KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

Terms of Reference (TOR) for the Supply, Design, Implementation, Commissioning, Maintenance and Support for Smart Gates and Transit Surveillance Solution

1. Executive Summary

The proposed tender seeks to procure, design, implement, commission, maintain and support a comprehensive Smart Gates and Transit Surveillance Solution aimed at modernizing Kenya's transit and border management operations. The deployment of 66 advanced smart gates, 123 AI-driven surveillance cameras, and two fully integrated command and control centers will result in enhanced security, streamlined cargo and passenger flow, reduced congestion, improved revenue assurance, and strengthened compliance across airports, seaports, OSBPs, highways, and other approved transit routes. Leveraging technologies such as biometrics, Radio Frequency Identification(RFID), Automatic Number Plate Recognition(ANPR), Automatic Container Number Recognition(ACNR), real-time video analytics and centralized monitoring, the solution will address existing operational challenges while ensuring seamless integration with current and future Customs systems. The selected vendor will be responsible for supply, installation, customization, training & Knowledge transfer and long-term support over a 18-month implementation period and a 1-year warranty period, ensuring sustainable, secure and efficient transit operations nationwide.

2. Background

The current rapid advancement of technology in recent years has necessitated significant improvements in the way transit systems operate. To meet the growing demands for enhanced security, efficiency, and passenger convenience, the implementation of Smart Gates and Transit Surveillance Solutions has become increasingly critical especially in East Africa and beyond.

Smart Gates, integrated with cutting-edge surveillance technologies like the Electronic Cargo Tracking System offer a robust solution to streamline cargo flow, reduce waiting times, and enhance the overall safety and security of transit systems. These intelligent systems should utilize advanced technologies such as facial recognition, Radio Frequency Identification

(RFID), Optical Character Recognition (OCR) for Automatic Container Number Recognition (ANCR) and Automatic Number Plate Recognition (ANPR), and automated ticketing to facilitate seamless cargo/passenger movement through transit points. Additionally, sophisticated surveillance systems equipped with high-definition Closed Circuit Television (CCTV), real-time monitoring, and analytics capabilities provide comprehensive security coverage, ensuring the safety of passengers and staff.

The primary purpose of this document is to develop and deploy a state-of-the-art Smart Gates and Transit Surveillance Solution. This solution aims to revolutionize the way transit authorities (Customs) manage cargo/passenger flow and security, providing a more efficient and secure travel experience for all users and concerned parties.

The selected bidder must deploy a cutting-edge technology solution that seamlessly integrates with both current and future infrastructures. This solution should effectively address existing challenges, including border point congestion and security threats.

3. Objectives

- **Enhanced Security**: Advanced security measures such as biometric authentication, RFID key cards, transit surveillance systems and remote access control help prevent criminal activities.
- **Efficiency in Border Management**: Facilitate the efficient management of queues, especially for high-traffic borders.
- **Improved Customer Service**: Streamline the entry process to reduce wait times and improve the overall customer experience.
- **Remote Monitoring and Control**: Enable remote monitoring and control of border operations, enhancing convenience and security.
- **Integration with Surveillance Systems**: Integrate with video surveillance and motion sensors to provide real-time monitoring and alerts for suspicious activities.
- **Enhanced Revenue Collection** – Improved efficiency, accuracy, and compliance will lead to enhanced revenues.
- **Reduced Operating Costs** – Process optimization, automation, resource efficiency will lead to lower operating costs.

4. Scope of work

The scope of the project will comprise the following:

- Supply, Delivery, Installation and Commissioning of Smart Gates and Transit Surveillance solution, 123 Surveillance cameras (intelligent AI driven) and 66 Smart

Gates and it weighing components to all transit POEs in Kenya, including but not limited to

  - Major transit points (e.g., railway stations, air ports, sea ports and borders).
  - Secondary transit points (e.g., smaller stations along the highway, bus stops).
  - Transit infrastructure (e.g., platforms, transit sheds and approved transit parking areas, "future" entrances/exits).

- The type of Surveillance cameras (intelligent AI driven) will include:
  - Dome Cameras
  - Bullet Cameras
  - PTZ Cameras
  - Thermal Cameras
- The type of Smart gates will include:
  - Swing Gates Sliding
  - Gates Barrier
  - Gates Bollard
  - Gates Turnstile

Establishment of 2 command and control centers for surveillance and analysis and monitoring of smart gates live feeds:

- Supply and installation of a primary and back-up command centers for centralized monitoring of cargo
- Integration of the 2 command centers one as primary site and the other as secondary/backup site
- Integration of the 123 procured and deployed surveillance cameras and 66 smart gates solutions.
- Training of staff & Knowledge transfer on Smart Gates use and surveillance
- Maintenance and support of both the smart gates and cameras

Proposed Smart Gates Installation sites – See Annex I

  - Airports
  - Seaports
  - OSBPs
  - Oil Depots

Proposed Surveillance Camera Installation sites along the Customs approved routes – See **Annex II**

Schedule of Requirements

No.	Item	Sub-item	QTY
1	Command Centre	Power Supply, Lighting, Cooling system, 2	2

		Servers, 30 work stations, 4 video walls, 2 routers, 2 switches, 100 phones/ intercom systems, 4 Printers/ scanners, operating system, specialized software, database management, security software, VPN, Data storage, Data Backup, 360 degrees/ omnidirectional cameras	
2	Smart Gates	Smart Gate system complete with its accessories	66
3	Cameras	Bullet cameras - 86, Dome cameras, PTZ cameras, Thermal cameras, network/IP cameras, wireless cameras	123
4	Support and Maintenance	For a period of 3 years	3
5	Training & Knowledge Transfer	Training staff on the system	1

5. Methodology

The vendor should clearly demonstrate a comprehensive understanding of the Terms of Reference (TOR) and all outlined requirements for the Supply, Delivery, Installation and Commissioning of Smart Gates and Transit Surveillance solution. In addition, they should present a well-defined delivery methodology that explains how they intend to execute the assignment.

6. Implementation team and responsibility

The vendor should clearly demonstrate the firm's overall experience, as well as present a detailed breakdown of the proposed team structure. This should include the qualifications, roles and relevant experience of all key experts who will be assigned to the assignment.

7. Implementation schedule workplan

Bidders shall propose an implementation schedule with clear milestones to which they will be contractually bound. The vendor is expected to complete the entire assignment within a maximum period of 18 months and a warranty period of one year.
The maintenance and support period is three years.

8. Expected Deliverables

- Automated Identification and Verification:
    - Biometric identification systems (facial recognition, fingerprint scanning) for accurate and rapid verification of individuals.
    - Automated number plate recognition (ANPR) for vehicle identification.

    - Automated Container number recognition (ACNR) for container identification.
- Improved Surveillance:
    - Real-time monitoring through CCTV and sensor networks.
- Data Integration and Sharing:
    - Integration with existing and future infrastructure.
- Reduced Processing Times:
    - Automated smart gate systems for faster passage of legitimate travelers and goods.
- Improved Traffic Flow:
    - Optimized traffic management systems to minimize congestion.
    - Designated lanes for pre-approved travelers and cargo.
    - Real-time monitoring of traffic flow for proactive management.
- Enhanced Data Accuracy:
    - Reduced human error through automated data capture.
    - Improved data integrity and reliability.
    - Electronic tracking and tracing of goods in transit.
- Increased Revenue Collection:
    - Improved accuracy in the valuation of goods.
    - Reduction of smuggling, which increases the amount of collected customs duties.
- Smart Gate Infrastructure:
    - Installation of automated gates with integrated biometric and document scanning systems.
    - Network infrastructure for data transmission and communication.
- Surveillance Systems:
    - Deployment of CCTV cameras, sensors, and other surveillance equipment.
    - Implementation of video analytics and other advanced monitoring tools.
- Data Management Systems:
    - Development of centralized databases for data storage and analysis.
    - Implementation of data security and privacy measures.
- Standard Operating Procedures (SOPs):
    - Development of clear guidelines for the use of smart gate and surveillance systems.
    - Establishment of protocols for responding to security incidents.
- Training Programs:
    - Training for customs officers and other border personnel on the use of new technologies.

- Maintenance and Support:
    - Provide Maintenance and support services for smart gate and surveillance systems.

9. Detailed Technical Specification/Requirements

TECHNICAL SPECIFICATION REQUIREMENTS

Instructions to Bidders:

1. Bidders MUST complete the Table below in the format provided.
2. Bids MUST meet all mandatory (MUST) requirements marked "M" in the Tables below in order to be considered for further evaluation.
3. Bidders MUST provide a clear commitment to meeting the requirements for all features irrespective of any attached technical documents in the table format (bidders Response) below.
4. Use of Yes, No, tick, compliant, blank spaces etc. will be considered non-responsive.
5. Bidders MUST provide a clear commitment to meeting the requirements for all features irrespective of any attached technical documents in the table format (bidders Response) below. Use of Yes, No, tick, compliant, blank spaces etc. will be considered non-responsive.
6. Bidders who do not comply with any of the below requirements will NOT be considered for further evaluation

A. FUNCTIONAL REQUIREMENTS

Functionality Requirements and Technical Requirements

Bidders are required to demonstrate how their proposed solution meets the listed requirements. Each requirement will be evaluated and scored according to the following criteria.

Table 1: Functional Requirements

No	Feature	Bidder's detailed Response (Pass/Fail)
1	**Functionality: Presence detection**	
a)	Through Automatic Number Plate Recognition (ANPR), ability to detect oncoming motor vehicle and record registration number. Should cater	

No	Feature	Bidder's detailed Response (Pass/Fail)
	for different fonts 1. The license plate recognition camera can independently identify license plates without requiring additional servers or backend algorithms. 2. License plate recognition rate >= 95% 3. Supports Kenyan license plate recognition.	
b)	Through Automatic Container Number Recognition (ACNR), ability to capture and record container number. Ability to cater for all container sizes. 1.The container number recognition camera can independently identify container numbers conforming to ISO standards without requiring additional servers or backend algorithms. 2. Container number recognition rate >= 95%	
c)	After recognition of the license plate, the license plate number (or container number) to be relayed on a screen for the control officer. And the system supports manual addition or modification of license plate numbers and container numbers.	
d)	Maintain a unique number for all motor vehicles accessing the smart gate. This record should indicate the truck number, time stamp, container number (if available)	
e)	Integration with existing Regional Electronic Cargo Tracking system (RECTS) at bidders own cost.	
f)	Maintain a time stamp for all traffic accessing the smart gates. To include time in and time out of the Point of Exit (PoE).	
g)	Ability to scan documents and store the data. Ability to perform facial recognition for drivers	
h)	Ability to detect object (optical barrier). Installed in the barrier gate area, this device identifies the presence of vehicles or other objects and can be integrated with Smart Gate for comprehensive decision-making to prevent accidental impacts on passing vehicles and pedestrians. Main Specifications: Input Voltage: DC12V-36V Rated Power: < 10W Operating Temperature: -20℃~ +70℃ Number of Infrared Radiation Units: 3 (Matrix Layout) Installation Environment: Indoor/Outdoor	
2	**Functionality: Image Capture**	

No	Feature	Bidder's detailed Response (Pass/Fail)
a)	Ability to capture and store surveillance images/videos of traffic flow The camera should cover the entry gate and exit gate	
b)	Ability to store the captured images in a local storage that can be shared on need basis	
3	**Functionality: Traffic Control**	
a)	Ability to control traffic within the Point of Exit (PoE) through gantry signage or overhead traffic lights.	
b)	The smart gates should provide for a Gate House for monitoring and lane control (optional)	
c)	The manual lane barrier should cater for safe and efficient passage of the trucks in terms of height and width	
4	**Functionality: Anti-Tailgating**	
a)	Implement measures to prevent tailgating (unauthorized entry behind an authorized user) through methods like sensors	
5	**Functionality: Exchange of data & Compatibility with other systems**	
a)	Ability to share truck details and other data with identified customs system(s)	
b)	Ability to receive data from identified customs system(s)	
6	**Functionality: Validation of Data**	
a)	The system should be able to validate received data against set parameters	
b)	The system should notify the driver on the outcome of the validation checks (either to exit or to return back)	
7	**Functionality: Triggering**	
a)	The system should allow opening or closing of the barrier gate depending on the identified trigger criteria	
b)	The barrier gate should allow for automated, manual and mixed mode(s)	
c)	The system should keep records for the manual and automated operations for reconciliation and audit.	
8	**Functionality: Profiling**	

No	Feature	Bidder's detailed Response (Pass/Fail)
a)	The system should be able to identify trends for risk management purpose. The database may contain information about any infringements previously made by the carrier on the territory of the country - AI.	
b)	The system should have a mechanism to flag suspect cases -Such information can then be automatically displayed to the control officer at the border crossing before the vehicle enters the inspection zone - AI	
9	**Smart Gate Management Software at Headquarter**	
a)	Cloud-based centralized management platform for smart gate Functionality: Supports centralized supervision and operation of various port checkpoints at three levels: General Administration of Customs/Headquarters, Directly Subordinate/Regional, and Subordinate/Port. Capacity: Supports 500 sites, with each site capable of managing 300 lanes, and a maximum of 15,000 intelligent clearance lanes under unified management. All the above functions require proof of the software interface.	
b)	**Features of Cloud-based centralized management platform for smart gate** Support the central station to manage the release rules of all port stations, ensuring that stations strictly follow the rules to release passengers and avoid problems such as gray-area enforcement and port shifting. **Centralized Monitoring:** 1. Supports comprehensive map-based display of business status for all stations, including clearance traffic, clearance time, automatic/manual release ratio, etc., and ranks stations by metrics. 2. Supports displaying and analyzing clearance metrics for each station on the dashboard using various graphs (bar charts, line charts, pie charts, etc.). 3. Supports querying detailed vehicle information for all stations based on multiple combined criteria, including license plate number, container number, driver information, clearance time, and captured images. **Centralized management:** 1. Supports remote opening and closing of checkpoint channels at a specific site. 2. Supports remote configuration of vehicle release rules for a specific checkpoint at a specific site.	

No	Feature	Bidder's detailed Response (Pass/Fail)
	3. Supports user access control, allowing users to be assigned different permissions based on region, site, and function. 4. Should have unified identity authentication, allowing HQ users to access the port iGate system smoothly without having to re-enter their account information when accessing it from the Center. All the above functions require proof of the software interface.	
10	**Smart Gate Application Features**	
a)	1. Supports comprehensive display of station business status, including clearance traffic (current day's traffic, historical traffic), clearance timeliness (current day's timeliness, historical timeliness), automatic/manual release ratio, ratio of different vehicle types, and lane operating status. 2. Supports real-time lane monitoring, including: monitoring video, lane dynamic simulation map, license plate capture images, container number capture images, driver face capture images, lane name, lane number, vehicle clearance sequence number, recognized license plate number (supports front and rear license plates), recognized container number (supports dual container numbers), vehicle entry time, and vehicle release time. 3. Supports manual addition or correction of license plate numbers and container numbers. 4. Supports remote manual control of the barrier gate's raising and lowering for vehicle passage. 5. Supports recording all operation logs and related operator information. 6. Supports real-time monitoring of device status and real-time pop-up of barrier device alarms on the smart checkpoint application's web page. 7. Supports querying detailed vehicle information at checkpoints based on multiple condition combinations, including license plate number, container number, customs declaration number, country, entry date and time, departure date and time, dwell time, and captured images. 8. Supports report query functions, including customs clearance flow reports, customs clearance timeliness reports, and automatic/manual vehicle release reports. 9. Supports offline release mode. In offline release mode, vehicle customs clearance information is stored locally. When the network is restored, the vehicle customs clearance information will be synchronized	

No	Feature	Bidder's detailed Response (Pass/Fail)
	with the cloud checkpoint centralized management platform. 10. Ports can use either local or single-point accounts; local accounts are used by default to avoid identity verification failures due to network outages. 11. Supports comparison of facial images captured by the front end to determine if they belong to the same driver. It can automatically calculate scores from multiple captured images and select the best one. 12.All the above functions require proof of the software interface.	
11	**Functionality: Scalability**	
a)	The system should be scalable, allowing for easy expansion or modification to accommodate changing requirements	
12	**Functionality: Weight Control**	
a)	The system should be able to weigh a truck with or without cargo by means of sensors and/or electronic weighing scales.	
b)	These details should then be transferrable to the identified customs system(s)	
13	**Functionality: Reports**	
a)	Ability to generate reports on gate usage, security incidents and access logs for auditing and analysis	
14	**Smart Gate Lane Kiosk**	
a)	The integrated cabinet,installed on the safety island, is configured for vehicle clearance applications. It can integrate a QR code scanner, video intercom, driver facial recognition terminal, and display screen. It is an important component of the self-service clearance process. The panel integrates the necessary operating equipment for clearance, and drivers only need to stop in front of the cabinet once to complete all the necessary operations Main Specifications: ● Outdoor cabinet, installed on a safety island; cabinet material: 2mm high-quality steel; protection rating: not less than IP55; ● Internal modular structure, with integrated display screen and power supply module; ● Display screen: 8-inch LCD screen, supports text, images, and	

No	Feature	Bidder's detailed Response (Pass/Fail)
	animation display. Integrated with the checkpoint system, it displays relevant information and guidance during the vehicle inspection and release process, prompting drivers to perform corresponding operations. ● It can be integrated with QR code scanners, video intercoms, ticket printers, driver face capture terminals, etc., primarily providing drivers with self-service operations such as scanning codes, intercoms, and ticket collection; ● The panel can be customized to integrate other devices as needed, featuring a modular design; ● An alarm indicator light is installed at the top; the light flashes when an abnormality occurs, alerting the driver; It has anti-interference, wind and sand resistance, shock resistance, and corrosion resistance capabilities.	
15	**Lane Controller**	
a)	The lane controller connects to the lane's front-end equipment and is a crucial component of traffic control. It collects and uploads front-end data and can distribute and execute commands to control the front-end equipment. It can also execute system commands to restart the front-end equipment, enabling remote operation and maintenance. **Main Functions** ● Integrated device, ready to use after external device wiring ● Supports connection to lane-based data acquisition and execution devices (including lane emergency controllers) ● Comes with built-in logic control program, which can be programmed as needed ● Supports remote operation and maintenance, and can control lane device restart **Key Specifications** ● I/O Interfaces: 14 inputs + 6 outputs ● Communication Interfaces: 2 RS485, 2 RS232 ● Network Interfaces: 1 LAN 10/100/1000 Mbps port ● Other Interfaces: TTL x1, CAN x1 ● Power Conversion: Supports AC 220V to DC 24V and DC 12V output conversion	
16	**Smart Gate Lane Kiosk -** QR Code Scanner	

No	Feature	Bidder's detailed Response (Pass/Fail)
a)	The QR code scanner is embedded in the integrated cabinet, with the scanning window facing the driver, making it convenient for the driver to scan QR codes on their mobile phone or paper when passing through customs. **Main Specifications** ● CMOS High-Sensitivity Sensor ● Hidden White LED Light ● LED Light Source ● Supports scanning at medium to long distances of 200-1200mm ● Fast reading of barcodes and QR codes (including paper codes and mobile phone screen codes) in strong outdoor light environments ● Fast scanning response, single scan within 50ms ● Reading accuracy ≥5mil ● Provides USB and TTL-232 interfaces Reading modes support hardware trigger/induction/continuous reading modes	
17	**Smart Gate Lane Kiosk -** Passport Reader	
a)	Used to detect and scan various travel documents, enabling the collection of information from drivers , and supporting travel documents (electronic ID cards or electronic passports) . Key Specifications ● Supports both ICAO-compliant and non-compliant travel documents ● IP50 protection rating, suitable for harsh environments ● Ergonomically designed full-page reader ● All documents conforming to ICAO 9303 Standard Part 1-4 specifications ● ISO 14443 Type A/Type B Smart IC Card (13.56MHz) ● ISO 7816 Class A/AB Smart Card ● Barcodes (2 of 5 interleaved, Code 128, Code 39) QR Codes (PDF 417, QR, Data Matrix, Aztec formats)	
18	**Smart Gate Lane Kiosk -** Facial Capture Terminal	
a)	The face capture terminal is embedded in the lane-integrated cabinet and is mainly used to capture driver faces at the entrance and exit, sending the images to the backend. Main Specifications Sensor: 2MP 1/2.7" CMOS, dual sensors Lens: 2.8 mm	

No	Feature	Bidder's detailed Response (Pass/Fail)
	Image Size: 1920×1080 Audio Interface: 1 audio input Communication Interface: 1 RJ45 10M/100M adaptive Ethernet port Power Interface: Φ5.5mm round connector Power Supply: DC12V±20%	
19	**Smart Gate Lane Kiosk -** Video Intercom Extension	
a)	The video intercom extension is embedded in the integrated cabinet, facing the driver. In case of customs clearance problems, the driver can use the extension to communicate with the on-duty personnel at the center to request assistance, so that the problem can be resolved quickly and customs clearance efficiency can be effectively improved. **Main Specifications** Network Interface: Standard RJ45 interface Network Protocols: TCP/IP, UDP, IGMP, RTP Video Resolution: 1080P Video Bitrate: 512Kb～4Mb Casing Material: Metal	
20	**Smart Gate Lane Kiosk - vehicle detector**	
a)	This dual-channel intelligent loop sensor is primarily used for vehicle detection to determine vehicle location. It can connect to two inductive loop coils. Main Specifications: Coil inductance range: 50-1000μH Nine sensitivity levels selectable Response time: ≤100 milliseconds Relay output mode Front-side reset button	
21	**Lane Emergency Controller**	
a)	As an auxiliary device in the vehicle inspection and release process, the lane emergency controller is used to allow the operator to perform emergency operations on the barrier gate when the system malfunctions and manual release is required or when there is a breaching attempt. The control log can be uploaded to the smart gate system to achieve strict management of each operation. **Functional Requirements:**	

No	Feature	Bidder's detailed Response (Pass/Fail)
	1. Emergency manual switching is only possible via a key knob to prevent accidental operation by inspection personnel and improve safety margin of error; 2. If suspicious behavior or attempted passage is detected in a vehicle during the inspection process, pressing the emergency stop knob will initiate an emergency interception. 3. The emergency controller has RS485 communication capabilities, and control logs are uploaded to the intelligent checkpoint system in real time for easy monitoring of passage. ● **Main Specifications:** ● Input Voltage: DC12V±5% ● Rated Power: ≤2W ● Operating Temperature: -20℃~+65℃ ● Installation Environment: Indoor/Semi-outdoor ● Communication Interface: RS485 Protection Rating: IP53	
22	**Video Intercom Host**	
a)	The video intercom host is deployed in the monitoring center or duty room. When it receives a driver's intercom request, it can promptly understand the driver's situation and quickly provide a response strategy, effectively improving customs clearance efficiency. **Main Specifications** ● Supports two-way high-definition video full-duplex intercom, with both hands-free and handset-based intercom modes. ● In intercom mode, the unit can simultaneously display the extension camera feed and the feed from the linked IPC. ● Network Interface: Standard RJ45 interface ● Network Protocols: TCP/IP, UDP, IGMP, RTP ● Video Resolution: 1080P ● Display Resolution: 1280x800 pixels	

B. NON-FUNCTIONAL REQUIREMENTS

Bidders are required to demonstrate how their proposed solution meets the listed requirements. Each requirement will be evaluated and scored according to the following criteria.

Table 2: Non-Functional Requirements

No	Feature	Bidder's response (Pass/Fail)
1.	**Usability**	
	The system should have a user-friendly dashboards and interfaces	
	The system should be scalable and adaptable to handle different traffic volumes and environmental conditions	
	The system should allow an officer to generate, view and print customizable report(s).	
	System should provide an audit trail for all the traffic accessing the designated Point of Exit(s)	
2.	**Configuration Management**	
a)	The system should have the following capabilities:	
b)	Access control management	
c)	User role management with nomenclature of roles	
d)	Audit trail of any accesses or adjustments made to the system	
3.	**Integration Requirements**	
a)	The system should have an Application Programming Interface (API) that allows other systems to access and interact with its functionality and data.	
b)	The system should be able to integrate with existing authentication and authorization systems to enable single sign-on (SSO) for users.	
c)	The system should be able to import and export data in different formats, including XML, CSV, JSON, or other relevant file formats, to enable seamless data exchange with other systems.	
d)	The system should be able to integrate with databases used by other systems or applications, such as ICMS, RECTS	
e)	The system should be able to integrate with notification systems to alert users of important events or changes related to smart gate operations	
f)	The system should be able to integrate with web services to enable data exchange and communication between different systems or applications.	
4.	**Security**	
a)	Each user must be authenticated with a unique user-id and password on the application.	
b)	All user and account management changes and attempts must be logged	

c)	User authentication data must be stored and maintained securely in a centralized location on the system	
d)	The application must support password expiry features with a configurable frequency. Parameterize this to allow flexibility in adjusting this value as required.	
e)	The password must be secure on entry, at no point must the password be in clear text	
f)	All new user accounts must be created with reference to existing authoritative databases of approved persons e.g., identifying numbers in KRA's active staff database (HR)	
g)	All network communications between components must be authenticated, and must not explicitly trust other network devices	
h)	Systems directly facing the Internet must not store or cache confidential data, even for a short duration. This includes file uploads and downloads, source code, etc.	
i)	Applications must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle	
j)	Applications that connect to a database, application server, or any system that utilizes application IDs must do so using an account that has been granted access to only objects and functions needed for operation of the application	
k)	All servers should be kept in sync with a time synchronization mechanism. All communication sessions must use secure protocols	
l)	Any vendor proprietary protocols used must be well documented (i.e. the vendor must provide comprehensive documentation on the protocols such as technical specifications or white papers).	
m)	All relevant session information should be captured and stored in a secure & auditable location	
n)	System to implement automatic timeouts for user authentication to prevent unauthorized access in case a user leaves the session unattended	
o)	System to have the capability to promptly revoke access permissions when a user status changes or when a security breach is detected	
5.	**Other System Features**	
a)	Secure Smart Gate control system operating platforms regularly monitored and prevented from system downtime, systems attacks	
b)	Audit trail for all functions executed through the Smart Gate control system	
c)	System to be safe from data loss	

d)	System to be available in different devices including Windows, Android, IOS	
e)	Technology: The various components of the smart gates including the barriers, cameras, to be from reputable internationally recognized brand, in existence for at least 5 years	
	Remarks – Pass / Fail	

Mandatory Minimum Technical Specifications

A. SMART GATES FOR PERSONNEL CLEARANCE:

Table 3: Minimum technical specifications of the smart gate for personnel clearance hardware

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Authentication Method	The system supports multiple methods such as face recognition, fingerprints recognition, identity document reading, IC card, and barcode scanning.	
2	AI Intelligent Recognition Technology	The system automatically detects whether the faces of passers-by are covered by masks, sunglasses, glass, etc., and provide voice prompts.	
3	Intrusion Alarm	When the channel gate is closed, and a person enters the channel in abnormal authentication, the channel will sound an alarm.	
4	Face Recognition	Recognition accuracy FAR＜0.0001%, FRR＜0.01%; Binocular camera with 2 million pixels.	
5	Operating Temperature	-20℃~+60℃	
6	REMARKS **PASS/FAIL**		

B. SMART GATES FOR VEHICLE CLEARANCE:

1.Container Number Recognition System

1.1.Overview

Container number recognition system is a digital recognition system which is composed of advanced OCR recognition technology, image acquisition technology, container detection technology, network technology and database query technology.

The container number recognition system uses four groups of cameras. The cameras are installed on the truck aisle to capture the box number images of the front, rear, left, and right containers. When a container truck passes through the checkpoint aisle, no manual intervention is required. The camera automatically captures container images. The back-end container ID recognition software automatically collects and identifies data, obtains the identification result, and sends the result to the cloud checkpoint system for processing.

1.2.System Composition

The container number recognition system consists of the HD digital camera, lens, illuminator, infrared trigger, signal collection controller, installation pole, and recognition software.

1.3. Main Specifications

A. Container Number Recognition Camera

- Sensor: ≥ 2 megapixels
- Maximum Resolution: 1920×1080
- Shutter: 1 sec-1/100,000 sec
- Operating Temperature: -30°C-70°C
- Humidity: ≤95%(noncondensing)
- Power Footage: ≤10W
- Lens Interface Type: C/CS interface
- Power: DC12V / DC24V
- Network Interface: 1 RJ-45 10M/100M adaptive network interface

B. Camera Lens

3.8-16mm auto-iris lens, target surface: 1/1.8", resolution: 2 million,

F-stop 1:1.5±10%.

C.Correlation Detector

Detection distance ≥ 5m, switch output: PNP/NPN, response time: 2 ms, Power: DC12V.

D.System Characteristics

- Be able to recognize the container numbers of ISO 6346:1995 and process the printing of multiple numbers, including one line, two lines, three lines, one column, and two columns.
- Can handle a variety of 20-foot boxes, 40-foot boxes, 48-foot boxes, standard boxes, refrigerated boxes, super-high boxes, super-long boxes, frame boxes, etc.
- Requirements for normal system snapshot recognition: The vehicle speed is limited to 15 km/h.
- The system can automatically identify the number of containers loaded by the vehicle, detect one long container or two short containers, and identify the respective container numbers.
- The system outputs processing information in TCP/IP mode and supports secondary development and integration.
- Identification records can be queried.

- It can operate continuously 24 hours a day and adapt to different situations such as insufficient illumination and lamp interference.
- In normal weather conditions, the overall recognition rate of the system is greater than or equal to 95% (excluding containers with damaged carton numbers).

☐Overall container number identification speed: less than 2 seconds.

2.Release Control System

2.1.Overview

The release control system sends the data collected by the front end equipment to the Smart Gate System through the lane controller/serial port server, including the container number, license plate number, electronic tag information, weight information, and IC card information. The Smart Gate System uploads the data to the Customs background verification and release system through the data transmission service, receives the release instructions returned by the Customs system, and performs release control according to the release instructions. In case of abnormal, authorized personnel can manually release the vehicle through lane controller.

2.2.System composition

The release control system mainly consists of lane controller, emergency controller, serial port server, network switch, LED display screen, traffic lights, vehicle safety protection equipment, vehicle detection equipment, loop detector, electronic arm barrier and intercom equipment etc.

2.3.Main Specifications

A.Serial port server

- Standard 19-inch rack size;
- Number of ports: 16;
- Interface mode: TCP server, TCP client, and UDP;
- Network management protocol: SNMP MIB-II;
- Voltage input range: 100 to 240 VAC;
- Electromagnetic isolation protection: 1.5 kV (built-in);
- Operating temperature: 0 to 55°C (32 to 131°F);
- Relative humidity: 5 to 95% (non-condensing).

B.Electronic Arm Barrier

- Lifting and falling time of Arm Barrier: no more than 3s;
- Type of Arm Barrier: regular straight barrier, 3.5-5m long;
- MTBF: More than 1.5 million reciprocating times;
- Anti-smash safety protection function: during the falling process, if the loop detector detects the vehicle, the arm barrier will be lifted to the vertical state quickly, and the arm barrier will fall again after vehicle pass, so as to prevent damage to the vehicle.
- Anti-collision function: when the arm barrier is in horizontal position, the vehicle hits the barrier, and the anti-collision mechanism can make the barrier rotate 90° to avoid damage.

3.Kiosk

3.1.Overview

To meet the information collection and operation requirements of trucks, buses and cars, a kiosk is installed on the Gate safety island. The kiosk is an important device in the vehicle clearance process. It

can interact with the driver in the automatic Customs clearance process without personnel attend. The panel of Kiosk adopts modular design and can flexibly integrate devices such as fingerprint recognition, face recognition, infrared temperature measurement, QR code recognition, and visual intercom. It supports data collection and height adjustment of the operation panel.

3.2. System composition

The integrated machine is mainly composed of cabinet body, lifting device, panel and industrial air conditioner.

3.3. Main Specifications

- Outdoor cabinet, installed on a safety island, material of cabinet: 2 mm high-quality steel, protection level: IP56;
- It has up and down control function, which can meet the operation requirements of freight cars, buses and trolleys;
- Vehicle self-adaptation function, which can identify the current vehicle type and automatically adjust to the corresponding position;
- Equipped with manual control button, the driver can adjust the lifting height according to needs;
- The distance between the acquisition system and the vehicle in the passage can be automatically adjusted.
- The cabinet panel can be designed with modular panels, such as fingerprint recognition, face recognition, infrared temperature measurement, two-dimensional code recognition, and visual intercom.
- A 19-inch standard cabinet can be installed inside the cabinet, and the power distribution equipment layer is configured.
- Built-in installation of industrial air conditioner cooling, overhaul door automatic lighting design;
- Working voltage: single-phase 200V-240V 50/60HZ.

4.Lane Management System

4.1. System Overview

The lane management system of the gate controls the devices (Camera, QR code scanner, RFID reader, etc.) on the lane according to the defined sequence. It realizes the automatic collection of vehicle information, receives the release instruction from the management system, and controls the automatic release or rejection of the electronic arm barrier.

4.2. System composition

The system is mainly composed of sequence configuration module, data acquisition module and equipment control module.

4.3. Main Specifications

- Collection configuration: supports the configuration of information collection requirements for different types of aisles (trucks, buses, and administrative services).
- Sequence configuration: Supports the configuration of the collection sequence requirements for different types of channels (trucks, buses, and administrative services).
- ID configuration: supports the configuration of the channel number (the channel number is assigned by the customs office) and the in/out identifier.

- Lane rule switchover: The switchover requirements of different types of lanes (trucks, buses, and administrative cars) are supported.

5.ANPR System

5.1. System Overview

The ANPR system uses advanced technologies such as photoelectricity, computer, image processing, pattern recognition, and remote data access to capture the image data of vehicles passing through the lane of gate. The ANPR software analyzes the captured images and automatically obtains data such as the passing time, license plate number, license plate color, and vehicle type. The system uses high-performance HD cameras as the front-end information acquisition equipment, with high-resolution images. The HD intelligent ANPR system can accurately record the vehicle information passing through the Gate in a timely manner and upload the license plate recognition result to the Customs background verification system, which is an important basis for comparison in the process of vehicle clearance.

5.2. System composition

The system mainly consists of the digital HD license plate recognition integrated device, lighting lamp, installation accessories, ANPR software, etc.

5.3. Main Specifications

- Image sensor: 3 megapixels
- Sensor pixel: 1 / 1.8' 3 megapixel progressive scan CCD
- Resolution: 2048 x 1536
- Minimum illumination: 0.15Lux@(F1.2, AGC ON)
- shutter: 1 / 25 sec to 1 / 30000 sec
- Lens interface: CS
- Auto iris: DC interface
- Image algorithms: AWB, AGC, WDR, and 2D/3D noise reduction
- Image format: JPEG
- Image resolution: 2048 x 1536
- Video compression standard: H.264
- Output bit rate: 256 Kbit/s to 16 Mbit/s
- Frame rate: 25 fps
- Snapshot synthesis: Two or three snapshots can be synthesized.
- Time calibration: NTP network time calibration and local time calibration are supported.
- Protocols: TCP/IP, RTSP, NTP, and FTP uploading
- Signal lamp synchronization: Supports signal lamp power synchronization input.
- Internal storage interface: SD card and USB storage
- Network interface: 1000 Mbit/s network interface
- Serial port: 1 RS485 port, 3 RS232 port
- Flash ports: 3
- Trigger input: 3
- Trigger output: 1
- Working voltage: 9–36 V DC
- Power consumption: < 10 W

- Operating temperature: -40°C ~ 80°C
- Supports license plate recognition in Chinese Mainland, Hong Kong, Macao, Vietnam, Russia, Pakistan, Kyrgyzstan, Uzbekistan, Tajikistan, Laos, Mongolia, and North Korea, and integrates with the Smart Gate System.

6.QR Code Scanner

6.1. System Overview

The QR code scanner is used to automatically identify the bar code, two-dimensional code or mobile phone two-dimensional code information on the relevant business documents, so as to improve the pass efficiency and speed of vehicle entry and exit gates. The two-dimensional code scanner is installed on the faceplate of the kiosk in embedded installation mode. The scanner is installed in the direction of the driver to facilitate the operation of the driver. When the vehicle enters or exits the gate, the driver places the QR code on the voucher or mobile phone in front of the scanner. The scanner automatically scans and recognizes the relevant information and sends it to the checkpoint system.

6.2. System composition

The system mainly consists of QR code scanner, installation accessories and recognition software.

6.3.Main Specifications

☐Image sensor: 640 x 480 CMOS

☐Reading precision: ≥ 5 mils

☐Reading code system: (mobile phone + paper) one-dimensional code, two-dimensional code

☐Read speed: 70 ms/time

☐Reading distance: 0-11cm

☐Sweeping feedback: buzzer, LED red and green indications

☐Protection rating: IP66

☐Communication ports: USB and RS232

☐Operating temperature: -20°C to 70°C

☐Ambient illumination: 0-80000LUX (non-direct sunlight)

☐Supported systems: Windows (XP, 7, 8, 10), Linux, Android, and Mac

7.LED Screen

7.1.System Overview

The LED screen is mainly used to display relevant guidance information in the process of vehicle clearance at gate, combined with the inspection and release instructions of the Customs, so that the driver can perform the next operation according to the guidance information.

7.2.System composition

The module mainly consists of LED screen and installation accessories.

7.3.Main Specifications

☐Application scenario: outdoor

☐Base color number: bibase color

☐Pixel spacing: 4.75 mm

☐Viewing angle: ≥ 120°

☐Control mode: asynchronous control

☐Pass mode: RS485/RJ45

☐Baud rate: 38400

☐Power supply mode: 220 V AC

☐Dimensions: 600 mm x 400 mm x 120 mm (length x height x thickness)

8.Video Intercom System

8.1.System Overview

The video intercom system is installed between the monitor room and the gate lanes. It is mainly used for the driver to call the on-duty staff in the monitor room through the video intercom system when the vehicle passes through the gate and needs to seek help from the on-duty staff. The staff can learn about the driver situation in time and provide assistance in the monitor room. The video intercom extension is embedded on the panel of the Kiosk, which facilitates the operation of the driver.

8.2.System composition

The system mainly consists of the video intercom host, the video intercom extension, and the IP address box.

8.3.Main Specifications

A.intercom host

☐15 extensions can be managed.

☐10.2" touchscreen display, 1080p HD video, desktop mount.

☐Visual intercom: supports bidirectional visual full-duplex intercom, and supports two intercom modes: handle and hands-free.

☐Host hosting: Host hosting can be hosted on other hosts in the system.

☐Listening monitoring: supports single-channel listening monitoring and cyclic listening monitoring.

☐One-click call: supports one-click call to any device in the system.

☐Network interface: standard RJ45 interface;

☐Network protocols: TCP/IP, UDP, and IGMP;

☐Audio sampling rate: 16–48 kHz;

☐Audio mode: 16-bit stereo CD sound quality;

☐Broadcast audio format: MP3 and WAV;

☐Output frequency: 20 Hz to 20 KHz;

☐Harmonic distortion: < 0.5%;

☐Signal-to-noise ratio: > 70 dB.

B.intercom extension

☐1080P HD video, all aluminum alloy CNC machining, hexagonal stainless steel fixing screws, special loading and unloading tools, with anti-dust and anti-dismantle, anti-manufactuary violence damage functions.

☐Two-key call: used for alarm and event consultation in case of emergency.

☐Duplex intercom: The IP network host can be used for duplex intercom.

☐Network interface: standard RJ45 interface;

☐Network protocols: TCP/IP, UDP, and IGMP;

☐Audio sampling rate: 16–48 kHz;

☐Audio mode: 16-bit stereo CD sound quality;

☐Broadcast audio format: MP3 and WAV;

☐Video stream: 512 kbit/s to 4 Mbit/s;

☐Harmonic distortion: < 0.5%.

Table 5: Minimum technical specifications of communication and networking

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Network Interfaces	• **Ethernet**: 10/100/1000 Mbps • **Wi-Fi**: IEEE 802.11a/b/g/n/ac • **Bluetooth**: Version 4.0 or higher	
2	Protocols	• **TCP/IP**: For network communication • **HTTPS**: For secure web-based management • **SNMP**: For network management and monitoring	

Table 6: Minimum technical specifications of software and integration

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Operating System	• **Embedded OS**: Linux-based or custom real-time OS	
2	Access Control Software	• **Features**: User management, real-time monitoring, reporting, integration with other security systems • **Database**: SQL-based, support for distributed architecture	
3	API Integration	• **Restful API**: For third-party integrations • **SDKs**: Available for various programming languages (Java, C#, Python)	

Table 7: Minimum technical specifications of surveillance integration

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Camera Integration	• **Types**: IP cameras, dome, and bullet types • **Resolution**: 1080p Full HD or higher • **Field of View**: Adjustable, typically 90° to 120°	
2	Storage	• **Local Storage**: microSDHC/microSDXC, capacity 64GB to 1TB • **Network Storage**: Integration with NAS/SAN systems	
3	Video Management Software (VMS)	• **Features**: Live view, playback, motion detection, AI analytics • **Compatibility**: ONVIF compliant, supports RTSP streams	

Table 8: Minimum technical specifications of user interface and control

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Display Units	• **Type**: LCD/LED screens • **Size**: 7 inches to 15 inches • **Resolution**: 1280x800 pixels or higher	
2	Control Panels	• **Touchscreen**: Capacitive touch, multi-touch support • **Buttons**: Mechanical or capacitive touch buttons for basic controls	
3	User Feedback	• **Indicators**: LED lights (green/red) for status indication • **Audio**: Speakers for voice prompts and alerts	

Table 9: Minimum technical specifications of security and encryption

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Data Encryption	• **Methods**: AES-256 for data storage, TLS 1.2/1.3 for data transmission	
2	User Authentication	• **Multi-Factor Authentication (MFA)**: Support for combining RFID, biometrics, and PINs	
3	Tamper Detection	• **Sensors**: Embedded tamper switches and accelerometers	

Table 10: Minimum technical specifications of maintenance and support

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Remote Management	• **Capabilities**: Remote diagnostics, firmware updates, and configuration	
2	Warranty and Support	• **Warranty**: Typically, upto 1 year • **Support**: 24/7 technical support, on-site maintenance options.	

C. CAMERAS:

Table 11: Minimum technical camera specifications

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
	Camera Types	• **Dome Cameras**: Ideal for indoor and outdoor use, with vandal-resistant features. • **Bullet Cameras**: Suitable for long-range viewing, typically used outdoors. • **PTZ Cameras**: Pan-Tilt-Zoom capabilities for wide area coverage and detailed monitoring.	

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
		• **Thermal Cameras**: For monitoring in low-light or no-light conditions.	
2	Resolution	• **Standard**: 1080p Full HD • **High-Resolution**: 4K Ultra HD	
3	Image Sensor	• **Type**: CMOS • **Size**: 1/2.8 inch or larger	
4	Lens	• **Fixed Lens**: 2.8mm to 12mm • **Varifocal Lens**: 2.8mm to 12mm adjustable • **Zoom Lens**: Optical zoom up to 40x for PTZ cameras	
5	Field of View	• **Wide-Angle**: 60° to 90° • **PTZ Cameras**: 360° pan, 90° tilt	
6	Low-Light Performance	• **IR Illumination**: Up to 50m (standard) or 100m (long-range) • **Low Lux Rating**: 0.01 lux or better	
7	Weather Resistance	• **Ingress Protection**: IP66 or IP67 for outdoor cameras • **Vandal Resistance**: IK10 rating for dome cameras	

Table 12: Minimum technical requirements (camera) – network and connectivity specifications

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Network Interfaces	• **Ethernet**: 10/100/1000 Mbps RJ-45 • **PoE (Power over Ethernet)**: IEEE 802.3af/at	
2		•	
3	Protocols	• **Streaming**: RTSP, ONVIF Profile S/G/T • **Security**: HTTPS, SSL/TLS, 802.1X	

Table 13: Minimum technical camera – storage and archiving

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Local Storage	• **Memory Card**: MicroSD/SDHC/SDXC slot, up to 256GB	

2	Centralized Storage	• **NVR (Network Video Recorder)**:
		  ○ **Channels**: 16, 32, 64, or more
		  ○ **Storage Capacity**: Up to 32TB per unit
		• **NAS (Network Attached Storage)**:
		  ○ **Interfaces**: 1GbE or 10GbE
		  ○ **Capacity**: Up to 100TB or more	

Table 14: Minimum technical camera – video management software (vms)

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	**Features**	• **Live View**: Real-time monitoring of multiple camera feeds • **Playback**: Search and playback recorded footage • **Alerts**: Motion detection, tampering alerts, analytics-based alerts • **User Management**: Role-based access control	
2	**Analytics**	• **Basic**: Motion detection, line crossing, intrusion detection • **Advanced**: Facial recognition, license plate recognition, object tracking, heat mapping	
3	**Integration**	• **Access Control Systems**: Integration with existing access control for comprehensive security	

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
		• **Alarm Systems**: Integration with fire and security alarms	
4	**Interface**	• **Web-Based**: Accessible through web browsers • **Desktop Application**: Windows, MacOS • **Mobile Application**: iOS, Android	

Table 15: Minimum technical camera – power supply and backup

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Power Options	• **Standard**: 12V DC or 24V AC • **PoE**: IEEE 802.3af/at	
2	Backup Power	• **UPS (Uninterruptible Power Supply)**: To provide continuous power during outages • **Battery Backup**: For critical cameras and NVRs	

Table 16: Minimum technical camera – installation and mounting

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Mounting Options	• **Ceiling Mount**: For indoor dome cameras • **Wall Mount**: For bullet and PTZ cameras • **Pole Mount**: For outdoor installations • **Corner Mount**: For 360-degree coverage	
2	Installation Tools	• **Cabling**: Cat5e or Cat6 Ethernet cables for network connectivity • **Brackets and Mounts**: Specific to camera models and installation environments	

Table 17: Minimum technical camera – environmental specifications

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Operating Temperature	• **Standard Cameras**: -10°C to +50°C • **Outdoor Cameras**: -30°C to +60°C	
2	Humidity	• **Operating Range**: 10% to 90% RH, non-condensing	

Table 18: Minimum technical camera – compliance and certification

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
	Certifications	• **Safety**: CE, FCC, UL • **Environmental**: RoHS, WEEE • **Interoperability**: ONVIF, PSIA	

Table 19: Minimum technical specifications and bills of quantities of items for two (2) centralized command centres

NO.	ITEM	SPECIFICATION	QTY	Bidder's response Pass/Fail
1.	Inspection Supervision Station (Image Processing Work Station CPU)	CPU: Xeon E5-1620 v3 (4 cores, 3.5GHz 10M), Memory: 16GB DDR4, Hard disk: 500GB SATA3 7200RPM, Optical drive: DVD+/-RW, Power supply: 685W, USB keyboard (English) + Optical mouse. Installed with Kaspersky antivirus	30	
2.	Displays	98 inches, 8K UHD (7680 x 4320), **High Brightness:** 700 to 2500 nits or higher for video walls, High contrast ratios (3000:1 and above), Wide viewing angles (178°/178°), Support for wide color gamuts (e.g., sRGB, Adobe RGB, DCI-P3)	4	
3.	Routers	Wireless Standards802.11ax (Wi-Fi 6)802.11be (Wi-Fi 7)Speed(e.g., 600 Mbps on 2.4 GHz, 1300 Mbps on 5 GHz)	2	
4.	Switches	24-Port Layer 2 Switch	2	

5.	Graphics card	Interface: PCI-E 3.0 GPU: NVIDIA Geforce GTX 1050 Ti Memory: 4G, DDR5, 128bit 3D API: DirectX supports up to 12.1 Interface: DVI*1, HDMI*1, DP*1 Maximum resolution: 2560×1600 Recommended power: 300W or more	30	
6.	Workstation Monitor	32 inch flat-screen display Resolution: 2560*1440 Interface: DP & HDMI & VGA Stand: Flexible stand with capability to: Adjust height, rotate on horizontal axis, and rotate on vertical axis	60	
7.	UPS (for workstation)	1000w	30	
8.	UPS (for workstation)	8000w	2	
9.	Operating System (for workstation)	Windows 10 IOT Enterprise 2016 LTSB 64-bit English version	30	
10.	Network Switch（PoE)	48 Port POE Switch, 48x10/100/1000Base-T Ethernet ports(PoE)，4x1000Base-X SFP Ethernet ports	2	
11.	NVR	64-channel camera access and forwarding, with an access capacity of 320Mbps, and 32-channel playback and download, with a playback capacity of 160Mbps.Compute power：20TOPS, h.265 1080P decoding circuit, VGA, HDMI 1 1/2 Gigabit RJ45 interface, 2usb3.0 1CH), 1/audio input/output, support 8 bays (6TB per hard disk), 16 / 4 alarm interface input / output, face detection, RAID0 / 1 / 5	4	
12.	LED TV	85", Wall Mount Bracket	4	
13.	Splicing Screen	46” splicing screen and accessories for installation	30	
14.	Bullet Camera 128	2CD4A26FWD-IZS/P: A 2MP varifocal bullet camera with WDR, IR, and PoE, designed for license plate recognition.	1	

15.	Dome Camera	See the included minimum specifications	6	
16.	Cabinet	600 x 1000 x 205542U, Black Colour	1	
17.	Dimensions	Command centre – 30 by 15 metres Equipment room 4 by 4 metres	1	
18.	Accessories	Network Cable, Network Registered Jack (RJ-45, Cat5E), DVI Monitor Cable, PDU power for cabinets	1	
19.	Image analysis software	Tailor Made for KRA image analysis	For 30 CPUs	
20.	Other Items, Accessories, etc. necessary to operationalize the command centre	List all the other Items and Accessories necessary to operationalize the command centre	LOT	
	Furniture			
21.	Lockable compartments	Pigeon-Hole Lockout Box Storage System	60 lockable compartments	
22.	Command Centre Desks	Standard command centre desks	30	
23.	Command Centre Chairs	Orthopaedic chairs	30	
24.	Fridge	STANDARD 210LTRS DOUBLE DOOR FRIDGE- RT26HAR2DSA FEATURES: • cu. ft. • 210 Litres Capacity • Net Dimensions: 56cm(W) x 63cm(D) x 145cm(H) • Digital Inverter Compressor with a 20 Year Warranty • Multi flow Air System • LED Lighting • Easy Slide Shelf • Cool Pack – up to 8 hours • In-built Power Stabilizer • No Frost Technology • Big Door Guard • Easy Space Manager • Tempered Glass Shelves	2	

		• Silver Technology Deodorizer • Recessed Easy Handle • Multi Storage Basket • 5 Star Energy Rating • Colour: Silver/black		

Table 20: High Level Security Requirements

No	Feature	Requirement	Bidder's detailed Response (Pass/Fail)
1	Data Encryption	All data, both at rest and in transit, must be encrypted using industry-standard encryption algorithms to prevent unauthorized access.	
2	Access Control	The system must implement robust access control mechanisms, including multi-factor authentication, role-based access controls, and the principle of least privilege.	
3	Auditing and Logging	Comprehensive audit trails must be maintained for all system activities, enabling traceability and accountability. Ensure the logs are in a format that is consumable by Security information and event management (SIEM) system.	
4	Incident Response	An effective incident response plan must be established by the vendor to address security breaches or incidents promptly and minimize impact.	
5	Data Integrity	Mechanisms must be in place to ensure the integrity of data, including checksums, digital signatures, and blockchain technology where applicable.	
6	Continuous Monitoring	The system must have continuous monitoring capabilities to detect and respond to security threats in real-time.	
7	Security Training	Vendors must provide security training for system users and administrators to foster a culture of security awareness.	
8	Secure Development	The solution must be developed following secure coding practices, and vendors must demonstrate a commitment to security throughout the software development lifecycle.	
9	Authentication	No identification and authentication information must be hard-coded or scripted into the application.	
10	Compliance to Detailed KRA Security Requirements	The solution must be implemented in compliance with the detailed KRA Application Security requirements (Annex III) and API Security requirements (Annex IV). The detailed requirements will form part of the Information Security testcases.	

Vendor Technical Evaluation

	Bidder Experience	**Maximum score**
No.	**Requirement Description**	
1.	**<u>Firm's Experience</u>** The firm should have Five (5) years' Experience in Installation, Supply, Commissioning and Maintenance of Smart Gates and Transit Surveillance solution and support. The bidder to provide a Company profile demonstrating ability to Supply, Deliver, Install and Commission, and respond to all maintenance issues. **(*3 marks*)** Certificate of Incorporation: Above Five (5) years…**(*3 marks*)** Certificate of Incorporation: 5 years…… **(2 marks)** Bidder is required to describe and provide evidence of **3 similar projects** undertaken within the last 5 years: a) Contract or LSO/LPO; b) Completion certificate/ Reference/recommendation letter from client For each satisfactory reference, the bidder will be scored per areas listed above: **i)** Contracts or LPO/LSO **(1.0 Mark),** ii) Completion certificate Reference or Recommendation letter from client **(2.0 marks)** (3 marks per client) References required should be for sites where the bidder or its partners in the project implemented solution.	11
2.	**Project Team**	
	<u>Personnel's Qualifications and Experience</u> Bidder is required to provide a responsibility matrix and profiles of delivery leads (Project Manager, Development Lead, Solution Architecture Lead, and Infrastructure Lead). Bidders are required to submit actual and current project team members of the core team expected to be involved in the project and clearly indicating where the teams have carried out similar implementations. Bidders must provide the following documents for the core team: a) Detailed CV b) Academic qualifications/certificates c) Years of experience d) Relevant certifications	24

	For each lead the scoring will be as follows per lead (At least for the following roles **Project Manager, Development Lead, Solution Architecture Lead, Infrastructure Lead – 4 Leads to be evaluated)** Detailed CV demonstrating lead having worked in a successful Smart Gates and Transit Surveillance project implementation in the proposed role **Project Manager** a) Lead (Project Manager) with relevant qualification i. Degree in Information and Communication Technology (Computer Science, IT, Engineering) or other related field **(2 Marks)** (attach certificate) ii. Diploma in Information and Communication Technology or other related field **(1 Mark)** (attach certificate) b) The Lead (Project Manager) must have certification in Project Management (PMP/ Prince2) or any other similar/related course. (Must attach copy of certificate) **– 2 marks** c) Must have a minimum of five (5) years' experience in Project Management (Must provide detailed and signed CV) i. Above 5 years – **2 marks** ii. 1 to 5 years – **1 mark**	6

	Development Lead a) Lead with relevant qualification i. Degree in Information and Communication Technology or other related field **(2 Marks)** (attach certificate) ii. Diploma in Information and Communication Technology or other related field **(1 Mark)** (attach certificate) b) The Lead must have certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) – **2 marks** c) Must have a minimum of five (5) years' experience in Project Management (Must provide detailed and signed CV) i. Above 5 years – **2 marks** ii. 1 to 5 years – **1 mark**	6
	Solution Architecture Lead a) Lead with relevant qualification i. Degree in Information and Communication Technology or other related field **(2 Marks)** (attach certificate) ii. Diploma in Information and Communication Technology or other related field **(1 Mark)** (attach certificate) b) The Lead must have certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) **– 2 marks** c) Must have a minimum of five (5) years' experience in Project Management (Must provide detailed and signed CV) **i.** Above 5 years – **2 marks** ii. 1 to 5 years – **1 mark**	6
	Infrastructure Lead a) Lead with relevant qualification i. Degree in Information and Communication Technology or other related field **(2 Marks)** (attach certificate) ii. Diploma in Information and Communication Technology or other related field **(1 Mark)** (attach certificate) **b)** The Lead must have certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) **– 2 marks** c) Must have a minimum of five (5) years' experience in Project Management (Must provide detailed and signed CV) **i.** Above 5 years – **2 marks** ii. 1 to 5 years **– 1 mark**	6
	Total	24

10. Methodology & Work Plan

Adequacy of the proposed Methodology and Work Plan in responding to the Terms of Reference will be evaluated on how the consultant proposes to address the areas listed below	**Maximum score**
Supply, Delivery, Installation and Commissioning of Smart Gates and Transit Surveillance solution In this section the bidder is expected to provide a detailed and comprehensive work plan and methodology(s) on how they intend to execute the items indicated below (Starting second bullet) • Development of detailed Work plan with specific and clear milestones **(2 Marks)** • Supply, Delivery, Installation and Commissioning of 66 Smart Gates and it weighing components to designated POEs in Kenya **(5 marks)** • Supply, Delivery, Installation and Commissioning of 123 Surveillance cameras (intelligent AI driven) **(5 marks)** • Establishment of 2 command and control centers for surveillance and analysis and monitoring of smart gates live feeds **(2 marks)** • Integration of the 2 command centers (one as primary site and the other as secondary/backup site) **(2 marks)** • Integration of the 123 procured and deployed surveillance cameras and 66 smart gates solutions. **(1 mark)** • Training of staff on Smart Gates use and surveillance **(1 mark)** • Maintenance and support of both the smart gates and cameras **(2 marks)**	20

11. DEMO

Bidders who are successful in the Technical Requirements will be invited for a live presentation/demo that will form additional assessment of the solution capabilities and vendor experience.

The Components of the presentation/demo to broadly include:

i) The vendor should provide a comprehensive demonstration that highlights the smart gate's functionality, security, and convenience features. The Demo should showcase working Smart gates with its various components, e.g., weigh bridge and Integration

The vendor should show case surveillance cameras capable of character recognition/thermal imaging, high quality video and resolution, transmission to the command centre, Integration to existing platforms

	Component	Requirement	Expected output	Max Score (Points)	Score
1.	Access Control Mechanisms	How the gate grants or denies access, including keypads, card readers, biometric scanners, and mobile app integration.	Time taken to grant/deny access	2	
2.	Sensors and Alarms	The types of sensors used, such as motion detectors, and how they contribute to security and convenience.	Trigger mechanism	2	
3.	Motor and Mechanism	The operation of the gate's motor, its speed, noise level, and the mechanical parts that ensure smooth opening and closing.	Reliability and Sustainability of gate mechanism	2	
4.	Intercom System	If the gate includes an intercom, demonstrating how gate personnel can communicate between different gates and to a remote location e.g., to a command centre.	Enhanced communication	2	
5.	Camera Integration	Showcasing any cameras that are part of the system, their resolution, night vision capabilities, and how they integrate with recording systems.	Quality of Image/video feed capture Cloud connectivity	2	
6.	Safety Features	Demonstrating safety features like auto-reverse mechanisms that prevent the gate from closing on a person or object.	Warning signs, sirens, manual override	1	
7.	Integration with Smart Systems	How the gate integrates with other smart systems for a seamless automation experience.	Ease of data exchange	1	
8.	Weight Control	The system should be able to weigh a truck with or without cargo by means of sensors and/or electronic weighing	Weight and dimension measurements	2	

		scales			
9.	Camera Housing	Demonstrating the durability and protective features of the camera's housing	Durability and protection from weather elements	1	
10.	Lens	The quality of the lens affects image clarity, and vendors can demonstrate different types such as fixed-focus and zoom lenses	High Image Quality (4K)	1	
11.	Processor	The processor should convert signals into digital images in real time	Speed of transmission	1	
12.	Storage	Showing the options for video storage, whether it's built-in or external like an SD card or cloud storage	Internal or external storage	1	
13.	Power Supply	Power requirements and options like Power over Ethernet (PoE) for convenience	AC power or DC power	1	
14.	Networking Interface	Presenting the camera's networking capabilities for transmitting images and enabling remote monitoring and viewing	Wireless, Wired or Power over Ethernet (PoE)	1	
15.	User Interface	A system that allows configuration, live viewing and analytics, through a web browser. A system that provides advanced features and monitoring capabilities. A system that enables control through a smartphone.	Web Interface, desktop software or mobile application	1	
			Total Score	**22**	

Note:

The vendor must achieve 75%, which translates to a numerical cut-off of **16.5 points** (22 x 0.75).

OVERALL EVALUATION

SUMMARY OF THE EVALUATION SCORES

Criteria	Maximum Score / Requirement	Cut-off Score
Technical requirements/Specifications	**Mandatory**	**Met**
Methodology	**20**	**16**
Bidder Qualifications (Vendor)	**35**	**28**
Demo	**22**	**16.5**
Total Points	77	**60.5**

12. Financial Summary

No.	Item	Sub-item	QTY	UNIT COST (KSH)	TOTAL COST (KSH) Taxes inclusive
1	Command Centre	Power Supply, Lighting, Cooling system, 2 Servers, 30 work stations, 4 video walls, 2 routers, 2 switches, 100 phones/ intercom systems, 4 Printers/ scanners, operating system, specialized software, database management, security software, VPN, Data storage, Data Backup, 360 degrees/ omnidirectional cameras	2		
2	Smart Gates	Smart Gate system complete with its accessories	66		
3	Cameras	Bullet cameras - 86, Dome cameras, PTZ cameras, Thermal cameras, network/IP cameras, wireless cameras	123		
4	Support and Maintenance	For a period of 3 years	3		
Grand Total Cost –To be carried Forward to the FORM FIN 2 Summary of Costs					

N/B: Bidders to provide a breakdown of how they have arrived at the total cost

Notes

1. The quoted price shall be in Kenyan shillings encompassing all costs associated with the Project scope of work. Additionally, it shall cover maintenance services, transfer of knowledge, and acquisition of the source code. All these elements are to be included within the total quoted price without any additional charges.
2. The financial remuneration for the development, implementation, and maintenance of the Digital shipment solution will adhere to the following terms:
   Milestone-Based Payments: At the negotiation stage payment shall be structured around the successful completion of predefined milestones that correspond to the project's phases. Each milestone payment will be contingent upon the acceptance of deliverables as per the agreed-upon specifications and timelines.

Annex I: Proposed Surveillance Camera sites:

Customs Area	**Location:**	**Number of Smart Gates:**
OSBPs	Busia	2
	Malaba	2
	Namanga	2
	Taveta	2
	Isebania	2
	Lungalunga	2
	Moyale	2
	Suam	2
Airports	JKIA	2
	MBA	2
	KIS	2
	EDL	2
Seaports	Lamu	6
	Kilindini	10
	Kisumu	2
Oil installations	Various	24
Total:		**66**

Annex II: Proposed Surveillance Camera sites:

#	Route	Installation Sites
1.	Mombasa-Nairobi-Nakuru-Kisumu-Busia	Mazeras, Mariakani, Bonje, Taru, Samburu, Maungu, Voi, Mtito Andei, Emali, Kyumvi, Athi River, Gitaru, Mutarkawa, Maai Mahiu, Longonot, Naivasha, Gilgil, Elementaita, Nakuru, Salgaa, Mau Summit, Chepsir, Kericho, Oyugis, Kisumu, Bumula, Busia
2.	Mombasa-Nairobi-Nakuru-Eldoret-Malaba	Mau Summit, Timboroa, Chepsiret, Leseru, Turbo, Lwandeti, Kanduyi, Malaba
3.	Namanga-Nairobi	Namanga, Ngatataek, Bisil, Kajiado, Isinya, Kisaju, Kitengela, Athi River
4.	Eldoret - Suam	Eldoret, Kitale, Endebess, Suam
5.	Mombasa – Lunga Lunga	Likoni, Waa, Kombani, Ukunda, Msambweni, Ramisi
6.	Mombasa – Voi - Taveta	Mazeras, Mariakani, Bonje, Taru, Samburu, Maungu, Voi, Mwatate, Maktau, Ziwani, Taveta
7.	Nairobi – Isiolo – Marsabit – Moyale	Thika, Karatina, Nanyuki, Isiolo, Laisamis, Marsabi, Moyale
8.	Nairobi – Isiolo-Modogashe – Wajir-Rhamu-Mandera	Thika, Karatina, Nanyuki, Isiolo, Modogashe, Wajir, Rhamu, Mandera
9.	Lamu - Garissa-Isiolo-Lokori – Lokichar (LAPSSET)	Lamu, Garissa, Isiolo, Lokori, Lokichar

Annex III API Security Requirements

General Rule: The solution must implement API-first design for integration i.e. API-first design for integration is a development strategy where APIs are designed, documented and defined before any application code is written, treating the API as a core product, not an afterthought.

	ANNEX I - API Security Requirements
	Review Area
1	**Governance**
1.1	Ensure the API is properly versioned. Versioning helps in keeping track and maintenance of the API.
1.2	Ensure that the API conforms to the organization set style and design guidelines such formatting of headers for consistency.
1.3	Ensure that the API is included as part of the organization's APIs inventory for Discoverability and Reusability
2	**Authentication**
2.1	Ensure that every request to the API or web service is authenticated.

2.2	Ensure a strong authentication mechanism is used; Required authentication mechanisms allowed for APIs/Web services in KRA are OAuth 2.0 and JWT
2.4	Ensure implementation of anti-brute force mechanisms on authentication endpoints such as account lock-outs, use Max Retry and jail features in Login.
2.6	When JWT is used, ensure: 1. Use a random complicated key (JWT Secret) to make brute forcing the token very hard. 2. Don't extract the algorithm from the header. Force the algorithm in the backend (HS256 or RS256). 3. Make token expiration (TTL, RTTL) as short as possible. 4. Don't store sensitive data in the JWT payload, it can be decoded easily.
2.7	When OAuth 2.0, ensure: 1. Always validate redirect_uri server-side to allow only whitelisted URLs. 2. Always try to exchange for code and not tokens (don't allow response type=token). 3. Use state parameter with a random hash to prevent CSRF on the OAuth authentication process. 4. Define the default scope, and validate scope parameters for each application.
2.8	Ensure no sensitive authentication details, such as auth tokens and passwords are sent in the URL through GET requests.
3	**Authorization**
3.1	Ensure a proper authorization mechanism is implemented that checks if the authenticated subject has access to perform the requested action.
3.2	Ensure that the issued authentication and authorization tokens have a set expiry time.
3.3	Ensure the use of random and unpredictable values as Globally Unique Identifiers (GUIDs) for records identification. Auto-incrementing IDs should never be used.
3.4	Ensure the use of proper HTTP method for each API operation: GET (read), POST (create), DELETE (to delete a record). No request should be processed if the method is not appropriate for the requested resource.
3.5	Ensure the integrating components only access the objects they require from the integrating systems. Responses should only return the data necessary to fulfil a request
4	**Data Protection**
4.1	Ensure that the responses from the API provide only legitimate requested data that is not excessive.
4.2	Ensure sensitive information such as access tokens, bearer tokens, pins, passwords etc are not being returned in request responses or stored in logs in clear text.
4.3	Error messages must ensure that sensitive information about the integrating systems is not disclosed
4.4	Ensure sensitive data parameters such as passwords, PINs, Credit card numbers etc. being passed to the APIs are hashed

4.5	Ensure minimization/masking of customer PII such as MSISDN and ID Numbers when such are returned in request responses and displayed in logs.
4.6	Ensure the communication channel is encrypted. The Endpoints should make use of HTTPS and not of HTTP
4.7	Ensure proper implementation of HTTPS; i.e current secure TLSV
5	**Resource and Rate Limiting**
5.1	Ensure implementation of a limit on how often a client can call the API within a defined timeframe. This helps mitigate DoS attacks by throttling or blocking IP addresses after making concurrent requests within a very short period of time.
5.2	Define and enforce maximum size of data on all incoming parameters and payloads such as maximum length for strings and maximum number of elements in arrays.
5.3	For APIs processing large amounts of data, ensure data is processed asynchronously. Processing large amounts of data synchronously can prevent the API from responding in a timely manner forcing clients to wait.
6	**Secure Configuration**
6.1	Ensure implementation of the **X-Content-Type-Options: nosniff** header to protect API against MIME sniffing vulnerabilities.
6.2	Ensure implementation of the **X-Frame-Options: deny** header.
6.3	Ensure implementation of the **Content-Security-Policy: default-src 'none'** header.
6.4	Ensure that fingerprinting headers such as **X-Powered-By**, **Server**, **X-AspNet-Version**, etc are not present
6.5	Force content-type for your response. If you return application/json, then your content-type response is application/json.
6.6	Return the proper status code according to the operation completed. (e.g. 200 OK, 400 Bad Request, 401 Unauthorized, 405 Method Not Allowed, etc.).
7	**Vulnerability Management**
7.1	Ensure that the API supports use of updated and vendor supported dependencies and libraries.
7.2	If the API is externally facing, ensure that it's behind a Firewall
7.3	Ensure that unused dependencies, unnecessary features, components, files, and documentation are deleted in production APIs
8	**Data/Input Validation**
8.1	Perform data validation using a single, trustworthy and actively maintained library.
8.2	Validate, filter and sanitize all client-provided data, or other data coming from integrated systems.
8.3	Special characters should be escaped using the specific syntax for the target interpreter.
8.4	Prefer a safe API that provides a parameterized interface.
8.5	Always limit the number of returned records to prevent mass disclosure in case of injection.
8.6	Validate incoming data using sufficient filters to only allow valid values for each input parameter.
8.7	Define data types and strict patterns for all string parameters.

9	**Auditing and Logging**
9.1	Log all failed authentication attempts, denied access, input validation errors and rate limit errors
9.2	Ensure all requests and responses are logged
9.3	Ensure the logs are in a format that is consumable by SIEM systems
9.4	Ensure the log contains sufficient details including the actual source IP instead of a Load balanced IP in cases where the service is hosted behind a load balancer.
9.5	Ensure both the raw http access logs as well as the transactional logs are sent to a SIEM
9.6	Based on the functionality provided by the API define use cases for monitoring at the SOC
9.7	A facility should exist to allow Manual triggering of transactions/actions under special circumstances (eg Integration breakdown, compromise etc) There must be audit trail on the facility
10	**Network controls**
10.1	All network communications between integrating components must be authenticated, and must not explicitly trust other network devices
10.2	API's must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle
10.3	All function calls between applications should implement digital signatures to verify authenticity of the invoking application (eg tokens, SSL)
11	**Encryption**
11.1	API Authenticating tokens must be random and unpredictable
11.2	Data sent between integrating systems must be encrypted in transit. Recommended algorithms (with minimum bit lengths), in order of preference, are: Hashing: SHA -512, SHA -256, RIPEMD160. Symmetric: AES256, AES192, AES128, 3 -DES (168 bits), Blowfish(minimum 128 bits), Twofish (minimum 128 bits), IDEA (128 bits),and RC4 (128 its). Public key: RSA(minimum 2048 bits) and DSA(minimum 2048 bits), ElGamal (minimum 2048 bits)
11.3	Encryption keys must be protected during transit and while stored in file system
11.4	A key used to decrypt data must not be stored in the same location as data encrypted with the key
11.5	Site certificates must be current and issued by a well-known certificate authority
12	**Documentation**
12.1	A design blue print with data flow or flow chart diagrams should be present as part of the integrating application system/module/component documentations
12.2	Signed user requirements/specifications document should be present as it forms the basis for the development of a new application or modification of an existing system

Annex IV: Application Security Requirements

	ANNEX II - Application Security Requirements
1	**Application Architecture**
1.1	Applications hosted in a shared hosting environment should be logically isolated from other applications in the same environment
1.2	Anti-virus scanning must be performed real-time on any file transmitted to the server
1.3	All network communications between components must be authenticated, and must not explicitly trust other network devices
1.4	If an application stores highly confidential information, data must be physically separated from other applications' data stores
1.5	Applications handling highly confidential data must not be hosted in a shared hosting environment or store its data in a shared database server
1.6	If an application shares a data store with another application, the data store must be segmented logically or physically. Logical segmentation should be implemented with access control mechanisms. Physical segmentation should be accomplished with a separate instance of the data store or a separate data store server
1.7	Any administrative functions that are not meant to be accessed by users from the Internet must be located in a private DMZ, which prevents direct Internet access to the servers
1.8	Systems directly facing the Internet must not store or cache confidential data, even for a short duration. This includes file uploads and downloads, source code, etc
1.9	Internet-facing systems must be placed behind a firewall that protects against network-based denial of service attacks, blocks ports that are not required for external access, and other network attacks
1.1	Applications must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle
1.11	Applications that connect to a database, application server, or any system that utilizes application IDs must do so using an account that has been granted access to only objects and functions needed for operation of the application
1.12	All function calls between application tiers should implement digital signatures to verify authenticity of the invoking application
1.13	Applications must be designed to enforce the least privilege principle for all processes
1.14	Application server interfaces must not be accessible from the Internet. This includes Web Services, DCOM, CORBA, SOAP, EJB, RPC, and any other method of invoking remote procedure calls
1.15	All application resources must require authentication for every call to each resource, and must be kept in compliance with the recommended password policies
1.16	All servers should be kept in sync with a time synchronization mechanism

2	**Network Communication and Session Management**
2.1	Sensitive information must be transmitted via a secure channel (SSL, SSH, etc.) or encrypted prior to transmission (PGP, etc.), using KRA approved methods
2.2	All communication sessions must use secure protocols
2.3	All transactions communication sessions must enforce session expiry so that after an unacceptable period of inactivity the session must terminate to guard against session hijacking
2.4	Any vendor proprietary protocols used must be well documented (i.e. the vendor must provide comprehensive documentation on the protocols such as technical specifications or white papers). Any vendor proprietary encryption algorithms must be FIPS-140 certified
2.5	Session IDs must use strong, non -predictable algorithms
2.6	All relevant session information should be captured and stored in a secure & auditable location
2.7	Only one session should be allowed per user operating from a single computer unless a specific business case has been established for allowing multiple sessions per user
2.8	Sessions should expire after a maximum set duration, regardless of activity
2.9	Session state must be maintained on the server for web-based applications, and be associated with a single client through the use of a session ID
2.1	Session state must be tied to a specific browser session through the use of a session cookie
2.11	Sessions must not be allowed to span both secure and non-secure connections
2.12	Applications must allocate session-based resources only after successful authentication. Allocating resources prior to this can lead to denial of service attacks, session fixation attacks, and others
2.13	Synchronization of time between servers and other relevant equipment must be implemented. This is instrumental in tracking time stamps between different systems particularly where systems share/exchange data
3	**Identification and Authentication**
3.1	Each user must be authenticated with a unique user-id and password on the application
3.2	User authentication data must be stored and maintained securely in a centralized location on the system
3.3	The application must support password expiry features with a configurable frequency. Parameterize this to allow flexibility in adjusting this value as required
3.4	The password must be secure on entry, at no point must the password be in clear text
3.5	All new user accounts must have a system-generated random password when created. A secure way of communicating the initial password to the user should be utilized e.g. via KRA e-mail account
3.6	All new user accounts must be created with reference to existing authoritative databases of approved persons e.g. identifying numbers in KRA's active staff database (HR) and National PIN certificate database
3.7	Users must be prompted to change their passwords the first time they log on to the application
3.8	Newly created accounts should be set to expire if not used for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required

3.9	The application must support password lockout after a configurable number of unsuccessful attempts. Parameterize this to allow flexibility in adjusting this value as required
3.1	The application must lockout a user account after the system is idle for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.11	The application must support a password change notification and a configurable number of grace logins
3.12	The application must support the ability to disable / remove / delete a user, after a number of days of inactivity, the number of days should be configurable
3.13	The application must not allow the re-use of a past password until a set number of password changes have been made. Parameterize this to allow flexibility in adjusting this value as required
3.14	The application must be flexible and enforce a minimum password length of 8 characters
3.15	The application must enforce the usage of strong alphanumeric passwords
3.16	Default / developer passwords should not reside within the application
3.17	No identification and authentication information must be hard-coded or scripted into the application
3.18	The application must provide last logon information
3.19	Backward process flows must clear all authentication fields
3.2	The application must support time-based access control
3.21	Login failure measures must not indicate which component of the username/password pair submitted was incorrect
3.22	During password changes the application must force the user to enter the new password twice
3.23	The application must support Multi Factor Authentication with at least 3 factors to choose from (OTP, TOTP, Mail)
3.24	The application should support Single Sign On at a minimum through Identity Directories for Non-Revenue systems
4	**Authorization and Access Control**
4.1	The application must support an additive access model which means by default no access is granted
4.2	Access control must be granular to facilitate adequate separation of duties, for example:
	· There should be separation of duties e.g. data entry, authorisation and final approval
	· Data entry staff should have the minimum access levels required to enter data
	· Authorisation staff should have an access level that allows them to authorise but not necessarily change the data that was entered
	· Final approval staff should have the required access level to finalise the process/transaction
4.3	Access control information should be securely stored and must be secure from unauthorized changes within and outside of the application
4.4	Reporting on all the access permissions per user must be available in the application
4.5	User must be able to explicitly terminate (logout) a session

5	**Operations**
5.1	Intrusion detection systems must be in place to detect intrusions of production systems that are Internet facing
5.2	Patch management software must be installed and regularly updated on all servers
5.3	Anti-virus software must be installed and regularly updated on all servers
5.4	A formal incidence response process plan should be in place for production systems
6	**Auditing and Monitoring**
6.1	Provision must be in place for application logs
6.2	All application logs must be in a user-friendly readable format and in English
	They should be delimited using space and allow activities to be captured per line of text Each user transaction such as printing, viewing, updates, inserts and other data manipulation should capture to the minimum the date and time, userID, the URL accessed the and source IP & remote IP. They should indicate the parameters passed where possible
6.3	All application logs must be secure from intentional or accidental modification under all circumstances by all users including administrators. Access to the logs must be restricted to authorized users only so as to ensure their integrity
6.4	It should NOT be possible for the Application Audit logs to be suppressed or modified
6.5	All logs must be viewable and printable
6.6	The application must have incident alerting capability e.g. in the event of system violations or when the audit logs are getting full
6.7	All utility or non-standard based access to the application must be captured in the logs
6.8	For all application audit logs, the log files must bear the following information:
	a) User-id
	b) Date & Time of event
	c) The source and remote IP
	d) Type of event / action performed by the user
	e) Module accessed by the user
	f) Success or failure of the event
	g) Source of the event
	h) Before and after values (where applicable, i.e. master files)
	i) Modifications to the application
	j) Account creation, lockouts, modification, or deletion
	k) Modifications of privileges and access controls
	l) Application alerts and error messages
	m) Accesses to sensitive information
	n) URL of the web page(s) accessed by a user for Internet facing applications
	o) Program used to access the system
	p) The userID at the application log should be tracked up to the database logs
6.9	The application must have a logging mechanism to log all transactions and exceptions

6.1	A violation log must exist to track any attempted unauthorized access to the application and should bear the following information:
	a) Particular action intended by the user
	b) Workstation-id or IP address of access
	c) Date & Time of event
6.11	All valid and failed login attempts must be logged with meaningful information that is actionable for investigative purposes if fraud is detected. However, passwords must not be logged
6.12	All password recovery reset attempts must be logged with meaningful information that is actionable for investigative purposes if fraud is detected
6.13	All security policy changes and attempts must be logged
6.14	All user and account management changes and attempts must be logged
6.15	Database audit trails should be present for all dynamic & static tables of interest e.g. Parameter tables, Transaction Tables etc.
6.16	Application logs should be implemented independent of database audit trails for purposes of correlation i.e. application servers should maintain their own application logs separate from database audit trails.
7	**Input – Processing – Output Controls**
7.1	Predictive input / menu based input functionality should be provided where possible, minimizing user interaction
7.2	Error messages should be standard and not provide too much application information eluding to the reason for the error allowing an attacker to deduce effective attack methods
7.3	Copy and paste must not work for data entry especially when authenticating to the application
7.4	All user input parameters must be validated by the server, and must be validated to accept only values pertinent to the values in the field in accordance with the data dictionary
7.5	Any sensitive content sent to the client machine must not be cached, unless encrypted using approved methods. The application is responsible to set the proper directive to cause the client to not cache the sensitive data
7.6	Sensitive information must not be presented to unauthenticated users
7.7	Sensitive information must not be stored in a persistent cookie, or other location on the client computer that does not have enforceable access control mechanisms.
7.8	Highly confidential data must be stored encrypted
7.9	Confidential data that is stored outside the systems that comprise the application must be encrypted by a firm approved method, such as PGP. This includes file shares, ftp servers, and e-mail
7.1	Functions should not be allowed execute on both encrypted and non-encrypted connections. If functions are required to exist on both encrypted and non-encrypted connections, then the user sessions must not be allowed to span both connections
7.11	Sensitive information must not be stored in hidden fields if the application is web-based

7.12	If data is supplied to the application from an authoritative source, the application must not allow users to modify this data
7.13	The application must not use a credential repository of a trust level less than what is required by the application's data
7.14	User credentials in one repository must not be synchronized with any other repositories unless their trust levels are equal
7.15	If an application uses more than one method or credential store for authentication, all methods and stores used must be at the same trust level
7.16	Web based interfaces should use a secure method to transmit data e.g. Using the HTTP POST method instead of the less secure GET method
8	**Cryptographic Key Management**
8.1	Cryptographic functions must be selected from an approved list. Any cryptographic functions used that are not previously approved require an exception
	Recommended algorithms (with minimum bit lengths), in order of preference, are:
	a) Hashing: SHA -512, SHA -256, RIPEMD160.
	b) Symmetric: AES256, AES192, AES128, 3 -DES (168 bits), Blowfish(minimum 128 bits), Twofish (minimum 128 bits), IDEA (128 bits),and RC4 (128 its).
	c) Public key: RSA(minimum 2048 bits) and DSA(minimum 2048 bits), ElGamal (minimum 2048 bits)
8.2	Any use of hashing must be salted. Values used for salting must be protected
8.3	Encryption keys must be protected during transit and while stored in file system
8.4	Encryption keys must not be disclosed to anyone who does not need access to them
8.5	If using public key cryptography, private keys must be protected by a pass-phrase
8.6	Pass-phrases protecting private keys or used as a share d secret with a symmetric key algorithm must be a minimum of 14 characters in length, and contain at least one upper case letter, one lower case letter, and one number
8.7	A key used to decrypt data must not be stored in the same location as data encrypted with the key
8.8	Site certificates must be current and issued by a well-known certificate authority
9	**Documentation**
9.1	A user manual should be developed as part of the application system/module/component documentation
9.2	A technical manual should be developed as part of the application system/module/component documentation
9.3	An online help facility should be present wherever possible and form part of the application system/module/component documentation
9.4	Signed user requirements/specifications document should be present as it forms the basis for the development of a new application or modification of an existing system
9.5	A Data dictionary should be developed as part of the application system/module/component documentation

9.6	A design blue print with data flow or flow chart diagrams should be present as part of the application system/module/component documentation
10	**Other Considerations**
10.1	A facility should exist to allow rolling-back of transactions/actions under special circumstances clearly documented in the user-specifications. There must be audit trail on the roll-back facility
10.2	Applications should be configurable to securely send audit data/Logs to a centralized data store that is external to the Application Server
10.3	Applications should reliably verify a user's identity using defined multi factor authentication techniques, and capable of secure communication with an external KRA E-directory service for centralized management of authorization and authentication of users to access functionality using security groups defined within the directory service
10.4	Applications should support service monitoring by logging all information that is required for effective monitoring of services based on defined service monitoring parameters
10.5	Applications should have a provision for incorporation of biometrics and related biometric solutions. The next generation of application security would be dependent on biometric identification, authorization and authentication of application users.
10.6	Security for People with Disabilities. Design of Applications should have considerations for people living with disabilities. Varied disabilities calls for design of elaborate mechanisms to enable these group of people to amicably, adequately and elaborately interact with applications. For instance, braille enhanced applications would aid the blind in interacting and using the applications in their endeavours.
10.7	The application should incorporate certified and legitimate digital certificates, which are used to verify that a particular public key (online identity). A PKI is a technical infrastructure that comprises of a Root Certification Authority (RCA) and a Certification Authority (CA), referred to as an Electronic Certification Service Provider (E-CSP) in Kenya's legal and regulatory framework. The generation and usage of the PKIs on an application should be provisioned by the National Public Key Infrastructure for global trust and recognition.
10.8	Personal Identification data(Information) is to be kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and. Personal data shall not be transferred or shared outside the application unless there is proof of adequate data protection safeguards or consent from the data subject. The guidelines for this subject matter are provided by the Kenya Cyber Security Act on Personal Identifiable Information (PII).Ensure the rules of data integrity, confidentiality and availability are adequately adhered to.