From APPENDIX 5 | To be copied to submitted APPENDIX 5 by Tenderer

Centralised Taxi Service System (CTSS) Functional Requirements

Statement of Compliance: Please rate each of the requirements against your platform as follows
4 = out of the box or configuration using business user tools
3 = minor development (2 days or less coding + unit testing)
2 = major development (3 days+) or integration to another system

A. Functional Requirements

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
1. Application Software (Taxi Control Centre, Centralised Booking & Dispatch, In-Taxi Vehicle Equipment)					
1.1	**Scope of application software**				
1.1.1	Perform requirements gathering. Deliverables must include (but not limited to) the following:	Mandatory			
1.1.1.1	User Requirement Specification (includes functional requirements, non-functional requirements, use-case analysis)	Mandatory			
1.1.1.2	System Requirement Specification (includes software, hardware and networking requirements specifications)	Mandatory			
1.1.1.3	Functional Specification	Mandatory			
1.1.2	Perform application design. Deliverables must include (but not limited to) the following:	Mandatory			
1.1.2.1	Technical Design Specification (includes functional designs, user stories, graphics design mockups, usability studies, UML diagrams, business process diagrams, data model specifications etc.)	Mandatory			
1.1.2.2	High-Level Design Document	Mandatory			
1.1.2.3	Detailed (Low-Level) Design Document	Mandatory			
1.1.3	Conduct walkthrough of design - high-level design and low-level design	Mandatory			
1.1.4	Application development - customisation. This includes coding effort required to address all requirements gathered throughout the project. Deliverables must include (but not limited to) the following:	Mandatory			
1.1.4.1	System Development Document - establishes the hardware and network development approach including methodologies, tools, and procedures to be employed.	Mandatory			
1.1.4.2	Integration Document - describes the assembly and interaction of the hardware, network, and any other components of the system.	Mandatory			
1.1.4.3	Test Analysis Report(s) - presents a description of the unit tests and the results mapped to the system requirements; also identifies system capabilities and deficiencies.	Mandatory			
1.1.4.4	Release Notes – provides summary information regarding the current release of the system being built; typically includes major new features and changes and identifies known problems and workarounds.	Mandatory			
1.1.4.5	Source codes: a. Main source codes (COTS): in escrow account b. Changes (customisations): Delivered to SPAD	Mandatory			
1.1.5	Application development - configuration. This includes all configuration required to address all requirements gathered throughout the project. Deliverables must include (but not limited to) the following:	Mandatory			
1.1.5.1	Configuration records - e.g. SQL insert/update/delete statements, ACL in routers.	Mandatory			
1.1.5.2	Configuration management methodology and plan.	Mandatory			
1.1.6	Conduct tests:	Mandatory			
1.1.6.1	Unit Test	Mandatory			
1.1.6.2	Integration Test	Mandatory			
1.1.6.3	System Test	Mandatory			
1.1.6.4	User Acceptance Test	Mandatory			
1.1.6.5	Performance Test	Mandatory			
1.1.6.6	Operational Readiness Test	Mandatory			
1.1.6.7	Post Deployment Test	Mandatory			
1.1.6.8	The following aspects must be configurable and not hard coded: a. Business rules e.g. taxi dispatching rules, rule to determine data mining criteria to analyse data b. Tariff for inter operator settlement rates c. Alarm thresholds to trigger alerts/alarms to call centre personnel manning the Taxi Command & Control Centre (e.g. to alert when offence occurs) d. Content e. Maps should be enterprise edition with richer features e.g. point-of-interest f. MSISDNs to send notification to passengers, to verify confirmed bookings	Mandatory			
1.1.7	Reports: Operational and Analytical reports **Note:** This must be part of the requirements gathering, design, build, test and deploy delivery lifecycle	Mandatory			
1.1.8	Documentation: Reports, user requirements specification, functional design, technical design, application diagram & setup, user manual & standard operating and maintenance procedure (including operations manual), service level agreement (SLA), training handbook.	Mandatory			
1.2	**General requirements**				
1.2.1	Multi-tier architecture whereby applications processing/business rules, data management (database) and presentation are logically separated for a scalable system: a. Presentation tier - displays information related to such services as playing back taxi route, listing business rules configured. It communicates with other tiers by outputting results to the browser/client tier and all other tiers in the network. b. Application tier - coordinates the application, processes commands, makes logical decisions and evaluations and performs calculations. It also moves data between the two surrounding layers. c. Data tier - Data is stored and retreived from a database or file system. The information is then passed back to the logic tier for processing, and then eventually back to the user.	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
1.2.2	Languages to be supported: a. Taxi Command & Control Centre: Bahasa Malaysia, English b. Centralised Booking & Dispatch: Bahasa Malaysia, English c. In-Taxi Vehicle Equipment: Bahasa Malaysia, English, d. TEKS1M Booking & Dispatch (Optional): Bahasa Malaysia, English	Mandatory			
1.2.3	Taxi Control Centre, Centralised Taxi Booking & Dispatch and In-Taxi Vehicle Equipment to be integrated: a. Standardised user interface as defined by SPAD during the Requirements Gathering session. b. Receive, store and process external data received via secure data transfer mechanism over web services: e.g. SOAP over HTTPS web services, REST over HTTPS web services etc. The protocol must be an open standard.	Mandatory			
1.2.4	Web-based interface and accessible via Internet and intranet	Mandatory			
1.2.5	Supports role-based access on users, so that only eligible users can view, update or delete data based on the roles assigned to him/her.	Mandatory			
1.2.6	Reporting features include development of standard reports, ability to create new reports by user and ability to query based on input parameters.	Mandatory			
1.2.7	Intellectual property rights, including interfaces and source codes, to be owned by the Government of Malaysia. If source codes cannot be handed over to SPAD or the Government of Malaysia, then the supplier must deposit the source codes in escrow, and must also demonstrate that the source code works.	Mandatory			
1.2.8	Information displayed on the In-Vehicle Equipment, Taxi Control Centre and all reports must be localised to Malaysian values, e.g.: a. Time zone: +0800 GMT b. Currency: RM	Mandatory			
2. Taxi Command & Control Centre					
2.1	**Performance Management System (for taxis)**	Mandatory			
2.1.1	To supply, install, configure and maintain application, servers, storage and network equipment for Performance Management System	Mandatory			
2.1.2	Provides capability to generate reports on the performance of taxi operators and driver including but not limited to the following, for forecasting and data planning purposes. The reports must be able to be exported to other formats e.g. xls, csv, txt, rtf. This is to enable these reports to be utilised by other parties within SPAD e.g. dashboard system.	Mandatory			
2.1.2.1	**Operational Report: Operating distance and duration of service covered by taxi operators** Usage: To determine if taxi drivers are covering the minimum operating daily distance, as mandated by SPAD. Fields (includes the following, but not limited to these): a. Drivers' names b. Company that the driver is attached with c. Taxi Network Operator that the driver is attached with d. Operating distance travelled by the driver, from 00:00 - 23:59 hrs on that day e. Operating time that is travelled by the driver, from 00:00 - 23:59 hrs on that day f. Date the report was generated	Mandatory			
2.1.2.2	**Operational Report: Comparison of no of passengers pickup by taxi operators** Usage: To determine the no. of passengers picked up by passengers on a daily basis. Fields (includes the following, but not limited to these): a. Drivers' names b. Company that the driver is attached with c. Taxi Network Operator that the driver is attached with e. The total number of passengers picked up by the driver in that day f. The number of trips completed by the driver in that day g. The number of passengers picked up by the driver for each trip (exact, not estimate or average) h. Start datetime and end datetime for each trip i. Date the report was generated	Mandatory			
2.1.2.3	**Operational Report: Analysis of booking, dispatch and actual passenger pickup timings** Usage: To determine how closely the taxi operators and taxi network operators meet their SLAs. This will also be used to monitor and track taxi ridership. Fields (includes the following, but not limited to these): a. Drivers' names b. Company that the driver is attached with c. Taxi Network Operator that the driver is attached with d. Booking time (i.e. exact time that the taxi booking request is sent by passenger, in YYYYMMDD hh:mi:ss format) e. Dispatch time: (i.e. exact time that the taxi is dispatched to the passenger, in YYYYMMDD hh:mi:ss format) f. Dispatch SLA missed by time (i.e. the time that the SLA is missed, in hh:mi:ss format) g. Passenger pickup time (i.e. exact time that the taxi picked up the passengher, in YYYYMMDD hh:mi:ss format) h. Pickup time SLA missed by time (i.e. the time that the SLA is missed, in hh:mi:ss format)	Mandatory			
2.1.2.4	**Operational Report: Average waiting time for taxis by taxi operator for peak & non-peak hrs** Usage: To determine the waiting time for taxis, as a proportion of the total trip time. This is to determine traffic patterns and to be used for planning purposes (e.g. when reviewing fares). Fields (includes the following, but not limited to these): a. Drivers' names b. Company that the driver is attached with c. Taxi Network Operator that the driver is attached with d. Start datetime and end datetime for each trip e. GPS coordinates of the trips (to enable playback of trip) f. GPS coordinates of the locations where the taxi waiting time exceeds a threshold pre-defined by SPAD (different threshold set for peak and off-peak periods) g. Wait times (in seconds) - broken down and rolled-up per trip h. Date the report was generated	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
2.1.2.5	**Operational Report: Customer complaints analysis by taxi operators and taxi network operators** Usage: To track and monitor the complaints, and flag out the top-3 taxi operators that garner the most complaints. Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Nature of complaint (e.g. delays, poor manners of the taxi driver) c. Taxi registration number d. Number of complaints (daily/monthly/quarterly/yearly) e. Dates and times when the complaints were lodged (in YYYYMMDD hh:mi:ss format) f. Location of the incident that triggered the complaint g. Date the report was generated	Mandatory			
2.1.2.6	**Operational Report: Traffic Offence/service violations analysis by taxi operators and taxi drivers (for enforcement purposes)** Usage: To track and monitor the offences and flag out the top-3 taxi operators/taxi network operators that accumulated the most offences/violations. Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Type of offences committed (e.g. non-usage of taxi meter, bringing taxi passengers on an unnecessarily long route) c. Taxi registration number d. Number of offences/violations committed (daily/monthly/quarterly/yearly) e. Dates and times when the offences were committed (in YYYYMMDD hh:mi:ss format) f. Location of the offence g. Date the report was generated	Mandatory			
2.1.2.7	**Operational Report: Taxi Breakdown Analysis by taxi operators and taxi network operators** Usage: To track and monitor the taxi breakdowns based on taxi operators and taxi network operators, and flag out the top-3 taxi operators/taxi network operators that has the most breakdowns. Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Date and time when the breakdown(s) occurred c. Date and time when the breakdown(s) ended (i.e. problem was fixed and the taxi was operational again) d. Duration of the breakdown e. Location of the breakdown f. Taxi registration number g. Date the report was generated	Mandatory			
2.1.2.8	**Operational Report: Supply and demand analysis for different areas (areas can also be defined as zones/sectors etc., if necessary)** Usage: To analyse and monitor the taxi supply and demand patterns on an hourly basis, based on areas/zones/sectors. **Note:** the granularity of the observation window must be adjustable, if SPAD needs to observe using smaller observation windows e.g. a snapshot once every 30 minutes. Fields (includes the following, but not limited to these): a. Area/Zone/Sector name b. Are/Zone/Sector ID c. Observation window start datetime d. Observation window end datetime e. Number of taxis actively working (plying the route) within the area f. Number of passengers that have placed taxi booking within the area g. Number of passengers that have been dispatched (fulfilled) with a taxi within the area h. Number of oversupply (***Note:*** *this value is tentatively based on Number of taxis actively plying the route - Number of passengers that have placed booking within the area. If there is an oversupply situation, this value will be positive. However, if there is an undersupply, then this value will become negative*) i. Percentage of oversupply	Mandatory			
2.1.2.9	**Operational Report: Fare charges analysis by taxi operators** Usage: To analyse and monitor the taxi fare charges based on taxi operators and taxi network operators. This is to determine fare patterns and to be used for planning purposes (e.g. when reviewing fares). Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Observation window start datetime c. Observation window end datetime d. Total fare collection within the observation window (in RM) e. Number of trips completed within the observation window f. Date the report was generated	Mandatory			
2.1.2.10	**Operational Report: Taxi Accident Rate analysis by taxi operators and taxi network operators** Usage: To track and monitor the accidents and flag out the top-3 taxi operators/taxi network operators that encounter the most accidents. Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Severity of accident: e.g. Fatal, Major, Minor c. Details of accident (e.g. fender bender with another car, collided a lamp post) d. Location of the accident e. Taxi registration number f. Number of accidents encountered (daily/monthly/quarterly/yearly) g. Dates and times when the accidents occurred (in YYYYMMDD hh:mi:ss format) h. Date the report was generated	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
2.1.2.11	**Operational Report: Driving Hrs Compliance Analysis by taxi operators and taxi drivers (for enforcement purposes)** Usage: To track and monitor the number of driving hours clocked by each taxi operator, taxi network operator and taxi driver, and flag out the drivers (and the taxi operators/taxi network operators they are registered with) that do not fulfill the minimum driving hours. Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Taxi registration number c. Taxi driver d. Operating driving hours clocked (in that day) e. Flag/indicator if the driving hours do not meet the minimum operating driving hours per day f. Date the report was generated	Mandatory			
2.1.2.12	**Operational Report: Distance travelled and fare charged per trip, broken down by taxi drivers** Usage: To track and monitor any anomalies with regards to taxi fares charged by drivers based on distance, and to facilitate trending and planning e.g. with regards to taxi fare review. In addition, this information will be used to facilitate enforcement. Fields (includes the following, but not limited to these): a. Drivers' names b. Company that the driver is attached with c. Taxi Network Operator that the driver is attached with d. Start datetime and end datetime for each trip e. Distance travelled for each trip f. GPS coordinates of the trips (to enable playback of trip) g. Fare charged per trip h. Taxi meter status for each trip (e.g. active, inactive) i. Start datetime and end datetime when the taxi meter was activated j. Date the report was generated	Mandatory			
2.1.2.13	**Analytical Report: Taxi Incident/Breakdown Rate Analysis** Usage: To track and monitor the rate of taxi breakdowns, based on taxi operators and taxi network operators. Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Number of breakdowns (daily/weekly/monthly/quarterly/yearly) c. Location of breakdowns (to identify hotspots) d. Cause of breakdowns e. Date the report was generated	Mandatory			
2.1.2.14	**Analytical Report: Taxi Operational Efficiency (Revenue/KM)** Usage: To analyse and compare the distance travelled versus fares collected, by each taxi operator and taxi network operator. Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Total distance travelled (daily/weekly/monthly/quarterly/yearly) c. Total collection (daily/weekly/monthly/quarterly/yearly) d. Taxi operational effeciency (daily/weekly/monthly/quarterly/yearly) e. Date the report was generated	Mandatory			
2.1.2.15	**Analytical Report: Taxi Maintenance (Cost / KM) analysis** Usage: To analyse and compare the taxi maintenance cost versus distance travelled, by each taxi operator and taxi network operator Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Total maintenance cost (daily/weekly/monthly/quarterly/annually) c. Total distance travelled (daily/weekly/monthly/quarterly/annually) d. Taxi maintenance ratio (daily/weekly/monthly/quarterly/annually)) e. Date the report was generated	Mandatory			
2.1.2.16	**Analytical Report: Taxi Cost Recovery Index** Usage: To analyse and compare the operational profitability of taxi operators/taxi network operators Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Total operational cost (daily/weekly/monthly/quarterly/annually) c. Total collections received (daily/weekly/monthly/quarterly/annually) d. Total profitability (daily/weekly/monthly/quarterly/annually) e. Taxi cost recovery index (daily/weekly/monthly/quarterly/annually) f. Date the report was generated	Mandatory			
2.1.2.17	**Analytical Report: Taxi Utilization Rate Analysis (e.g. % of total taxis in operation from total fleet)** Usage: To analyse and monitor the taxi utilisation rate of taxi operators/taxi network operators Fields (includes the following, but not limited to these): a. Taxi Operator/Taxi Network Operator b. Total number of taxis in fleet (daily/weekly/monthly/quarterly/annually) c. Total number of taxis in-service (plying the route and actively servicing passengers) (daily/weekly/monthly/quarterly/annually) d. Total number of taxis out-of-service (daily/weekly/monthly/quarterly/annually) e. Taxi utilization rate (daily/weekly/monthly/quarterly/annually) f. Date the report was generated	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
2.1.3	Able to perform data mining and perform detailed analysis of the data captured in CTSS, in order to detect offences committed by taxi drivers. This is done when the data mining module detects anomalous conditions above a pre-defined threshold. These insights will also be channelled into reports generated by the system. E.g. if a taxi is driven over a long distance but the percentage of time when the meter is turned on falls below a certain pre-defined threshold, then CTSS must flag this out to the Taxi Command & Control personnel (e.g. by flashing alarms on the Taxi Command & Control Centre).	Mandatory			
2.1.4	Able to interface with Driver Information System (DIS), including daily synchronisation of driver profiles from DIS to CTSS. Driver information that needs to be synchronised includes but is not limited to: a. Driver's name b. Driver's age c. Driver's date of birth d. Driver's driving licence details (e.g. licence class, licence number) e. Driver's IC number f. Driver's past traffic offences g. Outstanding summonses h. Zoning information	Mandatory			
2.1.5	Able to interface with SIKAP, the followings are information from SIKAP to be shared with CTSS: a. Licensing information b. Operator information c. Vehicle information d. Zoning information e. Driver information	Mandatory			
2.2	**Fleet Management System**	Mandatory			
2.2.1	To supply, install, configure and maintain application, servers, storage and network equipment for Fleet Management System				
2.2.2	Able to view and track taxi vehicle location and movement in real-time. The observation frequency suggested are: a. Once every 5 minutes, and/or b. Once every 500 metres travelled (whichever comes first) ***Note**: These parameters should not be hard-coded but should be flexible enough to be modified by SPAD in future via a configuration console.*	Mandatory			
2.2.3	Able to view and track taxi vehicle speed in real-time. The observation frequency suggested are: a. Once every 5 minutes, and/or b. Once every 500 metres travelled (whichever comes first) Note: These parameters should not be hard-coded but should be flexible enough to be modified by SPAD in future via a configuration console.	Mandatory			
2.2.4	Able to view information about the driver and passenger on the taxi vehicle that is being tracked.	Mandatory			
2.2.5	Able to display information about taxis on a real-time map which includes but not limited to: a. Estimated Arrival Time b. Estimated Distance c. Estimated Fare d. Notification for delay e. Driver Contact Information f. Taxi Registration No and other details such as make, model, color. g. Rating capability These information can be displayed on the Taxi Command & Control Centre, so that the personnel manning the Command & Control Centre can view on a map the following details: a. Taxi status (e.g. hired, available, reserved) - thse should be colour coded b. Taxi passengers including their waiting time (if the waiting time exceeds a certain threshold, then the colour indicator changes from green to amber to red)	Mandatory			
2.2.6	Has geo-fencing capabilities - set up geo-fences to monitor various vehicle movements into, out of and within the geo-fence territory (vehicle ID, geofence area ID, time of zone entry/exit, mileage driven within the zone). Geo-fences are monitored on a vehicle by vehicle basis. Information about entry and exit from a geo-fence boundary is stored as separate events that either get stored on the OBU or gets sent up the Taxi Command & Control Centre when data is communicated. Furthermore, user defines rules for vehicle fleet (single or several vehicles) and particular geofenced area (or several locations) at a time: a. Geofence direction (when vehicle enters the area and when it leaves the are; only when enters, only when leaves the area) b. Event severity (none, information only, alert) c. Event access level (limited, public) d. Audio alert in vehicle (yes, no)	Mandatory			
2.2.7	Fleet management server: comprise of performance monitoring application for SPAD operation and taxi management for taxi operator. This server shall communicate with the OBU installed in each taxis	Mandatory			
2.2.8	Fleet Management System must include the following sub-modules: a. Driver Management: display data on driver personal information, driving licence and driving training. Data can be pulled from external sources e.g. DIS. b. Vehicle Management: display data on vehicle registration information and vehicle licence. Data can be pulled from external sources e.g. SIKAP. c. Schedule Management: Manage allocation of drivers to vehicle and driver working schedule (e.g. to prompt drivers to move to a different area where the passengers are underserved). d. Route Management e. Telemetry Management Notification Management f. Performance Management g. Cost Management h. Fare Management i. Fuel Management j. Maintenance Management k. Phonebook & Contact Management	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
2.2.9	Vehicle location for relocation/re-deployment: Analyze the concentration of customers (base on booking data) to relocate taxi to more productive area.	Mandatory			
2.2.10	Taxi Command & Control Centre Operator can easily monitor and check the location and status of taxis to see any abnormal activities through the Execution Overview screen. For example, they can check is there any taxis go outside their authorized service zone if the company divides the territories into different service zones or areas taxi is not allowed to go. Furthermore, Call Center Operator also can track any abnormal journeys with the taxi status is 'Available', which might be a non-meter driving trip is taking right now.	Mandatory			
2.2.11	Graphical user interface that shows taxis details on a map so Taxi Command & Control Centre Operator can more easily to recognize the location and status of taxis.Taxi's current location will also be shown on the map and also taxi status such as such as 'Vacant', 'Reserved', 'Hired' or 'Out of Service'. Moreover, taxi information is near real time as it only has few seconds delay caused by mobile network latency.	Mandatory			
2.2.12	Routing information of current order or last order can also be shown. Furthermore, Taxi Command & Control Centre Operator will also be alerted if any aggressive driving or customize events happened and can show taxi log data in a chart, for example, the speed range of the taxi.	Mandatory			
2.3	**GIS Maps**	Mandatory			
2.3.1	To supply, install, configure and maintain application, servers, storage & network equipment for GIS and Map solution				
2.3.2	Able to find origin and destination address on a map based on street name, business name, places of interest, postcode, GPS coordinates and others	Mandatory			
2.3.3	Have geo-coding as part of location management functionalities. Geocoding enables to convert any street address or zip/postal code into associated geographic coordinates (longitude/latitude) and display it on the map. This feature offers the user possibility to: a. Quickly search for particular location, points of interest (POIs) b. Map multiple locations at a time c. Define several geo-fenced areas by a single click	Mandatory			
2.3.4	Able to support multi-layered map to support road, aerial and hybrid modes.	Mandatory			
2.3.6	Able to view job orders on a map real-time with ability to access information about the job including but not limited to the following: a. Job details when driver accepted jobs (e.g. customer contact, pickup, dropoff locations) b. Passenger name and other relevant information	Mandatory			
2.3.7	Map should be able to show up till street level.	Mandatory			
2.3.8	Map must show the latest road/terrain condition.	Mandatory			
2.3.9	Map server: comprise of updated GIS map system.	Mandatory			
2.4	**Auto Data Capturing**	Mandatory			
2.4.1	Obtain vehicle fault data information through proposed In-vehicle Unit. The fault data should be recorded in device, stored in system and displayed in statistical report form. Vehicle driver can check the statistic report for the detection and supervision to identify the vehicle condition proactively and statistically.	Mandatory			
2.4.2	Capture real-time position data (GPS coordinates - latitude and longitude) of taxis on periodic basis (once in 5 minutes or once every 500 metres, whichever occurs earlier), so that the data can be used to perform: a. Latest Tracing Display (Playback) b. Real-time Position Viewing c. Real-time Speed Trend Viewing d. Distance travelled - by taxi and driver e. Status of each taxi (e.g. hired, available etc.)	Mandatory			
2.4.3	Capture past route and path data, so that the data can be used to perform: a. Path and Journey Recognition b. Journey Kilometer Calculation c. Journey Average Speed Statistic d. Dangerous Behaviour Recognition e. View and playback past path tracking f. Past Journey Presence on GIS map	Mandatory			
2.4.4	Log the information such as driver behavior, RPM, speed, GPS location, any harsh brake or acceleration, etc. Alert message will be triggered to the taxi driver and operator for notification if certain event happens such as harsh brake or speeding.	Mandatory			
2.4.5	Collect traffic condition and taxis trajectories as probe data to profile road network and identify potential high pick up zone, and send this kind of information to taxis to try to get more customer there and to increase the income	Mandatory			
2.4.6	Able to automatically coordinate 2-way data transmission, receiving and handshaking from all taxis to the Taxi Control Centre, regardless of weather conditions (i.e. data transmission and receiving must be possible even in inclement weather).	Mandatory			
2.4.7	Data captured must include all (but not limited to) data parameters specified under the Performance Management System and Fleet Management System sections above.	Mandatory			
2.4.8	Able to report on driver's behavior which includes but not limited to the following: a. Speed Violation (including the number of occurrence for each violation, and flag out the top 3 most frequent violations) b. Harsh Braking c. Harsh Acceleration d. Taxi Meter Disconnection e. Onboard Unit Disconnection f. The list of drivers and taxi vehicle details, that have exceeded a pre-defined number of violations within a specific timeframe	Mandatory			
2.5	**Driver Tracking System**	Mandatory			
2.5.1	To supply, install, configure and maintain application, servers, storage and network equipment for Driver Tracking System				
2.5.2	Able to track position of their own vehicle on the map in real time	Mandatory			
2.6	**Merit & Demerit System**	Mandatory			
2.6.1	To supply, install, configure and maintain application, servers, storage and network equipment for Merit Demerit System				
2.6.2	Able to keep track and record merit and demerit points, operator licensing, vehicle and driver details for taxi drivers, taxi operators and taxi network operators - based on data flowthrough from DIS.	Mandatory			
2.6.3	Able to translate passenger ratings into: a. Merit points: if the passenger provides good ratings of the driver b. Demerit points: if the passenger provides poor ratings of the driver The merit and demerit points scale and criteria must be configurable. These points will then be fed into DIS - either via batch interface or online interface. If an online interface is used, it should not cause performance degradation to any of the modules within the CTSS or DIS systems.	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
2.7	**Content Management**	Mandatory			
2.7.1	Manages content creation, storage, updates and distribution to the Rear Seat Taxi Monitor and OBU	Mandatory			
2.7.2	Must allow playback media, display information & allow interactive communication	Mandatory			
2.7.3	Content management should support the folllowing modes of content distribution: a. Able to push content remotely (e.g. wireless connection, cellular network) b. Media stored on local storage (either OBU or Rear Seat Monitor), and incremental updates sent over the air	Mandatory			
2.7.4	Upload methodology a. Programming is transmitted autmatically to the vehicle via the internet by using wireless network b. Optional method: Direct to the point (DTTP) c. Update schedules by weekly basis	Mandatory			
2.7.5	Proposed section on the screen: a. Driver information b. Video playing & interactive area c. Settings - Brightness, volume d. Taxi information e. Rate your taxi f. Footer (Branding/ copyright) g. Selection menu: - Videos - Promotion - Events - Movie	Mandatory			
3. Centralised Booking & Dispatch					
3.1	**Taxi Order Forwarding Engine**	Mandatory			
3.1.1	To supply, install, configure and maintain application, servers, storage and network equipment for Centralized Booking and Dispatch System	Mandatory			
3.1.2	**New job**	Mandatory			
3.1.2.1	Passenger books a taxi - via telephone booking a. Passenger places a taxi booking via phone booking b. As per the current process, the booking is accepted via the call booking operator c. If the call booking operator is able to dispatch a taxi within the same network to the passenger, the process completes as per status quo (outlined in section 3.1.3). Else, the call booking operator invokes the SPAD order forwarding application portal (also in scope within this CTSS RFP), to 'sell' the job to other taxi networks, via CTSS (outlined in section 3.1.4).	Mandatory			
3.1.2.2	Passenger books a taxi - via booking app (smartphone or tablet) a. Passenger places a taxi booking via smartphone or tablet app b. As per the current process, the booking is accepted via the taxi network operator c. If the taxi network operator is able to dispatch a taxi within the same network to the passenger, the process completes as per status quo (outlined in section 3.1.3). Else, the taxi network operator invokes SPAD's web APIs (also in scope within this CTSS RFP), to 'sell' the job to other taxi networks, via CTSS (outlined in section 3.1.4).	Mandatory			
3.1.2.3	Passenger books a taxi - via web booking portal a. Passenger places a taxi booking via web booking portal b. As per the current process, the booking is accepted via the taxi network operator c. If the taxi network operator is able to dispatch a taxi within the same network to the passenger, the process completes as per status quo (outlined in section 3.1.3). Else, the taxi network operator invokes SPAD's web APIs (also in scope within this CTSS RFP), to 'sell' the job to other taxi networks, via CTSS (outlined in section 3.1.4).	Mandatory			
3.1.3	**Taxi Network Operator Accepts the Job**	Mandatory			
3.1.3.1	Taxi Network Accepts the Job - Source of Booking: Phone Booking a. Call booking operator confirms the booking in the same phone call (as outlined in section 3.1.2.1), and informs the passenger the details of the taxi: a. Taxi registration number b. Estimated time of arrival (ETA) c. Estimated fare d. Driver's name ***Note**: If the passenger is unable to hold the call (e.g. due to an urgent incoming call for the passenger), then the system should have the capability of sending notification SMS to the passenger, displaying the following details:* *a. Taxi registration number* *b. Estimated time of arrival (ETA)* *c. Estimated fare*	Mandatory			
3.1.3.2	Taxi Network Accepts the Job - Source of Booking: Booking App a. Taxi Network Operator confirms the booking via the booking app (as outlined in section 3.1.2.2), and informs the passenger (via the booking app) the details of the taxi: a. Taxi registration number b. Estimated time of arrival (ETA) c. Estimated fare d. Driver's name e. Suggested route	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
3.1.3.3	Taxi Network Accepts the Job - Source of Booking: Web booking portal a. Taxi Network Operator confirms the booking via the web booking portal (as outlined in section 3.1.2.3), and informs the passenger (via the web portal) the details of the taxi: a. Taxi registration number b. Estimated time of arrival (ETA) c. Estimated fare d. Driver's name e. Suggested route	Mandatory			
3.1.4	**Taxi Network Operator Forwards ('Sells') the Job to Other Networks**	Mandatory			
3.1.4.1	Taxi Network forwards the job - Source of Booking: Phone Booking a. Taxi Network invokes the SPAD CTSS order forwarding application portal (also in scope within this CTSS RFP), to 'sell' the job to other taxi networks. On this portal, the operator fills in the following details: i. Passenger name ii. Pickup point (location in terms of exact coordinates) iii. Destination iv. Date and time when booking was made by passenger b. The job details are received and processed by Taxi Order Forwarding Engine (a component in CTSS Centralised Booking & Dispatch), and relayed to all taxis connected to CTSS (except taxis associated/connected to the originating taxi network operator/taxi operator). c. Meanwhile, in each of the taxis, the job details are displayed on the on-board units (also in scope within this CTSS RFP) and the taxi drivers are alerted (via audio alerts). d. Once a taxi driver accepts the job, the details of the driver are transmitted by the on-board unit (OBU) to the Taxi Order Forwarding Engine. The details are: i. Taxi registration number ii. Estimated time of arrival (ETA) iii. Estimated fare iv. Driver's name e. The Taxi Order Forwarding Engine records this as a transaction that is fulfilled by a taxi connected to Taxi Network B (assuming that the taxi that accepted the job is connected to Taxi Network B), and are viewable via the application portal by the operator. Meanwhile, the Taxi Order Forwarding Engine sends a notification SMS to the passenger via SMS gateway (also in scope within this CTSS RFP) within 10 seconds. The notification SMS contains at minumum, the following details: i. Taxi registration number ii. Estimated time of arrival (ETA) iii. Estimated fare	Mandatory			
3.1.4.2	Taxi Network forwards the job - Source of Booking: Booking App a. Taxi Network invokes the SPAD CTSS order forwarding web API (also in scope within this CTSS RFP), to 'sell' the job to other taxi networks. The input parameters would include the following: i. Passenger name ii. Pickup point (location in terms of exact coordinates) iii. Destination iv. Date and time when booking was made by passenger b. The job details are received and processed by Taxi Order Forwarding Engine (a component in CTSS Centralised Booking & Dispatch), and relayed to all taxis connected to CTSS (except taxis associated/connected to the originating taxi network operator/taxi operator). c. Meanwhile, in each of the taxis, the job details are displayed on the on-board units (also in scope within this CTSS RFP) and the taxi drivers are alerted (via audio alerts). d. Once a taxi driver accepts the job, the details of the driver are transmitted by the on-board unit (OBU) to the Taxi Order Forwarding Engine. The details are: i. Taxi registration number ii. Estimated time of arrival (ETA) iii. Estimated fare iv. Driver's name e. The Taxi Order Forwarding Engine records this as a transaction that is fulfilled by a taxi connected to Taxi Network B (assuming that the taxi that accepted the job is connected to Taxi Network B), and are viewable via the application portal by the operator. Meanwhile, the Taxi Order Forwarding Engine sends the following details to the originating Taxi Network Operator within 10 seconds, and subsequently the originating Taxi Network Operator pushes the following details to the passenger's booking app: i. Taxi registration number ii. Estimated time of arrival (ETA) iii. Estimated fare	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
3.1.4.3	Taxi Network forwards the job - Source of Booking: Web Booking a. Taxi Network invokes the SPAD CTSS order forwarding web API (also in scope within this CTSS RFP), to 'sell' the job to other taxi networks. On this portal, the operator fills in the following details: i. Passenger name ii. Pickup point (location in terms of exact coordinates) iii. Destination iv. Date and time when booking was made by passenger b. The job details are received and processed by Taxi Order Forwarding Engine (a component in CTSS Centralised Booking & Dispatch), and relayed to all taxis connected to CTSS (except taxis associated/connected to the originating taxi network operator/taxi operator). c. Meanwhile, in each of the taxis, the job details are displayed on the on-board units (also in scope within this CTSS RFP) and the taxi drivers are alerted (via audio alerts). d. Once a taxi driver accepts the job, the details of the driver are transmitted by the on-board unit (OBU) to the Taxi Order Forwarding Engine. The details are: i. Taxi registration number ii. Estimated time of arrival (ETA) iii. Estimated fare iv. Driver's name e. The Taxi Order Forwarding Engine records this as a transaction that is fulfilled by a taxi connected to Taxi Network B (assuming that the taxi that accepted the job is connected to Taxi Network B), and are viewable via the application portal by the operator. Meanwhile, the Taxi Order Forwarding Engine sends a notification SMS to the passenger via SMS gateway (also in scope within this CTSS RFP) within 10 seconds. The notification SMS contains at minumum, the following details: i. Taxi registration number ii. Estimated time of arrival (ETA) iii. Estimated fare	Mandatory			
3.1.4.4	Able to support multi operator environment where each operator can only access to their own taxi fleet.	Mandatory			
3.1.4.5	Able to route jobs of a taxi operator to all taxis, based on pre-defined business rules (e.g. within a particular radius from the pickup point).	Mandatory			
3.2	**Billing & Collections**	Mandatory			
3.2.1	**Billing**	Mandatory			
3.2.1.1	Multiple billing rates and terms & condition, e.g. differentiated by: a. Taxi network operators b. Time of day c. Weekday vs weekends d. Public holidays e. City centre vs suburbs	Mandatory			
3.2.1.2	Billing rates must be configurable and not hard-coded.	Mandatory			
3.2.1.3	Billing functionality must allow definition of multiple bill cycles in a month.	Highly desirable			
3.2.1.4	Must support on-demand billing (hot billing), real-time billing, batch billing and pro-forma billing features.	Highly desirable			
3.2.1.5	The billing system must support the following features, among other features: a. Deposits b. Usages (for pay-per-use transactions) c. Adjustments d. Refunds e. Payments	Mandatory			
3.2.1.6	The billing system must be able to generate bills.	Mandatory			
3.2.1.7	The system must have the ability to email invoices from within system.	Mandatory			
3.2.1.8	The system must follow up the invoicing portion with additional features such as tracking payments, performing automatic billing and emailing overdue statements.	Mandatory			
3.2.1.9	The system must have features to offer mobile phone and email support, PDF or exportable reports.	Mandatory			
3.2.1.10	The system must provide instant access to Billing Reports by Invoice number or by taxi network operator/taxi operators. These reports must be viewable for 1 month, 3 months, 1 year or any interval specified by the user.	Mandatory			
3.2.1.11	The system must support viewing of billing information for just 1 customer or all customers.	Mandatory			
3.2.2	**Collections**	Mandatory			
3.2.2.1	The system must be able to record, track and update the following based on (but not limited to) the following: a. Aging accounts b. Aging status c. Collection status of accounts d. Aging amount for each account **Note:** Accounts here refers to taxi network operators and any other 3rd parties that connect with CTSS	Mandatory			
3.2.2.2	The system must have a collection center that gives historical data, account notes and payment histories to help with collection efforts.	Mandatory			
3.2.2.3	The system must provide instant access to Collections Reports by Invoice number or by customer. These reports must be viewable for 1 month, 3 months, 1 year or any interval specified by the user.	Mandatory			
3.2.2.4	The system must support viewing of collections (Debtors) information for just 1 customer or all customers.	Mandatory			
3.2.2.5	The system should support identification of collections trends throughout the year, to compare monthly performance.	Mandatory			
3.2.2.6	Detailed Aging Report should give a list of all outstanding Invoices, Credit/ Debit Memo. It indicates how old the debt is and displays customers (taxi network operators) telephone number if you need to give them a quick courtesy call.	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
3.2.2.7	At any time, you can send statements with a gentle reminder to customers having debts of less than 30 days overdue while at the same time send a firm message to customers with debts of more than 90 days overdue. You can send customer statements to all customers with balances or pick and choose who you want to send statements to.	Mandatory			
3.2.3	**Inter-operator Settlement Statements**	Mandatory			
3.2.3.1	Provide weekly settlement statements.	Mandatory			
3.2.3.2	Statements broken down by taxi network operators.	Mandatory			
3.2.3.3	The application must have clearing house features to facilitate settlement claims by other taxi network operators.	Mandatory			
3.3	**Middleware**	Mandatory			
3.3.1	To supply, install, configure and maintain application, servers, storage and network equipment for Middleware	Mandatory			
3.3.2	Build interface with Driver Information System (DIS), including daily synchronisation of driver profiles from DIS to CTSS.	Mandatory			
3.3.3	Set up Service Oriented Architecture (SOA) to integrate CTSS with taxi network operators.	Mandatory			
3.3.4	Set-up and publish service registry to all taxi network operators and other 3rd parties that need to interface with CTSS.	Mandatory			
3.3.5	Deliver an Enterprise Service Bus (ESB) that performs (but not limited to) the following: a. Monitor and control routing of message exchange between CTSS, taxi network operators, individual taxis and other 3rd parties identified by SPAD. b. Control deployment and versioning of services c. Event handling d. Data transformation and mapping e. Message and event queuing and sequencing f. Security or exception handling g. Protocol conversion h. Enforcing proper quality of communication service i. Receives (either by regularly polling or event-based triggers) from taxi network operators the following KPI data: - On time delivery - Non delivery / No Show - Abandoned calls percentage - Rejection percentage - Average hold time - Average Call time	Mandatory			
3.4	***Section 3.4 has been removed***				
3.5	**Computer Telephony Integration (CTI)**	Mandatory			
3.5.1	To supply, install, configure and maintain application, servers, storage and network equipment for Computer Telephony Integration	Mandatory			
3.5.2	Able to popup screen when calls are routed. Pop-up screen must contain the following: a. Automatic Number Identification (ANI) b. Dialled Number Identification Service (DNIS) b. MSISDN b. Customer name (if customer profile is already registered in the system)	Mandatory			
3.5.3	Able to perform automatic dialing	Mandatory			
3.5.4	Able to function as a basic phone	Mandatory			
3.5.5	Able to perform call transfers	Mandatory			
3.6	**Call logging and auditing**	Mandatory			
3.6.1	Able to record, store and retrieve telephone calls for quality improvements later	Mandatory			
3.6.2	Able to provide reporting on analysis on call rate, no of drop call, average call duration, average response time etc and other standard call centre reports	Mandatory			
3.6.3	Able to report on call centre performance which includes but not limited to the following: a. Incoming Call Analysis (Peak/Non Peak, Answered/Drop) b. Call Duration Analysis (Peak & Non Peak) c. Call Pickup Response Time (Peak & Non Peak) d. Drop Call Analysis (Peak & Non Peak) e. Call Operator Peformance Analysis f. Answered call per shift	Mandatory			
3.7	**Customer Relationship Management - Note: The CRM system proposed must be flexible and scalable enough to be able to add on other modules e.g. Sales**	Mandatory			
3.7.1	To supply, install, configure and maintain application, servers, storage and network equipment for Customer Relationship Management (CRM) System				
3.7.2	CRM would be used for CTSS, as well as for Complaints Management Department (CMD). If CTSS detects an offence has occurred, Fleet Management System will automatically create a case in CRM, which will be automatically routed to Complaints Management Department (CMD) in SPAD. It will also automatically transmit a warning message to the OBU in the offending taxi to warn the driver that he/she is committing an offence. Upon receiving this case, CMD will then investigate based on the details provided and if CMD confirms that it is a valid offence, then CMD will log the case within ISPAA. Once the case has been logged with ISPAA, SPAD Enforcement will then proceed to raise the Investigation Paper (IP) and take action against the driver.	Mandatory			
3.7.3	Allow help desk team to register a customer account on behalf of the network operator (passwords are auto-generated and emailed to customer)	Mandatory			
3.7.4	Able to track and manage network operator's profile	Mandatory			
3.7.5	Able to track and manage network operator's bookings for TEKS1M	Mandatory			
3.7.6	The CRM system shall be a web based system.	Mandatory			
3.7.7	The CRM system must support a combination of Web interface the same functionalities.	Mandatory			
3.7.8	The CRM system shall have sort-able and filter-able columns on all views.	Mandatory			
3.7.9	The CRM system shall provide users the capability to personalize all views based on the users preference.	Mandatory			
3.7.10	The CRM system shall have printing functions available on both soft and hard copy.	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
3.7.10	The CRM system shall support multi-channels customer interactions over phone, email, counter, letter/fax and sms.	Mandatory			
3.7.12	The CRM system must be designed to support future expansion of customer interactions such as web channel.	Mandatory			
3.7.13	The CRM system must provide a navigation pane for easy maneuvering of features and capabilities. The navigation pane can be collapsed or hidden for full view of the CRM information or data and can be call-out easily for futher navigation.	Mandatory			
3.7.14	The CRM system must present information in view forms. Each view form presents data in overview format (rows and columns) and a preview pane for the CRM record curently selected or highlighted is presented for quick review of the specific CRM record.	Mandatory			
3.7.15	Each view comes with native analytic or dashbord for graphical presentation of the CRM record being viewed.	Mandatory			
3.7.16	Each view comes with native analytic or dashbord for graphical presentation of the CRM record being viewed.	Mandatory			
3.7.17	Personalized conditional formatting can be applied to each view to highlight CRM records.	Mandatory			
3.7.18	Each view can be personalized by the user to enrich the experience.	Mandatory			
3.7.19	The CRM system must provide data search capability on every views.	Mandatory			
3.7.20	The search capability can be configured to search over pre-configured columns in the views.	Mandatory			
3.7.21	The CRM system shall be able to search and index all documents stored in the repository as well as the information on the database.	Mandatory			
3.7.22	Users shall be able to create and modify the search query with little or no programming required.	Mandatory			
3.7.23	Users shall be able to save the query created for future use.	Mandatory			
3.7.24	The CRM system shall be able to do an advance search, such as full text search, union search and Boolean search.	Mandatory			
3.7.25	The CRM system shall limit the search results to information the users are granted access to.	Mandatory			
3.7.26	Users shall be able to select one or more items in the CRM system and to have the CRM system to alert the users when there are changes to those items.	Mandatory			
3.7.27	The CRM system shall track customer cases which is not being handled within SLA and automatically notify supervisors after a certain period of time.	Mandatory			
3.7.28	Users shall be able to export and import data based on access control configuration.	Mandatory			
3.7.29	The CRM system shall be able to import and export data for the following format Microsoft Office Excel or CSV.	Mandatory			
3.7.30	The CRM system shall be able to verify duplicate entries based on email, name and other fields.	Mandatory			
3.7.31	Creating New Cases (Service Requests)	Mandatory			
3.7.32	Case capability to manage enquiries, complaints, feedback and suggestion from customers.	Mandatory			
3.7.33	Quick access to recently created, modified, or viewed case records.	Mandatory			
3.7.34	Pre-configured case list views (case record subsets based on user-definable filter variables).	Mandatory			
3.7.35	A workflow engine is available to help implement "best practice" case management activities.	Mandatory			
3.7.36	Solution records can be associated with (hyperlinked to) case records.	Mandatory			
3.7.37	Open and closed (completed) customer service and support activities can be associated with (hyperlinked to) case records.	Mandatory			
3.7.38	Comment and note records can be input into case records.	Mandatory			
3.7.39	Documents and files can be associated with (hyperlinked to) case records.	Mandatory			
3.7.40	When a new case record is created via customer input (using a web form or a self-service portal), an e-mail can be automatically sent to the customer confirming that a new case record has been created.	Mandatory			
3.7.41	A configurable case "status" data field is used to track the status of each case (e.g., new, escalated, on-hold, closed, etc.).	Mandatory			
3.7.42	Any time a case record is created or updated, a history record (of the change) is automatically created and associated with the case.	Mandatory			
3.7.43	A variety of predesigned case management reports are available for immediate use.	Mandatory			
3.7.44	Predesigned case-related analytics (charts and graphs) are available for display on dashboards and reports.	Mandatory			
3.7.45	When new case records are created, they can be automatically assigned to the appropriate person using predefined assignment rules.	Mandatory			
3.7.46	When cases are assigned to someone, this person can be automatically notified of the case via e-mail.	Mandatory			
3.7.47	Case records can be automatically assigned to a work queue (using predefined assignment rules) that multiple people can access them from.	Mandatory			
3.7.48	When working from a work queue or a list of cases a user can simultaneously take "ownership" of multiple case records (i.e., assigning him or herself to the cases).	Mandatory			
3.7.49	When working from a work queue or a list of cases a user can simultaneously assign the "ownership" of multiple case records to another person (or queue).	Mandatory			
3.7.50	When working from a work queue or a list of cases a user can simultaneously change the status of and escalate multiple case records.	Mandatory			
3.7.51	When working from a work queue or a list of cases a user can simultaneously close multiple cases.	Mandatory			
3.7.52	Case escalation rules can be defined that will control the automatic escalation of a case if it is not resolved within a certain period of time.	Mandatory			
3.7.53	Case escalation rules can be defined that will control the automatic escalation of a case when specified conditions are met, including values input into custom data fields.	Mandatory			
3.7.54	Escalation rules specify to whom the case will be reassigned to.	Mandatory			
3.7.55	Escalation rules specify all of the people who will be automatically notified via e-mail about the escalated case.	Mandatory			
3.7.56	Solution records (a knowledge base) can be searched for possible answers to the customer`s problem.	Mandatory			
3.7.57	Solution records that address a case can be associated with (hyperlinked to) the case record.	Mandatory			
3.7.58	An e-mail can be automatically sent to the customer regarding the case and its possible solution (using a predesigned e-mail template).	Mandatory			
3.7.59	The reason for the customer`s problem can be input on the case record using a predefined list of "reason" codes or descriptors.	Mandatory			
3.7.60	The system must allow for configurable service level agreement management.	Mandatory			
3.8	**Customer Relationship Management – Integration to the Mitel IP Pabx System with "Screen Pop Function".**				
3.8.1	The proposed CRM must be able to support the Mitel IP Pabx system with Contact Center Solutions that required having a Computer Telephony Integration (CTI) function to support "Screen Pop functionalities" of the caller information via Caller ID.	Mandatory			
3.8.2	The system shall have the support of the Contact Center Solutions, which is based on Web Based system.	Mandatory			
3.8.3.8	The system proposed shall provide the Integration required of the CRM to the web based system proposed here with the Screen Pop Functionalities.	Mandatory			
3.8.4	The CRM system shall support at the initial of 32 Agents and up to maximum of 150 Agents and fully integrate with the Mitel Contact Center system used in SPAD.	Mandatory			
3.8.5	When an agent in the contact center receives a call, the caller ID information is available, and a "Screen Pop " of the caller information should be presented to the agent before answering the call.	Mandatory			
3.8.6	The system shall support "Web Page "from the Contact Center Screen Pop function that launch the Caller Profile when an agent answer an ACD call.	Mandatory			
3.8.7	Please refer addendum on Contact Center Screen Pop application or Web page when agent answers an ACD Call.	Mandatory			
3.9	**CRM Integration to ISPAA and SIKAP**				
3.9.1	CRM must be integrated with ISPAA and SIKAP. Please refer addendum on ISPAA and SIKAP background	Mandatory			
4. 1,500 In-Taxi Vehicle Equipment					
4.1	**On-Board Unit (OBU)**	Mandatory			
4.1.1	**Physical specification**	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
4.1.1.1	OBU casing must be rugeddized and must withstand the following temperature range: a. 0C to 60C @ 5% to 95% non-condensing (operating) b. -20C to 80C @ 0 to 95% non-condensing (storage)	Mandatory			
4.1.1.2	OBU must be preferably made up of 2 detachable components: a. Screen b. Interface terminal unit that can act as a bridging interface between the 12 types of taxi meters authorised by Jabatan Pengangkutan Jalan Malaysia and Android smartphones and tablets. Hence, it must contain both: a. USB ports b. Serial ports c. RJ-45 ports	Mandatory			
4.1.1.3	OBU must be compliant to IP 65 standard, including waterproof.	Mandatory			
4.1.1.4	OBU can withstand vibration and shock (protected against surge and vibration): complies with MIL-STD-810G, Method 514.4 standard (vibration); 20G operating condition (shock).	Mandatory			
4.1.1.5	Display screen must be at least 6.5 inch (diagonal)	Mandatory			
4.1.1.6	Display screen must be of certain technology (LCD)	Mandatory			
4.1.1.7	Display screen brightness (450cd/m2)	Mandatory			
4.1.1.8	OBU can be powered directly by vehicle's battery with the range of 9-26 Vdc	Mandatory			
4.1.1.9	OBU has an in-built battery capacity that can last up to 8 hours	Mandatory			
4.1.1.10	OBU supports remote (ie. over the air) updates to OBU's firmware and software	Highly desirable			
4.1.1.11	OBU supports data compression before transmission for smaller data volumes	Mandatory			
4.1.1.12	Able to automatically guide driver to pickup point and then to destination via real-time GPS navigation with an on-screen map and audio directions. This includes turn-by-turn & an electronic voice to inform the driver whether to turn left or right, the street name, and how much distance to the turn.	Mandatory			
4.1.1.13	OBU has built-in connectivity to GSM, 3G, Edge, LTE and/or WiMAX networks and WiFi. The supplier must specify if an additional antenna needs to be installed on the taxis, and the specification of the antennas.	Mandatory			
4.1.1.14	OBU has built-in global positioning system (GPS) capability. The supplier must specify which GPS technology is used e.g. Standalone GPS, Assisted GPS.	Mandatory			
4.1.1.15	OBU supports Wireless LAN connectivity	Highly desirable			
4.1.1.16	OBU supports VGA output with [800 X 600] resolution and above.	Mandatory			
4.1.1.17	OBU supports 6 x USB 2.0 ports that support a USB hub for future expansion. The supplier must specify which type of USB interface will be used, e.g. Type-A, Type-B, Mini-A, Mini-B. This is to enable to OBU to be connected to the following in-taxi vehicle equipment: a. Rear seat taxi monitor (LCD touch screen) b. LED taxi status panel c. 1 smartphone/ table/screen to be used as display for the OBU d. Panic button	Mandatory			
4.1.1.18	OBU supports: a. CAN bus 2.0B port b. 5 x External RS232 Serial Ports c. 1 x SD Card Slot d. 1 x Ignition Input e. 2 x Digital Inputs f. 1 x RJ-45 port (to connect to the Cashless Payment Terminal)	Highly desirable			
4.1.1.20	OBU supports interface to cashless payment, via RJ-45 port	Mandatory			
4.1.1.21	OBU supports interface to panic button for drivers. When the driver or passenger presses on the panic button (passenger's panic button is a virtual button on the rear LCD screens), the OBU will send alert to the Taxi Command &Control Centre along with the following information (but not limited to): a. Driver information b. Vehicle information & location	Mandatory			
4.1.1.22	Able to support 2-way voice communication (full duplex)	Highly desirable			
4.1.1.23	The setup of OBU (including its physical hardware and cabling) to be secure against vandalism, unintended case open, theft and illegal modification. This also means that the OBU cannot be switched off as long as the engine is turned on, and it turns on automatically once the engine is switched on.	Mandatory			
4.1.1.24	The OBUs must be able to receive content and pump data to the rear panel (rear panels are also in scope for this RFP). This should be done in both wired manner or wirelessly e.g. WiFi, via protocols with wide industry support e.g. via DLNA. In addition, the OBUs must support 2-way digital wireless data communications (based on GSM technology), to enable SPAD control centre to send announcements to OBUs. **Note:** GSM technology must be EDGE (i.e. 2.5G) and above.	Mandatory			
4.1.1.25	The OBUs must have the feature to be able to play content automatically only in the rear screens.	Mandatory			
4.1.1.26	The OBUs must have anti-theft features built-in, to make it theft-proof (e.g. through removable faceplate).	Mandatory			
4.1.1.27	OBUs must be able to interface with taxi status LED display (either in-taxi or mounted on top of the taxi)	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
4.1.1.29	The OBU must have at least 32GB non-volatile memory.	Mandatory			
4.1.1.30	The taxi driver can only accept jobs when he is logged in to the OBU. This login must be done using a device (e.g. RFID device or smartcard with embedded microchip containing driver details) that is unique for each driver and cannot be replicated for other drivers. The OBU must display the driver's card on the OBU screen and rear LCD screens, as soon as the driver logs in.	Mandatory			
4.1.1.31	The OBU must remind drivers when the expiry date of the following are near (1 month before expiry, 1 week before expiry and on the day of the expiry): a. Driver's Card b. Driver's Licence	Mandatory			
4.1.1.32	The OBU should suspend the meter and display a message on the LED status panel that the taxi is suspended, when there are: a. Outstanding traffic offences/summonses against the driver b. Driver's licence has expired c. Driver's card has expired.	Mandatory			
4.1.1.33	The OBU must be able to detect and monitor the following (possibly via sensors or probes): a. Harsh Braking b. Harsh Acceleration c. Dangerous Behaviour Recognition d. Speeding	Mandatory			
4.1.1.34	OBU must have 24-month warranty	Mandatory			
4.1.2	**Taxi meter integration**	Mandatory			
4.1.2.1	OBU supports interface to taxi fare meter. This interface must be tamper-proof	Mandatory			
4.1.2.2	Must comply with JPJ's regulations on taxi meter specification and use	Mandatory			
4.1.2.4	The OBU must be able to integrate with the taxi meter via RS232 to extract these parameters from the taxi on a periodic basis (e.g. once an hour), and transmit it to the Taxi Control Centre: a. Total Travelled Distance (Km) b. Total Hired Distance (Km) c. Total number of hired trips d. Total number of trip in after midnight (when surcharge is applied) e. Distance travelled breakdown - by trips (Km) f. Time of each hired trip (YYYYMMDD hh:mi:ss) g. Daily total travelled distance h. Daily operating starting time i. Daily total hired distance j. Drops total fare k. Daily total amount l. Daily total number of hired trips m. Paid Km n. Start Date & End Date o. Max Speed	Mandatory			
4.1.2.5	The OBU must be able to activate or deactivate the taxi meter via the RS232 connection	Mandatory			
4.1.3	**Application specification**	Mandatory			
4.1.3.1	OBU supports audio input and output	Highly desirable			
4.1.3.2	OBU application must support 2 language options which include Bahasa Malaysia, English.	Highly desirable			
4.1.3.3	Able to display information about taxi job which includes but not limited to: a. Pickup point b. Destination c. Customer name d. Customer contact number e. Number of passengers for the trip f. Luggage space requirement g. Additional remarks from passengers e.g. special requests from passengers h. Route of trip i. ETA *Note: It should be possible to disable these infomation from being displayed on the OBU via configuration alone*	Mandatory			
4.1.3.4	Able to accept or decline jobs	Mandatory			
4.1.3.5	Able to provide confirmation to the driver once the driver has successfully accepted the job	Mandatory			
4.1.3.6	Able to show history of jobs accepted with information which includes but not limited to: a. Distance travelled b. Amount charged c. Time taken d. Customer name(s) e. Payment method (cash/credit card/debit card/Touch'N'Go) f. Number of passengers g. Additional remarks about each trip h. Receipt number for each trip i. Breakdown of each charge (e.g. base fare, surcharge, GST) for each trip	Mandatory			
4.1.3.7	Able to remind drivers on advance jobs that was accepted (pre-booking)	Optional			
4.1.3.8	Able to support 2-way text messaging with the call centre (only pre-defined text messages)	Optional			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
4.1.3.9	Able to inform driver and emit audible alarm when he is driving above the speed limit	Mandatory			
4.1.3.10	Able to receive broadcasted messages from Taxi Command & Control Centre	Mandatory			
4.1.3.11	Able to display the following information about projected taxi demand at KLIA & KLIA2: a. Number of estimated taxi passengers arriving at KLIA & KLIA2 in the next 3 hours, with breakdown of passenger count for each hour b. Number of airport limo in queue at KLIA and KLIA2 c. Number of budget taxis in queue at KLIA and KLIA2 d. Number of TEKS1M in queue at KLIA and KLIA2	Mandatory			
4.1.3.12	OBU able to store data if in offline mode and retransmit back the data once there is connectivity.	Mandatory			
4.1.3.13	Map on OBU can be updated over the air. Updates can be from Taxi Command & Control Centre or directly from the map provider.	Mandatory			
4.1.3.14	OBU can receive directions/navigation instruction from Taxi Command & Control Centre. This is to prevent on-hire taxi from taking the long route/cheating the passenger.	Mandatory			
4.3	**Panic Button**				
4.3.1	Able to install and set-up panic button so that it is not visible to the taxi passenger and accessible to taxi driver. This is to promote safety for taxi drivers	Mandatory			
4.3.2	Able to immediately alert both the Taxi Command & Control Centre with the following information: a. Vehicle details of the taxi in distress b. Details of the driver on vehicle c. Precise location (coordinates) of vehicle on a map	Mandatory			
4.5	**LED taxi status display panel**				
4.5.1	Tenderer must supply & install taxi status LED display that integrates with the OBU, to display to passengers on the street if the taxi is either: a. Hired b. Vacant/Available c. Reserved/On-call d. Off-duty e. SOS	Mandatory			
4.5.2	Taxi status LED display must display the statuses in distinct colours. However, the colour assignment must be configurable: a. Vacant: Green b. On-call/Reserved: Orange c. Hired: Red d. Off-duty: Yellow/Amber e. Distress/SOS: Red (flashing)	Mandatory			
4.5.3	The following are the proposed specifications for the taxi status LED display: a. Brightness: ≥ 5,000 cd/sqm (outdoor) b. Viewing Angle: H:110° V:50° c. Optimal Viewing Distance: 1 - 50 metres d. Working Temperature: -20°C - +60°C f. Working Humidity: 30% - 100% RH g. Diameter of LED: ~3.75 mm h. Pixel Pitch: ~6 mm i. Working Voltage: DC 5V – 10 V j. Power Consumption: 8W - 14W k. Control Mode: RS232, USB and wireless l. Multi-language Support: English, Bahasa Malaysia m. Self-contained clock and spare battery not paused once powered off n. High Contrast: 4000:1 o. Lifetime: 100,000 hours p. Mean-Time-Between-Failure (MTBF): 50,000 hours q. Dimensions of the panel (display area): Height: 76 mm, Width: 304 mm, Weight: 4.5 kg or lighter r. Waterproof and anti-vibration: IP65 s. Can be powered on and off according to ignition status ***Note:*** *As part of the submission, the tenderer must produce an authenticated warranty document to substantiate these specifications The equipment should also be*	Mandatory			
4.6	**Rear Seat Taxi Monitor**				
4.6.1.	**Physical specification**				

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
4.6.1.1	Rear seat taxi monitor must be supplied, that will be connected to the OBUs and will support display of content inside the taxi. The following are the recommended minimum specifications: a. Screen size: Diagonal 6.5" (16:9) (and above) b. Touchscreen: Interactive touchscreen c. Supported resolution: 640 x 480 - 1920 x 1080 d. Physical resolution: 800 (H) x 480 (V) WVGA e. LCD brightness: 650 cd/m² f. Contrast Ratio: 300:1 g. Viewing Angle: 140° Horizontal, 80° Vertical h. Response Time (Tr/Tf): 6/10ms (Typ.) i. Touch Screen Interface: USB port j. Operating Voltage Range: DC 10V - 24V k. Power Supply: DC 12V l. Power Consumption: <22W m. Operating Temperature: 10°C - 85°C n. Storage Temperature: 10°C - 95°C o. Dimension (mm): ~189.89W x 123.89H x 36.04D (mm) p. FCC, CE, E13 Certification q. ROHS Compliant r. 24 Month Warranty s. Supports Android OS *Note: As part of the submission, the tenderer must produce an authenticated warranty document to substantiate these specifications. The equipments should also be*	Mandatory			
4.6.1.2	Setup of rear seat taxi monitor must be secured against vandlism, unintended case open, theft and illegal modification.				
4.6.2	**Application specifications**	Mandatory			
4.6.2.1	Able to receive content & pump data to the OBU. This should be done in both wired manner, or wirelessly.	Mandatory			
4.6.2.2	Monitor must support playback media and audio output	Mandatory			
4.6.2.3	Able to display information & allow user interaction, for the following but not limited to: a. Driver information b. Map of trip c. Rate your taxi d. Taxi information e. Selection menu: - Video - Promotion - Events	Mandatory			
4.6.2.4	Allow programming of content where user can navigate the content being displayed on the monitor	Mandatory			
4.6.2.5	Able to support the folllowing modes of content distribution: a. Able to push & receive content remotely (e.g. wireless connection, cellular network) b. Media stored on local storage (either OBU or Rear Seat Monitor), and incremental updates sent over the air	Mandatory			
5. Change Management					
5.1	**End-User Training**				
5.1.1	Supplier to conduct end-user training to the intended target audience comprising: a. Taxi drivers b. Taxi Command & Control Centre (SPAD) c. Information Technology (SPAD) d. Road Based Licencing (SPAD) e. Complaints Management (SPAD) f. Enforcement (SPAD) g. Taxi Network Operators The course materials and structure should be tailored according to the audience	Mandatory			
5.1.2	End-user training shall be conducted in a classroom set-up with adequate hands-on training to the participants.	Mandatory			
5.2	**IT Administration Training**	Mandatory			
5.2.1	Supplier to conduct IT Administration Training to the identified personnel who will man the IT Operations of the Taxi Command & Control Centre and Centralised Taxi Booking & Dispatch system.	Mandatory			
5.2.2	IT administration training shall be conducted in a classroom set-up with adequate hands-on training to the participants.	Mandatory			
5.3	**System Training**	Mandatory			
5.3.1	Supplier to conduct System Training to the identified personnel who will maintain and operate the applications related to the Taxi Command & Control Centre and Centralised Taxi Booking & Dispatch (including Call Centre).	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
5.3.2	System training shall comprise: a. Technical, data and network architecture a. Configuration Management b. User ID Management c. System Installation d. System Monitoring e. Operations Management	Mandatory			
5.4	**Documentation and Knowledge Management**	Mandatory			
5.4.1	The supplier shall update all relevant documents whenever an update or patch is available, and shall provide SPAD with the updated documents.	Mandatory			
5.4.2	The supplier shall ensure that all documents are version controlled and notifies the designated SPAD personnel of the document versions.	Mandatory			
5.5	**Knowledge Transfer**	Mandatory			
5.5.1	The supplier shall conduct knowledge transfer sessions to (but not limited to) the following audience on a periodic basis: a. Taxi drivers b. Taxi Command & Control Centre (SPAD) c. Information Technology (SPAD) d. Road Based Licencing (SPAD) e. Complaints Management (SPAD) f. Enforcement (SPAD) g. Taxi Network Operators	Mandatory			
5.6	**Stakeholder Engagement**	Mandatory			
5.6.1	The supplier shall support SPAD in all stakeholder engagement sessions, as necessitated by SPAD.	Mandatory			

B. Non-Functional Requirements

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
6. Software Hosting & Licensing					
6.1	**Software hosting**	Mandatory			
6.1.1	The supplier must install the software in-house, hosted in SPAD environment. If the supplier wishes to propose a cloud computing model, the supplier should quote the hosted option as the primary option (with associated costing), and the cloud computing option as the secondary option with its associated costing.	Mandatory			
6.1.2	The supplier shall supply system software such as operating system, database, antivirus, intrusion detection system etc. This applies on both the primary site and the DR site.	Mandatory			
6.2	**Software licensing & support**				
6.2.1	Software licence pricing should be either open source or based on perpetual software licence. However, annual software licence can be considered with strong justification.	Mandatory			
6.2.2	The software proposed must have extensive vendor and industry support, i.e. it must be used in at least 10 active implementations worldwide.	Mandatory			
6.2.3	The supplier is responsible for supplying 3rd party software that will enable the web services to be exposed to taxi network operators.	Mandatory			
7. Back-end Infrastructure and Hardware					
7.1	To supply, install, configure and maintain application, servers, storage and network equipment for CTSS project. **Note:** At present, SPAD servers are all virtualized and runs on VMWare platform. Hence, the preferred solution should be based on virtualised solution rather than physical servers	Mandatory			
7.2	**Server operating system:** Windows Server (minimum: Standard Edition); Linux (minimum: Enterprise Edition). Depends on hardware selected and application. Vendor to ensure that it is the latest version. **Note:** At present, SPAD uses MS Windows based servers.	Mandatory			
7.3	Relational Database Management System (RDBMS): To supply, install, configure and maintain application, servers, storage and network related equipment for RDBMS. Tenderer must propose a fail-safe high availability optimized database environment with the ability to upgrade vertically and horizontally. At present SPAD uses MS SQL Server as its database, hence the preferred DB platform is MS SQL. However, if the system proposed does not support the preferred DB platform, the tenderer is to justify and provide alternative DB platform.	Mandatory			
7.4	Development framework for application server: Java or .NET Framework. However, tenderer can propose any better development framework but must use industry standard protocol and technology.	Mandatory			
7.5	Networking standard 1. Supports industry standards including TCP/IP, HTTPS. 2. Able to ensure IP address used in the applications must not be hard coded. 3. Able to provide all the TCP ports used by the applications and its subsystem. 4. Able to utilize Network design techniques to appropriately prevent broadcast congestion and outages. 5. Able to provide the Network bandwidth and/or volume assumptions and projections. 6. Able to provide expected Network performance and quality of service based on designs and plans. 7. Contains safeguards to prevent malicious attacks and system hijack e.g. DDOS. This refers to intrusion prevention solution that should be provided by the tenderer. This feature could be in the firewall itself or standalone IPS equipment. Advanced protection for web server will require Web Application Firewall ex: Fortiweb Web Application Firewall	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
7.6	Development languages: a. *Mobile development:* Android and iOS. However, other development language with strong industry support can also be considered. b. *Integration development:* Java, .Net. However, other development language with strong industry support can also be considered. c. *Web development:* Java, .Net, script based (e.g. PHP). However, other development language with strong industry support can also be considered.	Mandatory			
7.7	Integration technology / approaches: Must be based on open industry standards and protocol.	Mandatory			
7.8	Network equipment: Tenderer to propose all relevant network equipment such as switches, routers, firewall, load balancers, IPS etc. You can refer to network architecture setup in **Appendix 6** as a reference but might need to enhance where possible.	Mandatory			
7.9	Server: Server (rack mounted), KVM switch, keyboard, monitors - for both primary site and DR site. At present, SPAD servers are located in Menara Usahawan Putrajaya and the Disaster Recovery Centre (DRC) is at Platinum Sentral. In the future, SPAD might shift to MAMPU datacentre (might be in Putrajaya or Cyberjaya). The proposed solution must take this factor into consideration. There should also be a data link connecting the primary site to the DR site, from the primary to the call centre and from the DR site to the call centre.	Mandatory			
7.10	High speed, high availability, secure IP connectivity from all Taxi Network Operators and taxis to 1GovNet - a stable dedicated line (for example 10 Mbps or better) Tenderer needs to propose a fail-safe dedicated optimized bandwidth for CTSS. For mobile phones related services, the telco coverage must be nationwide. Please refer to the network diagram in ***Appendix 6*** , which illustrates how the taxi network operators and taxis will be connected to CTSS infrastructure which will be housed within 1GovNet.	Mandatory			
7.11	Supplier must set-up the test environment similarly to the production environment: a. Hardware: the tenderer must be able to specify the performance differential between the test environment and production environment and set it up accordingly (e.g. production 100%, test environment is 25% of production environment). b. Software: software and configuration must be identical as the one in production environment.	Mandatory			
7.12	The supplier must supply separate environment instances as follows: a. development/system testing environment b. UAT environment c. production environment d. disaster recovery (DR) environment	Mandatory			
7.13	**Requirement in *Pusat Data Sektor Awam* (PDSA) of MAMPU**	Mandatory			
7.13.1	To supply, install, configure and maintain all CTSS related hardware and accessories in PDSA.	Mandatory			
7.13.2	Rack are provided and the model is AR3100/APC by Schneider. If the proposed hardware unable to be mounted in provided rack, tenderer should provide related accessories end-to-end.	Information			
7.13.3	The connection to data center's core switch are using 10g or 1g connectivity. The tenderer must provide appropriate cable based on proposed solution.	Mandatory			
7.13.4	The distance between server rack to core switch is up to 20 metres.	Information			
7.13.5	The rack PDU are provided and use C13 or C19 connector only. The Tenderer must provide C13 or C19 connector for all hardware to be installed in server's rack.	Mandatory			
7.13.6	Patch panel is provided in server rack.	Information			
7.13.7	Power supply to the rack are 16amp or 32amp	Information			
7.13.8	Tray cable is on top of the rack	Information			
8. Implementation Services					
8.1	**Project Management Office:** Supplier must set-up and operate a project managament office to manage overall project from start to end. The project manager must be PMP/Prince2 certified or equivalent.	Mandatory			
8.2	**Security Requirements:** Ensure hardware set-up meet with SPAD and MAMPU's IT security requirements with all related system hardening (including but not limited to OS and DB) on all new servers.	Mandatory			
8.3	**IT Monitoring:** To supply, install, configure and maintain application, server, storage and network related equipment for IT Monitoring tool. The monitoring solution must be Enterprise version and has 2 modules: 1) hardware monitoring - to monitor servers' resources such as CPU, memory, network ports, windows services etc. 2) software monitoring - to monitor web application, web services, database etc.	Mandatory			
8.3.1	For hardware monitoring: - The proposed solution shall be able to monitor availability and response time of application servers. - The proposed solution shall be able to recognize data patterns in Windows event log to correlate raw networks events, filters events and display event notifications that are useful to administrator. - The proposed solution shall be able to provide root because analysis from the information gathered.The proposed solution shall be able to generate out of box reports such as business application performance in (but not limited to) CSV, HTML or PDF formats. -The proposed solution shall be able to provide Mean Time To Repair (MTTR) and Mean Time Between Failures (MTBF) for each application and services. -The proposed solution must be able to Record a sequence of HTTP requests and configure it to be checked at regular intervals of time. -The proposed solutions shall be able to seamlessly integrate all components to provide visual health views	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
8.3.2	For software monitoring: - URL Monitoring,URL Visitor total number, Record & Playback HTTP Request and URL Content Monitoring/page - The proposed solution shall be able to simulate web transitions - Support a series web page transaction. (For example, log into web mail, access mail inbox and log out) - Ability to check for keywords for each step or web page access. - Ability to record the time taken for each step or web page access - The proposed solution shall be able to monitor the health status of the database. - The proposed solutions shall be able to monitor Windows services using WMI. - The proposed solution should also be able to trace Performance metrics of Java/ J2EE components and SQL statements executed by the URL	Mandatory			
8.4	**Capacity planning:** System is to design for 5 years capacity. Tenderer to provide detailed capacity sizing breakdown, and justify it based on transaction volume.	Mandatory			
8.5	Data Retention Policy: All system logs, transactional logs and database logs must be stored at least for 7 years for auditing and investigation/enforcement purposes.	Mandatory			
8.6	Project nomenclature: Standard naming convention shall be used for all source codes, environment, documentations.	Mandatory			
8.7	Version control: All source codes, documentations, configuration and other deliverables in the project must be version controlled.	Mandatory			
8.8	Delivery approach: a. Custom development - resources should be based on-site at SPAD office b. Package implementation & integration - resources should be based on-site at SPAD office c. Application support - resources should be based on-site at SPAD office	Highly desirable			
9. Methodology & Testing Procedure					
9.1	On Testing Procedure, able to develop and maintain test data and repositories.	Mandatory			
9.2	On Testing Procedure, able to develop, document, plan and execute smoothly and successfully test the following: a. Unit Testing b. Functional Testing c. System Testing d. Performance Testing e. Load Testing f. Stress Testing g. Integration Testing h. Regression Testing i. Security Testing j. Post Production Testing. *Note: During the warranty period, the vendor should place resources at SPAD site for the 1st 3 months, to rectify any defects found with the system*	Mandatory			
9.3	All the test specified in Testing Procedure (except for User Acceptance Test) will be carried out by the Appointed Vendor to test and will be reviewed by MSTB, which shall act as the independent verification and validation (IVV) organization appointed by S.P.A.D.				
9.4	On Testing Procedure, able to and flexible to comply with SPAD documentation standards, testing specifications and requirements.	Mandatory			
9.5	On Testing Procedure, able to perform good and truthful recording and reporting of test results. On request, able to conduct walkthrough of test results with SPAD.	Mandatory			
9.6	On Testing Procedure, able to correct defects in a timely manner which does not impact the overall project timeline and recall for testing again.	Mandatory			
9.7	On Testing Procedure, specifically on User Acceptance Test, able to plan and conduct a smooth User Acceptance Test with environment, data, test script, test cases and clear instruction to assist Users to test fully and comprehensively all the processes, the different scenario and all the critical functionalities within the new system.	Mandatory			
9.8	On Testing Procedure, specifically on User Acceptance Test, the tenderer must be able to develop upfront a comprehensive user acceptance test plans and test cases and acceptance criteria for approval.	Mandatory			
9.9	On Testing Procedure, specifically on User Acceptance Test, able to perform the test embedded with the authorization test. Hence, upfront implement a matrix of Authorized User and design the test cycles and scripts to be tested by function in line with the processes.	Mandatory			
9.10	On Testing Procedure, specifically on User Acceptance Test, able to coordinate the entire testing, including to recommend and assist in the identification of the right role/candidate within SPAD to effectively perform the test. and provide support for all Authorized Users participating in the testing.	Mandatory			
9.11	On Testing Procedure, specifically on User Acceptance Test, able to provide support and guidance to all the Authorized Users participating in the testing.	Mandatory			
9.12	On Testing Procedure, specifically on User Acceptance Test, able to manage and effectively and truthfully record and report user acceptance testing results.	Mandatory			
9.13	On Testing Procedure, specifically on User Acceptance Test, able to rectify all the Problems log without impacting the timeline, conduct review of the new rectification enhancements needed to rectify the problem prior to make major change to the solution and to proceed with agreement by SPAD.	Mandatory			
9.14	On Testing Procedure, specifically on User Acceptance Test, able to produce documentation complying to SPAD standard to obtain management approval with supporting document of test script signed by the UAT participants.	Mandatory			
9.15	On Testing Procedure, depending on the changes during the testing phase, able to provide the updated documentation to reflect the final product.	Mandatory			
9.16	On Testing Procedure, able to provide system test (ST) test plans, cases and results prior to UAT.	Mandatory			
9.17	On Testing Procedure, able to provide post production support to monitor closely the defects and provide solution to resolve the defects (Problem Note) or inquiry (Problem Cases) in a timely manner.	Mandatory			
9.18	Supplier must plan and execute security testing according to well-established industry standards such as: a. OWASP Top 10 b. WASC Threat Classification c. SANS/CVE Top 25 d. CWE The tenderer must indicate in the proposal which standard that the solution complies with. **Note:** *Any weakness uncovered by Malaysian Software Testing Board (MSTB) or any other party appointed by SPAD will need to be rectified by the tenderer in a timely manner, where the timeline and rectification plan must be agreed upon with SPAD.*	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
9.19	Supplier must use appropriate test management tools for testing, e.g. the following or equivalent: a. Rational Quality Manager (IBM) b. Rational Team Concert (IBM) c. Quality Centre (HP) d. Testzilla (open source) e. Bugzilla (open source) f. Testopia (open source)	Mandatory			
9.20	The Appointed Vendor must investigate, identify, rectify, improve and overcome all the findings and recommendations made by the IVV to ensure the quality of the TPM system and its operation meets the needs and requirements	Mandatory			
10. Service Levels					
10.1	Hours of operation / downtime window: Hours of operation: 24 hours X 7 days Downtime window: 3 hours, between 2 am - 6 am	Mandatory			
10.2	Availability (% per calendar month): 99.9%	Mandatory			
10.3	Failover interruption (e.g. on loss of web / application / database server): a. RSO: 50% of service performance b. RTO: <= 2 hours c. RPO: close to 0 ***Note**: These metrics are confined to the primary site, DR site and Call Centre*	Mandatory			
10.4	Turnaround time: Duration expected of vendor to revert with root cause, workaround and issue closure plan: Severity-1: 2 hours Severity-2: 12 hours Severity-3: 48 hours Severity-4: 72 hours	Mandatory			
10.5	Resolution time: Duration expected of vendor to resolve issue (including providing hot fixes if relevant): Severity-1: 2 hours Severity-2: 12 hours Severity-3: 48 hours Severity-4: 2 weeks	Mandatory			
10.6	Severity Definition: Severity-1 being most severe, while Severity-4 being less severe a. Severity-1: Production server or other mission critical system(s) are down and no workaround is immediately available. - All or a substantial portion of mission critical data is at a significant risk of loss or corruption. - There is a substantial loss of service. - Business operations have been severely disrupted. Severity-1 support requires you to have dedicated resources available to work on the issue on an ongoing basis during your contractual hours. b. Severity-2: Major functionality is severely impaired. - Operations can continue in a restricted fashion, although long-term productivity might be adversely affected. - A major milestone is at risk. Ongoing and incremental installations are affected. - A temporary workaround is available. c. Severity-3 Partial, non-critical loss of functionality of the software. - Impaired operations of some components, but allows the user to continue using the software. - Initial installation milestones are at minimal risk. d. Severity-4	Mandatory			
11. Disaster Recovery, Business Continuity, Backup & Replication					
11.1	Disaster Recovery: Disaster Recovery (DR) site from SPAD's other office premise – SPAD HQ, Platinum Sentral.	Mandatory			
11.2	Business Continuity: Failover to DR site if a failure occurs shall be automatic with no loss in data during the failover. It should also be seamless to taxi network operators and passengers. The tenderer must successfully conduct at least 1 cycle of failover testing.	Mandatory			
11.3	Backup: Data backup shall be taken off the primary site once a day, and backed up onto SAN storage. However, tenderer can propose a better backup solution.	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
11.4	Replication: Data must be replicated real time (active-active) between the primary site and DR site.	Mandatory			
12. Performance Criteria					
12.1	The system and network must be able to run and support a minimum of these number of users per day: Year 1: 3,900 drivers Year 2: 5,300 drivers Year 3: 7,300 drivers	Mandatory			
12.2	The system and network must be able to run and support a minimum of these peak number of users per hour: Year 1: 2,000 drivers Year 2: 2,700 drivers Year 3: 3,700 drivers	Mandatory			
12.3	The system and network must be able to run and support a minimum of these job orders per day: Year 1: 42,900 jobs/day Year 2: 58,300 jobs/day Year 3: 80,300 jobs/day	Mandatory			
12.4	The system and network must be able to run and support a minimum of these peak job orders per hour: Year 1: 6,000 jobs/hr Year 2: 8,100 jobs/hr Year 3: 11,100 jobs/hr	Mandatory			
12.5	Web service performance: Web services which are exposed to external parties must be able to respond to requests within 10 seconds	Mandatory			
12.6	Performance testing: Performance testing to include load testing, stress testing, endurance testing and spike testing. This is to be done using automated tools such as (but not limited to) LoadRunner, Jmeter, Rational Application Development suite. Tenderer can propose a better tool if possible. Performance testing should provide the following details: a. Concurrency/Throughput b. Server response time c. System upper limit	Highly desirable			
12.7	Able to perform and support concurrent handshaking/session with up to 20 taxi network operators. Handshaking should include encryption e.g. SSL handshake.	Mandatory			
13. Client Support (of Booking Application Portal)					
13.1	Desktop screen resolution: Screen resolution support should be flexible and configurable. It should support screen resolution of 1024 onwards	Mandatory			
13.2	Develop, modify , enhance and integrate with current taxi operator system (if available)				
13.3	Desktop browser support: Safari, Mozilla Firefox, Opera, Chrome, Internet Explorer 7 onwards (i.e. industry standard browsers)	Mandatory			
13.4	Colour depth: Should support colour depth of minimum 24-bit onwards	Mandatory			
13.5	Can support both: a. Operation without JavaScript, cookies, Flash. b. Operation with JavaScript, cookies and Flash is required	Mandatory			
13.6	Connection speed: Supporting speeds from 56kbps. Support must cater for customers on fixed dial-up, ADSL, high-speed broadband, wireless broadband etc.	Mandatory			
13.7	Desktop operating system: Windows XP, Mac OS 9, Linux onwards	Mandatory			
14. Vendor Security					
14.1	***Border Control to protect information related to SPAD.***	Mandatory			
14.1.1	Ensures that the controls measures surrounding the systems are adequate and managed effectively.	Mandatory			
14.1.2	Managed border control devices (Firewalls, Routers, Intrusion Prevention Systems etc.) which are designed to protect the SPAD related infrastructure and data from unauthorized access and abuse are employed effectively to cover all the relevant systems.	Mandatory			
14.1.3	Access to these border control devices should be limited to those with a need and logged to provide traceability of work done.	Mandatory			
14.1.4	The network traffic and access control rules applied to such devices should be reviewed regularly to ensure the services rendered are secure.	Mandatory			
14.1.5	Network and Systems design documents detailing the storage, access, transport, protection of SPAD related data should be kept current to enable audits.	Mandatory			
14.2	***Access to Systems and Applications.***	Mandatory			
14.2.1	Ensures that the applications servicing SPAD are secured and access to these applications are managed effectively to allow only authorized users access to them.	Mandatory			
14.2.2	Public accessibility of the system component should be prohibited from all vectors of access (e.g.: wired and wireless).	Mandatory			
14.2.3	Data repositories containing SPAD confidential data (Database, files, etc) should be placed in a securely protected internal network segment and encrypted using the latest available and secured technology	Mandatory			
14.2.4	Access to such data should be limited to only to authorized users under the control of the Service Provider and authorized to work on the contract.	Mandatory			
14.2.5	The authorized user list for both application and systems must be validated periodically to ensure the list is current.	Mandatory			
14.2.6	Remote access to such data should be strictly controlled and monitored to ensure network connectivity is made over encrypted secure channels and authentication performed to validate the authorized users.	Mandatory			
14.3	***System and Application configuration***	Mandatory			
14.3.1	Ensure the Systems and Applications used to service SPAD are safe, secure and managed to provide optimal service.	Mandatory			
14.3.2	Systems hosting services for SPAD should be configured to perform safely, securely and provide availability to the defined SLAs.	Mandatory			
14.3.3	Place logical and physical separation on systems used for delivering the services of SPAD from others. If a shared hosting model is used, protect the SPAD related services to ensure separation of the data and access.	Mandatory			
14.3.4	Disable unnecessary and insecure services and protocols.	Mandatory			
14.3.5	Configure the systems to prevent misuse.	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
14.3.6	Encrypt all non-console administrative access using industry standards. (e.g.: SSH, VPN, SSL/TLS.)	Mandatory			
14.3.7	Ensure logging and audit trails are enabled to identify access to SPAD related systems and service platforms.	Mandatory			
14.3.8	Enable processes to provide timely forensic investigation in the event of compromise of any hosted system relating to SPAD.	Mandatory			
14.4	***Protect SPAD Confidential Data***.	Mandatory			
14.4.1	Keep SPAD Confidential data secure, develop a data retention and disposal policy, and limit the storage and retention to a limit that is required for business, legal and/or regulatory purpose.	Mandatory			
14.4.3	Do not store authentication data in any readable format even if encrypted.	Mandatory			
14.4.5	Keep Personally Identifiable Information (PII)* protected from casual access at all times.	Mandatory			
14.4.7	Ensure all PII and SPAD confidential data are stored and hosted in Malaysia. Any exception must be approved by SPAD security team	Mandatory			
14.4.9	Must have a solution in place to prevent sensitive data leakage either using known Data Loss Prevention (DLP) solution or other means that provide the same outcome	Mandatory			
14.4.11	Use strong encryption to protect PII related to all SPAD services.	Mandatory			
14.4.13	Manage access to confidential data centrally and reduce the number of repositories that hold such data.	Mandatory			
14.4.15	Do not allow confidential data to be copied to removable media unencrypted by keys available to the service provider.	Mandatory			
14.4.17	Protect the keys used to encrypt SPAD confidential information against disclosure and misuse.	Mandatory			
14.4.19	Document and enforce all key-management processes and procedures and avoid single points of failure in the key management scheme.	Mandatory			
14.4.21	Keep confidential data separate from the access and authentication keys used to access the data. And ensure both are securely protected.	Mandatory			
14.4.23	Use strong cryptography and security protocols when providing access to PII over open public networks.	Mandatory			
14.4.25	Never allow the transmission of access control information (usernames & pass codes) over an unencrypted channel.	Mandatory			
14.5	***Malware protection***.	Mandatory			
14.5.1	SPAD related infrastructure should be protected from malware at all times.	Mandatory			
14.5.2	Ensure all systems related to the SPAD Service delivery are protected by Malware prevention systems and are kept updated and active at all times.	Mandatory			
14.6	***Patch Management and Application Security***.	Mandatory			
14.6.1	Systems become vulnerable as software becomes obsolete or new exploits are discovered. Proper patch management and vulnerability assessment mitigates this risk.	Mandatory			
14.6.2	Ensure all system components have the latest vendor supplied patches	Mandatory			
14.6.3	Ensure usage of SPAD related services are done using software applications which have been secured using industry best practices.	Mandatory			
14.6.4	Testing security patches prior to release.	Mandatory			
14.6.5	Validation of input to prevent or safely recover from malicious content.	Mandatory			
14.6.6	Implementing secure communications.	Mandatory			
14.6.7	Separate development/test and live systems.	Mandatory			
14.6.8	Not using live PII in tests.	Mandatory			
14.6.9	Ensuring no test or preproduction data and scripts exist in live systems environment.	Mandatory			
14.6.10	Proper and documented code review process to remove vulnerabilities prior to release to the live environment.	Mandatory			
14.6.11	Documented change review process and enforce in the overall process	Mandatory			
14.6.12	For all web development initiatives, it should be based on secure coding guidelines (like OWASP) to prevent common coding vulnerabilities.	Mandatory			
14.6.13	For public facing web application, ensure on-going application vulnerability assessment (VA) and the use of web-application firewall.	Mandatory			
14.7	***Restrict access to PII***	Mandatory			
14.7.1	Handling and access to Personally Identifiable Information can result in leakage of confidentiality which affects SPAD and its reputation. Limiting access to this information is the one step in mitigating this risk.	Mandatory			
14.7.2	Practice principle of least privilege - provide privileged access to as few features as necessary to perform their job function.	Mandatory			
14.7.3	Provide privileged access to as few people as necessary to perform their job duties for Service Delivery.	Mandatory			
14.7.4	Collect and monitor and periodically audit use of privileged access.	Mandatory			
14.7.5	Access to sensitive and PII information should be denied to all and selectively allowed based on right to know.	Mandatory			
14.8	***User IDs and traceability of user access***.	Mandatory			
14.8.1	User's access to systems and applications that deal with PII should be kept to a minimum. However, where access is allowed it must be traceable back to an individual to account for the access.	Mandatory			
14.8.2	Users shall be given unique IDs and sharing of IDs or group IDs should be strictly prohibited.	Mandatory			
14.8.3	Use of multifactor authentication apart from pass codes where the information is confidential or where access is gained remotely.	Mandatory			
14.8.4	Render all tokens unreadable between the end points of the system and client devices during the authentication process by using strong cryptography.	Mandatory			
14.8.5	Have proper ID management process to ensure access is granted to valid individuals and pass codes are changed regularly.	Mandatory			
14.8.6	Regularly cleanup IDs of terminated users and disable access of inactive users.	Mandatory			
14.8.7	Restrict access to systems by vendors for the period of activity only and based on documented change management request.	Mandatory			
14.8.8	Ensure that passwords meet the best practices for complexity, size, validity and non predictability.	Mandatory			
14.8.9	Password failures after an acceptable number of times should lock out the account to prevent any further attempts to login.	Mandatory			
14.9	***Track and Monitor all access network resources and PII***.	Mandatory			
14.9.1	Logging mechanisms and the ability to track user activities are critical in preventing, detecting or minimizing the impact of data compromise. The existence of these logs allow the investigation of incidents and identifying improvements to networks.	Mandatory			
14.9.2	Ensure all network access to system components is tied to individual accounts which are not shared.	Mandatory			
14.9.3	Implement automated audit trails for all system components to identify individual access, action taken with elevated privileges, use of identification and authentication tokens, invalid logical access attempts, changes in audit logs, creation and deletion of system-level objects. For applications defined by SPAD as critical systems, logs on user viewing activities must also be captured where applicable.	Mandatory			
14.9.4	Record at least the following information in the audit trail entries: user identification, date and time, type of event, success or failure of attempt, origin of event, identity or name of affected data, system or resource component.	Mandatory			
14.9.5	Synchronize all critical systems clocks and times to approved Network Time Protocol (NTP) servers of at least level 2.	Mandatory			
14.9.6	Secure audit logs so they cannot be altered and use file integrity monitoring tools to detect changes and issue alerts when such changes occur.	Mandatory			
14.9.7	Limit access to audit trail logs to those with a need to know.	Mandatory			
14.9.8	Keep audit logs in a central log server or media that is outside the control or access of administrators whose system components are being logged.	Mandatory			
14.9.9	Keep audit logs of systems components on the external segments secured on internally hosted central log servers.	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
14.9.10	Review logs of all system components at least daily; the following systems should be included in such reviews: security control devices like firewalls, intrusion detection and/or prevention tools.	Mandatory			
14.9.11	Keep audit trail logs for at least 1 year; consider keeping 3 months online and the rest offline if resource is a constraint.	Mandatory			
15. Application security					
15.1	***Input Validation.***	Mandatory			
15.1.1	Ensure input received from the user is valid for the purpose and type requested and remove the possibility of using the input to perform unexpected actions.	Mandatory			
15.1.2	All data are validated for parameters like type, length, format and range	Mandatory			
15.1.3	The application must validate the input received from user at server side	Mandatory			
15.2	***Development Environment***	Mandatory			
15.2.1	All production data used for testing of application must be sanitised	Mandatory			
15.2.2	The software developed must use Version Controlling Application	Mandatory			
15.3	***Authentication.***	Mandatory			
15.3.1	The application user authentication credentials are not stored in plain text	Mandatory			
15.3.2	The authentication input and credentials are transmitted over secured channels (e.g.: SSL)	Mandatory			
15.3.3	Authentication failure message must be checked to ensure no sensitive information is revealed, which could be used to guess the credentials	Mandatory			
15.3.4	Password history is enforced so the last 4 passwords may not be reused	Mandatory			
15.3.5	The application should support change of password	Mandatory			
15.3.6	The application can support password creation of 8 to 255 characters in length	Optional			
15.3.7	The application must enforce complex password i.e. containing lower and upper case characters, numerals (0-9) and special characters (like !@$#)	Mandatory			
15.3.8	The application does not accept password change initiated by non-human account	Mandatory			
15.3.9	The application must validate the user's credentials on each session so that revoked credentials are immediately barred from access to the application	Mandatory			
15.3.10	The web application use POST method for transmission of user input	Mandatory			
15.3.11	The application or database should not store user credentials hardcoded or in plain text within the application.	Mandatory			
15.3.12	The application have an account lockout feature to address cases where the user's credentials are entered wrongly a few times consecutively	Mandatory			
15.3.13	The application must support creation and using User Groups or Role Based Access for privilege management.	Mandatory			
15.3.14	Privilege assignment in the application must be granular enough to support the principle of least privilege.	Mandatory			
15.3.15	The application must be able to authenticate to a central trust architecture like Active Directory (AD). At present, SPAD does not have AD infrastructure. The tenderer should propose AD if needed.	Highly desirable			
15.3.16	The application must prevent the creation of duplicate User ID	Mandatory			
15.3.17	Every module/page hosting sensitive data are being checked for authorization before they are being served by the application	Mandatory			
15.4	***Configuration Management.***				
15.4.1	The application configuration data and files are secured with appropriate file permissions	Mandatory			
15.4.2	Default TCP ports are configured for the application and other associated components	Mandatory			
15.5	***Sensitive Data***	Mandatory			
15.5.1	The error messages generated by the application are checked to ensure no sensitive information is passed back to the user (e.g.: Keys, query statements, other variables and values, debug information etc.)	Mandatory			
15.5.2	All sensitive (PII) data, as specified by the business sponsor, must be encrypted	Mandatory			
15.5.3	Any application functions to transfer PII data to 3rd party must get clearance from Security team in SPAD	Mandatory			
15.4	***Availability Management***	Mandatory			
15.4.1	The application must be designed and provisioned for business continuity / disaster recovery	Mandatory			
15.4.2	The application is designed with High Availability (HA).	Mandatory			
15.5	***Session Management***				
15.5.1	Authentication Cookies transmitted securely during transmit	Mandatory			
15.5.2	The content of authentication cookies are encrypted	Mandatory			
15.5.3	The application support idle session timeout of 30 minutes	Mandatory			
15.5.4	The application enforce re-authentication after idle session timeout	Mandatory			
15.5.5	A non predictive session ID is dynamically generated for the user accessing the application	Mandatory			
15.5.6	The application is prohibiting session based Cache	Mandatory			
15.5.7	The application is design to enforce the use of non persistent cookies	Mandatory			
15.5.8	The application logs must be stored separately from the application binaries so that access is not available thru the application	Mandatory			
15.5.9	The application must generate Audit Account Management logs	Mandatory			
15.6	***Core Requirements for All Applications and Systems.***				
15.6.1	Must store passwords in an encrypted form, using a one-way hash algorithm (e.g.: MD5).	Mandatory			
15.6.2	Must store password files separately from the main application or system data or apply stronger protection to the password file.	Mandatory			
15.6.3	Must not display passwords on the screen when being entered.	Mandatory			
15.6.4	Shall enforce a configurable password expiration (between 30 to 60 days, depending on its criticality.)	Optional			
15.6.5	Shall enforce password change by users prior to expiration.	Mandatory			
15.6.6	Must enable lock-out control on user accounts after a reasonable number of unsuccessful attempts (usually 3).	Mandatory			
15.6.7	Must provide a secure method for users to change their passwords.	Mandatory			
15.6.8	Shall provide audit trail of authentication successes and failures	Mandatory			
15.6.9	Must allow creation and usage of unique individual User ID; users should not be forced to use a common ID.	Mandatory			
15.6.10	Must protect critical file/programs from unauthorized access.	Mandatory			
15.7	***Mandatory for all critical applications & systems.***				
15.7.1	Must support authentication to the central trust architecture (LDAP/AD).	Highly desirable			
15.7.2	Must force users to change assigned first-time passwords on the first login.	Mandatory			
15.7.3	Must be random and comply with rules for complexity, size and content: i.e. >= 7 characters in length, contain mixed case, special characters, and numerals, and should not be a dictionary word or proper name. (See SPAD password guidelines.)	Mandatory			
15.7.4	must not display its system identifiers (e.g.: O/S type, last login date, ... etc.) until the user has logged-in successfully.	Mandatory			
15.7.5	must not have hard-coded passwords anywhere in the application/ system modules, scripts or batch files which can be read as plain text.	Mandatory			
15.7.6	must not transmit user-ids & passwords in plain text over the network between the user and the application server/system.	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
15.7.7	must have logs/audit trails of all system configuration changes or modifications to user accounts, access or profile settings.	Mandatory			
15.7.8	must have sufficient audit-log details to trace all critical activities to the individuals who initiate the change (e.g.: date time, user, machine & IP that connected to it) and even viewing confidential information (e.g. PII or information deemed sensitive to SPAD)	Mandatory			
15.7.9	must enable the display of warning banners restricting access to authorized users only.	Mandatory			
15.8	***Desirable Best Practices***				
15.8.1	Must maintain a history of previously used password hashes to prevent users from re-using the recent passwords.	Mandatory			
15.8.2	Must maintain a history of previously used password hashes to prevent users from re-using the recent passwords.	Mandatory			
15.8.3	Should display the date and time of the last successful login and any unsuccessful login attempts since the last successful login upon completion of a successful login.	Mandatory			
15.8.4	Should time-out and disable access after a period of users' inactivity (e.g. after 10 minutes idle).	Mandatory			
15.8.5	Should enable changes made to user accounts' access & profile settings be effective immediately (refreshed automatically).	Optional			
15.8.6	Should enable time based expiry of account (e.g. for contract/temporary staffs after which the account is automatically disabled.)	Mandatory			
15.8.7	Should automatically terminate user sessions upon improper logout / disconnection.	Mandatory			
15.8.8	Should support configuration of role-based access; i.e. it should allow creation of user accounts with administrator privilege to manage / administer user accounts (rather than having to use a shared single administrator account.)	Mandatory			
15.8.9	All important transaction processing (Application) activities including Viewing activities shall be logged or provide audit trails.	Mandatory			
15.9	***User account management***				
15.9.1	Create user IDs on the system in compliance with the naming convention used in SPAD Corporate Directory even if the system is not yet authenticated to the AD/LDAP source.	Optional			
15.9.2	Ensure Administrative users have both a privileged account and a basic user account; and that the system requires the user to login to the user account before escalation to privileged access.	Optional			
15.9.3	Do not share administrative accounts. If unavoidable, ensure sufficient controls (e.g.: logging) is in place to link the activity on the system to a unique user.	Mandatory			
15.9.4	De-activate the user accounts by resetting their passwords to a random string if they have not been used within a reasonable period. Then perform regular maintenance to remove the deactivated accounts.	Highly desirable			
15.9.5	Check the list of user accounts against the AD/LDAP for users who have left the company and then disable and flag them for removal within a reasonable period of time. (e.g.: remove dormant accounts after 3mths)	Optional			
15.9.6	Monitor logs for intrusion regularly and escalate suspicious activities to the security teams.	Mandatory			
15.9.7	Able to define common and specific roles tied to the authorization access rights for a more structured access matrix definition and ease of maintenance.	Mandatory			
15.9.8	Able to define/grant the lowest level of access rights; display rights, create rights, change rights, delete rights, etc.	Mandatory			
15.9.9	Able to create user ID as per user defined parameters and user access groups e.g. group by VIP/LOA etc.	Mandatory			
15.9.10	Ability to request for new password under all scenarios.	Mandatory			
15.9.11	System must have administrative function to enable administrator to configure / modify roles, access rights and access groups.	Mandatory			
15.9.12	Does the application come standard with System Administration Menu that consists of an easy to define and maintain Authorization Maintenance function?	Mandatory			
15.9.13	Able to clearly design and segregate internal and external type of access to protect and detect wrong assignment of internal access right to external parties.	Mandatory			
15.9.14	Does the application come standard with System Administration Menu that consists of online real-time system monitoring with the ability to perform system health check and diagnosis to analyse and monitor system performance on daily, weekly, monthly and yearly basis?	Mandatory			
15.9.15	Able to design screen accessible to group of Users based on the common role defined but only able to perform transaction or draw information specific to the User-id.	Mandatory			
16. System security					
16.1	***Security Architecture***				
16.1.1	Security infrastructure architecture diagram provided	Mandatory			
16.1.2	Network properly segmented: Public access, network service, and back-end.	Mandatory			
16.1.3	Passengers and drivers-originated traffic separated from O&M traffic	Mandatory			
16.2	***Physical Security of System. (facility management)***				
16.2.1	Single points of failure have risk mitigation plans.	Mandatory			
16.2.2	Physical intrusion into system internals sets off alarms/logs.	Mandatory			
16.2.3	Device is secured in managed network environment with strict physical access controls.	Mandatory			
16.2.4	Network and Physical Segregated from end-user computing equipment.	Mandatory			
16.2.5	System has adequate power/electricity supply	Mandatory			
16.2.6	System has adequate temperature controls in place. (e.g.: air-conditioning)	Mandatory			
16.3	***Network Security (for O&M)***				
16.3.1	Static route or policy based dynamic routing updates.	Mandatory			
16.3.2	Approved Encryption used for sensitive information (e.g. O&M traffic)	Mandatory			
16.3.3	Split-tunnelling disallowed, if VPN is used	Mandatory			
16.4	***Logical Access Security (Console, Remote, Dial-in, LAN) (for O&M)***				
16.4.1	System / application authentication required on all systems & network elements	Mandatory			
16.4.2	TACACS+ / RADIUS / LDAP used.	Mandatory			
16.4.3	User Id. to privilege level matrix provided	Mandatory			
16.4.4	No attached modems. If required for OoB maintenance then modems must require a password to login and call back method implemented.	Mandatory			
16.4.5	Warning banner setup	Mandatory			
16.4.6	Inactivity timeout set and activated.	Mandatory			
16.5	***User Account and Password***				
16.5.1	Supports creation of unique Userids	Mandatory			
16.5.2	Supports privilege escalation	Mandatory			
16.5.3	Supports group privilege (Role based privileges)	Mandatory			
16.5.4	Guest account disabled	Mandatory			
16.5.5	Force change user account password for first time login	Mandatory			
16.5.6	Supports password expiry. (Max age 30-60 days)	Mandatory			
16.5.7	Supports password change min age. (2-5 days)	Mandatory			
16.5.8	Supports password history (keeps >= 6 previous passwords).	Mandatory			
16.5.9	Supports min password length (>=8 characters)	Mandatory			

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
16.5.10	Supports strong passwords (i.e.: passwords must have Alpha, Numeric, Special character and be composed of mixed case).	Mandatory			
16.5.11	Disallows use of passwords from dictionary list	Mandatory			
16.5.12	Password not stored in clear text	Mandatory			
16.5.13	Default passwords disabled/changed	Mandatory			
16.5.14	Password not hard-coded anywhere in the system (e.g. applications, scripts, batch files)	Mandatory			
16.5.15	Password masked when being input	Mandatory			
16.5.16	Remote passwords must not be transmitted in the clear. (e.g.: use SSL, HTTPS)	Mandatory			
16.5.17	Lock and log after min of 3 and max of 5 unsuccessful login attempts.	Mandatory			
16.5.18	Display date & time of previous successful login after successful login	Mandatory			
16.5.19	Display details of unsuccessful login since the last successful login	Mandatory			
16.5.20	Privileged Userid (e.g.: Root) to be handed over to Ops. & Changed.	Mandatory			
16.6	***Security Logging and Auditing (for O&M)***				
16.6.1	Security events log enabled for all type of access (e.g. console, remote, terminal, etc)	Mandatory			
16.6.2	Log time & date available	Mandatory			
16.6.3	Log entries be sent to remote log server. (e.g.: using syslog).	Mandatory			
16.6.4	Time sync performed on SPAD time server (NTP)	Optional			
16.7	***Application Security***				
16.7.1	Applications updated with latest patches at time of release.	Mandatory			
16.7.2	All services not required by the system are turned off.	Mandatory			
16.7.3	All test and pre-production data/scripts/programs removed.	Mandatory			
16.7.4	Backup / BCP arrangements agreed and documented	Mandatory			
16.7.5	Rebuild/Restore/Recover process, media and documentation has been provided in sufficient detail to build system from scratch.	Mandatory			
16.7.6	Programs and Data components within the system are sufficiently protected to enable implementation of Data Classification.	Mandatory			
16.7.7	File System security should protect and ensure that O/S and Configuration files can only be modified by privilege access with logging.	Mandatory			
16.8	***Host Security***				
16.8.1	Network services updated with latest stable patches/fixes.	Mandatory			
16.8.2	System hardening checklist provided and signed-off by vendor (Microsoft based systems also require Microsoft Baseline Security Analyzer audit report with no critical failures).	Mandatory			
16.8.3	Antivirus installed and auto update enabled.	Mandatory			
16.8.4	Host Intrusion Detection System (HIDS) installed and activated and notices sent to a SPAD managed response center.	Mandatory			
16.8.5	Vulnerability Assessment (VA) performed by qualified security personnel* and found clean of any vulnerabilities.	Mandatory			
16.8.6	For non-standard appliance/servers - vendor has provided baseline security document containing firewall rules (ports and protocols) required for service on host/server.	Mandatory			
16.8.7	Firewall configured to permit only required services to and from the host.	Mandatory			
16.9	***Operation & Management Security***				
16.9.1	Out-of-band management path separated from normal data path.	Mandatory			
16.9.2	Secure remote access implemented, if remote access is required (SSH)	Mandatory			
16.9.3	SNMPv2 or higher used	Mandatory			
16.9.4	Default SNMP community strings (public & private) changed.	Mandatory			
16.9.5	Fixed source and destination IP used for SNMP & Syslog traffic	Mandatory			
16.9.6	No insecure network services enabled (e.g. FTP, TFTP, Telnet, 'r' services, RPC, NFS, NetBIOS, X Windows, Naming Services, POP3, SMTP, etc.)	Mandatory			
16.9.7	Unused network interfaces have been disabled (e.g.: Bluetooth, Wi-Fi, eth2...)	Mandatory			
16.10	***Maintenance & Support***				
16.10.1	Maintenance / Support plan includes continuous fixes/patches to be provided and supported by vendor	Mandatory			
16.10.2	Support contact information and escalation process provided.	Mandatory			

C. General Questions		Answer
ID	General	
G1	What are the key factors which cause a taxi Performance management System, Fleet Tracking System and Taxi Booking & Dispatch implementation project to be complex, long running or costly?	
G2	Do you have any accreditation with industry bodies or certifications (e.g. ISO 9000)? Please list out the accreditations and certifications possessed by you.	
G3	Please propose an offer whereby a public-private partnership (PPP) model is used.	
ID	Services and Support	
S1	Please describe the location of the support team after the project	
S2	Please describe the option and costs around levels of support	
S3	Please describe the numbers of support, core platform development and professional services resources available and their geographic location	
S4	Please describe the ongoing relationship that SPAD will have with you once contracts are signed.	
S5	Please describe the extent of warranty provided with the implementation (duration, cost, process for accessing it).	
S6	Please describe the ongoing Application Maintenance services recommended (application operations, maintenance and support).	
S7	After go live what is the process and cost structure for implementing a small change (e.g. 3 days)?	
S8	After go live what is the process and cost structure for implementing larger projects?	
S9	After go live what restrictions do you expect there to be for technical resource to make changes?	
S10	Please describe the service levels you will adhere to for 1st, 2nd and 3rd line support in and outside of business hours (Malaysia time-zone). *Please note, the requirements in this area are listed in the NFR requirements spreadsheet.*	

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
S11	Please detail your account management structure and where the Account Manager will be based.				
ID	**Implementation**				
I1	Please provide a high level project plan, broken down by phase, to illustrate the delivery of the Taxi Control Centre and Centralised Taxi Booking & Dispatch solution. Use 23rd December, 2013 as your project start date. SPAD understands this is indicative only, as is the start date.				
I2	Please describe the project team structure required for the implementation of the Taxi Control Centre and Centralised Taxi Booking & Dispatch platform.				
I3	Please describe the resource requirement you need from SPAD to complete the project				
I4	Please describe the location of the implementation and project team throughout the project.				
I5	Please indicate who will be responsible for implementing your solution. i.e. the software provider or a sub-contractor.				
I6	Please describe and provide documentation of your implementation approach. Include which activities take place in which stage of your implementation plan.				
I7	What are typical timescales for an implementation of this kind? If the typical implementation timeline is different to that being proposed, please explain the differences.				
I8	What is the shortest and longest implementation of your solution?				
I9	Please describe some of the key lessons you have learnt from your previous implementation experiences?				
I10	Are you aware of any unsuccessful attempts to implement your solution? If so, please detail.				
I11	What risks do you envisage for this project and how would you mitigate these risks?				
ID	**Product Details**				
PD1	Please itemise the software packages, versions and modules that you are proposing for the Taxi Control Centre, Centralised Booking & Dispatch and In-Taxi Vehicle Equipment solution				
PD2	Please itemise any 3rd Party software packages and/or modules that are required as part of the solution you are proposing.				
PD3	Please provide product roadmaps for all products / modules recommended as part of your solution.				
PD4	Please detail the upgrade cycle of your solution.				
PD5	Are future purchases of software licenses at the same price?				
PD6	Please advise how many clients are currently live on the proposed version of the software. Please include a list of clients current on this version and an indication of their booking transaction volumes.				
PD7	Please advise how many new implementations of your solution have been completed and now live in 2012.				
PD8	Please provide as an attachment(s) any documentation, marketing or otherwise, that you believe describes the Vision, Capabilities, Market Positioning and solution fit as in relation to this Invitation to Tender.				
PD9	How long are product versions supported for?				
PD10	How long is a specific installed version supported for and are there options to provide support after end of life (extended support)				
PD11	Please provide examples of product documentation, including developer and business user documents				
ID	**Technical**				
T1	Please outline any independent security certification that you solution have acquired				
T2	Please describe your experience of integrating with Oracle Fusion Middleware (Oracle Service Bus), IBM WebSphere Enterprise Service Bus or other similar platforms as a middleware layer. Please also clearly indicate the middleware layer.				
ID	**Hosting and Structure**				
H1	Please describe the systems software that is required (OS, web server, app server, DBMS, etc) to support the Taxi Control Centre, Centralised Taxi Booking & Dispatch Network and In-Taxi Vehicle Equipment solution				
H2	Please describe the ideal hosting configuration of the solution, include a high level network diagram in order to meet a 99.5% uptime				
H3	Please illustrate how you create, amend and delete application server instances				
ID	**Application**				
A1	Please describe the application layers contained within the solution				
A2	Please describe how the application is architected, highlighting, where available the following key points: a. Structure/grouping of functionality, levels of configuration available, b. Standards and frameworks employed, c. Caching, d. Provision of APIs, for other devices or services, to access platform functionality, e.g. iPhone application. e. Ability to integrate to datasources, data abstraction and data management, Security; single sign on support, active directory, Certification management				
A3	Please outline how the data model of the solution can be altered and detail areas that can be extended and can't be extended				
A4	Please indicate the out-of-the-box integration points for the following data objects: a. Taxi location and GPS coordinates b. Estimated distance c. Estimated fare d. Driver name, age, language and other relevant information e. Passenger name and other relevant information f. Expected arrival time g. Job details (e.g. customer contact, pickup, dropoff locations) h. Ignition Status i. Login status j. Taxi Registration No and other details such as make, model, color.				
A5	Please outline the nature of any import / export framework / tools included in the solution				
A6	Please outline any staging / production features within that platform and the process for promoting content and data from staging to production. Please include details of rollback processes (if any)				
A7	Please describe the upgrade process for the solution, including tools available and high level steps required				

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments
A8	How long does a typical major version upgrade take?				
A9	What additional functionality is in the platform that isn't included in the functional requirements spreadsheet				
A10	Please describe how the business tools can be extended to meet new functional requirements				
A11	What level of configuration can be carried out within the business tools without requiring development, e.g. changing workflow, altering form fields, creating new data objects				
A12	Would you recommend customising the business tools to meet the requirements?				
A13	What is the process for training a developer on the required solution and how long would this typically take				
A14	Are the customer services tool(s) configurable / customisable? If so how				
A15	What are the key technical differentiators of the platform?				
A16	What Quality Assurance processes are used during development of the software?				
A17	Is there a scaling model that can be applied? Please provide benchmark statistics per CPU or unit license, including page throughput / pages per second				
A18	Describe how the application can support multiple test, staging and production environments. Please list any key function points and processes to supporting this approach				
A19	Describe how a code release can be rolled back				
A20	Describe the features available within the platform to support the deployment of code/updates across the environments, in particular deployment to the production environment?				
A21	Which testing approaches/tools are supported?				

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments

ID	Technical Requirement	Requirement Priority	Statement of Compliance	Development Mandays	Supplier Comments