



---

# Business Requirements

## KZN Department of Transport Multi-functional Personal Operating Devices

Document No: <Doc number>

Revision: A0 (Draft)

Author: I Abdulla

Effective Date:

Electronic File:



s t a t e · i n f o r m a t i o n · t e c h n o l o g y · a g e n c y

<CLASSIFICATION>

## Notice

© 2016 SITA. All rights reserved.  
No part of this document may be reproduced or transmitted in any form or by any means  
without the express written permission of SITA.

Document enquiries can be directed to: [Click and type **Configuration Department / Division**]  
SITA (SOC) Ltd. P.O Box 26100, MONUMENT PARK, 0105, SOUTH AFRICA

Attention: [Click and type **Contact person**] - [Click and type **e-mail address**] @sita.co.za  
Telephone: [Click and type **Telephone number**]

## Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

_____	_____
<SITA>: <Description>	Date
_____	_____
<Client>: <Description>	Date

## Foreword

<Contextual clause>  
<Applicability clause>  
<Acknowledgement clause>  
<Outline clause>  
<Conventions used>

## References

1. <Document Description> Rev <revision> - Author/Source [<Doc number> - <date>]

## Amendment history

Revision	Date	Change request	Change comment
0.1		New document	Draft
0.2		Updates	Review after client review held on 21/09/2016

## Peer Review

VERSION	AUTHOR/S		REVIEWER		FINAL CHECK	
	DESCRIPTION	DATE	DESCRIPTION	DATE	DESCRIPTION	DATE
0.1						
1.0						

## Drafting tools

Document body text: Microsoft Word

## CONTENTS

---

Notice .....	2
Approval .....	2
Foreword .....	2
References .....	2
Amendment history .....	2
Peer Review .....	2
Drafting tools .....	2
<b>1. Introduction .....</b>	<b>5</b>
<b>2. Scope .....</b>	<b>7</b>
2.1 High Level Scope .....	7
<b>3. Primary Business Requirements .....</b>	<b>8</b>
3.1 Interfaces .....	8
3.2 App's .....	8
3.3 Device .....	9
3.3.1 Device Authorisation .....	9
3.3.2 Scan Details .....	9
3.3.3 Interface Implementation Capability .....	9
3.3.4 App Execution Capability .....	10
3.3.5 Provide Print Capability .....	10
3.4 Device Management .....	11
3.4.1 Manage Device .....	11
3.4.2 Manage Configuration Data .....	11
3.5 Device Security and Reports .....	12
3.5.1 Security .....	12
3.5.2 Audit .....	12
3.5.3 User Account Management .....	12
3.5.4 Provide POD Reports .....	13
<b>4. Enhanced Personal Officer Device (POD) solution .....</b>	<b>13</b>
<b>5. Non-functional requirements .....</b>	<b>14</b>
5.1.1 "Rugged" device .....	14
5.1.2 Device size specifications .....	14
5.1.3 Location and number of users .....	14
5.1.4 Offline capability .....	14
5.1.5 Timescales .....	14
5.1.6 Training, change management and skills transfer .....	15
5.1.7 Other contributing cost elements .....	15
<b>6. Technical requirements .....</b>	<b>17</b>
6.1.1 Hardware .....	17
6.1.2 Server Operating System .....	17
6.1.3 Desktops/laptop/device Operating System .....	17
6.1.4 Database .....	17
6.1.5 Application .....	17
6.1.6 Network .....	17
6.1.7 Support and Maintenance .....	17
<b>Annex A : Abbreviations and Definitions .....</b>	<b>19</b>
A.1 Abbreviations .....	19
<b>Annex B : Service Level Metrics .....</b>	<b>20</b>

## FIGURES

---

Figure 1 – Overview of RTI POD's .....	6
--	---

## TABLES

---

No table of figures entries found.

## 1. Introduction

The KwaZulu-Natal Department of Transport (KZN DoT) is seeking to modernise its traffic law enforcement and road safety operations in the province. Central to this modernisation is the use of technology to provide better support to officers in the field, and to provide better information to management in support of decision making.

This specification forms part of an RFB issued for the Traffic Contravention Management System (TCMS) for KZN DoT. It defines the requirements for the provision of multi-functional personal operating devices (POD's) that will be used by KZN DoT traffic officers in the field.

Figure 1 summarises the overall scope, and the rest of the document then details each of the requirements contained in Figure 1.

**KZN DoT reserves the right to not to award this particular requirement as part of the RFB or award this part of the RFB to a different bidder.**

## <CLASSIFICATION>

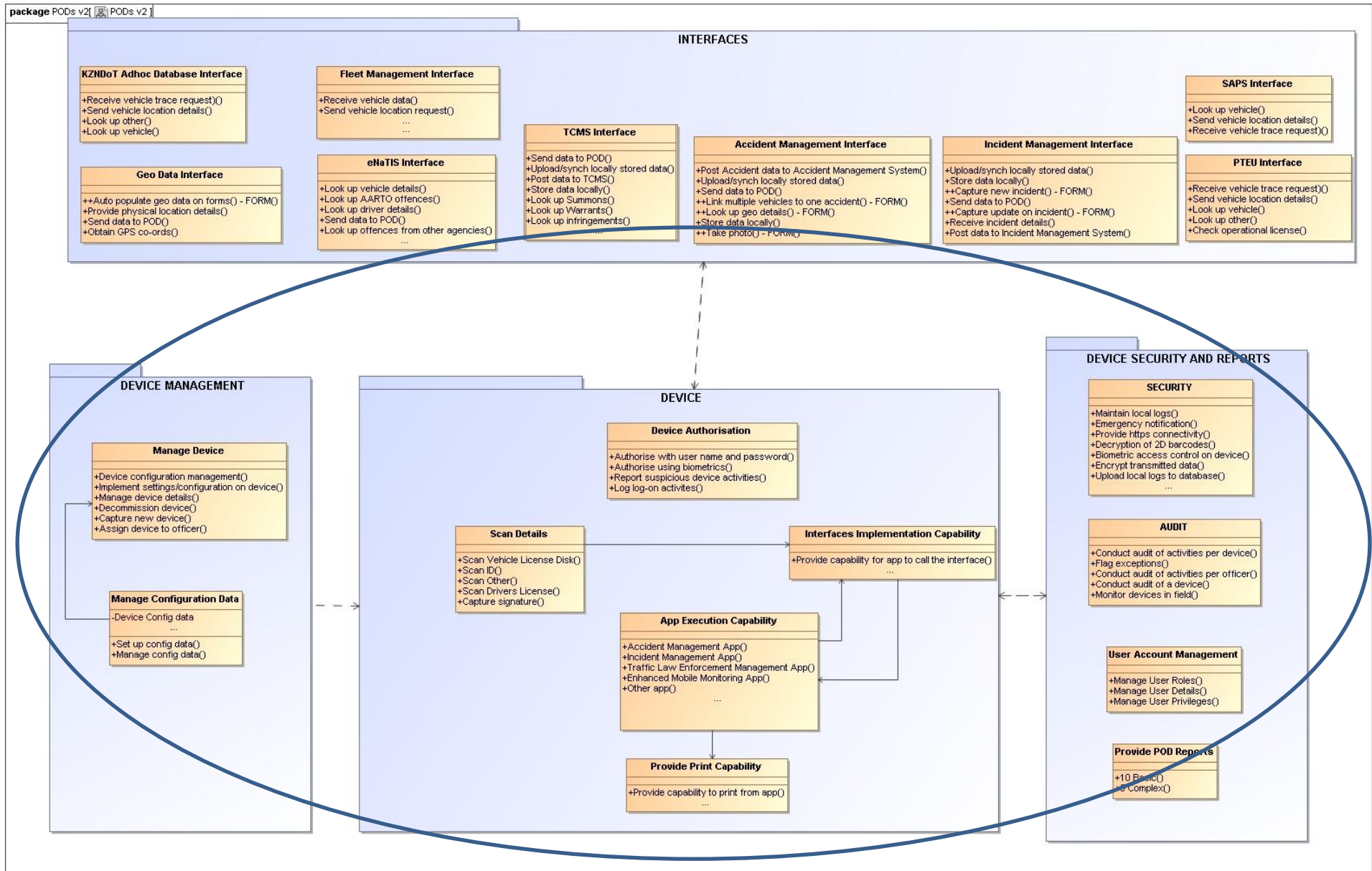


Figure 1 – Overview of RTI POD's

## 2. Scope

### 2.1 High Level Scope

The service provider is required to provide Personal Operating Devices (POD's) for the KZN Department of Transport's RTI unit. The devices may take any form including but not limited to: smartphone, Personal Digital Assistant (PDA), tablet, netbook etc. so long as the device is capable of meeting all the requirements stipulated in this specification.

At a high level the scope includes:

- a) Provision of required devices with scan, print, app execution and interface implementation capability;
- b) Development and implementation of management console for the devices (Device Management, Device Security and Reports);
- c) Project management;
- d) User training, change management and skills transfer required to capacitate end users and optimize value from the POD's; and
- e) The total contract duration is 5 (five) years as follows:
  - i. Develop and implement solution in a period not exceeding 12 months;
  - ii. Providing support and maintenance for the remaining term of the contract after go-live of the solution;

### **3. Primary Business Requirements**

#### **3.1 Interfaces**

The interfaces mentioned below will be packaged into a re-usable set of Service-Oriented Architecture (SOA) interfaces that exposed for utilisation by any application within KZN DoT.

The devices are therefore required have the capability to implement these interfaces to meet the business requirements. Interfaces will be called from the relevant app's.

- a) Geo Data Interface
- b) eNaTIS Interface
- c) TCMS Interface
- d) Accident Management Interface
- e) Incident Management Interface
- f) SAPS Interface
- g) PTEU Interface
- h) Ad-hoc Query Database Interface

#### **3.2 App's**

The device must be capable of executing app's. The following app's are the minimum set that will be developed and implemented by KZN DoT:

- a) Traffic Law Enforcement App
- b) Accident Management App
- c) Incident Management App
- d) Enhanced Mobile Monitoring App

Devices must have capability to run other app's developed and deployed at a later stage.



### 3.3 Device

#### 3.3.1 Device Authorisation

Description	Functional Requirement
<ul style="list-style-type: none"> <li>Authorise using biometrics</li> </ul>	<p>Allow a user to authenticate to the POD using fingerprints.</p> <p>Once authenticated the user should be able to select the shift that s/he is working (from a list of pre-defined shifts) make himself/herself available for the duration of the shift. The availability notification is interfaced back to the Traffic Management Center (Incident Management System) so that the officer is available for dispatching to incidents that may occur during that shift within their vicinity (geo-location).</p>
<ul style="list-style-type: none"> <li>Authorise with user name and password</li> </ul>	<p>Also allow username and password authentication, which the department may decide to implement required.</p> <p>Once authenticated the user should be able to select the shift that s/he is working (from a list of pre-defined shifts) make himself/herself available for the duration of the shift. The availability notification is interfaced back to the Traffic Management Center (Incident Management System) so that the officer is available for dispatching to incidents that may occur during that shift within their vicinity (geo-location).</p>
<ul style="list-style-type: none"> <li>Log log-on activities</li> </ul>	<p>All activities undertaken by the user must be logged on the device. Log data will periodically be uploaded to the database server and local storage cleared.</p>
<ul style="list-style-type: none"> <li>Report suspicious device activities</li> </ul>	<p>Multiple unsuccessful attempts at log-on, a number of successive posts via the interfaces or a device dormant with no activity for a pre-defined period must be</p>


#### 3.3.2 Scan Details

Description	Functional Requirement
<ul style="list-style-type: none"> <li>Scan ID</li> </ul>	<p>The POD must be able to scan a user's South African ID barcode. Decryption of barcode must be applied for interfacing with eNatis.</p>
<ul style="list-style-type: none"> <li>Scan Drivers License</li> </ul>	<p>The POD must be able to scan a user's South African driver's license barcode. Decryption of barcode must be applied for interfacing with eNatis.</p>
<ul style="list-style-type: none"> <li>Scan Vehicle License Disk</li> </ul>	<p>The POD must be able to scan a vehicle's South African license disk barcode. Decryption of barcode must be applied for interfacing with eNatis.</p>
<ul style="list-style-type: none"> <li>Scan Other</li> </ul>	<p>POD must allow the user to scan and save other documents as required. This would include taking photographs where applicable.</p>
<ul style="list-style-type: none"> <li>Capture signature</li> </ul>	<p>Parties must be able to sign on the POD as required by the calling app e.g. offender accepting a S56 notice.</p>


#### 3.3.3 Interface Implementation Capability

Description	Functional Requirement
<ul style="list-style-type: none"> <li>Provide capability for app to call the interface</li> </ul>	<p>Relevant interfaces as per section 3.1. will be called from the app's . The device must provide the capability to call such interfaces.</p>

### 3.3.4 App Execution Capability

Description	Functional Requirement
 App Execution Capability	The device must be capable of executing app's. See section 3.2 and note that this is only a minimum set of app's. Additional app's will be included at a later stage.







### 3.3.5 Provide Print Capability

Description	Functional Requirement
 Provide capability to print from app	App's must be able print relevant documents from the POD.
Note	<p>The POD may be capable of printing itself, or the POD may be capable of communicating wirelessly to a printer/print device in the vehicle for printing purposes. All costs associated with the printing solution over and above the standard POD costs are to be included in the cost of the POD as part of the service provider's response.</p> <p>It may be assumed that one printer per vehicle will be adequate, currently there are 465 vehicles in the DOT fleet. If printers are attached to the vehicle then the printer should be capable of charging in the vehicle.</p> <p>Printer should possess a minimum battery life of 3 hours whether attached to the vehicle or whether printing directly from the device.</p>




### 3.4 Device Management

The functions detailed in this section are applicable to a central “management console” for the POD devices.

#### 3.4.1 Manage Device

Description	Functional Requirement
 Capture new device	Capture details of all new POD's including the region and station that the POD is allocated to.
 Manage device details	Maintain details of all existing POD's such as corrections to colour, details around servicing done on the POD etc.
 Decommission device	Record details of POD's that have been decommissioned and are no longer in use
 Assign device to officer	<p>Link a POD to an officer for a particular shift (check-out) and check-in the POD when the officer returns the POD at end of shift. The condition of the device should be recorded at check-in and at check-out. The officer should only be able to authenticate to a POD that has been checked out to him/her.</p> <p>At any one time one officer will be assigned to one device (i.e. one officer cannot be assigned to multiple devices concurrently). However one device may have more than officer assigned to it for a shift with only one officer able to log in at a time (enabling sharing of devices where required).</p>
 Implement settings/configuration device	Where there are software updates or new settings/configurations, these should be rolled out centrally from the “management console”. Details must be retained of which devices were updated successfully and which were not. See below – configuration management.
 Device configuration management	<p>A standard baseline configuration should be maintained with version control of the baseline which would apply to all POD's.</p> <p>There must also be a record linked to each POD for it's configuration details and version control thereof i.e. record all changes to a POD's software are hardware over time.</p>

#### 3.4.2 Manage Configuration Data

Description	Type
 Device Config data	See 3.3.1. Manage Configuration. The data related to the baseline configuration of the POD's (images) are to be maintained as look-up tables which can evolve over time with version control applied. i.e. no hard coding on the device as far as possible. This will enable easier device management through the central management console, and the console then makes use of central configuration data.
 Set up Config data	Functionality to capture and record the initial configuration data described above
 Manage Config data	Functionality to make updates over time to the existing configuration data described above

### 3.5 Device Security and Reports

#### 3.5.1 Security

Description	Functional Requirement
● Biometric access control on device	User must be able to use fingerprints and authenticate on a device
● Decryption of 2D barcodes	Certain barcodes are 2D encrypted and the device must be capable of decrypting same
● Provide https connectivity	The connection between the device and the system interface will be secured
● Encrypt transmitted data	Data exchanged between the device and the system interface will be encrypted
● Maintain local logs	<p>Logs will need to be retained locally until the device is able to connect to a network and upload the logs onto a database. At that point local logs can be deleted.</p> <p>Included as part of the device logs will be a full history of GPS co-ordinates of the device as it moves, to enable reporting on activities undertaken on a particular day with the device.</p>
● Upload local logs to database	Enable uploading of local logs to a database. This is necessary to allow for auditing, however there is an appreciation that the storage on the device will be limited.
● Emergency notification	The device must be capable of sending an emergency/"officer down" signal to the Traffic Management Centre together with the geo-location details.

#### 3.5.2 Audit

Description	Functional Requirement
● Conduct audit of device	Audit the changes to configuration, settings etc. that have been applied on a device.
● Conduct audit of activities per device	The user must be able to conduct a full audit of activities undertaken by on a particular device (which may have been used by different users), over a specified timeframe. This audit must also provide the geo-location data.
● Conduct audit of activities per officer	The user must be able to conduct a full audit of activities undertaken by a particular officer (which may be across multiple devices and utilising different app's per device), over a specified timeframe. This audit must also provide the geo-location data.
● Monitor devices in field	Provide ability to monitor which devices are currently out in the field, by which officer they are being used and where they are used, and which devices are not in use and in the office. This audit must also provide the geo-location data.
● Flag exceptions	Exceptions must be identified and flagged for an administrator or super user to investigate. Some exceptions will be flagged periodically whilst others are to be flagged real time e.g. multiple sequential log in attempts.

#### 3.5.3 User Account Management

Description	Functional Requirement
● Manage User Details	Register and manage a user's details and credentials.
● Manage User Roles	Define the user access roles that a particular user will be assigned to and manage updates required thereafter.
● Manage User Privileges	Within a particular user access role, define the privileges that a particular user will be assigned to (e.g. read, update, create, delete) and

**<CLASSIFICATION>**

Description	Functional Requirement
	manage updates required thereafter.

#### 3.5.4 Provide POD Reports

Description	Functional Requirement
10 Basic	Provision to be made in scope for 10 basic reports.
5 Complex	Provision to be made in scope for 5 complex reports

## 4. Enhanced Personal Officer Device (POD) solution

KZN DOT currently utilises ±800 Zebra TC77 handheld devices, each paired with a Zebra ZQ500 mobile printer. These devices are primarily used to generate handwritten S56 notices. The proposed solution must enhance the functionality of these devices to support revenue enhancement and operational efficiency as follows:

Description	Functional Requirement
Support Revenue Enhancement and Operational Efficiency	<ul style="list-style-type: none"><li>Ability to query vehicle registration and driver licenses to identify outstanding fines, active summonses and warrants of arrest. It is therefore vital that the solution integrates with the back-office contravention system in real time.</li><li>The solution should also be integrated with NaTIS in real time to identify stolen vehicles, vehicles with suspected cloned numberplates and expired licenses.</li><li>Ability to print statements of outstanding fines, summonses and warrants of arrest using the printer linked to the PODs</li><li>The POD solution must support the generation and printing of QR codes on all notices and statements issued (e.g., S56 and S341). These QR codes should link directly to the official fine payment platform, enabling offenders to make instant and convenient payments using their mobile devices. In addition to facilitating immediate payment, this also serves as an awareness mechanism, making offenders aware of outstanding fines and encouraging prompt resolution.</li></ul>

## **5. Non-functional requirements**

### **5.1.1 “Rugged” device**

Devices must be “rugged” and suitable for day-to-day use in the field. The device must have an Ingress Protection (IP) rating of IP68.

If the device itself does not possess the IP68 rating, then appropriate protection mechanisms must be provided for to ensure that the device is compliant and factored into the overall price of the device. The service provider will need to provide independent verification of the device’s IP68 rating if not provided as standard.

### **5.1.2 Device size specifications**

- a) Maximum allowed device dimensions: 200 x 150 x 30mm (L x W x D)
- b) Main Product Weight: 360g
- c) Continuous Usage Time: Minimum 6 hours
- d) Battery Standby: Minimum 120 hours
- e) Charging Time: Minimum 3 hours and should be possible to charge from the vehicle

If additional protection mechanisms are included to provide IP68 rating protection, then such needs to be included when considering the device dimension and weight.

### **5.1.3 Location and number of users**

The devices will be used by RTI officers across KZN at all RTI stations. A pool of devices is to be allocated to a station and checked in and out to officers as the shift starts and ends.

There are currently 786 RTI officers on average and hence a total of 786 devices are to be catered for as part of the scope with total number of devices phased in over a two year period.

There are currently 465 RTI vehicles on average and hence a total of 465 printing devices are to be catered for as part of the scope should the printer be a separate device to the actual POD, with total number of devices phased in over a two year period.

### **5.1.4 Offline capability**

The device must be capable of operating offline in a limited mode. All data will be synchronised onto the main server of the application when connectivity is re-established. For example this will include ability to:

- 1. Capture Accident details on the device;
- 2. Capture Incident details on the device;
- 3. Issue new notices on the device;
- 4. Upload local logs stored on device;

For purposes of conducting offline operations, the user must be able to download a limited database of vehicle, driver and infringement information from TCMS onto a laptop. The ANPR and handheld device will then be configured to communicate to the laptop to retrieve data and make queries, instead of querying the server directly. This will allow operations to be conducted in areas where there is limited network coverage.

### **5.1.5 Timescales**

The implementation of the solution should be in place within a period not exceeding 12 months.

### 5.1.6 Training, change management and skills transfer

Device training, change management and skills transfer will be combined and delivered together with the app training, change management and skills transfer i.e. devices will be a specific module in the overall programme.

Training	Change Management	Skills Transfer
Basic Training RTI officers: 786	On start-up: 1 interventions	RTI super user: 10
Advanced Training RTI officers: 100	During project: 1 intervention per project phase	IT super user: 3
Administrator Training: 20	Pre go-live: 1 interventions	
RTI Management Training: 20	Post go-live: 2 interventions	

### 5.1.7 Other contributing cost elements

The following additional cost elements have been identified which will need to be factored into the overall bid price. Bidders are to use the following as a standard for consistency in costing and equitable price comparison.

Cost Element	Parameters for costing	Comments
Device costs	<p>The service provider must propose the optimal costing approach for the devices whether this be outright purchase, lease option or other. The department does not have a preference for the approach however seeks the most cost-effective solution.</p> <p>Costs of devices are to be contained to a maximum of R650 per device per month vat excl. over the 60 month contract duration. This cost includes the provision of devices, refresh cycle of all devices, provision of printers if applicable, development and implementation to meet the business needs, training and change management, support and maintenance over the contract duration.</p>	
Cellular data costs	N/A	To be provided by the department. Service provider will need to provide an estimated average data requirement per month per device.
Certificates for https (secure connection)	Each device to establish secure connection and only communicate securely with the interfaces. Costs associated with implementing this requirement are to be factored into overall bid price	Service provider may choose the appropriate approach to deliver on this requirement in the most cost-effective manner.
Device support/maintenance	See requirements below in 5.1.7 with regards to support and maintenance costs for devices,	To make provision for a full device replacement once during the contract period.

<CLASSIFICATION>

Cost Element	Parameters for costing	Comments
	included the need for a replacement device where needed. Costs associated with implementing this requirement are to be factored into overall bid price	



## 6. Technical requirements

### 6.1.1 Hardware

All hardware will be provided by KZN DoT.

### 6.1.2 Server Operating System

The system should be capable of running on Windows Server 2012 R2 Standard. Operating system licenses will be provided by KZN DoT.

### 6.1.3 Desktops/laptop/device Operating System

There is no preference for operating system of the devices; however operating system costs for devices are to be included in the cost of device.

### 6.1.4 Database

The system should run on Oracle or MS-SQL. Database licenses will be provided by KZN DoT.

### 6.1.5 Application

There is no particular requirement on the platform the application is developed in as long as it supports the business requirements.

### 6.1.6 Network

The handheld and laptop devices must be able to work over an appropriate cellular network in order to call the necessary interfaces.

As per section 4.1.3 there is a need to be able to continue functioning in cases where there is no network connectivity.

### 6.1.7 Support and Maintenance

Support and maintenance are to be included for a after go-live, limited to 5 year total contract duration. This includes support on the application, interfaces, technical platform and the devices as per below:

Support and Maintenance Consideration	Support and Maintenance Requirements
Type of support and maintenance requirements post go-live	A full end-to-end Service Level Agreement (SLA) will be required.
Devices (including separate printer if applicable)	The service provider is required to support all the devices (including separate printer if applicable) as part of the SLA, as well as conduct routine maintenance and health checks on devices.  Defects on devices/printers are to be resolved within 4 hours, where this timeframe cannot be achieved and replacement device/printer must be provided whilst the device/printers is repaired.
Device Refresh (including separate printer if applicable)	Refresh of all devices(including separate printer if applicable) to be done once during the contract timeframe i.e. new devices (including separate printer if applicable) issued initially, and all devices (including separate printer if applicable) are to then be refreshed once.
Exclusions	The support and maintenance SLA does not cover hardware and networking as this will be addressed in a separate SLA.
Geographical requirements of support personnel	Although KZN DoT will accept resourcing from outside the province, the service provider must have KZN-based

**<CLASSIFICATION>**

<b>Support and Maintenance Consideration</b>	<b>Support and Maintenance Requirements</b>
	resources who will participate in the project and who will be available to provide support services post-go live. i.e. under no circumstances can there be an exclusive reliance on resource from outside the province.
Offsite support requirements	First line may be provided telephonically and through e-mail. Remote support must be catered for.  Service provider to provide a facility to log user requests, incidents, faults etc.; report on turnaround times against the SLA.
Site visits	Provision must be made for 2 site visits per month.
User groups	Formal user groups are to be constituted and convened quarterly.
Adhoc support and maintenance on T&M basis	Provision to be made for 40 hours of adhoc support and maintenance per annum, to be used as per plan agreed with the department and billed only on actual time utilised.
Adhoc training post go-live	Provision to be made for 1 training session per quarter post go-live i.e. 4 per annum.
SLA metrics	See Annex B.

## Annex A : Abbreviations and Definitions

---

### A.1 Abbreviations

ANPR	Automated Number Plate Recognition
DoT	Department of Transport
KZN	KwaZulu-Natal
POD	Personal Operating Device
RTI	Road Traffic Inspectorate
SITA	State Information Technology Agency

## **Annex B :   Service Level Metrics**

---

The following table lists the service elements and service levels applicable to this requirement:

<CLASSIFICATION>

Service Elements and deliverables	Response time	Measurement criteria / Target	Service Category / Priority	Required resource/s
<p>Provide Incident Management services – records an event that has an impact on delivery of the service and is used to track the incident from the logging of the call through to resolution.</p> <p>Provide Problem Management services – identification, investigation, diagnostics and classification of problems as a proactive attempt to prevent future occurrences of these types of incidents.</p> <p>Change Management – assessment of the impact, obtaining of approval for the change, and monitoring the change from change request to completion.</p> <p>Service Level Management – the design and monitoring of agreed service delivery targets and resources used and reporting thereof</p> <p>Reporting on incidents, problems and SLA management</p> <p>Provide day-to-day user support</p> <p>Application maintenance</p> <p>Installation and operational support procedures will be provided as part of the information required for the DRP documentation. DR testing to be conducted and support services to be provided for recovery and resumption during an actual disaster.</p>	Technical response within one hour, together with confirmation that the fault has been assigned to an appropriate expert and the likely timescale for fixing the fault where this timescale shall not exceed 8 hours.	A total loss of use of the installed software products; and the software product installation is mission critical.	Severity 1	Technical and Applications support personnel
	Technical response within two hours, together with confirmation that the fault has been assigned to an appropriate expert and the likely timescale for fixing the fault where this timescale shall not exceed 24 hours	Some operations can continue in a highly restricted fashion but there is some severe and critical loss of use and the affected software product(s) is/are mission critical.	Severity 2	Technical and Applications support personnel
	Technical response within two days. Fault resolution times are four weeks	The software product(s) can be used with some restrictions but some do not function correctly and there are no alternative features available to achieve equivalent functionality.	Severity 3	Technical and Applications support personnel
	Technical response within five days. Severity 4 faults are resolved by the next maintenance or enhancement release.	The software product(s) can be used with some inconvenience because some features do not function correctly. Users can work around the problem or may use alternative features in the standard software product(s) to achieve equivalent functionality.	Severity 4	Technical and Applications support personnel
	Technical response within five days. Severity 5 faults are resolved by the next major release.	The standard software product(s) contains a minor or cosmetic error, which does not materially impede use.	Severity 5	Technical and Applications support personnel

<CLASSIFICATION>