the Port to administer physical

access of persons and vehicles to Port limits. There are two types of passes:

1. **Term permits:** Permanent permits/ passes are directly printed on the cards.
 2. **Daily permits:** Temporary passes are used for the one time visitors.
- The Passes are usually issued for a limited period (Non KoPT employees)and are called as:
 - a. Daily
 - b. Monthly
 - c. Yearly
 - d. Biannual

1.24. Validity of various RFID permits/ passes:

- Permanent RFID permits would be issued to all employees of KoPT having validity of five (5) years. However, passes issued to contractual employees would be valid for a period of maximum 1 (one) year or the specific period of contract.
- Biennial permits to be issued to the Port Users would be valid for a period of two years
- RFID based permits to be issued to man and vehicles on daily basis which will be valid for twelve hours and twenty four hours respectively, should allow multiple entry/exit during the validity period.
- Free RFID permits to be issued:
 - To all regular KoPT employees and contractual persons engaged directly by KoPT

1.25. Construction of temporary cabin structures for CISF/ PSO officials at gates:

- Build and erect a shock proof, weather proof and thermal resistant pre-fabricated cabins for the CISF/ PSO officials at the gates
- Structure should be strong enough to hold 32" LED displays, ACs, etc.
- Cabin should accommodate at least 2 people comfortably including space for tables, chairs, PC
- Cabin's height should be such that the official sitting inside the cabin should comfortably see the inside of vehicle's driver cabin including driver for

inspection.

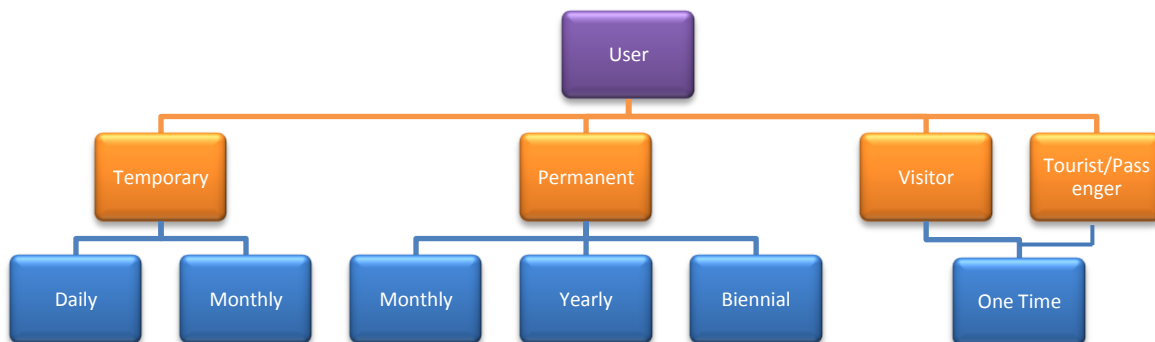
- Service Provider should provide AC, power connection, lights at all the cabins.
- Raw power will be provided by the Port and the cabling till the cabins shall be in the scope of Service Provider.
- Secondary power backup at cabins is in the scope of Service Provider

2. Indicative Pass Issuance Process:

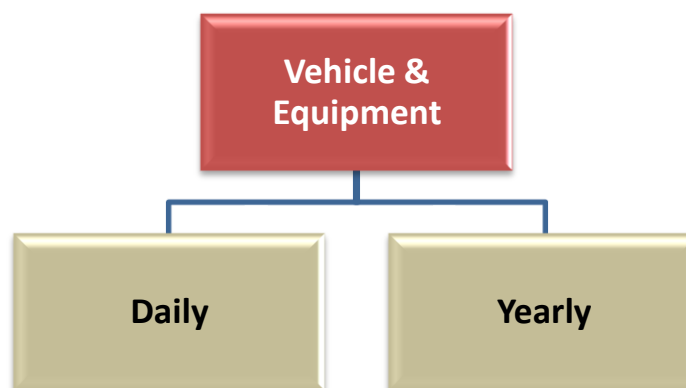
Passes are issued for following:

- a) For User
- b) For Vehicle

2.1. The user passes are broadly categorized into



2.2. The vehicle and equipment passes are broadly categorized into daily and yearly:



2.3. Steps in issuing RFID pass/ de-tagging:

Steps involved in issuing the passes/ permits to the port users, vehicles and materials, for a controlled entry/ exit within the port premises and movements happening in the port area.

- For every pass/ permit issued, there will be a permanent RFID card with unique

number which is helpful to identify and differentiate every port user. The unique number is called as Pass generation Number (PGN)

- The company or the organization will have the PGN number(s) which can be generated by the digital key.
- The users, with the help of this PGN, can request for the pass anywhere like pass counter or any other place as indicated by Port authorities.
- The pass/ permit shall consist of all the required information of the users/ vehicle/ material that would be necessary for identification and verification by CISF/ PSO.
- Details like user photograph, name, ID details, permitted area, vehicle number, type of vehicles, material name, destination, etc. are a few details that would be printed directly on user/ vehicle/ material RFID pass/ cards.
- When the user/ vehicle/ container passes through the gates, they flash the RFID card/pass and the details are displayed on the LCD present at the gate.
- Simultaneously, user picture is captured, the vehicle number plate is captured, and also the front and back image of the container is captured.
- In case of trucks & trailers, the license plate is also captured along with RFID tag reading
- The passes to the users, vehicles, drivers, cleaners, containers etc. are issued on temporary or permanent basis depending upon the type of vehicle and the type of user with direct printing on the card itself. Such permits are non-transferable, and shall be returned on expiry/damaged.

Note: This process flow is indicative only. Service Provider/ System Integrator needs to study and understand the actual process or workflow of the Port and finalize the modalities in consultation with Port authorities/ CISF/Customs/Traffic officials.

- **Daily pass issuance and authentication process: (indicative only)**

- The users have to first register themselves at the port office by providing their details and purpose of work in the port, on their company's letter head (optional) and purchase a permanent RFID card having a permanent RFID Tag No. which needs to be printed on the face of the card.

- After all individuals, vehicles and equipment are issued with permanent RFID Tags the same will be used for issuance of permits against requisition by specific companies only.
- At present there are two basic types of permits for (i) individual, (ii) vehicles and (iii) equipment and they are
 - Term permits
 - Daily permits
- For term permits, each RFID Tag for the three categories mentioned above can be activated for the desired term on verification and collection of requisite fees.
- For daily permits the RFID tags for the three categories mentioned above can be activated for a desired zone and desired time slot after approval by Traffic Department.
- At present, for issuance of daily permits there are certain companies which can procure unlimited number of individual permits per day without any specific approval from KoPT. They have earned this status based on their past procurement of certain number of permits per day or category of company (e.g., Steamer agent even if new can procure any number of permits without specific numerical approval).
- For other case approval is given covering a specific period and specific number of permits per day and no separate daily approval is required as long as the procurement does not exceed the daily limit set at the time of giving approval.
- This is a broad guideline and detailed procedure will be shared with the appointed vendor at the time of system integration.
- When the user flashes the card at the Port gates, the data including the picture stored in the RFID database against the 8 digit unique code are displayed on the LCD screen present in the CISF office/ booth at the gate. A separate real-time picture of the user is taken by the camera setup at the gate for verification by CISF/ PSO. The data printed on the RFID card may also be verified simultaneously.
- On successful verification/ authentication, the turnstile/ flap barrier opens and user is allowed inside port premise or else the entry access is denied
- If the card is lost, following activities will have to be carried out by the user for

getting a replacement card:

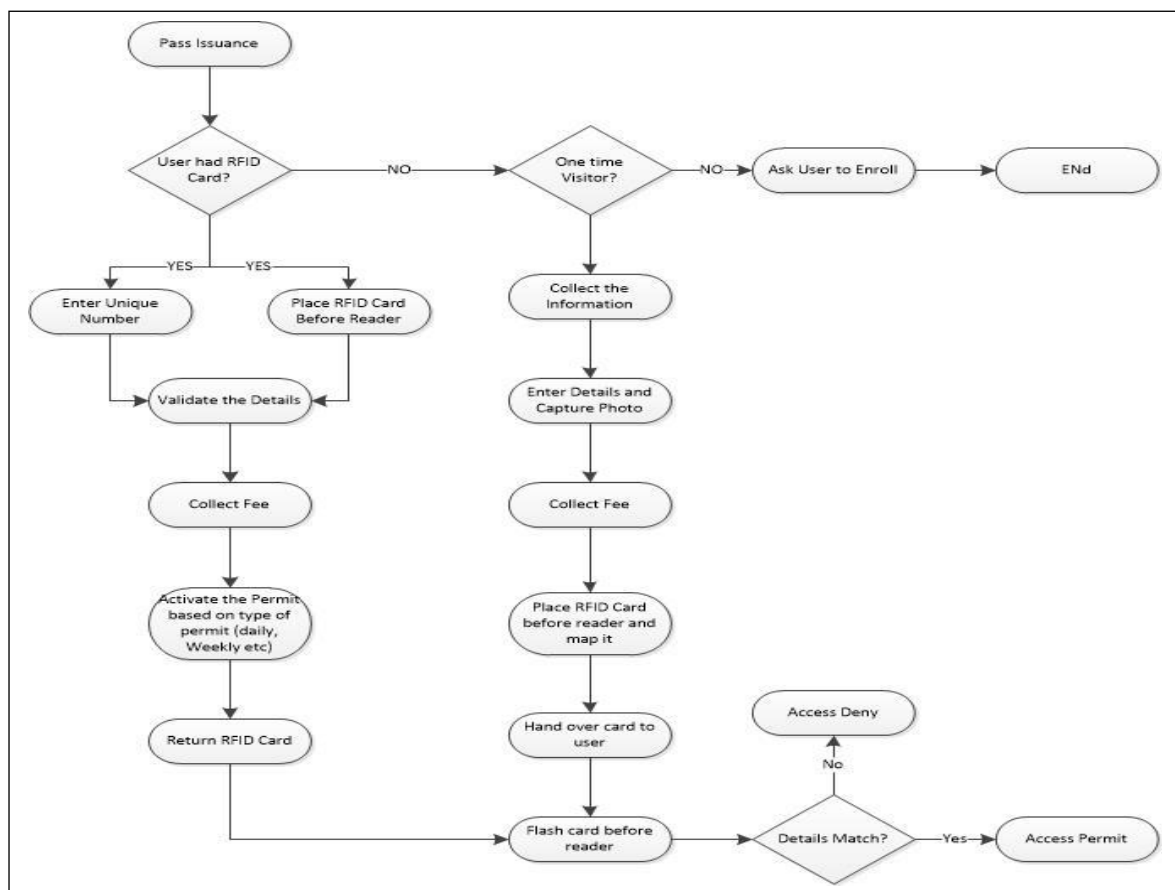
- File an FIR and submit a copy to the Port authorities
- by giving old unique authentication number
- By making the payment for the new/ replacement RFID card.

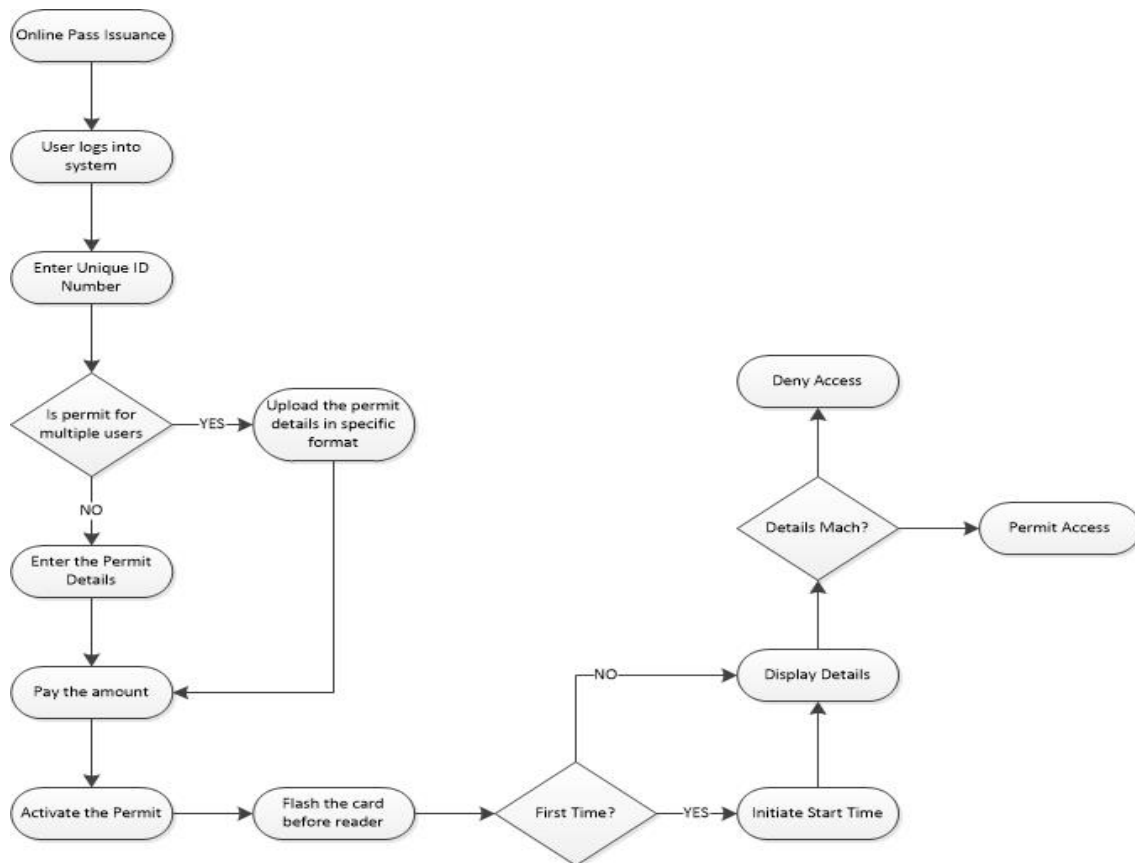
• **Permanent pass issue process (Employees)(Indicative Process)**

- The users have to first register themselves at the port office.

To register, employee details will be captured from existing database and fresh high resolution photograph taken for printing / preparation of RFID Cards. The Service Provider will consult KoPT, before printing of permanent cards, for the correctness of data.

Pass Issuance at Counter





- Simultaneously, the RFID card attached to the vehicle is also read by the RFID reader.
- If the authentication is successful, the boom barrier opens and both the driver and vehicle are allowed into the port, or else the entry/ access is denied

3. Port Access Control System (PACS):

Design, Implement, and Maintain application software titled “Port Access Control System (PACS)” for automating the business processes associated with physical access control to Port premises. The application software to have capabilities such as:

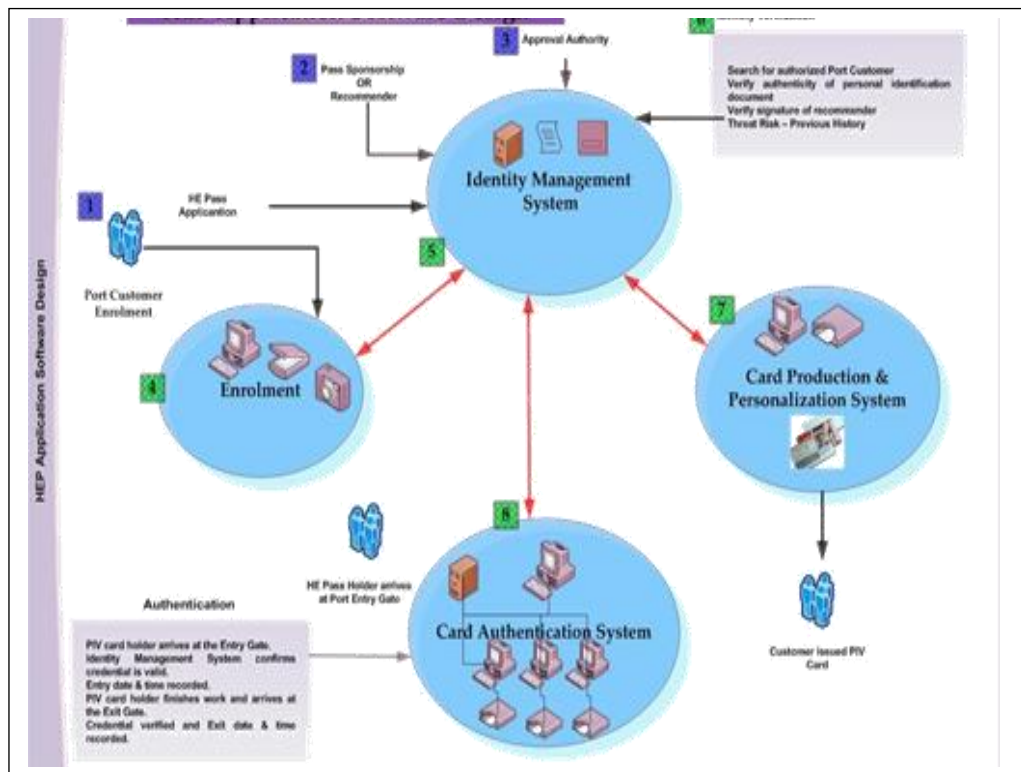
- Multi-user and multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations
- Should Support:
 - Enrolment and authentication:
 - Pass Verification
 - Expiration date check, Blacklisting and its management
 - Digital photo display/check,
 - Validate signature of authorizer / recommender etc.,

- Electronic Payment collection

- Graphical user interface to show pull-down menus and a menu tree format that complies with interface guidelines of Microsoft Windows operating system.
- Real time tracking and monitoring of entry / exit of vehicles to Port through GPS technology.
- System license shall be for the entire system and shall include capability for future additions that are within the indicated system size limits specified in this Section
- Systems shall have open architecture that allows importing and exporting of data and interfacing with other systems.
- Accountability of system components - audit trail.
- System Administration of the Application including Access controls for access to various modules
- Operator login and access shall be via integrated smart card reader and password protection.
- Interactive Reporting: It should be equipped with suitable MIS for enabling Port Management to get business information as well as monitor the system. The application software to be customized to include all business rules applicable to issue of Passes in KoPT.
- Information Transfer: Transfer transaction information on daily, monthly and yearly basis to port information system in mutually agreed format.
- CFS & Bulk Cargo should be able to issue passes by login into the system. The system should allow printing of only authorized port users after authentication.
- Information & software interface with third parties such as CFS, Security Agencies, etc.
- Server reconciled with the payment collected.

3.1. High Level Design

A typical Physical Access Control Software design is given in the diagram below:



3.2. Business Processes:

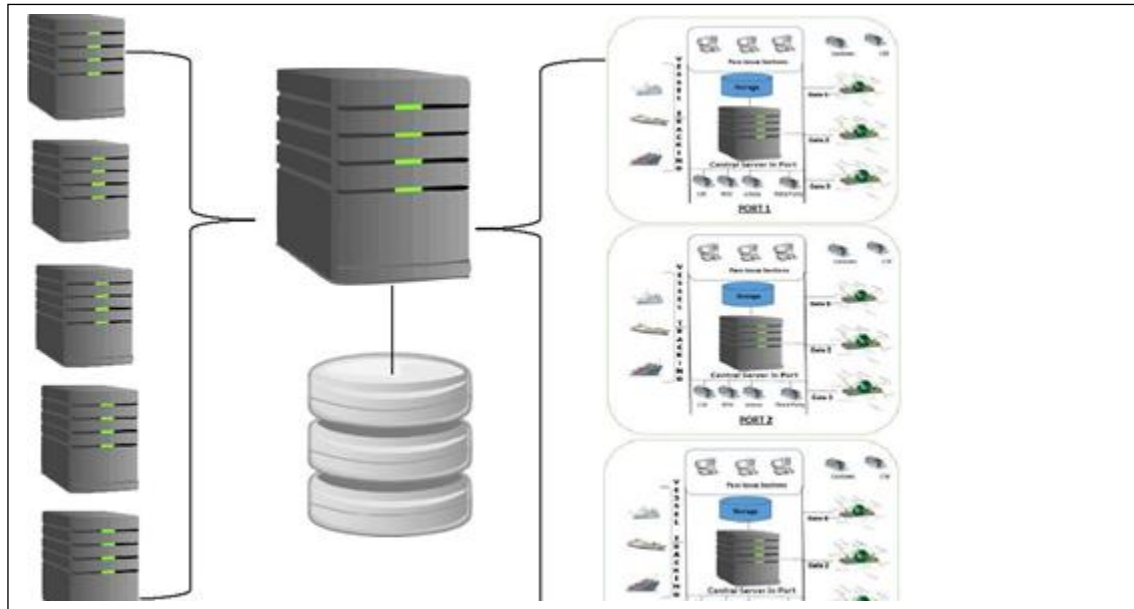
The RFID based Port Access Control System should by design fulfill the business rules defined in KoPT's organization policy & procedures on "Physical Access Control to Port Limits".

- The business processes associated with same are detailed and major processes are listed below for quick reference. Please refer to the indicative process mentioned under Clause 2.3 Daily pass issuance and authentication process (indicative only)
 - Discretionary Access Control Model based on Port's organization policy & procedures on "Physical Access Control to Port Limits".
 - Payment Gateways – Electronic (Credit / Debit card / Net banking enabled cum Cash counters.)
 - Smart card printing and management
 - Identification and Authentication of Passes at Port Gates, Monitor Track and Record traffic at Port Entry Gates.
 - Information & software interface with third parties such as Kolkata Police, CFS, Security Agencies, etc.
 - Information Exchange: Provision to transfer information electronically to the Port Information System through the network connectivity and the proposed

RFID based vehicle tracking system by Kolkata Police.

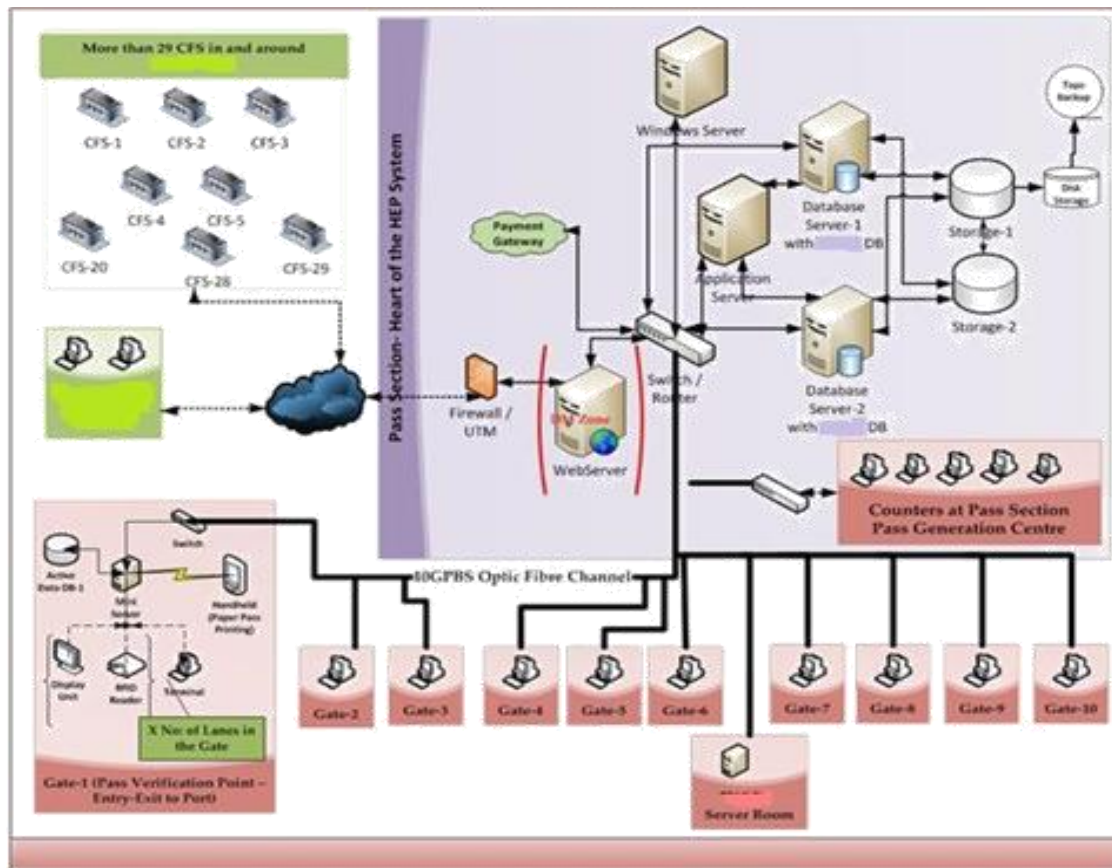
- The detailed specifications of the Port Access Control System Software are listed under Technical Specifications Section

3.3. High Level Server Architecture



3.4. Detailed System Architecture

Supply, Install, commission and maintain hardware and system software essential for implementing the RFID based Pass System with minimum system architecture detailed below:



The minimum hardware components of the RFID PACS System are listed below: (Refer to Technical Specifications Section for detailed specifications of the hardware components)

- Date Center consisting of PACS server
- Mini Servers with capabilities to host the active passes database at the Pass Verification Centers at Each Gate.
- Storage Systems - Storage capacity of around 20 TB of data for Ten years with archival and retrieval facilities.
- Backup - Disk as well as tape backups including the licenses.
- Security components - Unified Threat Management devices and all essential security components.
- Computer Terminals
- Printers - For printing directly on passes. Heavy duty printers are essential
- Bullet cameras and 360 degree cameras
- RFID Transceivers for Vehicles

- HF RFID Transceiver for Users & Vehicle Passes
- Flap Barrier for Users
- Photo capture camera for registration counters and capturing vehicle driver/ pedestrian image
- Digital display units – LED Screens for command centre
- Handheld devices
- Database
- System Software – Systems for server, terminals, hand-held devices.

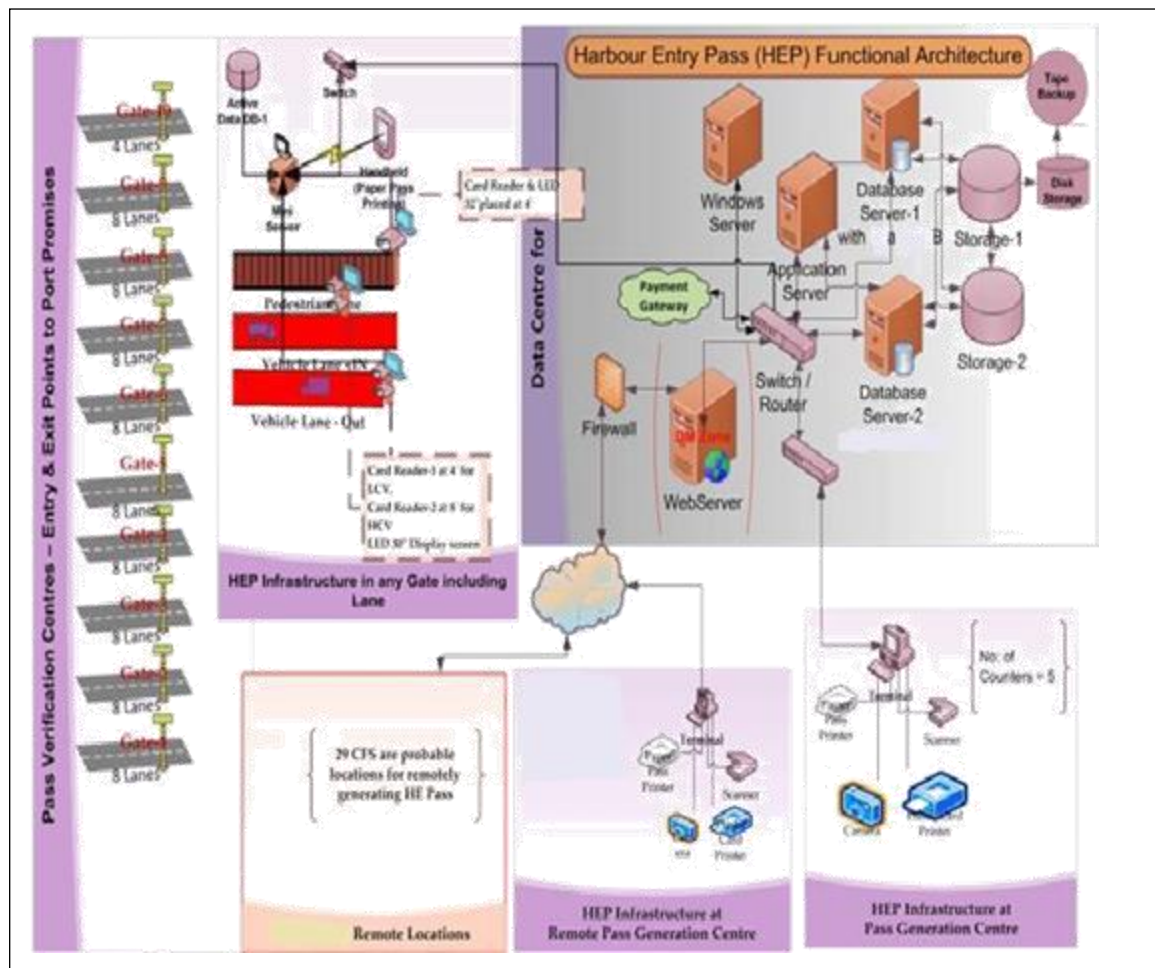
3.5. System Software:

Supply, install and maintain the system software essential for successfully implementing and operating the RFID based Port Access Control System in KoPT. The minimum system software identified are as follows:

- Server Platform:** The operating system for the server farm of the latest version. The necessary optimal licenses to be included as part of the solution.
- Database:** Supply and install the server and client database licenses with clustering facility to provide high availability and minimum Recovery Point Objective (RPO) and Recovery Time Objective (RTO).
- Front-end:** Industrial standard GUI developed in 3rd/4th generation software languages such as .Net, Java, Python, etc. The online UI should be compatible with latest browsers such as IE 9 and above, Chrome, Firefox, & Safari
- Backup / Disaster Recovery:** High availability and reliability are the hallmarks of the system. Therefore, a good backup / disaster recovery solution is essential for fulfilling the above.

3.6. Functional Architecture of RFID based Port Access Control System:

The RFID system will be operated from different locations in the port to meet the business requirements of providing physical access control to port premises.



The major location / functional categorization are as follows:

- i. **Data Center:** The data centre will be the nerve center of RFID based Access Control system and will house the server farm along with the backup components.
- ii. **Pass Generation Counters/ Centers:** Pass could be generated from any of the 10 counters location situated at Subhas Bhawan, KPD, Budge Budge and PSO, with internet connectivity, in the 1st year and any of the 03 counters at above locations from the 2nd year onwards as per requirements of KoPT.
- iii. **Pass Verification Centers:** The passes generated by the RFID system authorizes the holder, physical access to port premises and restrict access to controlled areas according to the level of authorization. The objective of this process is to verify the genuineness of the “Pass” and to capture the “In Time” / “Out Time” of the pass holder to the port.
- iv. **Entry Pass:**

Provision for issue of RFID (ISO) cards with details of user like name, ID details,

permitted area and time along with photo and other details directly printed on the front and back side with terms and conditions (revised by Port from time to time.) .

3.7. Implementation Points:

- RFID PACS should replace the existing Access control system with enhanced functionalities.
- It should encourage KoPT to use the RFID based Smart Card for multiple functionalities/ process in future like Identity Card, Access Control, Time and Attendance, canteen debit card, access key for medical card, etc.
- The System should be freely scalable with modular design and supporting Open and standardized interfaces.
- The system must be compatible with existing Contact less 4KB Mifare card (ISO 1443A/B wherever it is implemented).
- The card should be programmed based on the flow of visitor and to one or more than one gate, one or more than buildings and in some cases full permission
- There shall be bi-directional access control based retractable flap barrier gates and access-controlled gates. Provision to use Turnstile/ Tripod readers for time and attendance
- The RFID PACS shall validate the cards presented at the card readers corresponding to each Flap barrier/ Turnstile
- The System should be capable to identify , verify visitor on the basis of card
- Acceptable interval between card reads
- The Access controllers/Readers for each gate should be independent and with integrated Ethernet connection to communicate with main access server.
- Each gate shall be capable of working in the off line mode.
- The event of passage across the flap barrier without a valid card shall be detected by the access control system
- Provision for data retrieval from readers (in case of network failure) through laptop shall be made available to authorized users.
- Selectively adjust flap barrier / Gate open period to accommodate cardholders

with disabilities and other situations that require additional time for passage through the Gates / gateway.

- All the cameras and sensitive equipment should be mounted inside suitable casings to prevent entry of dust, smoke, moisture, etc.
- System to display Photographs and other details on LED monitors at Each gate during access/ exit
- The details of card holders should register on real time immediately after presenting the card. The date and time stamp should also be registered
- All special tables, queries, macros, reports, and code modules shall be open ie source code be available to Port and Port may share the same with other users who wish to make their system compatible. This will be strictly for non-commercial purpose only
- The System should be capable of generating various types of reports relating to daily attendance/movement, daily/temporary/monthly/yearly visitors reports, cards lost, blacklisted individuals/vehicles etc. and other types of reports. The contractor shall get the reports approved by the Port before installation.

3.8. Gate Types in KoPT

Broadly the gates could be

- a) 'Vehicle-only gates'
- b) Vehicle and Pedestrian Gates

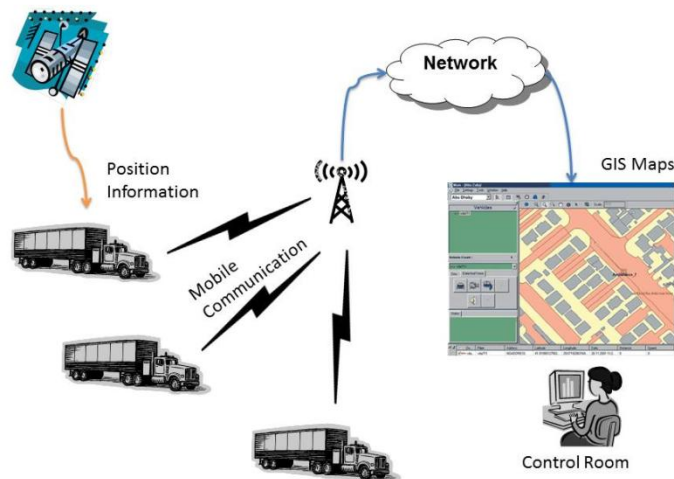
3.9. Gate Function

- a) Gate arrays shall be the normal-means of controlling entry and exit. Control shall be by means of actuating a physical barrier on recognition of a valid card at the gate.
- b) The barrier may be retractable type. The gate shall be capable of operating either normally open or normally closed.
- c) Gate array shall be providing for user throughput of at least 25 persons per minute in peak hour
- d) All gates in the array shall allow access to users on presentation of a valid card.
- e) In case of emergency Exit mode or loss of power, the access-controlled gates shall not prohibit movement of users in the direction of the emergency exit.

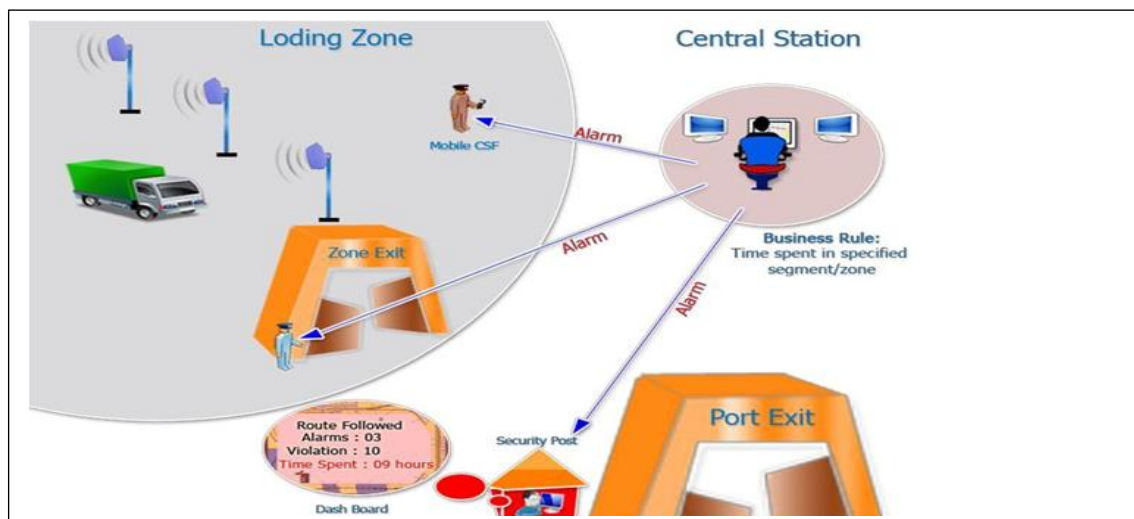
- f) Emergency switch should be provided at the gate for manual setting of all the access controlled gates to emergency mode.
- g) The Gates should be made free independently or together, Emergency Mode – All gates shall open whenever the operating mode is in emergency.
- h) Provision to open gates independently in emergency mode
- i) The design of the gate arrays should be such that the user uses the reader placed on the right hand side while passing through the gate.
- j) The design and construction of the reversible Gate shall have common component and sub systems shall be possible to convert an Entry gate to an Exit gate by changing software and display module information.
- k) The gates shall read, check and verify data on the RFID card and give passage by releasing a barrier only if the card is valid. If the RFID card is not valid the barrier shall remain closed. (Normally open swing / retractable type gates shall close).
- l) After validation of RFID card, in case no passage is detected, the flaps shall remain open for a maximum of 10 seconds. The time can be reduced or increased as per the need.
- m) Layout spacing for gates to be decided and based on the individual gate survey by the Service Provider.
- n) The positioning of the reader has to be designed in such a way to ensure users to proceed without stopping through the gate. As the driver's cabin height of heavy vehicles and light motor vehicles etc. are different, placement of RFID card reader(s) needs to be made such that flashing of card at the reader is easy for all types of drivers.

3.10. Application to track GPS enabled Tracking within Port Premises

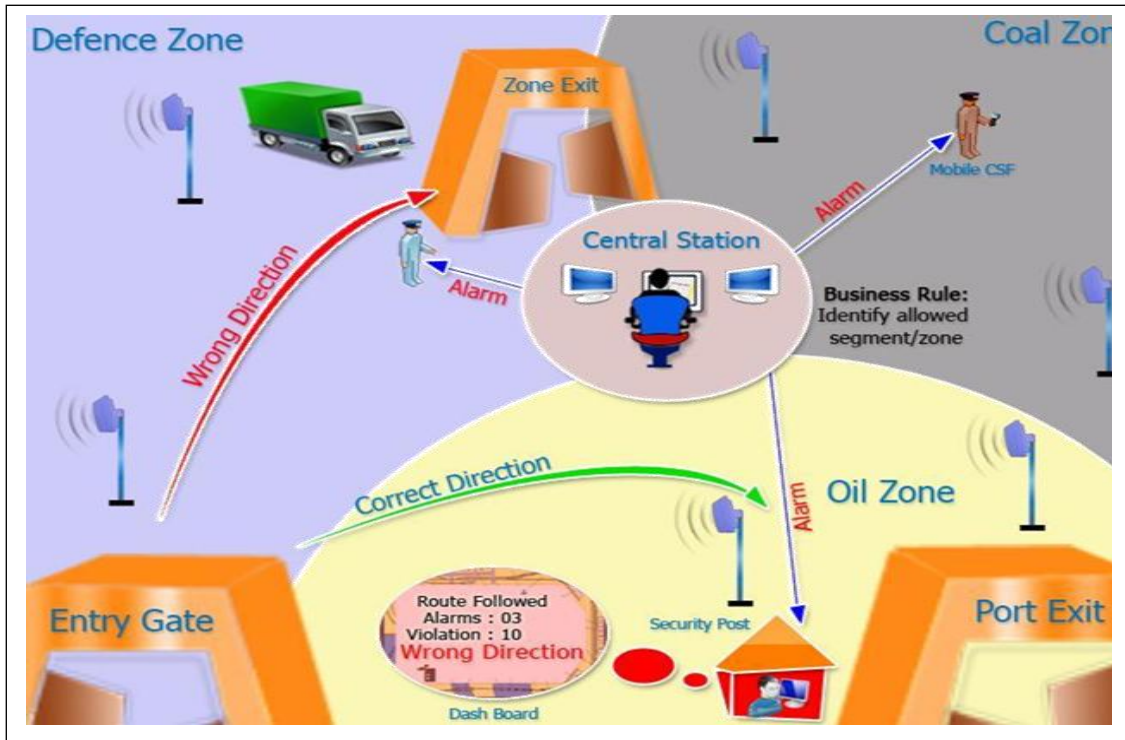
- a) Each vehicle entering the port premises should have a GPS based mobile communication device with pre-defined entry/ exit zones, accessible areas/ route maps, etc.
- b) The mobile communication number shall be registered in the system and when the vehicle enters into the port premises, the communication shall be established and shall start tracking the vehicle.
- c) The location and movement of the each vehicle will be displayed on a GIS maps in the control room.



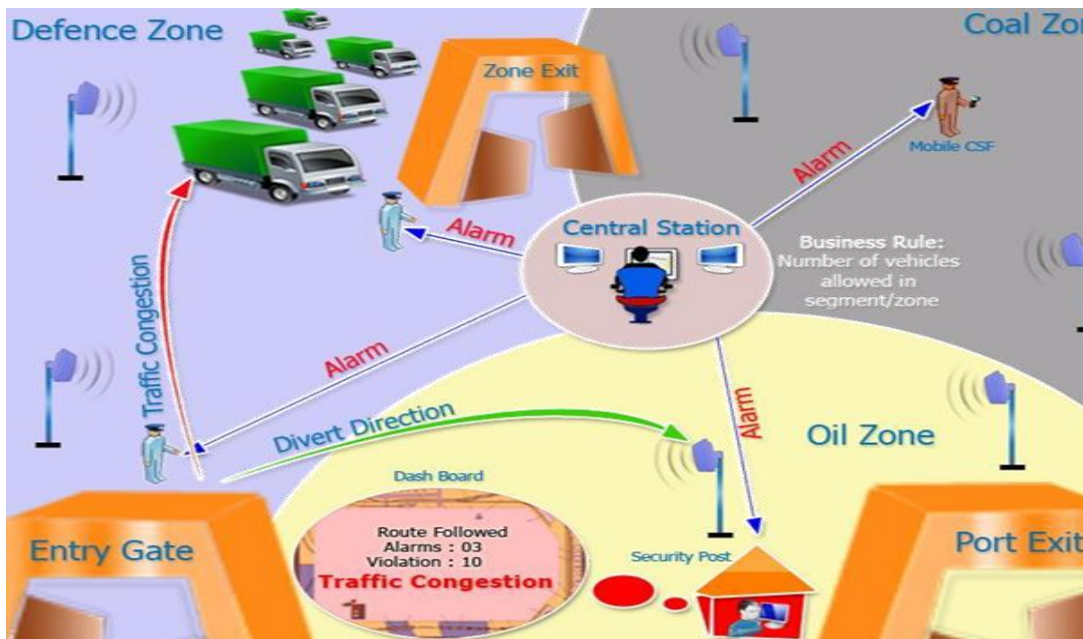
- d) If a vehicle is in a given zone in the Port for more than the specified time or in a zone which is not permitted as per the specific permit status, alarm is raised on the central dashboard; the security person can either redirect the alarm to a particular exit gate or take action on the same on his own by calling the nearest security post to check on the vehicle.
- e) This would allow CISF to locate and track the vehicle movement of vehicles within the port.



- f) If vehicle entering into a wrong segment. Alarm can be raised on the central dashboard, the security person can either redirect the alarm to a particular exit gate or take action on the same on his own by calling the nearest security post to check on the vehicle.)



- g) If number of Vehicle exceeding the limit on a given segment (Alert for possible traffic congestion). In this case system might give information like which entry gate allowed most vehicles in the congested area and other information etc. Vehicles can be directed to change to route to avoid the congestion.



3.11. Data Transfer Protocol

The RFID PACS interfaces with the IPA Server essentially includes the following transfer of data

<u>S.No</u>	<u>Item</u>	<u>Direction</u>	<u>Frequency</u>
1	Clean Transactions	KoPT RFID system pushes to the IPA server	As decided by IPA
2	Master Database	KoPT RFID to IPA	IPA scheduled
3	Violation Transactions Supported by images	KoPT RFID system pushes to the IPA server	As decided by IPA
4	Transaction reconciliation files	KoPT RFID system downloads from the IPA server	As decided by IPA
5	Blacklist update	KoPT RFID system downloads & uploads from/to the IPA Server	As decided by IPA

Table 2 Data transfer between KoPT RFID system and IPA Server

3.12. The System should

- a) Validate each transaction for completeness (e.g. possessing all the related information like Tag ID, Vehicle class RFID)
- b) Check for duplicate transactions (e.g. the same tag cannot be used in the same direction within a specified duration at the same Port)
- c) Support generation of a wide variety of reports as given below but not limited to:
 - (a) Revenue reports
 - (b) Traffic reports
 - (c) Daily / Weekly / monthly reconciliation reports
 - (d) Violation reports

- (e) Equipment availability reports
- (f) and more
- d) be highly secure
 - (a) Login feature for accessing the System
 - (b) Access the system based on roles definition
 - (c) Storage of sensitive data like passwords in encryption mode
 - (d) Use of Complicated passwords: password should be more than 6 characters and should have at least one numeric character.
 - (e) Automatic logging of every sensitive action in the system.
 - (f) OTP based authentication key
- e) Scalability:
 - (a) The System / Servers shall be scalable to support increase in Tag Users / RFID transactions in future.

3.13. Addendum Points:

- a) Raw electrical power from the Port will be provided at a single location at each site for system operation. The successful bidder shall make his own arrangements to provide a 24 X 7 uninterrupted power supply to the proposed system in order to meet the SLA conditions described in this document. This may include a UPS of suitable capacity supported by a Diesel Generator set including fuel
- b) For any incidental costs like civil / electrical related works at the sites, the successful bidder shall assess the quantum of work and the same shall be quoted under "ANY OTHER ITEM" item of BOQ or club the cost with the relevant line item where such works would be required.
- c) The responsibility of major civil/electrical/networking works if required for the RFID PACS is not in the scope of this tender
- d) The successful bidder shall make his own arrangement for material storage
- e) The successful bidder shall make his own accommodation for his workers, if necessary
- f) The system should be able to interface & interoperate with wide variety of

systems. As security & safety is a key requirement in Port Operations, the Contractor's personnel, as part of the contract, shall in the course of performing their duties, keep a round-the-clock watch on the general security & safety of RFID Operations at the Port and initiate appropriate prompt alerts & actions on any untoward incident(s).

- g) The no. of units in the given BOM is indicative only. KoPT will not be responsible for any compensation, in case of any increase or decrease in the numbers. Bidders are encouraged to make their own assessment based on their own site visit and experience. KoPT reserves the right to allocate/change BOQ, as it may deem fit.

3.14. Additional Functional Requirements

The minimum required fields are as follows:

- a. Transaction Sequence Number
 - b. Chip Serial Number/Unique ID
 - c. Date
 - d. Time
 - e. Gate
 - f. Lane
 - g. Allowed/Denied
 - h. Privileges Granted with short codes wherever applicable
 - i. Colour codes
 - j. Person Image/Vehicle Image
 - k. Vehicle Tag
 - l. Vehicle License Plate &Class
 - m. Container Image ID
 - n. Image (in case of a violation transaction)
 - o. Shift
 - p. Security Person Id at the gate
- a) The transaction time shall be the time when an RFID Pass or Tag is detected at transaction area.
- b) This device shall be connected with the server through a USB port and shall be of

any reputed make with service and support availability in India and of RAID configuration.

- c) This device shall contain all the archived data on a monthly basis after the 10 year retention period. It shall be possible to restore a COPY of the archived data for selected months to the live database as and when required and can be removed immediately after it serves its purpose. Since, this data is to be utilized only for reporting purposes, all the transaction and related data shall be retained in the Archive until the end of contract period

3.15. System Image Storage Device

- a) A separate secure external HDD shall be supplied for storing the ghost images of all fresh installation of Gate, AVI controller, and other modules, local RFID Server, etc.
- b) After restoring this ghost image, it shall be possible to import / configure the lane /equipment specific characteristics before normal operation of the equipment.
- c) Any data required shall be restored from the back-up device. In case of local RFID Server restoration, the current day data after backup to external storage device can be retrieved from the lanes.

3.16. System Software

- a) The system shall be in Domain environment and all workstations must connect to that domain.
- b) An additional secondary server shall be provided, which shall take over immediate charge of Primary server in case of its failure. In other words, this shall be a hot stand by to the primary server in all aspects.
- c) The specification, make, model of all the accessories of the secondary domain controller shall be same as that of the primary domain controller.

3.17. Licensing

- a) License for each server, workstation operating system, Database management system software, database maintenance software or any other software (MS-OFFICE package, Adobe, etc.) used in RFID PACS, which requires a license, shall

be provided by the Contractor in the name of the KoPT without any additional cost to the KoPT

3.18. Database Management System

- Database shall be a relational database management system.
- RFID PACS shall not have any direct database access. Data from the gate going to the database shall be through dedicated software that runs on database server.

3.19. Data Network

- The data network shall be Ethernet format. The network shall use TCP/IP protocol and the cabling shall be STP / MM OFC and it shall be compatible with all network system and equipment.
- Care shall be taken to ensure that the cable and the network switches used between two equipments shall be able to cater to the speed of the higher NIC.
- All network devices should be IPv6 compliant.

3.20. Remote Access

- Remote access shall be through a safety system as a remote connection server or firewall system. The RFID PACS network shall be compliant with the majority remote access equipment and remote access system and it shall be configured with any remote system available at site.

3.21. Hardware and Software Control System

- Hardware and Software fault logging system. This shall include all information regarding faults, downtime and repair time, imported from the three level Servers.

3.22. Help Menu

- An intuitive and interactive help system that can be activated from anywhere in the RFID PACS.

3.23. Security System

- A facility to allow the KoPT to manage users and their access levels.

- The Port RFID PACS shall at its highest level determine access to the separate modules by any employee. It shall have the facility to define the employee according to an associated level or duty, and provide a mechanism, whereby access is restricted.
- All CD R/RW/ USB slots of workstation shall be disabled and except Administrator no one shall have any right assigned to add, remove or modify any program on any of the workstations.
- Nothing other than RFID PACS and operations function shall be accessible to any level of RFID operation function. If need arises, then the user shall logout, exit the application using administrator rights.
- After this Logoff from the system the user shall login into Windows/Linux with Administrator rights and perform any required action. This is applicable for all levels of the RFID PACS.

3.24. Workstations Management

- At any time, if the purchaser wants to add additional workstations and its peripheral hardware from the system, shall be able to do so without any additional cost to the purchaser.

3.25. Interfaces

- The system shall be designed using Open interface architecture at all levels of hardware used. In future, it shall be possible for the KoPT to change any make / model of any hardware without dependency on the bidder.

3.26. Data Management and Integrity

a. Data Integrity

- The basic need for data integrity is the account closing at the administrative level. The closing process assumes that all data from the lanes has been introduced into the database.

This can be resumed to:

- a) Guarantee the data in database is complete
- b) Guarantee the data in database is correct

- This is accomplished with:
 - a) Checksum: detect errors in data
 - b) Data type sequencing: detect missing sequence
 - c) Communication sequence: this is a periodic messaging to allow detection of Communication failure
- Since, the whole RFID PACS is designed to detect and subsequently prevent misuse in any manner and collect all collectible revenues, any transaction / operation performed in any level of the KoPT RFID PACS shall be recorded in the system on detecting a definitive positive / negative confirmation only. Usage of any other irrelevant keys under such conditions shall display a warning message to use the correct keys.

b. Data Sequence

- Each message / transaction shall have its own sequential number.

c. Missing Data Detection and Resolution

- The conditions to be sure all data is in the database in a given moment are:
 - a) All message sequences received were correct (no checksum errors)
 - b) There were no jumps in message sequential number
 - c) There were no jumps in message type sequential number
 - d) The Communication sequence is being received with no gaps and small permissible delays.
 - e) The message sequence type counters into Communication sequence are in accordance with the counters received in actual messages.
- The program used to insert messages into the database keeps making the above checks. If any problem is detected, it is signalled to Port level monitoring system.
 - If any of the conditions above fail, the system signals a problem with the data on a connected workstation in graphical form i.e. for each lane by hour. The resolution of the problem is:
 - If there is a data error (message received with bad checksum or bad

data fields) the system automatically tries to read the message again.

- If data is missing, the normal way to solve this will be to make an export from local system and import in Administrative System using data import function. If the problem persists,
- The specific situation will have to be analyzed by going in details like which kind of data sequence is missing.

d. Data Import / Export, System Reports Information

- To a Microsoft Excel, Comma separated CSV, and XML compatible database file.

e. Data Backup & Restore System

- Data shall be backed up onto a removable medium on a regular basis for removal from the premises. Bidder shall submit a backup process and plan with the proposal, KoPT's agreement and approval is required before its implementation.

f. Data archiving / restore

- All data shall be transferred / appended to removable electronic media / USB based Archive Storage device at monthly intervals and stored after the expiration of the prescribed period for retention of the data on various system levels, the data may be removed from the system. The Port RFID PACS shall provide the facility to perform these functions.

g. Data Redundancy

- All transaction and incident data shall be retained duplicated and stored within the various levels of the RFID PACS such that should any level or component of that level suffer a partial or total failure, the data is not irretrievably lost to the system. In addition, it shall be possible to reconstruct and restore the data for the failed level from the stored data into its original format.
- Data retention times within the various levels shall be at least:

a)	Data		
	At Gate Level:	1 month	
b)	Port level:		
	Detailed Data:	36 months	
Activated Data on physical media archive storage			5 Years

h. Data Transfer

- No workstation / controller can be used as a router to send data to the server database; all data shall be reported directly to the server.

i. Operational functional features:

- The following functions shall be performed by the Supervisor of the operations. RFID PACS should support all the below
 - a) Data Completeness
 - b) Shift Consolidation
 - c) Day Consolidation
 - d) Month Closure
 - e) Lists Transfer Status
- The above functionalities are explained in detail below.

Data Completeness

- The Supervisor can verify the status of data transfer between the gates and workstations on an hourly basis. Wherever, the data transfer status is not OK, a separate process shall be available through which the Supervisor can re-request data transfer to correct the status.
- The Data completeness procedure shall check at least the following minimum items:
 - i. Transaction sequence jump
 - ii. Transaction sequence reset
 - iii. Gap in time (if regular data packets are not updated), etc.

- iv. The Data completeness procedure needs to be defined and a separate document shall be provided by the Supplier on how this feature is to be accomplished in the system

Day Closure

- The Day Closure option is used by the Supervisor to close each Operational day. When the Supervisor selects this option, the system shall display the current status of Operation in terms of data exchange.
- When, the supervisor closes the day, the following conditions shall be verified by the system before generation of Day Closure Report:
 - i. Data completeness
 - ii. Data transfer to Port Server completeness
- If any of the above checks fail, the system shall display an
- Alert (POP-UP) to the Supervisor to perform these pending operations before day closure.
- This procedure shall ensure that no data generated is left unattended for review / reconciliation.

Month Closure

- Month closure is performed on a monthly basis on a complete calendar month. Once, this option is selected any day pending closure shall be brought to the notice of the Supervisor. For ensuring that all data and all corrections are complete and no deconsolidation whatsoever shall be required any further, the month closure for a particular month shall be performed on the 2nd day of the subsequent month (configurable).
- Once, this operation is performed, no changes whatsoever can be made through the application to the transaction data of the corresponding month whatsoever. Deconsolidation option shall not be available and all manual overrides with respect to these transactions shall not be possible.
- Whenever, this operation is confirmed, system shall ensure that this

operation is performed after incident reporting. A warning message to this effect shall still appear for the Supervisor to ensure and confirm that the incident reporting process for the month for which month closure is being performed is already complete.

Lists Transfer Status

- In addition to the transaction data, there can be various lists related to users, media, classification, configuration, parameters etc. which shall be transferred between servers.
- The status of all such lists shall be displayed on selection of this option. The status shall include the following:
 - i. Name of the list
 - ii. Version of current transfer
 - iii. Version of previous transfer
 - iv. Date & time
 - v. Frequency of transfer (in HH:MM format)
 - vi. Transfer Status
- It shall be possible for the supervisor to re-request / re-transfer any failed list transfers.
- Also, all lists shall be retained in the system along with date of activation and date of expiry in addition to the version details.
- All the above listed functionalities are the core responsibilities of the Supervisor and only he / she can perform the above functions. Any user of a higher user-group though can view the actions performed by the Supervisor / current status but cannot modify anything unless explicitly so mentioned.

3.27. RFID PACS Manager Functions

- **Incident Management**
 - The Port manager can view and access all features / options of this function. However, he / she cannot perform any modifications / corrections.

- Data Completeness
- On certain conditions when the Data completeness status cannot be corrected due to false triggers, non-revenue data missing, revenue data missing, etc., an option shall be available for the Port manager to manually override such statuses in order to restore the operational flow.
- Users Management

The following are the various user groups that shall be available in the system:

Operations	Finance	System
Project Manager	Finance Manager	Administrator
RFID PACS Manager	Cashier	Maintenance
Supervisor	Traffic department officials	Pass issuance counter officials

When the user is created for the first time, an indicative list is given below:

- Name
- Address
- Date of Birth
- Contact Person
- Contact Number
- Email ID
- User ID
- Activation Date
- Valid from and upto
- The status of account and Date of creation shall be displayed against all the existing users in the system. User account can never be deleted from the system once created, as there can be operations / transactions performed by the user that exists in the database and is required for reporting purposes.
- **Administrator Functions**
 - In addition to the normal functions listed above, administrator can

perform the following operation.

- **Lists Transfer Management**
 - The administrator can manually copy the latest version of lists from the local RFID Server and restore the same in all the gates
- **Incident reporting levels**
 - The system will allow the assignment of a level of importance to each incident and also define if the incident should be acknowledged by the supervisor.
 - The system has different levels of importance that can be assigned to different types of incidents. They shall be colour coded to facilitate easy visualization by the supervisor.

3.28. Report Validation

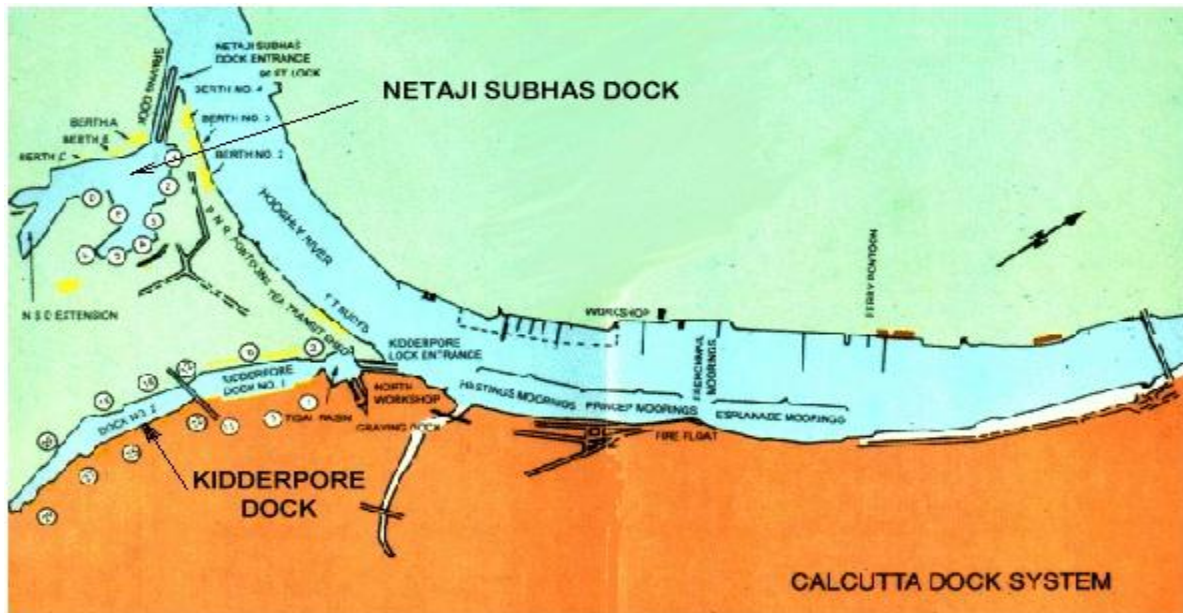
- The Port RFID system interfaces with the Central IPA essentially includes the following transfer of data

S.No	Item	Direction	Data Frequency	Data Format
1	Pass Issue Transaction Data	Port RFID PACS to Central IPA System	As decided by IPA	As decided by IPA
2	Daily Traffic Movement Data	Port RFID PACS to Central IPA System	As decided by IPA	As decided by IPA
3	Access Violations Data (including images)	Port RFID PACS to Central IPA System	As decided by IPA	As decided by IPA
4	Port blacklist data	Port RFID PACS to Central IPA System	As decided by IPA	As decided by IPA
5	MoS/IPA blacklist data	Central IPA System to Port RFID PACS	As decided by IPA	As decided by IPA
6	Port user data	Port RFID PACS to Central IPA System	As decided by IPA	As decided by IPA
7	Reconciliation Data	Central IPA System to Port RFID PACS	As decided by IPA	As decided by IPA

8	RFID PACS Status & Performance Data	Port RFID PACS to Central IPA System	As decided by IPA	As decided by IPA
---	-------------------------------------	--------------------------------------	-------------------	-------------------

Table: Data Transfer between Port RFID PACS and Central IPA System

4. Kolkata Port Trust Layout



Netaji Subhash Dock



5. Port Details for RFID PACS

Sl. No.	Details	Number
01	Total Number of Gates(NSD and KPD)	14
02	Total Number of Lanes (Vehicle & Pedestrian)	28
03	Total Number of vehicle lanes	15
04	Total number of pedestrian lanes	9
05	Total Number berths under RFID	21
06	Total Pass Issuance Counters (At Subhash Bhawan, KPD, Budge Budge and PSO)	10

6. Historic Traffic/ permitData:

Type of Permit	2013	2014	2015
Daily Man Permit	1,658,703	1,670,429	1,837,039
Daily Vehicle Permit (Lorry)	53,981	55,101	75,100
Daily Vehicle Permit (Trailer)	230,395	231,068	242,273
Daily Mobile Crane	4,689	4,753	4,812
Daily Reach Stacker	7	8	8
Daily Top Lifter	0	0	0
Daily Dumper	346	378	383
Daily Pay Loader	1,256	1,289	1,303
Daily Forklift	548	565	570
Daily Permit for Ship Personnel	0	0	0
Daily Permit for using Truck Terminal	0	0	0
Daily Free Man Permit	248,435	254,634	215,746
Monthly Man Permit	0	0	0
Quarterly Man Permit (3 months)	7,374	7,216	7,276
Biennial Man Permit	403	357	290
Annual Vehicle Permit (Trailer)	628	546	581
Annual Vehicle Permit (Lorry)	54	51	47
Annual Mobile Crane	0	0	0
Annual Reach Stacker	99	75	121
Annual Top Lifter	0	0	0
Annual Dumper	0	0	0
Annual Pay Loader	0	0	0
Annual Forklift	40	35	19
Annual Vehicle Permit (CART)	10	3	9

Type of Permit	2013	2014	2015
Daily Free Vehicle Permits	4,920	5,896	3,863
Temporary free Permits	2,307	2,231	2,114

===== END OF DOCUMENT=====

Annexure-II

S.NO	Table of Contents
1	Port Access Control Software Specifications (PACS)
2	Database
3	Access Controller
4	RFID reader
5	RFID Transceiver
6	UHF RFID card
7	HF RFID card
8	Handheld Terminal
9	Smartcard Printer
10	DC and DR
11	Port Server
12	Gate Server
13	Bullet- Digital web Camera
14	Incident Capture Camera
15	360 deg Cam
16	PC
17	Boom barrier
18	Flap barrier
19	55" LED display
20	32" LED display
21	RFID R-W
22	UPS
23	Wired Network
24	Wireless Network
25	Digital Signpad
26	CISF Cabins

PACS

Sl.NO	Functionality	Compliance	Reason for Not complying
Mandatory compliance (These are the mandatory requirements. Bidder will be disqualified if he fail to comply with these requirements)			
1	The system should be off-the-shelf (OTS) and ready to Implement in KOPI		
2	The proposed RFID based Port Access Management System should be a comprehensively ISPS compliant system.		
3	The OEM of the proposed RFID based Port Access Control System to have experience of supplying at least 5 lakh RFID tags in the last 5 years to any number of clients in any industry.		
A. Port officer Authorization Module			
4	Provision to admin access into the complete system by a Port Authority		
5	Provision to Audit every pass issued		
6	Provision to restrict pass issue permission by Port Supervisor/ Scrutinizer		
7	Provision to restrict number of passes per Company by a Port Authority		
8	Direct access to all software & database by authorized Port Authority		
9	Provision to limited access to PortSupervisor/Scrutinizers at the Gates		
10	Provision to scan activity of pass issue by each operator at any counter		
11	Provision to get summary report of all activities by operators on shift wise, daily, weekly, & monthly basis		
12	Provision to log all activities of logged in operators issuing the passes		
B. Sponsoring Company Registration has			
13	Provision to define company type		
14	Provision to register a company under one company type		
15	Provision to define category and its rules		
16	Provision to register one or more category under one Company		
17	Provision to define validity based on the license date, bank guarantee date, and documents expiry date and categories validity period		
18	Provision to define companies without any basic validity		
19	Provision for Pre-renewal		
20	Provision for renewal after expiry of registration		
21	Provision for extension of validity for Company- Category and Category on the basis of validity Provision for parameterized, Dynamic definition Provision to declare defaulter and or blacklist a category and or a company immediately or with future date		
22	Provision to declare defaulter and or blacklist all the permits under the category and or Company automatically due to default/blacklist of Company or category		
23	Provision to restore the Company and or Category separately or together along with their Permits		
24	Provision to cancel the Company/Company- Category as per rules		
25	Provision to define Maximum Validity period for the type of permit of any Category in Category Master		
26	Provision for not allowing cancellation without cancelling all permits under it or if the company is defaulted or blacklisted		
27	Provision for forcible Cancellation of a Company		
28	Provision to cancel all the permits under it automatically		
29	Provision to declare quota for various types of Permits and provision to increase/decrease quota permanently, daily or for a specific period.		
30	Provision to maintain the list of authorized signatories under company-category with Photo and Signature		
31	Provision to maintain the list of Director/Partners/Proprietors with their photo and signature		
32	Provision to define the Issuing Authority for different types of Permits		
33	User authentication should be based on OTP on the registered mobile including user-id and password		
C. Authenticated User Enrolment and Issuance of permits has			
34	Provision to enroll User – Employee biometrics, identification details, photograph.		
35	Provision to attach Scanned documents.		
36	Provision to generate uniqueness for every User		
37	Provision to retrieve information based on Biometrics, User Identification details		

38	Provision to verify User credentials like biometrics etc before issuing the Permit		
39	Provision to issue User permit till the Company- Category's Validity date, Document Validity date, Maximum validity period		
40	Provision to Generate, Print Permit on Smart Card, Water proof sticker, Paper		
41	Provision to link Smart card / RFID tag/ paper pass with Users credentials		
42	Provision to renew / issue duplicate permits		
43	Provision to blacklist or restore a user permit		
44	Provision to record IN / OUT movement of User / vehicle / Employee		
45	Provision to issue permits for different span of time like daily, weekly, Monthly, Quarterly, yearly		
46	Provision to issue permits to a group or to every member of group individually		
47	Provision to limit access of pass holder to specific areas		
48	Provision to declare defaulter and or blacklist a user		
49	Provision to restore defaulter and or blacklisted user		
50	Provision to display Users Photograph on the LCD when moving in or out of the gate		
51	Provision to push data of defaulters and or blacklisted user on all the readers. Thus controlling access of black listed persons		
52	For out entry Flap barrier to be operated physically/ automated		
53	Provision for various parameterized reports. User can generate their own MIS		
54	Provision for customizable forms for storing user data along with photo identification, finger prints		
55	Maintaining unique data of Users from which passes isto be generated quickly		
D. Authenticated Vehicle Enrolment and issuance of Vehicle Permit features			
56	Provision to enroll Vehicle		
57	Provision to Link passengers with Vehicle		
58	Provision to generate Vehicle permits for different time period like Quarterly / yearly, Daily		
59	Provision to renew / issue Duplicate Vehicle permit		
60	Provision to change the Owner of the Vehicle		
61	Track the IN /OUT movement of Vehicle at gate through RFID tag		
62	Provision to limit access of vehicle to specific areas		
63	Maintaining unique data of Vehicle from which passes is to be generated quickly		
64	RFID based Internal Tracking of Equipment, Container, Vehicle,& Visitors within the Port premises.		
E. Cash Collection and Remittance features			
65	Provision to Define various permit		
66	Provision to enter tariff for each definition of Permit.		
67	Provision to Change Tariff for each Definition of Permit and should be applicable for a specific period		
68	Provision to Collect Cash as per the rules defined		
69	Provision for remittances made		
70	Provision to collect deposit in advance against each company		
71	Provision to collect cash against each permit as per the rules defined by making necessary withdrawal entry (Credit/Debit)		
72	System should integrate with a Payment Gateway for remittance of fees by users as per requirement of the Port. Provision for online payment to Port Account Directly		
73	Conveniently available Pass Collection Counters including third party such as (ICDs, CFS, e-Governance Centers, Authorized Centers, etc.)		
F. Blacklisting & Policy Enforcement Module			
74	Provision to blacklist user, vehicle, company		
75	Provision to auto-block pass issue to blacklisted entities		
76	Provision to raise alert for blacklisted related requests		
77	Provision to report suspicious or anomalous activities with severity levels		
78	Provision to create rules defining Port Gate Entry Policy		
79	Provision to enforce Gate Entry Policy such entry restricted from a specific gates, etc.		
80	Provision to restrict individuals & vehicles to specific areas or zones		
81	Provision of rules to generate alerts by email, SMS, or Phone Cal		
G. User Module Features:			

82	Hierarchy of the users maintained Levels of the users and rights given to the levels could be changed through system		
83	Maker Checker facility for the user creation		
84	Log of creation of User, User Validity, password Validity, and Password Policy maintained		
85	Copy / Paste not allowed in the login / Password Fields		
86	Validation in such a way that no compromise by SQL Injection Techniques Password encrypted		
87	Last login Date/time stored in the system and displayed on the screen to the user		
88	Enforcement of the initial default password and forcing the user to change password after certain No. of days parameterized		
89	After certain no. of attempts the user gets locked and the no. of attempts parameterized		
90	Disabling the user automatically after certain period parameterized if the login is not at all used		
91	Facility to disable the user manually		
92	History of login details to the user of their own login & of all users for administrator / Super User login		
93	System should be secured enough for preventing of un-authorized attempts for access over web and security should be based on Cert-In guidelines		
H. RFID Card Management Module			
93	Advance enrolment of the port sponsor companies, users, vehicles, etc.		
94	Pre-personalization and Personalization of cards		
95	Printing of cards & stickers		
96	Management of Temporary users		
97	Provision to Issue Passes from authorized locations outside the Port		
98	Remote disabling of cards		
99	Alerting on expired card usage attempts Security & data encryption in card or server end		
I. Comprehensive MIS Reports & Integration Module			
100	Provision for Dashboard to view the current status of traffic at the Port		
101	Tracking of each and every individual, vehicle, visitor across Port area		
102	Category based reporting of traffic inside as well as at the gates		
103	Classification of Users by pass type, usage activities, access zones		
104	Classification of Vehicles by pass type, usage activities, access zones		
105	Report on Vehicles associated by Drivers & Cleaners		
106	Report of pass issued in by day, week, month, year, as well as by gates.		
107	Graphical view of all the reports summary		
108	Detailed report pass issue activities by Gate, by Period, by Operator		
109	Summarized report of pass issue activities by Gate, by Period, by Operator		
110	Reports providing anomalous activities at the gate		
111	Report providing time spent by each and every man & vehicle		
112	Report providing areas visited by individuals & vehicles		
113	Report detailing overstay by individuals & vehicles		
114	Report detailing additional movement by Individuals & Vehicles beyond a defined threshold		
115	Report classifying internal and external vehicle movements		
116	Report on pass payment collections and reconciliation		
117	Provision to check complete details of vehicle or individual on handheld System		
118	Provision to transfer data to Port servers on real-time or scheduled basis		
J. Gate Interface Module			
119	Gate Barrier Interface Module		
120	Flap barrier Interface Module		
121	License Plate Capture Camera Integration Module		
122	Display Unit Controller		
123	AVI Interface Module		
124	User Photo Capture Interface Module		
125	Container Reader & 3D Capture Interface Modules		
126	Handheld Terminal for Mobile Spot Checking as well as speedy movement at the gates		
K. Control Room & 24/7 Monitoring			
127	Summarized dashboard		
128	Real-time Data updates and Visuals		
129	Anomaly & Policy Break Reporting		

L. Backup, Archival & Retrieval Management			
130	Backup server for record keeping		
131	Regular synchronization with front-end server		
132	Historical data keeping for audit trail		
133	Fallback server		
134	Doubles up as load balancing server		
135	Distributed Architecture		
136	High Availability Master Database		
137	Archival & Retrieval System		
138	Backup & DR		
M. Policy Framework & Rules Engine			
139	Configurable policy framework and rules engine		
140	Simplified Approval System with Email, SMS, & Mobile alerts to Scrutinizer		
N. Integration APIs			
141	System should support integration or data exchanges with legacy or future systems as per requirement of Port. 3 level comprehensive APIs to connect to various existing & future integrations		
142	XML & Web service based open interfaces		
O. Biometric Aadhaar Integration			
143	RFID Pass should be linked to Aadhaar biometrics		
144	Handheld based spot checking with Aadhaar database		
145	All the parameters of Biometric Devices for Authentication should be as per certification of UIDAI as per latest STQC Scheme for certification of UIDAI Biometric Devices (Authentication)		
P. Kiosk Module			
146	RFID Pass renewal through standalone remote kiosk		
147	Ability to make payment using kiosk		
148	Provision to update & renew card using kiosk		
149	Provision to spit slip of acknowledgement		
150	Provision to remote health monitor the kiosk		
151	Provision for information dispersal through kiosk		
Q. Equipment & Asset Tracking Module			
152	Provision to get real-time visibility of assets & equipment in the port premises under surveillance		
153	Provision to identify asset or equipment on a 2D or 3D layout		
154	Provision to track assets & equipment over longer distances		
155	Provision to track multiple assets with conflict resolution		
156	Provision to search all, one, or many assets on a single screen		
157	Provision to search by individual attribute or entire set of attribute		
158	Provision to save search results on a CSV, Excel, PDF, Print, or Copy		
159	Multi-paging of results		
160	Dashboard of summary of assets & equipment and their status		
161	Provision to add, delete, edit assets & equipment		
162	Provision to add unlimited features to an asset or equipment		
163	Provision for bulk import & export		
164	Provision to assign assets to department, person, role, etc.		
165	Provision for individual user to login and check the status of the assets assigned to them		
166	Provision to request for asset assignment, return, repair, etc.		
167	Provision of Comprehensive asset & equipment lifecycle management		
R. Image Processing			
168	Offline comparison of man, material images captured by cameras		
169	Alerts when images are not consistent		
170	Comparative results and anomaly reports		

Database

SI.NO	Functionality	Compliance	Reason for Not complying
1	Highly performance reliable database with uptime		
2	High availability with redundancy & clustering		
3	Should support existing system & IT security rules and processes		
4	Should also support OS security services		
5	Database replication & migration should be real time without affecting the operations		
6	The database should be highly scalable and should sustain incremental & peak loads over the operation period		
7	Minimum 300 concurrent user connections support		
8	Performance should not degrade with significant incremental data each day		
9	Should be able to support both Windows & Linux		
10	Should support audit trail and policy compliance of sensitive data		
11	Should support periodic & occasion backup and restore without having to hold the operations		
12	Both incremental & full back up to be supported		
13	Should have inbuilt alert mechanism to warn potential issues		
14	Crash recover mechanisms to be supported.		
15	Should be able to distribute data onto physical storage devices for record keeping		
16	Should support offline DB setup and quick search for record keeping		
17	Relational Database Management System		

Access Controller

SI.NO	Functionality	Compliance	Reason for Not complying
1	The networked gate controller shall provide access control processing, host functionality and power for a single gate, including reader, lock, gate status, request- to exit device and auxiliary sounder.		
2	The networked gate controller shall accept Wiegand output card readers and card formats up to 128 bits in length.		
3	The networked gate controller shall provide a complete, fully featured access control hardware		
4	Receives and processes real-time commands from the host software application while reporting all activity to host configurable across a minimum of 255 activity priorities.		
5	The networked gate controller shall communicate with hosted access control software 6using TCP/IP protocol over Ethernet or Internet.		
6	Supports Power Over Ethernet (PoE) enabling cost-effective installation utilizing existing network infrastructures		
7	The networked gate controller shall be capable of deploying AES 256 with symmetrical key encryption for all communications between the controller and host(s) system(s).		
8	The networked gate controller shall be capable of supporting custom encryption ciphers implemented using libtomcrypt open source cryptography mechanisms for all communications between the controller and host(s) system(s).		
9	The networked gate controller shall support 802.1X authentication.		
10	The networked gate controller shall provide full distributed processing of all access control functions.		
11	The unit shall provide fully functional off line operation when not actively communicating with the host access control software application; performing all access decisions and event logging.		
12	Upon connection with the host access control software application, the networked gate controller or networked controller/reader shall upload all buffered off-line transactions (minimum of 99,999) to the host software.		
13	The networked controller shall be capable of supporting cardholder databases of 125,000 cardholders (without database change over) and 62,500 cardholders (with database changeover).		
14	The networked gate controller shall incorporate a 32-bit 200 MHz ARM9 processor running the Linux operating system		
15	The networked gate controller shall not be a proprietary product of the manufacturer of the host access control software application, and must have the ability to migrate to an alternative manufacturer's host access control software application by remote reconfiguration or firmware upgrade and without intervention from the original controller manufacturer. A dual partitioning file system enables online firmware download		
16	The networked gate controller shall provide diagnostics and configuration operations through connection to a local laptop computer. Installation webpages shall be interfaced using HTTPS and provide abilities to set product security including encryption keys		
17	Flexible Input / Output Linking engine that enables the status of any input to be linked to any		
	a. Track with the input status.		
	b. Reverse track.		
	c. Latch.		
	d. Reverse latch.		
	e. Latch for a configurable time period.		
18	Utilizes on-board jumpers to select 12 or 24 VDC power to locks and AUX output when		
19	The networked gate controller shall provide on-board Flash memory to allow program updates		
	a. 128 MB on-board Flash memory b. 64 MB RAM		
20	The networked controller input/outputs shall be expandable to a total of 16 inputs and 6 outputs utilizing modular plug-in IO interface devices all operating on a Hi-O CAN bus backbone		
21	The networked controller controls a single access and up-to 2 readers for in/out reading. Readers can be either a Hi-O compliant (attached directly to Hi-O CAN bus backbone) reader or Wiegand attached via a Hi-O compliant Wiegand interface module.		
22	Provides three implementations of anti-pass back and area control, including timed, hard and soft control		
23	Provides locally controlled multi-man feature that includes schedule dependent access for a		
24	Supports host lookup on card numbers in cases where cardholder capacity is reached or in high security threat level scenarios where host controls limited access.		
25	The networked gate controller shall provide the following certifications:		
	a. UL294 Listed Access Control Unit		
	b. UL1076 Recognized Proprietary Burglar Component		
	c. CSA 205		
	d. FCC Class A		
	e. ICES-003 Class A		
	f. CE Mark: ENEN 301 489-3, EN 55022, EN 50130-4, IEC 60950-1		
	g. C-Tick AS/NZS CISPR22		
	h. KCC		
	i. EMC Directive 2004/108/EC		
	j. LVD 2006/95/EC		
	The networked gate controller shall meet the following physical specifications:		

26	a.	Dimensions: 6.1" W x 4.8" H x 1.5" D (154.9 mm x 121.9 mm x 36.3 mm)			
	b.	Weight: 11.3 oz (320 g)			
	c.	Cover Material: UL94 Polycarbonate			
	d.	Power Requirements DC Input (MAX):			
		1. Using PoE input power is 14.4W			
		2. Using +12VDC AUX input power is 18W			
		3. Using +24VDC AUX input power is 36W			
	e.	Temperature: 32° to 122° F (0° to 50° C)			
	f.	Humidity: 5% to 95% relative, non-condensing			
	g.	Visual Indicators on Ethernet connector:			
		1. Network Activity LEDs			
	h.	Communication ports and connectors:			
		1. RJ-45 connector for Ethernet TCP/IP (10/100baseT)			
		2. Wiegand/Clock-and-Data reader data port			
		3. Total system power output (MAX)			
		a. PoE input power: 9.6W			
		b. 12VDC input power: 14.4W			
		c. 24VDC input power: 28.8W			
		4. Gate position input with programmable End of Line supervisory capability up to 6K Ohm.			
	27	5.1	Request to exit (REX) input with programmable End of Line supervisory capability up to 6K Ohm.		
		5.2	Non-latching configurable gate lock output relay		
		a.	Unpowered (Dry) contact rated 2A @ 30VDC		
		b.	Powered (Wet) contact rated for up to:		
			i. PoE input power: 6.9W (12VDC) or 8.6W (24VDC)		
			ii. 12VDC input power: 8.4W (12VDC)		
			iii. 24VDC input power: 8.4W (12VDC) or 16.8W (24VDC)		
		iv. Note: The overall system power cannot be exceeded.			
	7.	Non-latching alarm annunciation output relay			
	a.	Unpowered (Dry) contact rated 2A @ 30VDC			
	b.	Powered (Wet) contact rated for up to:			
		i. PoE input power: 6.9W (12VDC) or 8.6W (24VDC)			
		ii. 12VDC input power: 8.4W (12VDC)			
		iii. 24VDC input power: 8.4W (12VDC) or 16.8W (24VDC)			
		iv. Note: The overall system power cannot be exceeded.			
	8.	12VDC, 24VDC or PoE Power input			
	9.	Tamper input (Can have a built-in additional external tamper)			
	10.	AC Power Fail input (Can be configured for general purpose use)			
	11.	Battery fail input (Can be configured for general purpose use)			
	i.	Cable Distances:			
		1. TCP/IP: 328 feet (100m) using CAT 5 cable			
		2. Wiegand: 500 feet using 9-conductor stranded, overall shield 22 AWG cable (Alpha 1299C)			
		3. Input circuits: 500 feet using 2-conductor shielded 22AWG cable (Alpha 1292C) or 18AWG cable (Alpha 2421C)			
		4. Output circuits: 500 feet using 2-conductor 22AWG cable (Alpha 1172C) or 18AWG cable (Alpha 1897C)			
28		The networked gate controller shall be warranted against defects in materials and workmanship for 18 months			
29		Network discovery and update tools shall enable the discovery and queued update of multiple controllers on the network.			

RFID reader

SI.NO	Functionality	Compliance	Reason for Not complying
1	The contactless smart card reader(s) shall be designed to securely read, interpret, and authenticate access control data from 13.56 MHz contactless smart card credentials		
2	Customized security protection through support of the device-independent portable credential methodology to provide enhanced security and performance features		
3	Unique read selection that enables reading of the Secure Identity Object™ (SIO) and standard technologies		
4	Participates in an advanced, bounded and trust-based Access Control system		
5	Guaranteed compatibility to read all data formats and ensuring card-to reader interoperability in multi-location installations and multi-card and reader populations		
6	Backwards compatibility with legacy 13.56 MHz contactless smart card access control formats (E.g. 26-bit, 32, 35-bit, 37-bit, 56-bit, etc.). Compatibility across the product line shall be assured without the need of special programming		
7	The contactless smart card reader shall be Secure Identity Object™ (SIO) enabled. The contactless smart card reader platform shall support the standards-based, device-independent Security Identity Object™ (SIO) portable credential methodology to ensure data authenticity and privacy. The SIO shall be able to reside on any number of identity devices, including iCLASS SE, MIFARE Classic SE, and MIFARE DESFire EV1 SE credentials		
8	The contactless smart card reader shall be a certified end-point (TIP Node) within a Trusted Identity Platform™ (TIP) infrastructure. TIP shall provide a scalable, on-demand, secure identity delivery system that validates, registers and provides lifecycle management support for certified trusted end-point contactless smart card readers		
9	The contactless smart card reader shall increase security by narrowing the possibility of unwanted configuration changes and denials of service. The contactless smart card reader shall utilize TIP-enabled secure configuration of contactless smart card readers with counters and uniquely diversified configuration cards		
10	The contactless smart card reader shall utilize Secure Element Technology™ to protect keys and cryptographic functions to the international standard Evaluation Assurance Level (EAL) 5+.		
11	The contactless smart card reader shall be configurable to utilize Velocity Checking to provide breach resistance against electronic attacks that invoke multiple improper authentication attempts		
12	The contactless smart card reader shall be configurable to provide multiple hierarchical degrees of key compatibility for accessing the smart card access control data.		
13	The contactless smart card reader shall simplify troubleshooting through Anti-pass back Notification that the card has already been processed and it must be removed from reader field temporarily prior to processing again		
14	The contactless smart card reader shall provide enhanced user feedback options through the use of clear and bright tricolored LEDs configurable to support any three color combinations (RGB - Red, Green, and Blue)		
15	The contactless smart card reader shall enable backwards compatibility with legacy 13.56 MHz access control formats (E.g. 26-bit, 32, 35-bit, 37-bit, 56-bit, and others).		
16	The contactless smart card reader manufacturer shall provide global, off-the-shelf availability.		
17	Contactless smart card reader shall allow the reader firmware to be upgraded in the field without the need to remove the reader from the wall through the use of factory-provided Programming Cards		
18	Contactless smart card reader shall allow for secure installation practices through mounting methods utilizing tamper resistant screws		

19	<p>Contactless smart card reader shall provide the ability to transmit an alarm signal via and integrated optical tamper switch if an attempt is made to remove the reader from the wall. The tamper switch shall be programmable to provide a selectable action to provide a selectable action compatible with various tamper communication schemes provided by access control panel manufacturers. The selectable action shall include one of the following:</p> <ol style="list-style-type: none"> 1. The reader open collector line changes from a high state (5V) to a low state(Ground). 2. During a tamper state, the "I'm Alive" message is inverted 		
20	<p>Contactless smart card reader shall provide ability of an online "I'm Alive" message so the reader's functional health can be monitored at all times when paired with a compatible access control panel</p>		
21	<p>The contactless smart card reader shall provide customizable reader behavior options either from the factory, or defined in the field through the use of pre-configured command cards. Reader behavior programming options shall include:</p> <ol style="list-style-type: none"> 1. Audio/Visual Templates for card reads, and attack detection. 2. Velocity Check timing and thresholds 3. Optical tamper actions 4. RF scan delay 5. Hold Mode 6. Intelligent Power Management 7. Key diversifiers 8. Key rolling 9. CSN output configuration 10. Data Model prioritization 11. Default LED Colour 12. Hold Mode 		
22	<p>Contactless smart card reader shall provide the following programmable audio/visual indication:</p> <ol style="list-style-type: none"> 1. An audio beeper shall provide various tone sequences to signify: access granted, access denied, power up, and diagnostics. 2. A high-intensity red/green/blue (RGB) light bar shall provide clear visual status. The light bar shall provide uniform distribution of light eliminating individual bright spots 		
23	<p>Contactless smart card readers shall provide the following enhanced performance features</p> <ol style="list-style-type: none"> a. The contactless smart card reader shall enable user prioritization of High frequency/ High-frequency credential reads. Technology prioritization shall synchronize a site's credential technology read priority to the access panel configuration while reducing unintended credential reads. b. The contactless smart card reader shall have the ability to provide consistent optimal read range by implementing an auto-tune function that adjusts for manufacturing tolerances to enhance consistency of performance from reader to reader. c. The contactless smart card reader shall be field programmable to provide secure upgrades for migration and extended lifecycle. d. The contactless smart card reader shall be designed as a system to provide optimal read range and read speed for increased access control throughput. 		
	<p>Contactless smart card reader shall provide enhanced environmental and sustainability features.</p> <ol style="list-style-type: none"> a. The contactless smart card reader shall reduce power consumption by as much as 75% through the use of Intelligent Power Management (IPM) technology. b. The contactless smart card reader shall be manufactured with 10% recycled material to provide the potential of LEEDS building credits in new construction projects. 		

24	c. Contactless smart card reader shall be fully compliant with Restriction of Hazardous Substances directive (RoHS) restricting the use of specific hazardous materials found in electrical and electronic products. The substances banned under RoHS are lead (Pb), mercury (Hg), cadmium (Cd), hexavalent chromium (CrVI), poly brominated biphenyls (PBB) and poly brominateddiphenyl ethers (PBDE).		
	d. Contactless smart card reader shall be manufacturers with 10.5% (Pigtail) and 11% (Terminal Strip).		
25	Contactless smart card reader shall comply with the following 13.56MHz related standards to ensure product compatibility and predictability of performance		
	a. ISO 15693		
	b. ISO 14443A		
	c. ISO 14443B		
26	Contactless smart card reader shall be suitable for global deployment by meeting worldwide radio and safety regulatory compliance including:		
	a. UL294 (US)		
	b. cUL (Canada)		
	c. FCC Certification (US)		
	d. IC (Canada)		
	e. CE (EU)		
	f. C-tick (Australia, New Zealand)		
	g. SRRC (China)		
	h. MIC (Korea)		
	i. NCC (Taiwan)		
	j. iDA (Singapore)		
27	Contactless smart card reader shall provide the following typical contactless read ranges:		
	a. 2.8" (7.1 cm) reading SIO on iCLASS SE Card		
	b. 1.6" (4.1 cm) reading SIO on MIFARE DESFire EV1 SE Card		
	c. 2.6" (6.6 cm) reading SIO on MIFARE Classic SE Card		
	d. 1.5" (3.8 cm) reading SIO on iCLASS SE Tag or Fob		
	e. 1.2" (3.0 cm) reading SIO on MIFARE Classic SE Tag or Fob		
28	Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended Current requirements and power consumption:		
	1. 45 mA (Standard Power Mode)		
29	2. 25 mA (Intelligent Power Management Mode)		
	3. 75 mA (Peak Current Draw)		
	4. 0.7 W (Standard Power Mode @ 16VDC)		
	5. 0.4 W (Intelligent Power Management Mode @ 16VDC)		
30	Material: UL94 Polycarbonate		
31	Operating temperature: -31 to 150 degrees F (-35 to 65 degrees C)		
32	Operating humidity: 5% to 95% relative humidity non-condensing		
33	Storage Temperature: -67 to 185 degrees F (-55 to 85 degrees C)		
34	Weatherized design suitable to withstand harsh environments with a certified rating of IP55		
35	The contactless smart card reader shall provide a lifetime warranty against defects in materials and workmanship		

RFID Transceiver

SI.NO	Functionality	Compliance	Reason for Not complying
1	Read Range : 13 meters		
2	Antenna : Integrated, Built-In		
3	Protocol : ISO18000-6C, EPC UHF Class 1 Gen 2. With optional Dense Reader Mode (Class 3 Gen 2 compliant)		
4	Frequency Range : UHF		
5	Polarization : Circular Polarization Antenna, choice of LHCP or RHCP		
6	S203 Axial Ratio : Less than 0.5 - 1.0 dB		
7	External Control : 2 x GPO and 2 x GPI		
8	Supports True DRM : Required		
9	Operating Temp: : -20°C to 60°C (-4°F to 131°F)		
10	Storage Temp: : -40°C to 85°C (-40°F to 185°F)		
11	Humidity: : 98% Non-condensing		
12	Environment Protection : IP68 with all Weather and MIL-STD-810 Ruggedized		
13	Shock : MIL-STD-810F Method 516.5 Procedure V, 75g, 6ms, 2 shocks per axis		
14	Vibration : MIL-STD-810F Method 514.5 Category 24		
15	Mechanical Impact Resistance : Free falling ball impacting test at 1 meter in height with weight of ball at 500 grams loads		
16	Connectivity : Ethernet		
17	Power Supply : DC supply (12 V, 2.5 A), or use POE+ (IEEE802.3at)		
18	Weight : Max. 2 Kg		
19	Physical Characteristics (LxWxH) : Max. 300 x 300 x 75 mm		

UHF RFID card

Sl.NO	Functionality	Compliance	Reason for Not complying
1	UHF Contactless Smart Card		
2	UHF RFID frequency bands (860-960 MHz)		
3	Dimensions 86 x 54x 0.8mm		
4	Material PVC,PET		
5	EPC Class1 Gen2, ISO 18000-6C		
6	IP68		
7	Reading distance upto minimum of 10 meters		
8	512 bit user memory		
9	White		
10	Data retention: 100,000 cycles		
11	Card should have a standard lifetime of minimum 10 years		

HF RFID card

Sl.NO	Functionality	Compliance	Reason for Not complying
1	The contactless smart card shall function as an access control card, used with access readers to gain entry to controlled portals and to hold identification information specific to the use.		
2	The contactless smart card shall be a passive device, with an operating frequency of 13.56 MHz, and shall meet the following ISO/IEC standards: 7810, 7816 and contactless cards (14443 A). Generic command set should be based on ISO/IEC 7816-4.		
3	The card shall be available as a single RFID solution designed for interoperability with 13.56 MHz readers or optionally in dual technology in conjunction with a 125 KHz proximity interface.		
4	A presentation within the typical maximum read range of 3-4" to the access control reader shall result in an exact reading of the card.		
5	The card shall offer a memory size of 8K-Bytes or 16K-Bytes for applications		
6	<p>a. The contactless smart card shall meet the following physical characteristics:</p> <p>b. Dimensions, per ISO/IEC 7810 (ID-1 format) 2.127"x 3.375"x 0.033" (5.40 cm x 8.57 cm x 0.084 cm) Weight: 0.20 oz. (5.5 g).</p> <p>c. Material and construction: Composite card materials. Card surface shall be glossy and of a material compatible with direct to card dye-sublimation or thermal transfer printing. Card construction shall meet durability requirements of ISO 7810.</p> <p>d. The card shall be marked with an external ID number, either in inkjet or laseretched numbering that may match the internal programmed ID number.</p> <p>e. Optionally, the card may contain a magnetic stripe (with support for up to 3 tracks, Hi-Coercivity or Lo-Coercivity).</p> <p>f. Optionally, the card may be printed with custom graphics, may be built to a custom thickness and may contain security and anti-counterfeiting features.</p>		
7	Contactless smart card shall meet the following environmental specifications: <p>a. Operating Temperature: -40oF to 158oF (-40oC to 70oC).</p> <p>b. Operating Humidity: 5% to 95% relative humidity non- condensing.</p>		
8	The warranty of contactless smart cards shall be lifetime against defects on material.		
9	All cryptographic algorithms, modes of operation, protocols and mechanisms used by the card shall be based on open standards (such as ISO/IEC, NIST, IEEE, EN, ETSI) and not subject to any patents or royalty payments.		
10	The smart card shall support ISO/IEC 14443 specifications parts 1-4 (with communication type A) and exposes a random UID. It can be programmed with different card data formats (with variable length) including standards-based and secure Data Object credentials		
11	The card shall be available as a single RFID solution or dual technology in conjunction with a 125 KHz proximity interface.		
12	The card shall be loaded with an application that leverages existing standards for maximum interoperability and heightened protection against attacks.		
13	Programmable platform: The card shall use a microprocessor to support post-issuance update in the field and support retrieval of protected data formats. The card shall be ready to support future applications		
14	The card shall be programmable with one or more Secure Identity Objects (SIO) for each application		
15	The card shall support secure messaging compliant with ISO/IEC 7816-2:2005, Section 6 (Secure Messaging)		
16	All contactless communications shall be secured by a secure messaging established after mutual authentication between the card and the off-card application. Each secure session relies on diversified AES keys that are setup at the start of each session. Keys are AES-128 bit. The secure messaging is based on European Standard EN14890-1 as well as ISO/IEC 7816-4.		
17	For security risk remediation and protect efficiently against common attacks, the security level of the card including its cryptographic stack/key size shall be upgradable through an application update		
18	The card shall support efficient privacy protection to ensure that personally identifiable information or cards identifiers (such as contactless UID, key diversifier) are not accessible & cannot be retrieved by unauthorized parties. To prevent sequence replay or Cloning, transmitted secrets or previously transmitted identifiers are not revealed in the clear to the off card application.		
19	The card shall cover use cases combining physical and logical access supporting OTP – One Time Password – generation functionality based on OATH algorithm		
20	The card shall support multiple applications as part of the available memory. Each application can be loaded with different data set and memory size		
21	The card shall support adding or removing applications after the card has been issued, with full support for data integrity and consistency and confidentiality of any secrets such as authentication keys contained in the applications. The application management commands shall be based on ISO/IEC 7816-13:2007.		
22	The card shall include multi-application support for on-card database application with a firewalled architecture (to ensure data separation between applications). To increase return on investment, the default application can be updated to support other services without card replacement.		
23	The card application (command/response set) shall be based on ISO/ IEC 7816-4 (no proprietary command is accepted to ensure maximum interoperability).		
24	The card memory shall guarantee a data retention of 20 years; Card data integrity and consistency shall be preserved at all time during the life span of the card.		
25	Communication: The card shall be fully compliant with the ISO/IEC Standard "Identification cards / Contactless Integrated Circuit Cards / Proximity card" (ISO/IEC 14443 Parts 1 to 4). The compliance with the requirements of the ISO/IEC 14443 shall be tested against the standard test procedures as specified in ISO/IEC 10373-6:2011		
26	All commands and responses defined by the card shall be compliant with the syntax of command-response pairs as defined in ISO/IEC 7816- 4:2005, Section 5.1 (Command-response pairs).		
27	Data Organization The organization of all data on the card shall be based on ISO/IEC 7816- 4:2005, Sections 5.2 (Data Objects) and 5.3 (Structures for applications and data). The encoding of data shall be BER TLV, compliant with ISO/IEC 7816-4:2005 Section 5.2.2 (BER-TLV data objects)		
28	The card shall ensure that all operations available by the card command set can be interrupted at any time without any impact on the integrity and consistency of the card data. This mechanism must be fully implemented in the card and shall not require any special functionality from the reader or terminal.		
29	Security architecture The card shall support authentication methods compliant with ISO/IEC 7816-4:2005, Section 7.5 (Basic Security Handling). The actual authentication protocol shall be one of the standard authentication protocols defined in ISO/IEC 24727-3:2008. The card shall be fully compliant with ISO/IEC 11770-2.		
30	The card shall fully align with NIST recommendations: Solution has to implement NIST approved mode of operations and cryptographic recommendations from NSA Suite B. Card key diversification shall rely on approved method from NIST SP800-108.		
31	The card shall protect the privacy of the holder of the card. As minimum privacy measures, the card shall:		
32	a. Not reveal any static value which is either unique for a single card or can be considered unique in a typical population of cards in a given system, without a prior authentication (proxy tracking)		
33	b. Prevent any profiling of the card holder without the knowledge of secrets specific to a card		
34	c. Prevent the ability to identify if two valid sessions are with the same card or not		
35	Application management The selection of applications shall be based on a standards based name space, so that the application names can be globally unique and managed by multiple independent entities. The top of the name hierarchy shall be managed by an independent international standards body (such as ISO or ITU-T) and the name structure shall allow delegation of name management at multiple levels of hierarchy. The selection of applications shall be based on a standards based name space, so that the application names can be globally unique and managed by multiple independent entities. The top of the name hierarchy shall be managed by an independent international standards body (such as ISO or ITU-T) and the name structure shall allow delegation of name management at multiple levels of hierarchy.		
36	Card should have a standard lifetime of minimum 10 years		

Handheld Terminal

SI.NO	Functionality	Compliance	Reason for Not complying
1	Read Range : 8 meters		
2	Read Rate : 400 tags / second		
3	Protocol : ISO18000-6C, EPC UHF Class 1 Gen 2 with optional Dense Reader Mode (Class 3 Gen 2 compliant), HF cards		
4	Tag Information : All banks, any sizes; RSSI value		
5	Frequency Range : 865-867 MHz and 13.56Mhz. Should be able to read both UHF and HF RFID cards		
6	Barcode Scanner : 1D and 2D: Codabar, CodablockA and F, Code 11, Code 39, Code 93/93i, code 128/ISBT 128/UCC EAN 128/EAN.UCC composite, Industrial and Standard 2 of 5, Interleaved 2 of 5, Aztec, Data Matrix, (and all other Matrix type barcodes), MSI, PDF417/MicroPDF417, MacroPDF417 (unbuffered d mode), Plessey, RSS, Telepen, TLC39, UPC/EAN/ISBN		
7	Antenna Polarization : Option of vertically linear polarized, horizontally linear polarized or circular polarized		
8	Operating Temp : -20°C to 50°C (-4°F to 122°F)		
9	Storage Temp : -40°C to 75°C (-40°F to 167°F)		
10	Humidity : 5% to 95% Non-condensing		
11	Ruggedized Designs : Drop test 1.5 meters on 6 sides; IP65		
12	User Interface – Input : Full QWERTY keyboard, Touch Screen, Trigger Button		
13	User Interface – Output : 3.5" Transmissive LCD, 320 x 240 pixels, LED x 2, Buzzer		
14	Connectivity : Inbuilt Wi-Fi (802.11 b/g), USB, GPRS, RTLS		
15	External Memory : SD Card, Standard SD and SDHC		
16	Processor : 400 MHz		
17	Memory : 128 MByte Flash, 64 MByte RAM		
18	Battery Life : 1.5 hours turbo read, 20 hours standby, field replaceable battery		
19	Weight : Maximum 1 Kg		
20	Physical Characteristics (LxWxH) : Max. 197 x122 x 223 mm		

Smartcard printer

Sl.NO	Functionality	Compliance	Reason for Not complying
1	Printing specifications : Single- or dual-sided printing		
2	Standard features :		
	a. 100 card covered feeder (30 mil)		
	b. 45 card capacity output hopper (30 mil)		
	c. 16-character LCD operator control display		
	d. 300 dpi (11.8 dots/mm) print resolution		
3	Communications Interfaces : USB V2.0		
4	Optional Features : Built-in 10/100 Ethernet connectivity		
5	Operating range : 90-132VAC and 190-264VAC		
6	Operating Temperature : 60o F to 86o F (15o C to 30o C)		
7	Storage Temperature : 23o F to 131o F (-5o C to 55o C)		
8	Auto-switching : single-phase AC power		
9	Frequency range : 47-63 Hz		
10	Environmental Specifications : Printer should withstand high level of humidity and salty conditions		
11	Print speed : 180 cards per hour		

DC & DR

Sl.no.	Minimum specification/ feature required	Compliance	Reason for Non-compliance (if any)
1	Modular design		
2	Scalable based on future requirements		
3	Should have racks/ blade chasis for housing PACS server		
4	Sufficient Air condition, dust free environment and fire detection and suppression		
5	Temperature and Humidity sensors		
6	Connectivity & structured cabling		
7	Fixtures such as plumbing and lighting as required		
8	Security cameras, card readers, restricted and controlled access		
9	Adequate redundancy measures for equipment, power, data, etc.		
10	Partitioning as required		
11	False ceiling as required		
12	Fire rated doors and paintings		

Port Server

Sl.no.	Description	Minimum specification required	Compliance	Reason for Non-compliance (if any)
1	CPU	Intel Xeon E7 family-based 4-socket, 3.2 GHz processor or better, 32 Cores		
2	No. Of Processors	2 expandable to 4, hot pluggable		
3	Motherboard	OEM/ Intel original Motherboard		
4	Memory	128GB expandable up to 2TB, hot pluggable		
5	Hard Disk Drive	3x1.8 TB SAS 10k RPM hot pluggable		
6	Storage Controller	12Gbps SAS Controller. Controller should support RAID level 5.		
7	Certifications	Windows, Red Hat or Novell certified, Compliance & Support		
8	I/O Slots	Minimum 3 PCI slots and 3 should be active		
9	Power Supply	Hot plug redundant power supply fully occupied		
10	Fans	Hot plug redundant fully occupied		
11	Networking	1GB Ethernet 4 Port adaptor		
12	Accessories	For mounting in a rack accessories should be supplied		
13	Operating System	MS Windows server2016 std or latest with down grade usage rights		
14	Keyboard	101 keys		
15	Mouse	Optical		
16	Features	Server for mission-critical applications in corporate data centers and workloads needing the highest performance, reliability and I/O scalability		
		Should have 20" monitor for management purpose		
		The Blade Chassis with Dual process Socket Half Height Blade Servers		
		FC Pass-Through and HBA Cards for connectivity		
		Powerful Management Tools		
		Flexible Remote Management		
		Extensive I/O Flexibility		
		High Performance, Hyper-Dense Design, Flexible and Scalable Networking		
		Optimum Performance now, but still room to increase as per the requirement		
		Industry leading Blade Solutions with redundant Power Supply and passive Midplane		
		Server should be easy to manage and Scalable		

Gate Server

Sl.no.	Description	Minimum specification required	Compliance	Reason for Non-compliance (if any)
1	CPU	Intel Xeon E7 family-based 4-socket, 3.2 GHz processor or better, 8 Cores		
2	No. Of Processors	2 expandable to 4		
3	Motherboard	OEM/ Intel original Motherboard		
4	Memory	16 GB expandable up to 1 TB		
5	Hard Disk Drive	1.8 TB SAS 10k RPM hot pluggable		
6	Storage Controller	12Gbps SAS Controller. Controller should support RAID level 5.		
7	Certifications	Windows, Red Hat or Novell certified, Compliance & Support		
8	I/O Slots	Minimum 3 PCI slots and 3 should be active		
9	Power Supply	Hot plug redundant power supply fully occupied		
10	Fans	Hot plug redundant fully occupied		
11	Networking	1GB Ethernet 4 Port adaptor		
12	Operating System	MS Windows server2016 std or latest with down grade usage rights		
13	Keyboard	101 keys		
14	Mouse	Optical		
15	Features	Server for mission-critical applications in corporate data centers and workloads needing the highest performance, reliability and I/O scalability		
		Should have 20" monitor for management purpose		
		The Blade Chassis with Dual process Socket Half Height Blade Servers		
		FC Pass-Through and HBA Cards for connectivity		
		Powerful Management Tools		
		Flexible Remote Management		
		Extensive I/O Flexibility		
		High Performance, Hyper-Dense Design, Flexible and Scalable Networking		
		Optimum Performance now, but still room to increase as per the requirement		
		Industry leading Blade Solutions with redundant Power Supply and passive Midplane		
Server should be easy to manage and Scalable				

Bullet - Digital Web Camera

SI.NO	Functionality	Compliance	Reason for Not complying
1	Camera type : Camera shall be Fixed color IR Bullet IP Camera		
2	Image sensors : 1 / 2.8 " mm CMOS		
3	Resolution : 2 Megapixel-60 fps in 1920 x 1080		
4	Lens type : 3-9mm power zoom lens,F1.2		
5	Day/night : Day and Night Mechanical cut filter		
6	Light : 0.05 lux color and 0 lux with IR		
7	IR distance : Built-in IR Light up to 30m		
8	Video compression : H.264 (High Profile supported) / MJPEG		
9	WDR : 100dB		
10	Card slot : MicroSD up to 32 GB		
11	Audio : 2-way audio with microphone input		
12	Alarm : Alarm Input and alarm output		
13	Power : POE / 12 V DC		
14	Mounting : Suitable for Pole and Wall mounting in Lanes		

Incident Capture Camera

SI.NO	Functionality	Compliance	Reason for Not complying
1	Camera Type : Charge Coupled Device (CCD)		
2	Capturing : Color camera Image & Video		
3	Lens : Fixed focal or varifocal Auto iris lenses		
4	Vision Capabilities : Day & Night Vision		
5	Lux : Min. 1.8Lux (Image & Video)		
6	Surge & lightning protection : Required		
7	Image compensation capability to ignore stray lighting / vehicle lighting : Required		
8	Snapshot Capturing : Required		
9	Camera Mounting : Pole/Wall/etc.		
10	Camera Location : Direct sunlight and stray lighting is negated		
11	Camera Protection : Resistant to high winds/salty/moisture/dust. IP-65		
12	Automatic adjustment of brightness : Required		
13	IR based 2 Mega Pixel-HD, Day night, with 1/3 inch CMOS or higher with Industrial NMEA enclosures to be fixed in counters/ gate cabins		

360 deg Cam

SI.NO	Functionality	Compliance	Reason for Not complying
	360 degree Camera for Pedestrian lanes		
1	2-Megapixel CMOS Sensor		
2	30 fps @ 1920x1080		
3	2.8 ~ 12 mm, Vari-focal, Remote Focus, P-iris Lens (IB836BA-HT/EHT)		
4	Removable IR-cut Filter for Day & Night Function		
5	Built-in IR Illuminators, Effective up to 30 Meters		
6	Smart IR Technology to Avoid Overexposure		
7	WDR for Unparalleled Visibility in Extremely Bright and Dark Environments		
8	SNV (Supreme Night Visibility) for Low Light Conditions		
9	3D Noise Reduction		
10	Video Rotation for Corridor View		
11	Weather-proof IP66 and Vandal-proof IK10-rated Housing		
12	Extreme Weather Support with PoE (IB836BA-EHT/EHF3)		

PC

Sl.NO	Minimum specification required	Compliance	Reason for Not complying
1	Processor : Intel(R) Core i5-6500 Processor (Quard Core HT, 3.2GHz, 6MB, 4T, 65W)		
2	Graphics : Integrated HD Graphics		
3	Memory : 4GB (1x4GB) 1600MHz DDR3 NON ECC, supports upto 32 GB		
4	Hard Disk Drive : 1 TB 7200 rpm HDD.		
5	Monitor : 19.5" LED Digital Color Monitor		
6	Keyboard : 104 Keys or Better		
7	Mouse : Optical Scroll Mouse		
8	Ports : Minimum 4 USB Ports with at least 2 in front, minimum 2 USB 3.0, 1 Serial audio port for microphone and headphone in front, Display/ VGA port		
9	DVD Drive : 16x DVD R/W		
10	Ethernet: 10/100/1000 on board integrated Network Port		
11	Operating System : Windows 10 Professional (64 bit) preloaded with media.		

Boom barrier

Sl.NO	Functionality	Compliance	Reason for Not complying
1	Application : Outdoor		
2	IP Rating : 54		
3	Housing : Barrier Housing Unit: Powder Coated Boom : Powder Coated White RAL 9010 with Red reflective strips.		
4	Housing Dimension : Modular		
5	Housing Material Of construction : All Aluminum Housing with Base frame in SS-304 for high protection against corrosion.		
6	Protection : All Housing and internal parts will be rust & corrosion free metals or alloys of high strength with suitable Epoxy coating as applicable.		
7	Housing Dimension (W X D X H) : 300mm X 245mm X 920mm		
8	Boom Specifications :		
	The Booms shall be extruded aluminum with octagonal profile (straight and articulated) 100mm. X 55mm. X 1.6 mm. shall be the structure of the profile.		
	The Octagonal Profile shall offer stability Against winds & better view when compared to Round & Rectangular profiles.		
9	Intelligence :		
	The barrier shall use a Block able DC High Torque Drive in combination with CAN bus communication. Standard interfaced Controller. It shall offer LCD Display & Graphic User Interphase for easy control setting. Possibility for integration via standard User interphases. In built Loop Detectors		
10	Motor : 24 V DC Motor		
11	Compliance & Safety : Compliance to CE. Adherence to Safety Requirements of the		
	a. EMC Directive 2004/108/EC,		
	b. Low Voltage Directive 2006/95/EC and c. The basic requirements of the Machinery Directive 2006/42/EC		
12	Power Supply : 230+/- 10% VAC, 50 Hz.		
13	Maximum Power Consumption : 110 Watts during startup and 25 Watts at peak operation		
14	Opening & Closing Time : 4Secs. for 3.5 – 6 meter Boom Barrier, 1.3 Sec for up to 3.5 meter Boom Barrier		
15	Safety :		
	a. S/W for Detection of Presence of Vehicle in Loop with in-built loop detector or in the path of Infrared Safety Sensors available. Loops or Sensors to be b. Used to prevent barriers from closing on the vehicle.		
16	Duty Cycle : 1		
17	Integration :		
	a. Shall function in integration with Smart cards, proximity reader based access control systems etc		
18	Performance Requirement :		
	a. MCBF- 10 Million Cycles		
	b. Requirement MTBF- 50,000 Hours c. MTTR- 30 Minutes		
19	Certification : UL Listed		

Boom Barrier, when in non operational state, if struck by Trailer / other equipment, should have the feature / facility to move/swing horizontally to prevent breakage of the Boom Barrier.

Flap Barrier

Sl.NO	Functionality	Compliance	Reason for Not complying
1	Application : OutDoor		
2	Drive Technology : The Combination of a Brush-less DC Motor with in-built resolver shall make it a Drive with no wear & tear components. Additionally the absence of limit Switches & Slip Clutches shall provide trouble free operation w/o the need for constant maintenance.		
3	Gate/ Barrier Controller : a. Micro Processor Based Motor Controller shall have in-built Speed and Dynamic Braking Features b. Micro Processor Based Barrier Controller with Logic for Motor, Safety Sensors and Lane Indicators		
4	Throughput : 25 to 30 persons per minute (excluding card validation time)		
5	Operation : Bi-directional		
6	Housing Dimension : a. Regular Lane : L 1300mm x W 250mm x H 1035mm b. Wide Lane : L 1300mm x W 280mm x H 1035mm with Telescopic Flap		
7	Lane Width : a. Regular Lane : 520mm b. Wide Lane : 900mm		
8	Flaps : a. Regular Lane: Soft Wing with metal reinforcement/Acrylic Flaps b. Wide Lane : Telescopic Soft Wing with metal reinforcement		
9	Power Supply : 230+/- 10% VAC, 50 Hz.		
10	Finish : Mild Steel Powder Coated in Structured Finish / Stainless Steel finished to Grade 4 also known as Satin Finish.		
11	Protection : All Housing and internal parts will be rust & corrosion free metals or alloys of high strength or with suitable epoxy coating		
12	Power off/ Emergency : Fail Safe Mode - Flaps shall Automatically Open during Power Failure. Also can be configured for Flaps to remain closed during		
13	Safety : Soft flaps & the use of Brush-less DC motor for very quick reversibility and enhanced pedestrian safety		
14	Duty Cycle : 1		
15	Ingress Protection : IP 54 minimum		
16	Braking : Dynamic Braking for smooth resting of flaps		
17	MCBF-Mean Cycle Between Failures : 10 Million Cycles, Certification to be provided by the OEM		
18	Integration : Shall function in integration with Smart cards, proximity reader based access control systems, Bio-metric systems etc.		

55" LED display

SI.NO	Functionality	Compliance	Reason for Not complying
1	Type : LED, size 55" (minimum) Professional display		
2	Display Resolution : 1920 x 1080p (min) (FHD resolution)		
3	Connectivity : 1 x HDMI & 1 x USB		
4	Screen Size (Diagonal) : 138 cms Minimum		
5	Refresh Rate : 50Hz-100Hz		

32" LED display

SI.NO	Functionality	Compliance	Reason for Not complying
1	Type : LED, size 32" (minimum) Professional display		
2	Display Resolution : 1920 x 1080p (min) (FHD resolution)		
3	Connectivity : 1 x HDMI & 1 x USB		
4	Screen Size (Diagonal) : 80 cms Minimum		
5	Refresh Rate : 50Hz-100Hz		

RFID R-W

SI.NO	Functionality	Compliance	Reason for Not complying
1	Reader : USB-5EC		
2	Development Kit : USB-5EC-DEVKIT		
3	RFID Protocol : Support EPCglobal Gen 2 (ISO 18000-6C) with Anti-Collision and DRM		
4	Antenna : Internal linear polarized antenna with peak Gain 1 dBi from 860–960 MHz		
5	RF Power Output : Separate read and write levels (into the antenna) are command-adjustable from 10 dBm to 23 dBm (200mW), +/- 1.0 dBm accuracy		
6	Frequency :		
	a. Pre-configured for the following regions: FCC 902-928 MHz (Americas)		
	b. ETSI 865.6-867.6 MHz, 869.85 MHz (EU) KCC 917- 920.8 MHz (Korea)		
	c. TRAI 865-867 MHz (India) ACMA 920-926 MHz (Australia)		
	d. SRRC-MII 920-925 MHz (P. R. China)		
	e. 'Open' (Customizable) 860-960 MHz		
7	Physical : USB mini-B connector, with 2 foot (61 cm) cable terminated in A-type plug		
8	Signaling : Asynchronous serial interface with 3.3/5V logic levels; baud rates from 9600 to 921,600 bps		
9	I/O : Two I/O command controlled LEDs and two I/O command queried switches		
10	Protocol : Command-response protocol protected by length field and 16-bit CRC		
11	Dimensions (not including stand) : 97 mm L x 61 mm W x 25 mm H (3.8 in L x 2.4 in W x 1.0 in H)		
12	Regulatory : FCC 47 CFR Ch.1 Part 15 Industrie Canada RSS-21 0 ETSI EN 302 208 v1.4.1		
13	Safety : IEC 60950-1 (ed.2) US-17650-UL		
14	DC Power Required : DC Voltage: 5 VDC (Powered by USB interface) DC Power: 2.7 W (540 mA) max Supplied interface cable terminates in two type-A plugs: one for power and signal, the second for additional power if needed		
15	Idle Power Consumption :		
	a. 1.7 W max at idle (Power management modes can be used to reduce this to b. as little as 0.1 W)		
16	Operating Temp. : Operating Temp. -20C to +60C		
17	Storage Temp. : Storage Temp. -40C to +85C Architecture		
18	User-accessible Flash Memory : 16 kB		
19	Tag Buffer : 200 Tags		
20	Tag Read Rate : Up to 200 tags/second		
21	Max Read Distance : Up to 3 ft (0.91 m) depending on tag sensitivity and orientation		

UPS

Sl.NO	Functionality	Compliance	Reason for Not complying
1	Design : Online UPS(1KVA & 2KVA)		
2	Full Load Power Supply Time : Min. 1 Hrs		
3	A.C Incoming supply 190-270 V, Single Phase,50 Hz +/-2.5 Hz.		
4	During intermittent interruption Cycle Continuously supplying power		
5	Makes : APC, Emmerson, TataLibert		

Wired Nw

SI.NO	Parameter	functionality	Compliance	Reason for Not complying
1	General	The switch should have 16 Gigabit Ports, and 4 Ports of GE for downlink and should be able to support 8 GE PoE/PoE+ Ports		
		Each switch should have 4 combo (one SFP and one Copper ports with one port active at a time) uplink Gigabit ports in addition to downlink ports.		
		Each switch should have Line Rate forwarding Rate for all ports		
		The switch should have atleast 16000 Unicast MAC addresses and 1000 IGMP Multicast Groups		
		Each switch should support atleast 1000 VLAN's and 4096 Vlan ID's		
		Switch should have Redundant DC input voltage with operating range: nominal 9.6 to 60VDC		
		Switch should have atleast 512MB DRAM and 128MB Flash memory		
2	Layer-2	The switch should support following Ethernet Standards : 802.3, 802.3x (flow control), 802.3ad (LACP), 802.1p, 802.1q		
		The switch should support loop avoidance mechanism like 802.1d (spanning-tree), 802.1s (MSTP), 802.1w(RSTP), PVST or PVST+		
		The switch should support Unidirectional Link Detection Mechanism to detect the failures of uplink port.		
		The switch should support Per port enabling/disabling of unknown unicast/ multicast flooding		
		The switch should support Layer 2 Multicast Features like IGMPv1, v2 and v3		
		The switch should REP or equivalent as ring convergence mechanism		
3	IPv6	The switch hardware should be capable of supporting IPv6		
		The switch should support following host based IPv6 features but not limited to IPv6 Addressing, IPv6 Option Processing, Fragmentation, ICMPv6		
		The switch should support IPv6 applications like Ping, Traceroute, VTY, SSH, TFTP, SNMP		
		The switch should support HTTP and HTTP (s) over IPv6		
		The switch should support IPv6 Stateless Auto Config		
		The switch should support IPv6 based Access Control Lists		
		The switch should support SNMP over IPv6 and Syslog over IPv6		
4	Security	The switch should have Port Security Mechanism with MAC Aging, Trunk Port Security and Port Security for Voice Vlan		
		The switch should support 802.1x, 802.1x Guest Vlan, 802.1x Mac-Auth-Bypass Features		
		The switch should support Secure Shell (SSH), TACAS+, RADIUS Server/Client		
		The switch should support MAC Address Notification		
		The switch should support BPDU Guard, Port Security.		

		The switch should support DHCP Snooping, Dynamic ARP Inspection and IP Source Guard Mechanisms		
		The switch should have Time Based ACL to control different policies at different times		
		The switch should support Private VLAN's		
5	QoS	The switch should support Ingress Policing and Ingress Rate Limiting of packets		
		The Switch should support 802.1p Port Priority Mechanisms		
		The switch should have Shaped Round Robin and Weighted Tail Drops mechanisms		
		The switch should support DSCP Mapping and DSCP Filtering mechanisms.		
		The switch should also support Auto Qos		
6	Multicast	The switch should support IGMPv1 and IGMPv2 Filtering		
		The switch should support IGMP v1,v2 and v3 Snooping		
		The switch should have IGMP Snooping Timer and configurable IGMP Leave timer		
		The switch should support Multicast Vlan Registration.		
7	Utility	The switch should support for GOOSE Messaging		
		The switch should support SCADA protocol Classification Support		
		The switch should have Utility specific Smart Port across/Templates		
		The switch should have MODBUS TCP/IP		
		The switch should support Dying Gasp Message support for Loss of power		
		The switch should have On Board Failure Logging and Generic online Diagnostics		
		The switch should support BFD		
8	Industrial Ethernet	Switch should have Swappable Flash memory which is ideal for quick and easy switch replacement.		
		The switch should support IEEE 1588 PTP v2 a precision timing protocol with nanosecond-level precision for high-performance applications		
		The switch should support CIP interface and CIP Time Sync functionality		
		The switch should support CIP Password Encryption as additional security measure		
		The switch should support Profinetv2 and ODVA industrial Ethernet/IP		
		The switch should have Industrial Automation Smart ports		
		The switch should support Layer 2 NAT Functionality		
		The switch should conform to various industrial standards like EN 61000-6-1 Light Industrial; EN 61000-6-2 Industrial; EN 61000-6-4 Industrial; EN 61326 Industrial Control ; EN 61131-2		
		Programmable Controllers		
		The switch should support Parallel Redundancy Protocol		
		The switch should support Static Routing		
		The switch should support Inter Vlan Routing		
		The switch should support Routing Protocols like RIPv1, RIPv2, OSPF, EIGRP, IS-IS and BGP 4		
		The switch should support Policy Based Routing		

9	Layer 3	The switch should support multicast features like PIM Sparse mode(PIM-SM), Dense Mode(PIM-DM), Sparse-Dense Mode		
		The switch should support DHCP with DHCP option 82 for data insertion and pass through		
		The switch should support HSRP or equivalent features		
		The switch should support RIPng, OSPFv3, EIGRP for IPv6, HSRPv6		
10	Ruggedization	The switch should be IP30		
		The Switch should sustain the Operating Temperature from - 40degree Celsius upto 75 degrees Celsius using a Fan Based Enclosure		
		Switch should conform to following Safety Standards like UL/CSA 60950-1; EN 60950-1; ANSI/ISA 12.12.01; CSA C22.2 No 213; IEC 60079-0, -15 IECEx test report; EN 60079-0, -15 ATEX certification (Class I Zone 2)		
		The switch should be Shock Proof, Vibration Proof and Noise Immunity		
		The switch should have Storage Temperature of -40 to 85 degree Celsius		
		The switch should sustain Relative Humidity from 5% to 90% Non-Condensing		
		The switch should comply to various Electromagnetic Emissions and Immunity standards not limited to the following :		
		FCC 47 CFR Part 15 Class A; EN 55022A Class A ; VCCI Class A; AS/NZS CISPR 22 Class A ; CISPR 11 Class A ; CISPR 22 Class A; ICES 003 Class A; CNS13438 Class A; EN55024 ; CISPR 24; AS/NZS CISPR 24; KN24 ; EN 61000-4-2		
Electro Static Discharge ; EN 61000-4-3 Radiated RF ; EN 61000-4-4 Electromagnetic Fast Transients; EN 61000-4-5 Surge; EN61000-4-6 Conducted RF ; EN 61000-4-8 Power Frequency Magnetic Field ; EN 61000-4-9 Pulse Magnetic Field ; EN 61000-4-11 AC Power Voltage; EN 61000-4-18 Damped Oscillatory Wave; EN-61000-4-29 DC Voltage Dips				
11	Manageability	The switch should have CLI as well as Web Based GUI for management		
		The switch should support Network Time Protocol		
		The switch should support Configuration Rollback		
		The switch should have USB console Port		
		The switch should be DIN-RAIL Mountable		
		Switch should have the option to apply a default global or interface level macro with a recommended configuration, allowing the user to easily set up the switch in a configuration optimized for the specific application		
		Switch Should have atleast 2 Alarm Inputs which can be used to alert external systems, ,and , one alarm output relay		
12	Makes	Cisco, Juniper, HP, Extreme networks		

Wireless Nw

Sl.NO	Parameter	functionality	Compliance	Reason for Not complying
1	Design Specifications	The wireless solution shall consist of a number of Wireless devices (including		
		Access point should support 802.11bgn and 802.11an standards		
		Access point should support Inbuilt Spectrum analysis feature to troubleshoot and analyze RF problems remotely		
		Access points should support feature to detect, classify and mitigate the non-Wi-Fi interference		
		Access point should support selective beam forming feature to improve performance of legacy 802.11abg clients		
		Each Wireless Access Node shall have the following capabilities :		
		Wireless access and at least 2 backhuals in separate radios		
		Capability to provide wireless backhaul to a wired LAN		
		The wireless system shall support multiple services like Data, Voice over IP, Video, and Mobility		
		The wireless network should support the following applications: Plant Extension, Cell site Backhaul		
		The network design should minimize the number of fiber/wired Ethernet connections required for backhaul at required throughput level		
		The total wireless system capacity shall increase as more nodes are added		
		The equipment shall support automatic over the air rate adjustment depending on signal strength and link conditions		
		Support Multiple Receiving Antenna on the access side for better Reception		
		In order to allow optimal channel selection, access points shall detect and measure the signal strength of other Access Points in the area		
		System should support 512 SSID's and the ability to choose at least 16 SSID's per Access points		
		Each access radio shall be capable of supporting different security profiles on a per SSID basis		
Multiple Authentication Servers should be supported				
The design should support the centralized architecture with Wireless LAN controller managed Access points				
2	Backhaul Specifications	The Wireless Backhaul shall operate in 5Ghz		
		The equipment shall support integrated wireless backhaul with a capability of delivering at least 20 Megabits/ TCP/ IP throughput for user traffic per backhaul link at 1200 feet		
		Support Encrypted and authenticated connectivity between all backhaul components		
		Wireless Access Nodes shall provide a 'wired' interface for connection to local area networks or backhaul of local clients		
		Wireless access node shall provide Power Over Ethernet through the wired interface to power other equipment		
		The following interface options shall be available;10/100/1000 Ethernet interface 1000 BaseFX single mode fiber interface		
3	Management	Support for SNMP version 2 as well as 3		
		Web Graphical User Interface must support HTTPS		
		Support Single management solution for both Indoor and outdoor wireless Networks		
		Support for TACACS+ or RADIUS for authentication of users to the network		
		All management interfaces supported via Access Control Lists		
		The solution supports redundancy / fault tolerance		
		The network management system must scale to support in excess of 1000 managed elements		
		The network management systems must support automatic configuration download to the network elements		
		Historical alarm information must be archived by the network management system		
		The network management system must be capable maintaining logs for all management activity performed to all components of the mesh network		
		The network management system must support client/server capabilities with separate access levels and defined user portals		
		The network management system must support standard northbound interfaces		
		The network management system must be capable of alarm filtering to the northbound interface		
4	Environmental and Electrical Specifications	Outdoor Equipment shall support powering from AC at 110- 240 VAC (50-60Hz) or 56VDC input		
		Equipment shall support POE		
		Equipment shall support pole, wall, and roof mounting options		
		Geographic orientation flexibility – tilt angle for pole, wall, and roof mounting units		
		The equipment shall support up to 100 MPH sustained winds & 165 MPH wind gusts		
		The Access point shall be IP67 / NEMA4 rated for dust and water ingress		
		The Access point shall be rated for operation over an ambient temperature range of -40 F (-40 C) to +122 F (+ 50 degree Celsius)		
		Power consumption shall be less than 120 Watts meeting all safety specifications		
Mounting of the unit cannot exceed 24 inches higher than the top of the light pole / structure				

Digital Signpad

SI.NO	Functionality	Compliance	Reason for Not complying
1	Pen Tablet to capture signatures & drawings to insert into documents & applications		
2	USB interface		
3	Cordless digital Stylus pen with pen-tip and two barrel buttons		
4	Dimensions: 305.5mm X 268.4mm X 10.5mm		
5	Minimum Work Area: 8X6 inches		
6	OS compatibility		
7	Suitable for port weather conditions		

CISF cabins

SI.NO	Functionality	Compliance	Reason for Not complying
	Features		
1	04'X06'X8.5'H		
2	TUBELIGHT:1		
3	FAN: 1		
4	WINDOW:1: 3ftx3ft SERVICE WINDOW/(3ftx3ft)		
5	DOOR: 1 (6.5x3ft) WITH SHED (6 Inch)		
6	MCB: 1		
7	MainSwitch : 1		
8	ELECTRIC POINT: 5 amps. – 2		
9	A.C POINT. 1		
10	Cooler point ; 1		
11	Exhaust fan ; 1		
12	LCD/ PC provision;1		
13	Chairs - 2		
14	Seating space for two officials		
15	BASE FRAME: 50x50mm square pipes. & cross members for nesting are used nesting are used 40x80, C'Channel /40x40 square pipes.18mm cement sheet mounted with vinyl flooring.		
16	ROOF FRAME : M.S 18swg Corrugated sheet welded with M.S. frame Structure. Top inner ceiling decorated with 9mm particle board.		
17	SIDE WALLS: M.S. frame work with square pipes, & wall thickness 50mm.		
18	EXTERIOR WALL: 18swg M.S. bended sheet welded on M.S. frame.		
19	INTERNAL WALL: 9MM particle board.		
20	CORNER POST: Made of specially 50mm x 50mm square pipe.		
21	DOOR: Frame work by tubular pipe of 40x20 external wall made by 18swg. M.S sheet & inner wall decorated by 4mm hardener board, with suitable looking arrangement.		
22	INSULATION: 50 mm thick Glass Wool insulation shall be used for selected walls and 25mm thick Glass Wool insulation to be provided for roof.		
23	ELECTRICAL: All wiring shall be concealed and shall be pvc insulated copper wires of ISI quality, gauge 1.5sqmm used for light, socket & 4sqmm for main incoming supply, 5amp plug with switches, & overhead light above the door and light.		
24	PAINTS: All components are externally painted with single coat of Zinc phosphate & final coat of corrosion free HD paint		
25	LEGS : 4 corner legs 4 inch		
26	SHADE: 18swg M.S. sheet above the door with a depth of 6"		



Kolkata Port Trust

KOLKATA PORT TRUST

Supply, Installation, Commissioning, and Maintenance of RFID Systems at Kolkata Dock System, Kolkata Port Trust

Request for Proposal

Annexure III: Installation Requirements

Document Reference No: **PIg/165/RFID/11667**

Date: 18th April 2017.

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

Table of Contents

1.	INSTALLATION REQUIREMENTS	4
1.1.	SITE INSPECTION FOR REQUIREMENT GATHERING	4
1.2.	SERVICE PROVIDER'S DESIGN RESPONSIBILITY	4
1.3.	APPROVAL BY THE KOPT AUTHORITY	5
1.4.	RFID SOLUTION CONFIGURATION AND IMPLEMENTATION:	5
1.5.	ELECTRICAL DESIGN REQUIREMENTS	5
1.6.	UNINTERRUPTIBLE POWER SUPPLY UNIT	6
1.7.	POWER DISTRIBUTION EQUIPMENT ELECTRICAL REQUIREMENTS	6
1.8.	UPS LOADS	7
1.9.	FEEDER TO UPS	7
1.10.	CABLING TO UPS LOADS	7
1.11.	CABLES AND CABLING MATERIALS	7
1.12.	LOW VOLTAGE P.V.C. INSULATED COPPER CABLES	7
1.13.	LOW VOLTAGE P.V.C. INSULATED ALUMINIUM CABLE	8
1.14.	INSTRUMENT CABLES	8
1.15.	COMMUNICATIONS CABLES	8
1.16.	DATA COMMUNICATION CABLES	8
1.17.	CABLE LUGS AND FERRULES	9
1.18.	CABLE LUGS AND FERRULES FOR CABLES RATED ABOVE 1000 VOLTS	9
1.19.	CABLE LUGS AND FERRULES FOR COPPER CABLES RATED BELOW 1000 VOLTS	9
1.20.	CABLE LUGS AND FERRULES FOR ALUMINIUM CABLES RATED AT BELOW 1000 VOLTS	9
1.21.	CABLE SUPPORTS	9
1.22.	CABLE TRAY	10
1.23.	CABLE RACKS	10
1.24.	CABLE NUMBERING	10
1.25.	CABLE WIRE NUMBERS	11
1.26.	CABLE DRAWINGS AND DOCUMENTATION	11
1.27.	CABLE TESTING	11
1.28.	FIBER OPTIC CABLE TESTING	11
1.29.	CABLE INSTALLATION	11
1.30.	CABLES IN PIPES OR DUCTS	12
1.31.	CABLE SUPPORTS	12
1.32.	CABLE JOINTS AND TERMINATIONS	13
1.33.	JOINTS FOR INSTRUMENT AND COMMUNICATIONS CABLES	13
1.34.	PROOF JOINTS	13
1.35.	CABLE TERMINATIONS	14
1.36.	TERMINATION OF ARMoured CABLES	14
1.37.	JUNCTION BOXES	14
1.38.	INSTALLATION OF EQUIPMENT ON CONCRETE BASES	15
1.39.	PREPARED BASES WITH CAST-IN HOLDING DOWN BOLTS AND DUCTS	15
1.40.	BASES OR SURFACES WITHOUT CAST-IN FIXING OR ENTRY DEVICES	15
1.41.	GROUTING IN OF BASES	16
1.42.	SUBMISSION OF INTERFACE DETAILS	16

1. Installation Requirements

This section covers the minimum requirements of all the Works with respect to the supply, installation, jointing, termination and connection of power, control, instrumentation, communications and earthing cables, the supporting and support materials required for the cable installations and the installation of RFID equipment. The Service Provider shall take note of the installation conditions on the site.

1.1. Site inspection for requirement gathering

Service Provider is responsible for inspection of the KoPT premise, gates, buildings, etc. where proposed RFID solution would be implemented. Service Provider should study the AS-IS situation for designing the solution. The functional process defined in the RFP Annexure I is after considering the As-IS situation. However, it is the responsibility of the Service Provider to re-validate the same including the proposed solution and obtain an approval from KoPT.

1.2. Service Provider's Design Responsibility

The RFID System Service Provider shall be required to produce engineering design drawings of all RFID System equipment / system electrical installation and computer network systems and shall be required to have these designs approved by an appropriate KoPT Authority authorized to do so. This also includes the equipment cable routing drawing in AutoCAD format which shall be approved by the KoPT Authority. The Service Provider shall be intimated in advance before the start of civil works to depute their representative to execute civil works requirements as submitted by Service Provider and approved by KoPT Authority. It would be the responsibility of the Service Provider to supply and lay the ducts and other installation accessories for all RFID Equipment's and accessories. The duct specifications shall be approved by the KoPT

Authority. Once the designs have been approved, only then the Service Provider may commence installation works on site. It shall be the Service Provider's responsibility to take required efforts to ensure that all required approvals are obtained in time to meet the contractual milestones and completion dates.

1.3. Approval by the KoPT Authority

Once the design drawings have been completed and finalized by the Service Provider, these shall be submitted to the KoPT Authority or any other authority indicated by the KoPT for review/ approval. Should there be any deficiencies in the design submitted by the Service Provider, KoPT Authority shall convey these to the Service Provider and the Service Provider shall modify and resubmit the design for KoPT Authority's approval. The minimum duration of this process shall be 10 working days and the Service Provider shall make adequate provision for sufficient iterations of the process to acquire the required approval.

1.4. RFID solution configuration and implementation:

- Service Provider shall configure the RFID solution and components as per the requirements stated in the RFP and/ or any further requirements that were finalized in consultation with KoPT
- All configurations and implementation should be such that it supports further scaling-up of the solution as per future needs
- Solution should be configured for redundancy so that there are minimal downtime
- Solution should support legacy systems or should support import of data from legacy systems in common standard formats
-

1.5. Electrical Design Requirements

- The Service Provider shall provide the detailed electrical load break-up (actual consumption) of each individual component as well as complete System for the design of Electrical system. This shall form part of PAT, FAT and SAT checklist.
- The Service Provider shall be required to comment / confirm on the design of the

power reticulation system for the RFID System

- Equipment, which shall include the cabling, distribution boards, uninterruptible power supply units and clean earthing system, in regard to the suitability for the RFID System.
- Port, Gate and administrative equipment and computer systems shall be separated from the RFID System earthing. This shall be done by Service Provider.

1.6. Uninterruptible Power Supply Unit

- The Service Provider is required to design, supply and install the Uninterruptible Power Supply (UPS) system for RFID system.
- The UPS design shall take the following into account:
 - The system shall be capable of maintaining an uninterrupted power supply to the UPS loads for a sustained period of at least 4 hours under full load conditions from a fully charged battery.
 - It shall also be capable of continuously supplying power to the system under an intermittent interruption cycle.
 - The UPS shall be capable of operating at input voltages of A.C Incoming supply 190-270 V, Single Phase, 50 Hz +/-2.5 Hz. .
 - The Service Provider shall issue a certificate to the KoPT Authority that the equipment has been tested for load capacity and insulation at the applicable rated voltages and loads. KoPT Authority shall reserve the right to witness these tests as part of SAT. The results of such tests however shall not relieve the Service Provider of any obligations of any nature.
 - UPS along with its battery shall be compact and shall be housed in a wall mountable enclosure with suitable ventilation arrangements. The design for the same shall be submitted by Service Provider and approved by KoPT Authority.
- The UPS make and the model shall be as quoted in the bid. Further the product will be approved by KoPT Authority during detailed engineering phase.

1.7. Power Distribution Equipment Electrical Requirements

The Service Provider shall supply and install the uninterruptible power distribution

equipment for the UPS units supplied. UPS distribution equipment for these UPS units shall be suitably sized for the loads. The ratings of circuit breakers shall be graded to ensure proper differential protection. Notwithstanding the abovementioned requirements, it is the responsibility of the Service Provider to ensure that the capacity and ratings of the distribution equipment are suitable for the application.

1.8. UPS Loads

The Service Provider shall be responsible for the design and sizing of the UPS power distribution equipment and shall submit it to the KoPT Authority. Dynamic loads shall be isolated from the main central UPS supply and it shall be the responsibility of the Service Provider to recommend a suitable scheme.

1.9. Feeder to UPS

The RFID System equipment will be supplied from a Utility/Emergency Power circuit breaker by KoPT. The Service Provider shall be required to specify the rating and capacity of this breaker based on the calculated loads and the line current for the RFID equipment UPS.

1.10. Cabling to UPS Loads

The Service Provider shall supply, install, terminate and connect all cabling from the power DB to all the RFID lane equipment and UPS. The cable shall be suitably sized 2-core and earth PVC insulated and steel wire armored copper cables. Wire armoring may be omitted if the cables are placed in a conduit.

1.11. Cables and Cabling Materials

The Service Provider shall be required to design the cable installation for the system to meet the performance criteria of the system and to comply with all local and national regulations and legislation. As a minimum requirement, the cables shall comply with the following:

1.12. Low voltage P.V.C. Insulated Copper Cables

All P.V.C. insulated cables shall be multi core P.V.C. insulated, P.V.C. sheathed,

galvanized steel wire-armored and P.V.C. covered 660 V graded cables of Heavy Duty or General Purpose type.

1.13. Low voltage P.V.C. Insulated Aluminium Cable

The cable supplied and installed shall be of solid aluminum conductor, P.V.C. insulated, P.V.C. bedded, aluminum strip armored and black P.V.C. overall sheathed.

1.14. Instrument Cables

All instrument cables required for data communications shall be P.V.C. insulated stranded or solid copper wire (as specified) in twisted pairs with surface printing on one core of each pair for circuit identification, tinned stranded copper drain wire per pair and each pair and drain wire screened with a helically applied metal-polyester laminate tape (Aluminum-Mylar). Single pair cables shall be given an outer jacket of P.V.C. for mechanical protection and multi-pair cables shall be given an overall Mylar screen and an outer PVC jacket. Where cables are installed on open cable tray/racks or are buried in cable earth trenches, the cable shall be given a steel wire armoring and P.V.C. outer jacket. All instrument cables shall be provided with a stripping cord between the outer Mylar screen and the jacket to facilitate removal of the jacket.

1.15. Communications Cables

Communications cables shall be in accordance with the applicable national standards for telecommunications with the added requirement of steel wire armoring and P.V.C. outer jacket when specified for direct burial in earth cable trenches or installed on open cable tray/racks.

1.16. Data Communication Cables

Communication cables for local area networks will be Shielded Twisted Pair (STP) cabling of suitable category to support at least 1 GB switch for distances of less than 100 m. Category 5e / 6 certification and detailed testing shall be required in the presence of Port Authority's Engineer. For connection lengths of greater than 100 m, fiber optic cable shall be used.

1.17. Cable lugs and ferrules

All cable lugs and ferrules shall be correctly sized to contain each and every strand of the cable conductor to be connected or terminated.

1.18. Cable lugs and ferrules for cables rated above 1000volts

Only electro tinned copper cable lugs and ferrules shall be used. The barrel of the lugs and ferrules shall be of the barrier type and shall be sufficiently long to accommodate two hexagonal crimps and allowing a half crimp length of barrel either side of each crimp. The spade of the lugs shall be sized to suit the current carrying capacity of the cable conductor.

1.19. Cable lugs and ferrules for copper cables rated below 1000 volts

The cable lug and ferrules shall be as specified above but may be indent crimped instead of hexagonal crimped.

1.20. Cable lugs and ferrules for aluminium cables rated at below 1000 volts

All aluminum cable terminations and joints shall be made using 99.9% pure sector shaped aluminum lugs. The lugs shall be supplied factory cleaned and greased and shall be installed without removing the layer of protective grease. The barrel of the lugs must be long enough to take two indent crimps.

1.21. Cable Supports

The Service Provider shall be required to provide and install all cable supports for all cables required for the system where these are not provided as part of the Civil and Building Contract. The Service Provider may however request certain brackets to be fabricated into support structures such as the canopy or cast into the concrete works. The Service Provider shall be required to supply any such details to KoPT Authority in sufficient time for these to be included in the construction works of others. Should the Service Provider fail to provide these details in sufficient time for their inclusion, this shall not reduce the Service Provider's responsibility to provide the required cable supports.

1.22. Cable tray

The Service Provider shall provide perforated cable tray fabricated from a minimum thickness of 1.2mm mild steel sheets and having a minimum turn up at the sides of 15mm. The width of the trays shall be 300mm for the main run along the length of the tunnel and branch tray shall be 50/100mm as found necessary by the Service Provider. The transitions to different planes or intersections with runs of racking shall be by means of prefabricated transition sections of correct radius for right/left hand bends, vertical bends, tee-sections or changes in racking width. The perforations shall run lengthwise and the fabricated tray shall be hot dipped galvanized. Any inter-section of a section of the cable tray shall be made with prefabricated transition sections only, i.e. right/left hand bends, vertical bends or tee-sections. Any damage to the galvanizing shall be restored by an approved method and no sharp edges shall be permitted that could damage cables or injure persons. The cable tray sections shall be bonded together with appropriately sized earthing straps of suitable material to prevent any galvanic or electrolytic action.

1.23. Cable racks

Cable racking shall be fabricated from rolled strip mild steel welded to form a ladder configuration. The construction shall ensure adequate rigidity of the racking under full loading conditions and shall not permit any noticeable deflection of the installed racking to exist. The fabricated sections shall be hot dipped galvanized.

1.24. Cable Numbering

- All cables installed at the RFID Port shall be numbered in accordance with the universal cable numbering system. There may be more than one Contractor designing portions of the Works requiring cable numbers. Random selection of cable numbers is therefore not permitted. Hence, it is the responsibility of the RFID Service Provider to provide the range of numbers of cables allocated to such contractor's portion of the total project.
- All cables shall be provided with the specified cable number tag at 5 m intervals unless otherwise specified and at all cable terminations just below the cable gland or end and at points where cables enter or leave cable ducts or pipes.

1.25. Cable wire numbers

Each core of each cable shall be ferruled with the core number on both ends of the cable.

1.26. Cable drawings and documentation

- All drawings prepared by the Service Provider shall be clearly marked up to show the cable numbers, wire numbers and core cross section.
- A comprehensive cable book shall be prepared covering the specifications and connection details of all cables with core color, connectors, lugs, etc. which shall be submitted by the Service Provider as part of Technical Specifications delivery and approved by KoPT Authority. This shall be also showing each individual equipment connection with parent equipment in PIN diagram format.

1.27. Cable testing

All cables shall be pressure tested to the relevant and applicable Specification, before connecting up and before backfilling of cable earth trenches commence.

1.28. Fiber Optic Cable Testing

The Service Provider shall be required to test all fiber optic cables supplied and installed, if any, irrespective of whether the core of the cable has been used in the installation or not.

1.29. Cable Installation

- Each end of all cables shall be provided with a cable tag as specified. All cables shall be run off drums such that the cables are always laid head to tail. When cables are required to be drawn through pipes, figure-of-eight techniques shall be employed.
- All drawing of cables shall be carried out in accordance with good practice using rollers, winches, RFID, and all precautions taken to prevent damage to the cables. Temporary provisions shall be made to all sharp edges to prevent any damage to the cables.
- KoPT Authority shall reserve the right to reject any cable damaged or affected by poor or non-compliant installation techniques.

- Where trenches are dug for laying of ducts / cables, the area shall be restored to earlier condition up to satisfaction of Port Authority after completion of works.

1.30. Cables in pipes or ducts

Where cables are to be installed in or drawn through pipes or ducts, these ducts will normally be installed by the Service Provider in the presence of KoPT authority's representative as nominated/ directed by KoPT Authority. The cable to be drawn through the pipes must be installed in such a way that the minimum length of cable is drawn through the pipe.

1.31. Cable Supports

All cables installed above ground on concrete, brick or steel surfaces shall be supported and fixed to the surfaces in the following ways:

a. Cable saddles

Where only one cable is to be installed in a specific location, the cable shall be supported by means of Fisher stand-off cable saddles spaced every 500 mm. The saddles shall be fixed to the concrete, brick or steel surface by means of stainless steel screws into either drilled and plugged holes in concrete or brick surfaces, or drilled and tapped holes in steel surfaces.

b. Cable tray

Where more than one cable is to be installed in a specific location and it is not practical in the opinion of KoPT Authority, to secure each and every cable to the given surface as specified in a) above, the cables shall be installed on galvanized perforated cable tray or racks. Each and every cable shall be individually strapped to the cable tray at intervals of 500 mm using adequately sized nylock strapping. The cable tray shall be supported at intervals of not greater than 100mm or as specified by the cable tray/rack designers, using Unistrut (or equal approved) support arms or cantilever shelf brackets when the cable tray is in a horizontal plane parallel relative to the floor or ground. Cable trays in all other places shall be supported with P1000 Unistrut (or equal approved) brackets at intervals of not greater than 1000mm. The brackets shall be secured to steel surfaces using stainless steel bolts in tapped holes. Stainless steel screws in drilled and plugged holes shall be used to secure the bracket

to brick and concrete surfaces. At least two suitably sized screws or bolts shall be used to secure each bracket. The main cable tray running along the length of Tunnel shall be provided to the Service Provider. All branch cable trays and Cable Management System ducts in the tunnel, booth, canopy, POS and Port building shall be supplied and installed by the Service Provider.

1.32. Cable Joints and Terminations

- The jointing of cables throughout the installation shall not be permitted unless the length of the cable between two consecutive termination points of the cable is greater than the manufactures standard drum length. Where cables are damaged or become faulty, these cables shall be removed and new ones shall be laid, as directed by KoPT Authority, but shall be to the cost of the Service Provider.
- All jointing of cables when approved by KoPT Authority shall be carried out in accordance with the requirements of the cable Service Provider. The joint shall maintain the mechanical and electrical strength of the cable. All screening, earthing and armouring contained in the cable shall be carried through in the joint. All conductors within the joints shall be physically separated from other conductors or conducting materials using prefabricated separators.

1.33. Joints for instrument and communications cables

The jointing of instrument and communications cables shall normally not be permitted. Where specifically approved by KoPT Authority in writing, the joints shall conform to the low viscosity resin, approved by the Department of posts and Telecommunications, shall be used and all screens and drain wires shall be separately carried through.

1.34. Proof joints

The procedure for all cable joints is subject to prior approval by KoPT Authority. Once the procedure has been submitted to KoPT Authority, the first joint for each type of cable shall be carried out in the presence of KoPT Authority and the referenced joint shall serve as a bench mark for all other joints on cables of the specified type.

1.35. Cable Terminations

All cable terminations shall be carried out in accordance with the requirements of the Service Provider. All hand operating crimping tools shall incorporate a mechanism to ensure that the crimping operation once commenced, is completed before the handles are released.

1.36. Termination of armoured cables

- All terminations of cables in switch boards, distribution panels and equipment specified on the drawings or in the specification shall be terminated on to an earthed gland plate using an approved mechanical cable gland fabricated from nickel plated high tensile brass or equal approved. The gland shall incorporate a self-centering cone bush, which shall wedge each and every strand of the cable armouring against a gripping cone as well as a lock nut for securing it to the gland plate. The gland, when completely installed, must be protected by a rubber boot enclosing the exposed portion of the armouring.
- Where Earth Continuity Conductor (E.C.C.) cable is used, terminations shall be made using integral-cone glands with a machined groove to accommodate the earthing strands. Glands with slots cut through the body are unacceptable. The tails of the conductors shall be neatly laid and bound together at intervals of 500 mm using nylock, or equal, approved strapping. Each conductor shall be ferruled with the terminal number given on the drawings.

1.37. Junction Boxes

Where the Service Provider is required to provide junction boxes, these shall be clearly identified in the design and shall only be permitted where multiple cable runs are not possible. Any junction box shall therefore require prior approval of KoPT Authority. The Service Provider will not be permitted to use a junction box as a cable distribution point.

- **Power cable junction boxes**

All junction boxes to be supplied and installed for power cables shall be fabricated from materials of suitable mechanical strength allowing for the installation of cable

glands, cable terminals with DIN rail connectors, IP65 sealing of covers and cable entry points and shall include for the supply and installation of the correct size mechanical cable gland with waterproofing shroud, connectors and connector shrouds.

- **Instrument and communications cable junction boxes**

All junction boxes to be supplied and installed for instrument and communications cables shall be sized to suit the number of pairs of cores of the relevant cables. The box shall be fabricated of moulded polycarbonate materials with breakouts for cable entries. The box shall have a waterproof cover of transparent polycarbonate material secured to the base with polycarbonate or cadmium plated recessed captive screws. The box shall be equipped with connector blocks and fixing DIN rails. The junction box shall be rated for IP68 for cover plates and cable glands.

1.38. Installation of Equipment on Concrete Bases

This section covers the installation of fabricated items of equipment on to concrete bases cast for the purpose of supporting the equipment.

1.39. Prepared bases with cast-in holding down bolts and ducts

Where the Service Provider has supplied cast-in items such as frames, ducts and holding down bolts, these will be installed by the Service Provider only. The Service Provider shall erect the equipment onto the concrete bases and shall supply and install two nuts and two washers for the securing and levelling of the equipment to the bases. All nuts and washers shall be galvanized. The equipment shall be levelled and aligned to the vertical, to the satisfaction of KoPT Authority, using the levelling nut and washer on the fixing bolt under the equipment. All holding down bolts shall be supplied and installed with sufficient length to accommodate both the levelling nut and washer and the fixing nut and washer. The nuts shall be correctly torqued tight after alignment. Where equipment is subject to vibration or cyclic loads, each holding down bolt shall be fitted with a spring washer under the fastening nut.

1.40. Bases or surfaces without cast-in fixing or entry devices

- Where the Service Provider has not required special cast-in items for fixing or entry ducts, the Service Provider shall drill and fit anchor bolts to secure the equipment.
- No drilling of any concrete surface shall be permitted without written approval of KoPT Authority. No explosive powered tools will be permitted to provide fixing devices for any equipment under any conditions. All holding down bolts shall be supplied and installed with sufficient length to accommodate both the levelling nut and washer and the fixing nut and washer. The nuts shall be correctly torqued tight after alignment. Where equipment is subject to vibration or cyclic loads, each holding down bolt shall be fitted with a spring washer under the fastening nut.

1.41. Grouting in of bases

After erection and alignment of the equipment to the satisfaction of KoPT Authority, the torqued holding down bolts and base plates shall be grouted with cement mortar, freshly mixed, in the volumetric proportions of 3 parts sand and 1 part cement or as directed by KoPT Authority. The Service Provider shall submit for approval a method statement of each type of base to be grouted and KoPT Authority will, upon the successful completion of a type of base, issue a certificate of acceptance for the base, which shall be used as a bench mark for all other similar bases.

1.42. Submission of Interface Details

a. Securing Brackets

Where the Service Provider requires specific mounting brackets or fixing mechanisms to be supplied and installed by others, the Service Provider shall provide the details of the physical interfaces, required or recommended materials and any possible alternatives, dimensions of the interfaces, fabrication tolerances, orientation details and any other information that will affect the installation and operation of the equipment. If the item of equipment requires a certain spatial degree of freedom, the complete locus of the arcs for each degree of free shall be given. The Service Provider shall provide all this information on drawings and schedules and on soft copy in the agreed contractual information interchange formats.

b. Holding down bolts

Where the Service Provider requires holding down bolts to be cast into concrete surfaces by other civil contractor/ Service Providers, the Service Provider shall provide the details of these bolts including the length of bolts, length of threaded sections, sizes, thread pitch, materials, tolerances, orientation details and any other information that will affect the installation and operation of the equipment. Where the Service Provider requires tolerances that are not normal to the civil and building industry, the Service Provider shall provide the bolt cages to other civil Service Providers for casting into the civil works. These bolt cages shall be sufficiently rigid to endure the installation process. These bolt cages shall be included in the part of works.

c. Cable Ducting

Any cable ducting required by the Service Provider between equipment in the field RFID and the RFID controller/server, or into the canopy or to the buildings, shall be indicated on the civil construction drawings provided by KoPT civil Service Provider/designer. Where the civil designs cannot accommodate the initial requirements of the Service Provider, the Service Provider shall develop alternative proposals to ensure that all equipment is properly and safely interfaced.

===== END OF DOCUMENT=====



Kolkata Port Trust

KOLKATA PORT TRUST

Supply, Installation, Commissioning, and Maintenance of RFID Systems at Kolkata Dock System, Kolkata Port Trust

Request for Proposal

Annexure IV : General Testing and Commissioning requirements

Document Reference No: **PIg/165/RFID/11667**

Date: 18th April 2017.

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

Table of Contents

1.	GENERAL TESTING & COMMISSIONING REQUIREMENTS.....	4
1.1.	COMMISSIONING	5
1.2.	FACTORY ACCEPTANCE TESTING.....	6
1.3.	ON-SITE TESTS AND INSPECTION	6
1.4.	ADDITIONAL TESTING.....	6
1.5.	PERFORMANCE TESTING	7
1.6.	ENDURANCE TESTING.....	7
1.7.	FINAL ACCEPTANCE – SITE ACCEPTANCE TEST (SAT)	8
1.8.	TEST PLANS	10
1.9.	ON-SITE CABLE TESTS	10
1.10.	PRE-TESTING	10
1.11.	TEST EQUIPMENT AND TOOLS.....	10
1.12.	MANUFACTURER'S FIELD SERVICES	10
1.13.	PROCEDURE FOR TESTS	11
1.14.	TEST REPORT	11
1.15.	OPERATIONAL TESTS	11
1.16.	DEFECTS LIABILITY PERIOD (DLP)	12
1.17.	SITE ASSISTANCE AND ADJUSTMENTS	12
1.18.	CUSTOMIZATION	12
1.19.	MAINTENANCE	13
1.20.	OPERATION AND SUPPORT:	14
1.21.	ON-SITE SUPPORT.....	14
1.22.	SPARE PARTS AND EXTRA MATERIALS	16
1.23.	CLEANING	16
1.24.	DEMONSTRATION.....	17

1. General Testing & Commissioning Requirements

- All Types of Tests Mentioned prior to proving period are part of Testing & Commissioning Phase
- The Testing shall be conducted in successive phases:
 - a) Factory acceptance test in Service Provider's premises
 - b) Integration test at Port's Site
 - c) Performance test at the Project Site
 - d) Endurance and stressing test at the Project Site
 - e) Final acceptance tests (FAT)at the Project Site
- The Service Provider shall design detailed test procedures to verify the full compliance of the installed System with tender requirements and Specifications. The test procedure documents must be sent for validation by KoPT authorities one (1) month before the commencement of the tests. This shall include Deployment and Commissioning Strategy with detailed Site Inspection plan for the Systems documentation delivery.
- The Service Provider shall be responsible for incorporating and testing any modification found necessary as a result of the tests. KoPT reserves the right to require any completed test to be re-run to verify that no adverse effects result from the change.
- The Service Provider shall also be responsible for updating all impacted documents, including the revised test procedures. The Service Provider shall propose a new schedule for the respective tests. Nonetheless, the Service Provider shall be responsible to ensure that the project key dates are respected and adhered to.
- There will not be any additional cost of any form for re-running the tests and making the required modifications to the source code and/or documents.

- All the functions of the System shall be tested. The tests will be of black box type, i.e. from the user point of view, without having to go through the step-by-step processing of the System.
- The Service Provider shall be responsible to prepare all the test data based on the KoPT's requirements/ scenario that may be required before running the tests.

1.1. Commissioning

- The Service Provider is required to perform a range of Site Acceptance Tests on the site for each individual sub-system to demonstrate that all items have been correctly installed and adjusted on a location-by-location basis and that the sub-system operates in every respect in accordance with the Specification.
- During this phase the equipment are powered and the automation and networking are gradually integrated layer by layer.
- The Service Provider is required to perform a full system test after end-to-end system implementation to demonstrate that the complete system, software and associated components are functioning properly.
- The tests shall be performed by the Service Provider and will be witnessed by the KoPT authority/ or any agency or unit nominated by KoPT.
- Any defects which may become apparent during the course of these tests shall be immediately rectified by the Service Provider at his expense.
- Any change in the design that may appear during the systems' coverage site surveys and/or testing and commissioning shall be rectified by the Service Provider at his expense.
- The Site Acceptance Test data shall be prepared by the Service Provider and submit to Port for approval.
- All Site Acceptance Tests shall be carried out in the presence of KoPT Authority's representatives who shall sign off the testing/ result documentation on satisfactory completion of the tests.
- The Site Acceptance Test Specifications, at every level, shall be subjected to configuration management and change control by the Service Provider.
- If modification or reprogramming is required as a result of the tests and site

surveys, all affected parts of the Site Acceptance Tests, as determined by the KoPT, shall be re-tested.

- The results of the Site Acceptance Tests, version of software and hardware tested, together with any re-testing as a result of changed requirement/ failure, shall be recorded and signed by the authorized personnel of the Service Provider and the KoPT's representatives.

1.2. Factory Acceptance Testing

- The Service Provider shall design detailed test procedures to verify the full compliance of the installed system with tender requirements and specifications
- The FAT shall be performed in Service Provider premises in India.
- KoPT will have the option to conduct /witness FAT of approve the equipment based on the factory test results.
- KoPT will bear all travel expenses of its team for conducting FAT.

1.3. On-Site Tests And Inspection

- The purpose of this phase is to check the assembly and the connection of the equipment without any power supply.
- The inspection/ verification can give rise to a punch list item either because of an anomaly or non-conformity with the tender documents.
- The inspection/ verifications are made sequentially for geographical area, each area giving rise to its own punch list.
- The punch lists are collated for each module and the phase report is only released when all the stipulations on the punch lists are cleared.

1.4. Additional Testing

- Each interface will be tested with the actual System from the other party. No simulator will be used.
- Every type of data exchange will be tested. For each type of data exchange, every case leading to a different processing by the one of the two systems will be tested.

- The Integration Testing shall be performed at site using PACS server. The Integration Testing shall be performed by the Service Provider in the presence of the KoPT Official and its assigned representatives. KoPT will reserve the right to perform some of the tests during the Integration Testing.
- All tests pertaining to the System will be conducted with the minimum interruptions to the Port operations and the operational functions of all existing systems. All tests affecting the Port operations and the reliability and availability of the existing systems will be scheduled during low traffic period in consultation with the KoPT. The Service Provider will be liable for all damages caused to the reliability and availability of the existing computer systems resulting from the testing of the proposed RFID System.
- The Service Provider shall be responsible to drive the interface tests and shall be responsible for the schedule, the test procedures (this shall include Deployment and Testing Method with detailed Site Inspection/Witnessing plan for the Systems documentation delivery), the organization of the tests, etc.
- All testing schedule shall be conducted with at least seven days' advance notice to KoPT authorities

1.5. Performance Testing

- Performances tests will include but not limited to response times, load tests, stress tests.
- The Service Provider shall be responsible to create the required scripts and sets of test data to perform the various performance/ load tests. If a tool is required to simulate required transactions at the same time and performing the same action simultaneously, the Service Provider shall be responsible to develop/ get such simulation tool for conducting the tests. Such a tool would not constitute a deliverable to the KoPT Authority.

1.6. Endurance Testing

- Endurance tests will include but not limited to the manual switch-over from the primary server to the secondary/ backup server , automatic switch-over from a

primary server to the secondary/ backup server in all possible failure modes, including but not limited to hardware failure, process failure, software failure, etc.

1.7. Final Acceptance – Site Acceptance Test (SAT)

- The Service Provider shall design detailed test procedures to verify the full functionalities and compliance of the installed System with reference to the tender requirements and specifications and user requirements finalized during the SRS study stage. The test procedures shall be submitted to the KoPT Authority for approval one (1) month before commencement of the SAT. This shall include Deployment and testing methods with detailed site Inspection/Witnessing plan for the Systems documentation delivery.
- These tests will form a part of the acceptance requirements by which the Service Provider shall demonstrate, to the satisfaction of the KoPT, that the installed System and solution fulfils KoPT's requirements.
- The SAT will be performed on-site at the KoPT's premises on the operational platform. The SAT will be performed by the Service Provider in the presence of the KoPT Official and/ or its assigned representatives. KoPT will reserve the right to perform some of these tests again during the SAT to re-verify the test results.
- There will be no modification to the source code after the beginning of the SAT until the tests have all been run/ completed.
- The Service Provider shall be responsible for incorporating any modification found necessary as a result of the tests and conduct the test again with the modified system. KoPT reserves the right to require any completed test to be re-performed to verify that no adverse effects result from the change.
- The Service Provider shall also be responsible for updating all impacted documents, including the revised test procedures. The Service Provider shall propose a new schedule for the respective tests. Nonetheless, the Service Provider shall be responsible to ensure that the project key dates are respected/ adhered to.
- There will not be any additional cost of any form for re-performed tests and making the required modifications to the source code and/or documents.
- All tests pertaining to the System will be conducted with the minimum

interruptions to the Port operations and the operational functions of all existing systems. All tests affecting the Port operations and the reliability and availability of the existing systems will be scheduled during low traffic period in consultation with the KoPT. The Service Provider shall be liable for all damages caused to the reliability and availability of the existing systems resulting from the testing of the System.

- The SAT will be conducted in accordance with the approved test procedures and will be witnessed by KoPT Official. All test results of the SAT will be properly recorded, documented and made available to KoPT Authority. The System will be deemed to have satisfactorily fulfilled the SAT when all the tests have been completed successfully.
- The Service Provider shall furnish all the necessary tools and test equipment required to run the SAT in accordance with this section.
- Any software or hardware failure, unscheduled restart or changeover during the SAT will be logged, reported and investigated by the Service Provider. The Service Provider shall be responsible to determine the cause of any failure and make the necessary modifications to rectify the problems.
- The SAT is split into Functional tests, Interfaces, Performances tests, Degraded modes tests.
- All the functions of the System shall be tested. The tests will be of black box type, i.e. from the user point of view, without having to go through the step-by-step processing of the System.
- The Service Provider shall be responsible to prepare all the test data that may be required before running the tests.
- The Service Provider shall be responsible to drive the interface tests: he shall be responsible for the schedule, the test procedures, the organization of the tests, etc.
- Each interface shall be tested with the actual System from the other party. No simulator will be used.
- All data exchanges involving different modules/ systems shall be tested.
- .

1.8. Test plans

- All tests are to be carried on according to a detailed test procedure, which shall be submitted by the Service Provider and approved by the KoPT.
- The tests are to cover every aspect related to the specification of the material and their operation; including, but not limited to, visual inspections, measurements, and operation.
- Conduct tests only in KoPT official(s) presence and/or as per KoPT Official's directives.

1.9. On-site cable tests

- Cables are to be tested to ensure that no damage has occurred during transportation to site and/or during the course of pulling-in and laying. The test results shall be compiled and submitted as document to KoPT officials for information & reference. This shall be done by the Service Provider prior to inspection request submitted for systems installation phase. The Service Provider shall verify that cable units and controls are properly labelled and interconnecting wires and terminals are identified as per relevant specifications and drawings approved by the KoPT.

1.10. Pre-testing

- Align and adjust system and perform pre-testing of all components, wiring and functions to verify compliance with specified requirements.
- Correct all deficiencies by replacing malfunctioning or damaged items with new items.

1.11. Test Equipment and Tools

- All equipment necessary to accomplish the tests specified herein shall be provided by the Service Provider. All tools required for operation and maintenance of the system shall be supplied by the Service Provider.

1.12. Manufacturer's field services

- Engage a factory- trained and authorized service representative to inspect field-assembled components and equipment installations and perform system pre-testing, adjustment and programming. This shall be done by the Service Provider prior to inspection request submitted for systems testing & commissioning phase.
- Report results in writing as document submittal to the KoPT for his information & reference.

1.13. Procedure for tests

- Notify KoPT not less than 30 days in advance, of proposed schedule, procedures and tests to be used in operational testing. Failure of the Service Provider to do so, KoPT reserves the right to withhold action on accepting inspection request requiring coordination, details and other pre-requisites (technical and QA/QC) until related requirements are received for the KoPT's effective evaluation of the System's readiness.
- Conduct operational tests only in the presence of KoPT officials.

1.14. Test Report

Prepare a written report of observations, inspections, tests and results, including:

- a. A complete listing of every device and circuit tests
- b. Date of each test and re-test, and by whom
- c. Results of each test and, if failure occurred, corrective action taken prior to retest
- d. Submit as document to the KoPT for information & reference.

1.15. Operational tests

- Schedule tests after system's testing & commissioning have been successfully completed.
- The Service Provider must be available with necessary resources (materials and human means) to support any of the Operation Readiness Trials with

coordination.

- Perform operational system tests to verify compliance with Specifications.

1.16. Defects Liability Period (DLP)

- Corrective action/ replacement of all defective materials and workmanship in the installation will be carried out as required within this period. All de-snagging will be expediently completed within this period. DLP will commence from Go-live date and will run for a period of 6 months.

1.17. Site Assistance And Adjustments

- To ensure continuity in the operation of the systems, the service representatives of the major equipment will provide a rapid site intervention at the Client's request during the whole warranty period in case of system malfunctions, detected anomalies, unusual ageing of the components, performance degradation, etc.. Each intervention will be handled by following the proper standards and applicable manufacturers' recommendations.
- The Service Provider shall provide Site assistance and Adjustments to users during DLP as per Systems scope and requirements related to defective components and workmanship in the installation, operation of the Systems. The technical and human means shall be applied by the Service Provider as required by KoPT.
- The Service Provider shall provide Site Adjustments as per scope of work and requirements mentioned in the RFP or as subsequently agreed during the SRS study.

1.18. Customization

- After implementation of the COTS product covering all systems high level scope of work, a period of 6 months will be open for Product customization to capture all additional user requirements which shall be incorporated without any additional cost to KoPT.
- During subsequent period too, if any change(s) is/are required arising out of wrong perception/ understanding of the Service provider towards the KoPT

operations, such changes shall also be done by the Service provider free of cost.

- At the beginning of the customization period initial user training is required.

1.19. Maintenance

- Preventive Maintenance: As per agreed Service level Agreement (SLA)
- Curative Maintenance: As per Service level Agreement (SLA)
- Maintenance service
 - The Service Provider shall maintain a Central facility to support on-site service by stocking adequate spares at site and strategic locations and to support emergency maintenance and repairs in order to meet the SLA requirements.
 - The Service Provider shall submit a Service-Call Report to be sent to KoPT immediately following every call out, indicating the time of call, out visit, cause, remedial action taken and the time that the service was restored.
 - A Maintenance Manpower Plan shall demonstrate the Service Providers committed resource level available for all types of activities to be carried out within the Warranty Period. Such plan shall be submitted for Approval 3 months before commencement of the Warranty Period.
 - The Service Provider's response time shall not exceed maximum of 30 minutes. The response time is defined as the time that elapses between the reporting of a fault and the maintenance personnel arriving at where the faulty equipment is located or fault reported.
 - The Mean Time to Repair (MTTR) shall not exceed 1 Hour. The MTTR shall include the diagnostic time, active repair/replacement time and the adjustment/testing time on site, but shall exclude the response time.
 - Under the supervision of Operator, the Service Provider shall liaise with KoPT and carry out safety and performance inspections for the installation on-site. Any necessary adjustments to the installation shall be made within 14 days of completion of such checks. A Safety and Quality Report shall be submitted, no later than 14 Days after such safety and performance checks, for KoPT's approval.

- The Service Provider shall be responsible to clear away from the Site all surplus materials, rubbish, temporary works of every kind and leave the whole of the Site and installation clean and in a workmanlike condition to the satisfaction of the KoPT, upon completion of each item of the repair, and maintenance works.

1.20. Operation and Support:

- The Product should be designed in such a way that there will be minimum manual intervention.
- The Bidder should transfer the knowledge to KoPT nominated Technical Team but however shall commit personnel support who will be responsible for maintaining and operating the system
- During the entire contract period the bidder has to provide the consumables viz 4 KB Mifare Smart cards ,RF tag ,Smart Card Printer Cartridge, Lamination , Cleaning Kit , Sticker rolls and any other consumables required for issuing the permits. The bidder should maintain an inventory of six months consumables. Two Technical resources consisting of a Project Manager and Solution Architect shall form the core team from Service Provider. Sufficient manpower should be deployed for fulfilling the SLA and smooth operations at each gate.

1.21. On-Site Support

- The contract Period shall be for a period of 07 (Seven) years from the date of go-Live.
- During the entire Maintenance period, the hardware will be under maintenance from the Service Providers. Coordination with the hardware vendors will be performed by the Service Providers maintenance team. Maintenance from the hardware vendors will be at no additional cost to KoPT.
- No spare parts will be provided for by KoPT. The hardware vendors shall provide all necessary spare parts and other necessary material for the maintenance and shall ensure that there are adequate spare parts available throughout the contract period (Maintenance). No additional cost will be paid by KoPT for such

provision.

- The Service Provider shall perform the maintenance, including Hardware /software correction and creation and delivery of patches and upgrades.
- The Service Provider shall provide a contact to report software faults to and a 24-hour telephone number that KoPT maintenance team can contact in case of urgent problem.
- If the Service Provider finds out a potential fatal software fault, i.e. a software fault resulting in the unavailability of the System, the Service Provider shall immediately inform his maintenance team, provide a backup solution to make the System available again within four (4) hours, deliver a hot-fix to correct the fault within one (1) day.
- If this type of fault is found out by KoPT's users directly, i.e. if the System becomes unavailable due to a Hardware / Software faults, the Service Provider shall immediately inform KoPT of the fault. The Service Provider shall immediately attend to the problem, propose a solution to make the System operational within two (2) hours, deliver a hot-fix correcting the software fault within four (4) hours.
- The Service Provider shall acknowledge reception of non-fatal software faults sent by KoPT maintenance team within twenty four (24) hours and inform KoPT maintenance team of the correction schedule within one (1) week
- When KoPT Server maintenance team reports a severe software fault, i.e. a fault that prevents the users from performing a function related to the operations, the Service Provider shall correct the fault and deliver a hot-fix within one (1) day.
- Other minor software faults shall be corrected by the Service Provider and delivered as part of the next patch.
- Severity of the software faults will be decided by the KoPT.
- A total System failure is defined as a situation where the System is not available for the users to operate. System unavailability caused by scheduled preventive maintenance shall not be regarded as failure.
- The systems procedure and levels shall be reviewed periodically by KoPT which

may be modified in consultation with the Service Provider.

1.22. Spare Parts And Extra Materials

A. Generalities

- The Service Provider shall maintain manufacturer recommended spare Parts for all major components in the system for 07 years fault free operation.
- Those spares required by the Service Provider to meet their maintenance Service Level of Agreement and to be held on site as required, apart from the above.
- Manufacturer's Recommended Spare Parts list is subject for KoPT's approval.

B. Test Equipment & Special Tools

- Service Provider shall maintain, together with an itemized list, all test equipment and tools required for routine maintenance, safety checks, and equipment repair.
- Deliver test equipment and tools at the same time as the system equipment.
- The list is subject for KoPT's approval.

1.23. Cleaning

- The Service Provider shall provide everything necessary for the proper protection of materials and completed works.
- The Service Provider will allow for protecting, moving and stacking existing materials, equipment, etc. as necessary by providing and completely covering them with tarpaulins, dust sheets or other materials as appropriate and cleaning and replacing them in their original positions on completion of the work.
- Any damage done to such existing work and property by the Service Provider's cranes, Lorries, equipment, employees, dust etc. or by operation under the agreement will be made good to the satisfaction of KoPT and at the Service Provider's own expense.
- The Service Provider shall maintain and remove on completion all coverings, materials, etc. used for protection.

1.24. Demonstration

- The Service Provider shall provide on-site demonstration of detailed maintenance procedure equipped with tools and equipment to KoPT Maintenance personnel by a trained, authorized service representative.

===== END OF DOCUMENT=====



Kolkata Port Trust

KOLKATA PORT TRUST

Supply, Installation, Commissioning, and Maintenance of RFID Systems at Kolkata Dock System, Kolkata Port Trust

Request for Proposal

Annexure V: Proposed Bill of Material

Document Reference No: **PIg/165/RFID/11667**

Date: 18th April 2017.

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

Table of Contents

1.	PROPOSED RFID GATE & LANE DETAILS (BILL OF MATERIAL)	4
2.	RFID BILL OF MATERIAL	4
3.	CUSTOM REQUIREMENTS OF KOPT:	10

1. Proposed RFID Gate & Lane Details (Bill Of Material)

- Netaji Subhash Dock and Kidderpore Dock

Sl. No.	Details	Number
01	Total Number of Gates(NSD and KPD)	14
02	Total Number of Lanes (Vehicle & Pedestrian)	28
03	Total Number of vehicle lanes	15
04	Total number of pedestrian lanes	9
05	Total Number berths under RFID	21
06	Total Pass Issuance Counters (At Subhash Bhawan, KPD, Budge Budge and PSO)	10

2. RFID Bill of Material

The following is the proposed bill of material for the implementation of RFID based Access Control system at Kolkata Port. The proposed Bill Of Material is only indicative.

Sl. No	Item	Unit	Minimum Required	Indicative Requirement by KoPT	Remarks
1	RFID-UHF Transceivers	Nos	01 per Vehicle Lane	19	Long range readers required 01 per vehicle Lane
2	RFID HF Controller	Nos	01 per pedestrians lane and 01 per vehicle lane	37	Controller with sufficient memory for immediate authentication & storage of RFID card data of employees, workers, drivers and others
3	RFID HF Readers	Nos	01 per pedestrians lane and 01 per vehicle lane	37	RFID reader to work with HF controller-

					employees,workers,drivers and other
4	RFID cards (UHF)	Nos	One card per vehicle	20,000	Total vehicles
5	RFID Cards (HF)	Nos	One card per individual	54,200	Employees, workers, drivers, visitors etc.
6	Photo capture Camera (For counters& Drivers)	Nos	01 per counter	06 + 19 = 25	For capturing photo of user at the counterand vehicle drivers
7	Photo capture Camera (For Pedestrian lane)	Nos	01 per lane	09	For capturing photo of the pedestrian
8	Front and back image capture camera	Nos	02 per vehicle lane	38	For taking image of container snapshot (1 camera in front and 1 in back)
9	32" LED display	Nos	01 for ped lane	10	To display name of person,photo.For vehicle enrolled number & owner details and one display to be installed in the chamber of the Traffic Manager, KoPT
10	RFID Pass Issue System comprising of 1.Industrial PC with client 2.HF Desktop Reader R/W 3. RFID card printer 4. 2 KVA UPS	Set	01 per Pass counter	10	*RFID pass counter for registering company, worker, vehicle and issue RFID passes. *Industrial PC with PACS enrolment software * RFID card printer to print permanent RFID cards. *UPS for power backup

11	Automatic Boom Barrier (3.5 -6 m)	Nos	01 Per Veh Lane	15	To permit and regulate vehicle movement
12	Automatic Flap Barrier (less than 1m)	Nos	01 per ped Lane	09	To permit and regulate person movement
13	Hand Held Terminal (HHT)	Nos	01 Per Lane	14+2 = 16 (For KPD Dry Dock and Lock Gate gates)	For spot checking of vehicle and persons by CISF at operational gates
14	Local Gate server	Nos	01 per Gate	14	Low end server or workstation to instantaneously perform & record all gate transaction and forward to central/port server.
15	Port Server including DR server	Nos	02 per port	01x2 servers=02	High end server to perform centrally and record all gates transactions, report generating including registration, pass issue etc. DR server to be of the same specifications as primary port server
16	Network switch to Connect central control	Nos	01 per gate	14	Switch to connect local control server through LAN
17	Internet Router to connect IPA server	Nos	01 per port	01x1=01	External router to connect IPA server through WLAN
18	UPS systems	Nos	01 per vehicle lane	14	Power back up for all servers, workstations etc
19	PACS-Client Software	Nos	01 per lane + 01 at Traffic Manager's chamber	28 + 1 = 29	Port access control systems (PACS) software integrating and communication all

					sub-systems
20	PACS-Server Software(including database,Backup,archive,integration, control room	Nos	01 per port	01x01=01	Port Access control(PAC) central server software at port level
21	Cabling/Installation(Lump sum)	Job	per lane and wherever required	41	Cabling, Installation of RFID,Network,Power,UPS,etc
22	Configuration/Commission (lump sum)	Job	01 per port	01x1=01	Hardware and system configuration and make entire system go live.
23	Training and Documentation	Job	01 per port	01x1=01	Technical, operational and Admin training to KoPT personnel & documentation
24	Signage Board marking RFID systems position and Instructions	NOS	02 per Lane	78	Sign boards indicating lanes, berths with RFID readers direction and locations including boards at pass issuance buildings
25	Display/Monitoring console at CCC using LED professional display having 55 inch (min) with all accessories to view each gate independently or consolidated view of all gates.	Nos	01 for Port's Command control centre	01	To monitor traffic (24x7)
26	Other items and works to complete the system(like minor modification civil concrete works to fix readers,	Lump sum	01 per port	01x1=01	Miscellaneous items & accessories not accounted above.(bidder shall make his survey prior to

	<p>controllers, flap and boom barriers etc, underground loop detectors for vehicle presence signal lights-Red, Green etc.</p>				quote)
27	<p>O&M charges for a period of 07 years duly deploying manpower as follows:</p> <ul style="list-style-type: none"> • Two Technical resources consisting of a Project Manager and Solution Architect shall form the core team from Service Provider. • Personnel for managing the Operational aspects at the Gates and counters • Pass issuance resource for issuing passes/ permits/ cards and registration, provide day-to-day services per pass issuance counter/ per shift. 3 shifts to be operated for 24 x 7 x 365 based service at 10 counters for first year and 3 counters 			07 years	For effective O&M by the system integrators

	in the subsequent years. (Additional counter/s, if required, at prorata basis)				
28	CISF Cabins	Nos.		15	Pre-fabricated cabins with seating options at an appropriate height to oversee the driver, driver's cabin, etc.
29	GPS tracking software including creation of GIS data/ Maps	No.	01 comprehensive software per port	01	For tracking of vehicle within port premises. Client software to be provided based on requirement.
30	Wireless connectivity including wireless routers, access points, switches, etc.	--	Based on requirement	-	To be used wherever wired network is not feasible or available
31	Storage device of minimum 20TB	No.	01	01	The storage indicated is based on operational requirement observation. However, it is the responsibility of the Service Provider to assess the actual situation based on the requirements of KoPT and software requirements for storing data including images for a period of at least 10 years and quote accordingly.

					Service Provider needs to take into consideration archiving of data based on KoPT's requirement.
32	Setup of Data Centre and Disaster Recovery centre				

Note: The above BoM is indicative based on present scenario and it is the responsibility of the Service Provider to survey the actual requirements based on requirements of KoPT and supply the requirement IT infrastructure like no. of readers, clients required, etc..Payment towards BoM, RFID cards for internal use of KoPT and deployment of resources by Service Provider shall be as per need.

3. Custom requirements of KoPT:

1. Complete IT infrastructure shall be in the name of KoPT from day one.
2. Proposed project should use existing established KDS fibre network wherever it is healthy to cover all proposed locations, berths, buildings for successful connectivity.
3. KoPT will provide raw power 1-Phase (A.C Incoming supply 190-270 V, Single Phase,50 Hz +/-2.5 Hz) at nearby source/building and Service Provider is responsible for last mile connectivity/ cabling for power requirements.
4. Proposed project should be based on the existing movement plan/traffic plan assigned to vehicles by Traffic dept.
5. Boom barriers, Flap barriers and all RFID infrastructures should be setup inside the physical gates.
6. Data Centre will be setup at Subhash Bhawan and Disaster Recovery will be setup at the KoPT Administrative building at 15, Strands Road, Kolkata.
7. Central Control & Monitoring will be done at Subhash Bhawan
8. OFC backbone to be laid wherever Port OFC/ wired N.W is not available/not healthy. Presently fibre N.W is available at almost all locations including gates, pass issuance counters, etc..
9. RFID gate infrastructure like, lane, dividers, security rooms, speed breakers, lighting,

A.Cs, furniture etc. are in KoPT Service Provider's scope.

10. Price should include all import, Excise, customs duties. CST/VAT to be mentioned clearly.
11. S.tax will be reimbursed at actuals and recoveries for I.T,VAT will be made as per the rules in force.
12. No financial commitment at this stage on either side and above BOQ quantity is an approximate. However actual quantity may vary as per the site conditions.

===== END OF DOCUMENT=====



Kolkata Port Trust

KOLKATA PORT TRUST

**Supply, Installation, Commissioning and Maintenance
of RFID Systems at Kolkata Dock System, Kolkata Port
Trust.**

Request for Proposal

Annexure VI: Documentation Scope

Document Reference No: **PIg/165/RFID/11667**

Date: 18th April 2017.

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

Table of Contents

1.	DOCUMENTATION.....	4
2.	GUIDELINES FOR DOCUMENTATION TRANSMITTAL	9

1. Documentation

- i. This section sets out requirements of the KoPT on documentation to be provided by the Service Provider on the Hardware and Software supplied. Some of the documentation may be progressively revised but the final edition of the documentation will be up-to-date capturing all the amendments up to Completion Date and will be fully in accordance with the System as finally accepted by the KoPT. The documentation requirements set out will cover both software and hardware, and will also apply to equipment not manufactured or designed by the Service Provider.
- ii. The applicable standard tools for documentation are:
 - a. Text documents: Microsoft Office 2007 or later, PDF
 - b. Modelling: Revit
 - c. Drawings: AutoCAD 2010 or later
- iii. All documentation will be written in good, simple and concise English employing generally accepted technical terms. All manuals supplied will be professionally bound with hard durable covers in accordance with acceptable commercial practice. It will be in standard format size and legibly printed on good quality paper. There shall be no incoherence, illegibility, manual scribbling or smudging in the text, drawings, diagrams, illustration, etc.
- iv. The Service Provider will also provide the manuals and all documentation or software on DVD and that all computer equipment is specified with DVD R/W and CD-ROM R/W capability.
- v. The following type of documentation and the quantities shall be delivered (with two (2) Soft copies):

Type of document	No of copies
System Design Documents / Functional Specifications	4
Material Submittals	4

Type of document	No of copies
Method Statement Submittals	4
FAT report	1
Installation Documents	4
Test Documents	4
Technical/Administration Manual	2
Training Documents for each trainee	1
(Additional 2 sets for the IPA)	
Interface Control Documents RFID – Port Server – PCS per interface	1
Operators Manual	8
Mock-up Drawings	As required
Labelling Scheme	As required
Shop Drawings and Coordination Shop drawings	As required
Detailed Drawings	As required
Schematic Drawings	As required
As Built Drawings	As required

- vi. The KoPT reserves the right to withhold action on a submittal requiring coordination with other submittals and additional requirements (technical and QA/QC) until related submittals are received for his effective evaluation.
- vii. The KoPT will not review submittals that do not bear Service Provider's approval stamp and will return them without action.
- viii. The final edition of all documents, except for the FAT report, and manuals will capture all the amendments up to the point of final acceptance and will reflect the System as handed over to the KoPT.
- ix. Interface Control document
 - a. The ICD shall clearly show the RFID-Port Server- PCS interfaces and data exchange flows.
 - b. The ICD shall be jointly approved by Port Server & PCS solution providers before being submitted for information to the KoPT. Once the ICD is

validated, updated and the tests meet in all respects its specified requirements, the Service Provider shall then submit for approval to the KoPT.

x. System Design Documents and Functional Specifications

- a. These documents define the operational requirements in details and will be prepared by the Service Provider immediately from the date of Letter of Acceptance. In preparing this document, the Service Provider will explicitly draw the KoPT's attention to the departure, variation, or non-compliance to this Specification as agreed upon. This will be done by way of a separate non-compliance or variation list to be prepared by the Service Provider showing explicitly the sections which have not been complied with, or which have been offered with an alternative proposal, if any. Any new or variation list will be subjected to the KoPT approval and if approved, the accepted or variation will form part of the System design document. If the Service Provider fails to secure an explicit approval from the KoPT to any of his proposed non-compliance or variation in this manner, and if a conflict exists between the System design document and this Specification, the KoPT will reserve the right not to accept the version in conflict.
- b. System design document and the relevant provisions of this Specification will remain contractually binding.
- c. Four (4) copies of System design documents and functional specifications and subsequent amendments duly approved by the KoPT and Users will be supplied by the Service Provider. Before final acceptance, two (2) complete volumes of the final and updated version will be submitted.
- d. The Service Provider shall include in this System design documents a cross-reference to this specification to facilitate the checking for completeness in design.

xi. Installation Document

- a. The Installation Document will be used to guide the installation works and to serve as a record of all installation details on site. This shall include Deployment and Commissioning Strategy with detailed Site Inspection plan

for the Systems documentation delivery.

- b. One (1) month prior to the delivery of Hardware to site, the Service Provider shall supply to the KoPT with four (4) copies of the Installation Document.
- c. Four (4) sets of preliminary edition and subsequent amendments will be supplied by the Service Provider one (1) month before the System installation. Four (4) sets of the final edition will be handed over to the KoPT on Commissioning of the System.
- d. The installation document will be updated regularly or as and when requested by the KoPT through the installation process.
- e. All changes made in the installation layout, wiring, cabling and design will be incorporated in its final edition.
- f. Method Statement for major works and activities shall be submitted equipped with comprehensive Inspection & Test Plan (ITP) and Site Safety Risk Assessment.

xii. Test Documents

- a. The Service Provider shall provide four (4) sets of test documents which will incorporate a cross reference to this technical specification to ensure that all testing are carried out completely and in accordance to this specification.
- b. The tests documents will include a test plan and test files
- c. The test plan will describe the strategy for all the tests of the System and will include at least the scheduling of the tests between hardware, network, functionalities, interfaces, training, parallel running, documentation and installation and the procedures to apply when errors or problems are encountered depending upon the situation's gravity (fatal, serious, minor).
- d. Method Statement for major tests and activities shall be submitted equipped with comprehensive Inspection & Test Plan (ITP) and Site Safety Risk Assessment.

xiii. Training Documents

- a. All training materials, stationery, training notes, handbooks, manuals, etc shall be provided according to the number of trainees from the KoPT.

- b. Additionally, two (2) complete sets of training manuals, programme and plan shall be supplied by Service Provider to the KoPT

xiv. Operational Manual

- a. The Service Provider shall supply two (2) sets of preliminary operational manual plus amendments and six (6) sets of the final edition. The preliminary edition will be supplied one (1) month before delivery of the Hardware on- site. Should there be any changes prior to final acceptance, amendment sheets will be supplied without extra costs to the KoPT.
- b. The operational manual shall contain adequate documentation of operating instructions for the System to be used by KoPT officials, pass issuance officials, CISF, port users, etc. The manual shall enable the operators to operate the System at all operational positions. It shall contain the commands and the procedures/ response in connection with each command, and the operation and maintenance Procedures required on the part of the technical control personnel. The initializing, restart and other emergency procedures to be followed in the event of a System failure/ abort during any job step must be spelled out in detail.

xv. Software :

- a. Equipment and software shall be delivered to the address indicated by the KoPT. A list for all software licenses, Manuals, and Backup copies, which are to be transferred to KoPT/ Owner, shall be transmitted to the KoPT/ Client for approval. The number of copies shall be agreed with the Client. The equipment, software, licenses, etc. shall be in the name of KoPT from day one.
- b. A hard disk picture (Norton Ghost or equivalent) shall be done for all Software Licenses (depending on the number of equipment to be installed), specific developments and parameters. It shall be handed over to the Client at the end of the project. Indeed, if a crash disk occurs, this back-up picture shall allow in a short delay a complete retrieving of the overall system.
- c. Software Version and Type for electronic file to be coordinated by the Service Provider for all systems to ensure homogeneity of the project.

xvi. Sample Warranty

- a. Copy of manufacturer's proposed warranty, stating obligations, remedies, limitations, and exclusions
- b. Provide copy of sub-Service Provider's warranty certificates.
- c. Provide Service Provider's warranty certificates.

2. Guidelines For Documentation Transmittal

- 1 Electronic Files followed by physical documents
- 2 Specifications shall be word processed on Microsoft Word Version 2003 and/or later version. Unless otherwise directed by KoPT, provide files on CD-ROM.
- 3 XLS format of Excel™, most recent version, for the tables and schedules
- 4 PDF format of Adobe Acrobat™, most recent version, for the technical Data sheet and manufacture catalogues

===== **END OF DOCUMENT** =====



Kolkata Port Trust

KOLKATA PORT TRUST

Supply, Installation, Commissioning, and Maintenance of RFID Systems at Kolkata Dock System, Kolkata Port Trust

Request for Proposal

Annexure VII: O&M Support Scope

Document Reference No: **PIg/165/RFID/11667**

Date: 18th April 2017.

Proprietary Notice:

This document contains confidential information of Kolkata Port Trust (KoPT) which is provided for the sole purpose of permitting the recipient to make a bid. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from KoPT or becomes publicly known through no fault of recipient, from KoPT or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to KoPT.

Table of Contents

1.	Operation and Maintenance from the date of Go Live	4
1.1.	Applications Functional Support (AFS) for the delivered RFID based Access Control solutions	4
1.2.	Application Software Maintenance and Support services	5
1.3.	Annual Technical Support (ATS) for the licensed software	8
1.4.	Warranty support for the IT hardware	9
1.5.	Operations and maintenance services for the IT infrastructure at the DC and DRC	11
1.5.1.	System Administration, Maintenance & Management Services	11
1.5.2.	Application Monitoring Services	13
1.5.3.	Storage Administration and Management Services	14
1.5.4.	Backup and Restore Services	14
1.6.	User Profiles and Account Management	15
1.7.	Antivirus Solution Management	15
1.8.	Maintenance of non-IT Infrastructure at DC and DRC	16
1.9.	Periodic reporting	16
1.10.	Centralized helpdesk	17

1. Operation and Maintenance from the date of Go Live

Operation and Maintenance of the entire RFID based Access Control System including, but not limited to, IT Application, IT & Non-IT infrastructure, Servers, Network and Equipment which were supplied to KoPT by the service provider from the date of Final Go live.

As part of the operations and maintenance services, the Service Provider shall provide support for the software, hardware, and other infrastructure that are in the scope of this RFP. The O & M support includes:-

- a. Application Software maintenance and support
- b. Warranty support for all the hardware procured as part of this RFP
- c. Annual Technical Support (ATS) for all the licensed software
- d. Operations and maintenance services for the infrastructure supplied and commissioned by Service Provider for the system at the Data Centre and Disaster Recovery Centre and project locations.
- e. Helpdesk at KoPT
- f. Periodic reporting

1.1. Applications Functional Support (AFS) for the delivered RFID based Access Control solutions

This shall cover all the solution components that are delivered as a part of the RFID PACS system. The Application Functional Support Services contemplated herein shall be provided for system implemented by the Service Provider. The Service Provider shall render both on-site maintenance and support services to KoPT.

The scope of the services is as below:-

- a. Enhancements and defect fixes.**

The Service Provider shall incorporate technological changes, and provide enhancements as per the requests made by KoPT. Service Provider shall perform minor changes, bug fixes, error resolutions and minor enhancements that are incidental to proper and complete working of the application.

b. Routine functional changes:

The Service Provider shall be responsible for user and access management, creating new report formats, and configuration of reports. Service Provider shall provide user support in case of technical difficulties in use of the software, answering procedural questions, providing recovery and backup information, and any other requirement that may be incidental/ancillary to the complete usage of the application. The Service Provider shall perform user ID and group management services. The Service Provider shall maintain access controls to protect and limit access to the authorized End Users of KoPT.

c. Tuning of the RFID based Access Control solution:

The Service Provider shall also undertake tuning of RFID based access control system, databases, any third party software and any other components provided as part of the solution to optimize the performance to match KoPT's time to time requirements.

d. Deployment/Re-Deployment of RFID based Access Control solution:

The Service Provider shall be responsible for deployment of the RFID based Access Control solution and re-deployment in case of any upgrades to the underlying hardware or operating System and carry out any necessary testing.

The key service level requirements need to be ensured by the Service Provider during the operations and maintenance period. These requirements shall be strictly imposed and either KoPT or a third party audit/certification agency shall be deployed for certifying the performance of the Service Provider against the target performance metrics as outlined in the SLA's defined in Volume III of the RFP.

1.2. Application Software Maintenance and Support services

As part of the software maintenance and support services Service Provider shall provide:

1. The IT Application Maintenance and Support services shall be provided for all components mentioned in this RFP or as part of Administrative orders / legal obligation.
2. The Service Provider shall render on-site maintenance and support services and off-site maintenance and support services from KoPT, Office premises in Kolkata.
3. The Service Provider shall be required to provide operational & maintenance services for System including, but not limited to, troubleshooting & addressing the functionality, availability & performance issues, implementing any system change requests, addressing the incidents/problems raised by the users (via IT Helpdesk) for problems/bugs in the application, etc.
4. The Service Provider shall keep the application software in good working order; meeting the requirements defined by KoPT from time to time based on functional, administrative or legislative priorities, perform any changes and upgrades to applications as requested by KoPT.
5. Tuning of application, databases, third party application and any other components provided as part of the solution to optimize the performance.
6. The Service Provider shall perform (at no extra cost) minor changes, bug fixes, different reports of KoPT, error resolutions and minor enhancements that are incidental to proper and complete working of the application.
7. Release Management for the interim releases of the application.
8. Centralized version and configuration control of the application.
9. Routine functional changes.
10. Any changes to the application code that may be required because of patches to licensed software being used (if any). The Service Provider shall migrate all the current functionality to the new / enhanced version at no additional cost to KoPT.
11. Updating and maintenance of all RFID based Access Control project documents (including user manuals, trainings etc.).

12. Change request management based on feedback from the users or the initiative of the Service Provider. All planned changes to the application, especially major enhancements and changes in functionality post go-live, shall be coordinated within established Change control processes.
13. The Service Provider will define the Software Change Management and version control process and obtain approval for the same from KoPT. For all proposed changes to the application, the Service Provider will prepare detailed documentation including proposed changes, impact on the system in terms of functional outcomes/additional features added to the system, etc.
14. The Service Provider shall carry out the configuration & deployment of new/modified software version at KoPT offices/gates as required by KoPT.
15. The Service Provider shall address all the errors/bugs/gaps in the functionality offered by system at no additional cost during the operations & maintenance period.
16. For performing of any functional changes to system that are deviating from the signed-off Functional Requirements/System Requirements including any subsequent changes till final go-live, a separate Change Proposal Form shall be prepared by the Service Provider and the changes in the application shall be implemented accordingly at no additional cost to KoPT. The time period for implementation of change shall be mutually decided between Service Provider and KoPT.
17. It is clarified that changes in software, hardware and other infrastructure required as a result of any legislative, administrative, policy changes in KoPT processes and workflow shall constitute change of 'Scope of Work' only if it is not covered in Change Request Schedule and updates/upgrades
18. Any changes/upgrades to the software performed during the operations & maintenance phase shall be subjected to comprehensive & integrated testing by the Service Provider to ensure that the changes implemented in the system meets the desired and specified requirements of KoPT and does not impact any other function of the system. The Service Provider shall provide a staging environment for testing of changes/ updates/ patches before applying them on production environment.

1.3. Annual Technical Support (ATS) for the licensed software

1. All software should be supplied with applicable OEM warranties and support for the entire duration of the project. During warranty period Service Provider has to provide updates and patches.
2. Annual Technical Support (ATS) will start from the date of acceptance of the installation. ATS should cover 24 x 7 escalation supports from OEM for all software products to be provided through Phone, Email or Onsite visit depending on the criticality and nature of the problem. The support has to be ensured by the Service Provider.
3. The Service Provider must carry out any requisite adjustments / changes in the configuration for implementing different versions of the application software.
4. The Service Provider shall provide from time to time the Updates/Upgrades/New releases/New versions of the software and operating systems as required. The Service Provider must provide free upgrades, updates & patches of the software and tools to KoPT as and when released by OEM. The Service Provider will implement from time to time the Updates/Upgrades/New releases/New versions of the software and operating systems as required after necessary approvals from KoPT about the same at no additional cost without disturbing the implemented RFID based Access Control system.
5. The Service Provider shall provide and apply regular patches to the licensed software including software, operating system, databases and other applications.
6. The Service Provider shall provide for software license management and control. Service Provider shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance. The Service Provider must perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of site license agreements, volume purchase agreements and other mutually agreed upon licensed software terms and conditions and report to KoPT on any exceptions to Service Provider's terms and conditions, to the extent such exceptions are discovered.

7. The Service Provider shall manage complete OEM technical support for all the licensed software problems and/or questions, technical guidance, defect and non-defect related issues. The Service Provider shall provide a single-point-of-contact for software support and provide licensed software support including but not limited to problem tracking, problem source identification, problem impact (severity) determination, bypass and recovery support, problem resolution and management reporting etc.
8. The Service Provider shall undertake regular preventive maintenance of the licensed software. If the Operating System or additional copies of Operating System are required to be installed / reinstalled / de-installed, the same shall be done as part of ATS.

1.4. Warranty support for the IT hardware

1. The Service Provider shall provide a comprehensive warranty and on-site free service warranty for all the hardware procured as part of this RFP.
2. The Service Provider shall provide comprehensive manufacturer's warranty in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. The Service Provider must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
3. The Service Provider shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
4. The Service Provider is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP.
5. During the warranty period, Service Provider shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost to KoPT in case the procured hardware or software is not adequate to meet the service levels.
6. Mean Time between Failures (MTBF): If during agreement period, any equipment has a hardware failure on four or more occasions in a period of less than three months or six times in a period of less than twelve months, it shall be replaced by

equivalent or higher-level new equipment by the Service Provider at no cost to KoPT. However, if the new equipment supplied is priced lower than the price at which the original item was supplied, the differential cost must be refunded to KoPT. For any delay in making available the replacement and repaired equipment for inspection, delivery of equipment or for commissioning of the systems or for acceptance tests / checks on per site basis, KoPT reserves the right to charge a penalty. The Service Provider shall track and report observed Mean Time between Failure (MTBF) for Hardware.

7. During the warranty period Service Provider shall maintain the systems and repair / replace at the installed site at no charge to KoPT, all defective components that are brought to the Service Provider's notice by KoPT.
8. The Service Provider shall as far as possible repair the equipment at site.
9. In case any hard disk drive of any server, SAN etc. is replaced during warranty / AMC, the unserviceable HDD will be property of KoPT and will not be returned to Service Provider. In case of faulty storage media, the malfunctioning storage media will not be handed over to Service Provider, this is applicable to all removable media.
10. Warranty shall not become void, if KoPT buys, any other supplemental hardware from a third party and installs it within these machines with intimation to the Service Provider. However, the warranty will not apply to such supplemental hardware items installed.
11. The Service Provider shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for malware/malicious software, if any, and must maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM. PM envisages all activities require to be undertaken for good upkeep of hardware.
12. The Service Provider shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
13. The Service Provider shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.

14. The Service Provider shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.
15. Any component that is reported to be down on a given date must be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the requisite time frame to meet the Service Level Agreement (SLA).
16. The Service Provider shall develop and maintain an inventory database to include the registered hardware warranties.

1.5. Operations and maintenance services for the IT infrastructure at the DC and DRC

1. The scope of the services for overall IT infrastructure management as per ITIL framework shall include 365x24x7 on site Monitoring, Maintenance and Management of the server and related infrastructure supplied and commissioned by the Service Provider for the application at the Data Centre and Disaster Recovery Centre.
2. The Service Provider shall provide the MIS reports for all the devices installed in the Data Centre and Disaster Recovery Centre in format and media as mutually agreed with the KoPT on a monthly basis. Whenever required by KoPT, Service Provider must be able to provide additional reports in a pre-specified format.
3. The indicative services as part of this support are as below:
 - a) System Administration, Maintenance & Management Services
 - b) Application Monitoring Services
 - c) Backend/Alert Services
 - d) Storage Administration and Management Services
 - e) Replication, Backup and Restore Services

1.5.1. System Administration, Maintenance & Management Services

The objective of this service is to support and maintain all the Systems and Servers provided as a part of this project by Service Provider, and shall include

1. 365x24x7 monitoring and management of the servers in DC and DRC.
2. Regular monitoring of all the applications hosted.

3. Operating System administration, including but not limited to management of users, processes, preventive maintenance and management of servers including updates, upgrades and patches to ensure that the system is properly updated.
4. Installation and Re-installation of the server and other hardware in the event of system crash/failures.
5. Regular analysis of events and logs generated in all the sub-systems including but not limited to servers, operating systems, security devices, etc. to identify vulnerabilities. Necessary Action shall be taken by the Service Provider in accordance with the results of the log analysis. Suitable mechanism has to be maintained for security and forensic related logs or as per requirement of IT act and that of other government regulations issued from time to time.
6. Adoption of policies and procedure, compliances, guideline, standard as defined by the KoPT.
7. Provide integration and user support on all supported servers, data storage systems, etc.
8. Troubleshoot problems with web services, applications software, desktop/server relationship issues and overall aspects of a server environment.
9. Problems shall be logged in at the Help Desk and resolved as per the SLAs defined.
10. Manage and monitor server configuration, performance and activity of all servers. Performance optimization and reporting - Process and Memory Management, Monitoring CPU performance, Monitoring Memory performance, Monitoring Input / Output performance, Monitoring Ethernet Traffic, etc.
11. Prepare and keep up to date document containing configurations of all server, IT infrastructure etc.
12. Hardening servers in line with security policies (ISO 27001:2005 information security control).
13. Carry out DC and DRC failure testing and half yearly BCP real drills.
14. Configuration of server parameters, operating systems administration and tuning
15. Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and

management of upgrades including migration to higher versions and patches to ensure that the system is properly updated.

16. Periodic health check of the systems, troubleshooting problems, analysing and implementing rectification measures.
17. Perform Database Administration activities for Database. The Service Provider agrees that all databases of the KoPT will be administered as per standards and requirements. The service covers all the databases run on servers / SAN at DC and DRC including but not limited to:
 - a) Start-up and shutdown of databases.
 - b) Daily / Weekly / Monthly backup of databases.
 - c) Database recovery when required.
 - d) Weekly database recovery checks.
 - e) Required logs maintenance as per policies of the KoPT.
 - f) Disaster recovery as per polices of the KoPT.
 - g) Documentation upkeep and records maintenance.
 - h) User account management.
 - i) Database problem resolution.
 - j) Performance tuning.
 - k) Replication of Database from DC to DRC.

1.5.2. Application Monitoring Services

The services to be provided by the Service Provider for Application Monitoring which includes following but not limited to:

- Web services
- Application server
- Portal Server
- Database server
- Middleware
- Network Monitoring Software
- Online Ticketing Tool
- Other components

1.5.3. Storage Administration and Management Services

The services to be provided by the Service Provider shall include:

1. Installation and configuration of the storage system.
2. Management of storage environment to maintain performance at desired optimum levels.
3. Management of any changes to database schema, disk space, storage, user roles etc.
4. Identify the available performance of interconnects in the storage solution.
5. Identify the zones being enforced in the storage solution.
6. Create/delete and enable/disable zones in the storage solution.
7. Identify the storage volumes in the storage solution.
8. Create/delete/modify storage volumes in the storage solution.
9. Identify the connectivity and access rights to storage volumes in the storage solution.
10. Create/delete and enable/disable connectivity and access rights to storage volumes in the storage solution.
11. To provide off-site storage of production data and KoPT RFID based Access Control System on appropriate media at regular intervals as required by KoPT.

1.5.4. Backup and Restore Services

The services to be provided by Service Provider shall include:

1. Backup of storage as per the defined policies.
2. Monitoring and enhancing the performance of scheduled backups, scheduled regular testing of backups and ensuring adherence to related retention policies as defined by KoPT.
3. Prompt execution of on-demand backups of volumes and files whenever required or in case of upgrades and configuration changes to the system.
4. Real-time monitoring, log maintenance and reporting of backup status on a regular basis.

5. Media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite).
6. 365x24x7 support for file and volume restoration requests at the DC and DRC.

1.6. User Profiles and Account Management

1. Routine functional changes that include user and access management, creating new report formats and configuration of reports.
2. The Service Provider shall provide user support in case of technical difficulties in the software, answering procedural questions, providing recovery and backup information, and any other requirement that may be incidental/ancillary to the complete usage of the application/ solution.
3. The Service Provider shall perform user ID and group management services. The user-id naming & protocol shall be designed and implemented for all the user ids. Such naming convention and protocol shall be signed-off with KoPT.
4. The Service Provider shall maintain access controls to protect and limit access to the authorized end users of KoPT.
5. The services shall include administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users and providing administrative support related to RFID based Access Control System.
6. System administration tasks such as managing the access control system, creating and managing users etc. and maintaining logs and history of access rights of the users.

1.7. Antivirus Solution Management

1. The Service Provider should ensure overall security of the system including installation and management of antivirus solution for protection of all the servers at DC & DR implemented for the project, application of updates/patches etc. The antivirus patches have to be updated and applied from time to time, after appropriate testing of the patches in the staging area.

2. Guarding the systems against virus, malware, spyware and spam infections using the latest antivirus suites which include anti-malware, anti-spyware and anti-spam solution for each server antivirus version and its upgrades. The antivirus suite and updates will have to be provided by the Service Provider at regular intervals as and when the new signatures are released by the OEM. The Service Provider for the purpose of support on new upgrades & patches shall have a back to back arrangement with the OEM from whom the antivirus suite is purchased. The copy of the same shall be submitted to KoPT.
3. The Service Provider shall supply antivirus enterprise edition. For DC & DR servers, the Service Provider has to procure antivirus licenses mandatorily. The license certificate has to be procured in the name of KoPT and submitted to KoPT. The antivirus should have the subscription for server download of real-time updates and upgrades from the OEM site during the entire duration of the project.
4. The Service Provider shall have back to back agreement with 24/7 premier support with antivirus OEM, which shall ensure that any critical issues with respect to virus/antivirus are addressed within the 24 hrs.
5. The copy of such agreement shall be provided by Service Provider to KoPT. Such agreement shall be valid throughout the agreement period.
6. The Service Provider should provide solution to virus alerts when they occur (within 24 hrs) or earlier in case of emergency. The Service Provider has to take corrective action in case systems get affected due to virus activity.

1.8. Maintenance of non-IT Infrastructure at DC and DRC

The cost of maintenance of the non-IT Infrastructure at DC and DRC would be borne by KoPT.

1.9. Periodic reporting

The Service Provider shall submit the following periodic reports (but not limited to) to KoPT:

1. Updation of Documentation on successful completion of O&M operations for each Month

- a) Regular updation of all policies designed by Service Provider for KoPT
 - b) Updated system design documents, specifications
 - c) Latest source code, application deployment files, configuration files for entire system Software change logs etc.
2. Corrective Action report in response to the any audit findings/ other concerns as identified by KoPT
 3. Monthly report on the central helpdesk centre operations
 4. SLA Monitoring Reports

1.10. Centralized helpdesk

1. The Service Provider shall establish and provide central helpdesk facility from KoPT corporate office in Kolkata
2. The Helpdesk service will serve as a single point of contact for all Application, hardware and network related incidents and service requests. The Helpdesk shall provide troubleshooting Services including maintenance for overall system stabilization, defect resolution, system maintenance, system administration, availability & performance issues, security administration, database administration, User administration and end-user problem resolution. The operational support will have to be provided, through a suitable Helpdesk system, to ensure that the solution is functioning as intended and that all problems associated with operations are resolved satisfactorily.
3. The Helpdesk service is required in two languages – English/ Hindi and Bengali.
4. The Service Provider in consultation with KoPT is required to provide necessary channels for reporting issues to the help desk. The incident reporting channels could be the following:
 - a) Specific E-Mail account
 - b) One/Two landline phone numbers, seating arrangement and electricity will be provided by KoPT free of cost to Service Provider. Service Provider needs to provision for converting these phone numbers into multiple lines as required and also provision for any other hardware / software required for the same.

- c) Portal – A web based functionality for service desk tool for registering the calls
5. Implement a call logging system in line with the severity levels as per the SLAs.
 6. The Service Provider to provide Help Desk services to track and route requests for service and to assist end users in answering questions and resolving problems related to the software application, hardware & network support, Data Centre, and Disaster Recovery Centre.
 7. Creation of knowledge base on frequently asked questions to assist user in resolving basic issues themselves.
 8. Services in this area include, but are not limited to, the following:
 - a) Logging all the calls, classifying the calls and render first level support
 - b) Assigning the call for appropriate action, within the stipulated time.
 - c) Tracking the call till closure and ensure SLA adherence.
 - d) Generate reports on a daily, weekly and monthly basis. Generate exception reports.
 - e) Provide need-based ad-hoc reports.
 - f) Interact with KoPT and stakeholders
 - g) Ensure adherence to escalation processes.
 9. It is expected that the Service Provider shall bring his service desk tool at no additional cost to KoPT. Vendor will integrate this tool with Enterprise Management system and Network management system for auto ticket generation, call logging from users and tracking till resolution. The service desk tool should track SLAs as mentioned in this RFP. The service desk tool shall be
 - a) Complies with ITIL compliant service delivery.
 - b) Service desk should track & record help desk jobs. (Monitor Helpdesk effectiveness in real-time)
 - c) Should have basic features for call management such as
 - i. Update & close jobs / Tickets.
 - ii. Place jobs / tickets on “Hold”
 - d) Ticket auditing facility should be provided by the “Service Desk tool”. (provides history of the ticket)
 - e) Assign priorities to Jobs / Tickets.

- f) Specify & track target job completion status based on various factors as, Dates, Priority etc.
- g) Services desk tool should have capability to categorize jobs as per the structure of a problem eg.: Server related problem should assign to hardware team.
- h) Service desk should have “SLA” mapping / monitoring & tracking feature. (When a ticket is raised, target Helpdesk calculates the most relevant service level agreement according to the issue and any asset identified)
- i) Service desk should record time duration spent on each ticket.
- j) Service desk tool should define unlimited no of end-users.
- k) Service desk should have facility to restrict specific functionality to certain operators.
- l) Service desk tool has to have inbuilt “Escalation Matrix” which help for the notification purpose to operators & users about their tickets.
- m) The proposed tool should maintain Asset information.
- n) The proposed tool should have facility to link files (error, log files) to help desk tickets.
- o) The monitoring tools deployed by the Service Provider shall be able to generate automated trouble tickets in an event of faults or threshold violations and escalate the same to predefined set of people across the organization and third party vendor. The ticket needs to be automatically closed as soon as fault is resolved.
- p) A unique Ticket Number should be created and assigned for any fault and using the same unique no., the history of call resolution and current status must be tracked.
- q) Help Desk should be directly and automatically integrated with Network management Software so that automated tickets get generated through the Help Desk whenever Network management Software receives a qualified alert. Similarly when Network Management Software detects that the fault has been restored then the ticket generated in Help Desk earlier should be automatically closed and history of the same ticket should be maintained for viewing.

10. The Service Provider will also submit an escalation matrix to KoPT on the procedures for escalation for different types of issues/error/bugs and implement the same.

===== END OF DOCUMENT=====